Programa de Security Awareness na Empresa PJ

Mestrado em em Cibersegurança e Informática Forense

Paula Alexandra Nascimento Joaquim

Leiria, setembro de 2019

Programa de Security Awareness na Empresa PJ

Mestrado em Cibersegurança e Informática Forense

Paula Alexandra Nascimento Joaquim

Trabalho de Projeto realizado sob a orientação do Professor Doutor Carlos Manuel da Silva Rabadão, Professor Coordenador do Departamento de Engenharia Informática da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria

Leiria, setembro de 2019

Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionado/a o/a Autor/a e feita referência ao ciclo de estudos no âmbito do qual a/o mesma/o foi realizado, a saber, Curso de Mestrado em Cibersegurança e Informática Forense, no ano letivo 2017/2019, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

Assinado por : **Paula Alexandra Nascimento Joaquim**
Num. de Identificação: BI09576021
Data: 2019.11.09 00:11:44 Hora padrão de GMT

Dedicatória

À Minha Família

Agradecimentos

Este trabalho reflete não só o meu empenho individual, mas toda a motivação que me foi transmitida pelos que estiveram presentes nos momentos mais importantes desta etapa da minha vida, que tornaram a conclusão deste mestrado possível.

Ao meu orientador, Professor Carlos Rabadão, pela forma como me orientou, pela sua disponibilidade e motivação.

Aos professores do mestrado em Cibersegurança e Informática Forense, pelo profissionalismo, experiência e organização das aulas com o objetivo de ir ao encontro das nossas expetativas.

Ao Professor Mário Antunes, pelo contacto permanente para que estivéssemos sempre atualizados relativamente a todas as dinâmicas do mestrado, pela disponibilidade na organização e orientação nas nossas estadias em Leiria.

Aos meus colegas de mestrado, pela simpatia, disponibilidade e companheirismo que sempre demonstraram, em especial ao Artur Varanda e Bruno Severino, companheiros das viagens Lisboa/Leiria/Lisboa.

Ao meu colega e professor, Inspetor Baltazar Rodrigues, pela sua disponibilidade, experiência e acompanhamento no decorrer do Mestrado.

À Polícia Judiciária, pela oportunidade e condições que me proporcionou para frequentar ao mestrado em Cibersegurança e Informática Forense.

Por último e mais importante, à minha família, pela compreensão e paciência nas minhas ausências, em especial ao Paulo, Olívia, Sofia e André.

Nota Prévia

O presente projeto foi realizado na Unidade de Telecomunicações e Informática da Polícia Judiciária. Existe recolha e tratamento de dados, os quais devido à sua sensibilidade, foram mantidos em anonimato e sob sigilo.

Awareness Program walks you through the step-by-step process of creating a program as unique as your organization so you'll be prepared when an attacker comes calling.

—Kevin Mitnick
speaker, consultant, and author of
The New York Times best-seller Ghost in the Wires

Resumo

Cada vez mais passamos o tempo ligados em rede e dependemos de serviços *online*. A maior parte dos indivíduos não pensa no que pode acontecer quando coloca os seus dados *online* para efetuar uma simples compra, um registo num serviço, uma consulta ao *e-mail* ou o uso das redes sociais. Todas estes dados podem ser roubados, manipulados ou adulterados. Todos os dias quando nos ligamos à *Internet,* colocamos as nossas informações em risco. No entanto, o risco pode e deve ser minimizado, se tivermos em atenção algumas medidas de prevenção através da ciberhigiene e a consciencialização para a segurança da informação. O macro objetivo deste projeto, é o de elaborar um Programa de *Security Awareness* que possa ser aplicado em qualquer organização. O projeto começa por apresentar o estado da arte sobre esta matéria, em relação às organizações existentes que trabalham na área da segurança da informação e da formação. Procura também estabelecer as boas práticas para a implementação de um programa de *security awareness*, identificando os principais ativos das organizações, ao nível da informação, pessoas e sistemas, físicos e lógicos. Identificar as principais ameaças que o fator humano representa para estes ativos. Propor medidas de consciencialização dos indivíduos, ao nível da transmissão de conhecimento. Por fim, estabelecer métricas para a medição e avaliação dos resultados obtidos. Conclui-se que as boas práticas de segurança e a consciencialização dos indivíduos são essenciais e devem ser aplicadas a todos, independentemente do cargo e da responsabilidade que detém cada um na organização.

Palavras-chave: Consciencialização, Cibersegurança, Indivíduo, Informação, Segurança

Abstract

We are increasingly spending time networking, on Internet and relying more on online services and e-commerce. Most individuals don't think about, what might happen when they put their data online. To make a simple purchase, register for a service, check email or use social networks, all this information can be stolen, manipulated or tampered with. Every day when we connect to the Internet, we put our information at risk. However, the risk can and should be minimized if we consider some preventive measures, through ciberhigiene and security awareness. The macro objective of this project is to develop a Security Awareness Program, that can be applied to any organization. The project begins by presenting the state-of-the-art information on existing information about security and training organizations. Establish the best practices for implementing a security awareness program, identifying main assets of the organizations, the level of information, people and physical and logical systems. Identify the main threats that the human factor poses to these assets. Propose awareness-raising measures through the transmission of knowledge, creation of information dissemination channels for the entire organization. Consider several strategies, according to the characteristics of the individuals of the organization. Finally, establish metrics to measure and evaluate the results obtained. Good practices and awareness of individuals are essential and should be applied to everyone regardless of their position and responsibility in organizations.

Keywords: Awareness, Cybersecurity, People, Information, Security

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

AP2SI	Associação Portuguesa para a Promoção da Segurança da Informação
CNCS	Centro Nacional de Cibersegurança
CSIRT	Computer Security Incident Response Team
CSV	Comma-Separated Values
EC3	European Cybercrime Centre
ENISA	European Network and Information Security Agency
FCT	Fundação para a Ciência e Tecnologia
GNS	Gabinete Nacional de Cibersegurança
GUI	Graphical User Interface
HTML	HyperText Markup Language
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PC	Personnal Computer
PDF	Portable Document Format
PJ	Polícia Judiciária
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
URL	Uniform Resource Locator
USB	Universal Serial Bus

1. Introdução

O fator humano é identificado como sendo uma das maiores fontes de risco da segurança da informação numa organização, além de ser uma das fontes mais difíceis de controlar. Com os avanços tecnológicos, as pessoas usam as Tecnologias de Informação e Comunicação (TIC) e introduzem riscos à segurança da informação de uma organização. A insuficiente perceção e consciencialização detida pelo fator humano sobre os riscos da segurança da informação é uma das principais vulnerabilidades, entendida como uma ameaça para os ativos das organizações.[1]

Neste campo temos três pilares fundamentais na segurança da informação: a confidencialidade, a integridade e a disponibilidade. Caso a informação esteja disponível para pessoas não autorizadas, deixamos de ter confidencialidade. Quando a informação é alterada, falsificada ou furtada, deixamos de garantir a sua integridade. A disponibilidade fica comprometida quando ficamos impossibilitados de aceder à mesma por motivos de ataque, invasão, ou de falha nos servidores.

Além destes três pilares, hoje em dia temos mais dois que acrescentam mais robustez na segurança da informação, a autenticidade e a irretratabilidade. A autenticidade é comprometida quando deixamos de poder garantir que a fonte da informação é da entidade que a originou. O não repúdio ou irretratabilidade garante que o autor da informação não possa negar as ações tomadas em relação a transações efetuadas a respeito de informações.

É fundamental melhorar o conhecimento e a atitude que os membros de uma organização possuem em relação à proteção dos seus ativos (informação, sistemas físicos e pessoas), através da implementação de programas de *security awareness*, garantindo assim os cinco pilares da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio ou irretratabilidade.

Segundo a Agência Europeia para a Segurança das Redes e da Informação (ENISA[2] - European Network and Information Security Agency), a consciencialização dos riscos inerentes à utilização das tecnologias e a existência de salvaguardas de segurança, é a primeira linha de defesa para a segurança dos sistemas de informação e redes.

O presente trabalho tem como tema a elaboração de um programa de *security awareness,* para aplicar numa organização.

1.1. Motivação e Objetivos

Este documento retrata um caso de estudo realizado no âmbito de um projeto piloto de implementação de um programa de *security awareness* na empresa PJ, com o intuito de promover o *awareness* entre os indivíduos dessa organização. O seu objetivo é o de responder a um conjunto de questões que as organizações enfrentam na implementação de um programa de s*ecurity awareness,* tais como: por onde começar, como deve ser planeado, desenvolvido, implementado, avaliado, como medir os seus resultados e conclusões.

A execução deste projeto permite minimizar os riscos de segurança a que a PJ está constantemente sujeita – o fator humano.

1.2. Metodologia

Para a elaboração deste projeto, a metodologia seguida está dividida em várias fases: a pesquisa, a implementação e o caso de estudo.

Na primeira fase, é feito um levantamento sobre as entidades existentes que estão diretamente ligadas à segurança da informação na sua vertente de consciencialização das organizações e dos seus indivíduos, na vertente da formação e apoio à conceção de um programa de *security awareness*, assim como, na vertente das normas e regulamentos que o permitem implementar e das ferramentas de *phishing* existentes e que permitem levar a cabo campanhas de *phishing* e sensibilização dos indivíduos. Este levantamento da literatura existente, contribui para uma visão dos materiais existentes, que de alguma forma são utilizados no planeamento de um projeto desta natureza e mais concretamente no caso de estudo implementado.

Numa segunda fase, elaboro uma estrutura do que deverá ser considerado na conceção e planeamento de um programa de *security awareness*, para que possa ser eficaz, contemplando diversas questões e propostas existentes, as boas práticas, que modelo seguir e implementar, a necessidade de promover o conhecimento sobre *security awareness*, como medir esse conhecimento, que medidas implementar para mitigar as ameaças existentes,

como avaliar os resultados obtidos após a implementação do programa de *security awareness,* conclusões e trabalho futuro.

O caso de estudo, consiste na elaboração de um questionário para avaliar o nível de *awareness* dos utilizadores. O estudo é efetuado através de um questionário que pretende aferir os hábitos e conhecimentos sobre segurança da informação. É proposto no final do questionário a frequência de um curso *online* sobre esta temática. Para medição do resultado destas medidas, é aplicado outro questionário para medição dos hábitos e conhecimentos de segurança da informação. Após estas medidas, elaboro uma campanha de *phishing*[3, p. 116] que consiste no envio de *e-mails* distintos utilizando duas plataformas: uma comercial e outra de acesso livre. É também efetuada uma pequena comparação entre as duas plataformas utilizadas. No final são elaboradas as conclusões.

1.3. Estrutura

O presente projeto foi estruturado em cinco capítulos.

No capítulo 1 (Introdução), é feita a contextualização do trabalho, é explicado o seu tema e objetivo, é explanada a metodologia e a estrutura utilizada.

No capítulo 2 (Estado da Arte), é efetuado um breve levantamento das organizações que produzem normas ou regulamentos, prestam formação ou dão formação na área da segurança da informação e das ferramentas de *phishing*.

No capítulo 3 (Planeamento de um Programa de *Security Awareness*), são descritas as várias etapas do planeamento de um programa de *security awareness*.

No capítulo 4 (Caso de Estudo), é aplicado um programa de *security awareness* a um pequeno universo de uma organização, tendo por base os pressupostos descritos no capítulo 3.

No capítulo 5 (Conclusões), são efetuadas as conclusões sobre o trabalho desenvolvido.

2. Estado da Arte

Para a elaboração deste projeto, é efetuado um levantamento sobre as organizações e normas existentes sobre a temática *security awareness*, onde procuro encontrar referências a nível nacional e internacional, sobre a consciencialização da segurança da informação e a ciberhigiene. A informação recolhida é agrupada em entidades a nível nacional e internacional; e pelas normas e recomendações existentes. É efetuado também o levantamento de algumas ferramentas de *phishing* existentes no mercado em regime *open source* e comercial.

2.1. Entidades Nacionais

A nível nacional, as organizações que destaco já existem há algum tempo e têm uma proximidade com o cidadão ou trabalham diretamente com organismos públicos e entidades reguladoras ou formadoras nesta área.

Assim, são recolhidas as melhores práticas utilizadas por estas entidades, para posteriormente proceder à implementação de um plano de *security awareness*.

Dentro das entidades nacionais, existem algumas que são referência na área da regulamentação e formação, tanto de empresas como de pessoas.

Em Portugal, já existe o hábito de falar em segurança da informação: começa no ambiente escolar, quando se fala sobre a *Internet* e sobre os seus perigos. Para o ambiente familiar e organizacional, no entanto, existem outras fontes de informação.

Dos projetos e organizações existentes, saliento os seguintes, descritos em seguida:

- Centro Nacional de Cibersegurança;
- Fundação para a Ciência e Tecnologia (FCT);
- Plataforma NAU;
- SEGURANET;
- Projeto Internet Segura;
- Miúdos Seguros na Net;
- Associação Portuguesa para a Promoção da Segurança da Informação – AP2SI.

2.1.1. Centro Nacional de Cibersegurança

O Centro Nacional de Cibersegurança (CNCS)[4] tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais. Atua junto dos operadores de serviços essenciais, dos prestadores de serviços digitais e das entidades do Estado na medida em que estes são cruciais para o bom funcionamento da sociedade portuguesa.

O CNCS funciona no âmbito do Gabinete Nacional de Segurança (GNS) e possui, entre outras, as seguintes competências vocacionadas para a consciencialização:

- Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança.

O CNCS atua também em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

O Centro Nacional de Cibersegurança promove um curso de *e-learning*, lançado no âmbito do Dia da *Internet* Mais Segura, que visa certificar o conhecimento dos cidadãos sobre os comportamentos de cibersegurança. O Curso permitirá, ao cidadão, adquirir um conjunto de competências relacionadas com os comportamentos seguros no ciberespaço e, desta forma, contribuir para a consciencialização em cibersegurança e para navegação livre e segura na *Internet*. Este é o primeiro curso *online* que o CNCS desenvolveu e conta já com cerca de 600 inscrições. “Ciberhigiene” é o nome da primeira edição do curso, sendo os conteúdos orientados para as boas práticas de segurança no ciberespaço, na vertente comportamental

da segurança da informação, por analogia à higiene pessoal, isto é, o equivalente a rotinas simples que minimizem os riscos de ameaças de cibersegurança de um cidadão/colaborador de uma organização.

Neste sentido, com a aquisição destes conhecimentos, o objetivo passa por prevenir incidentes de cibersegurança, promovendo certos comportamentos nos indivíduos que, por sua vez, evitam potenciais efeitos negativos nos equipamentos que usam, protegendo assim as próprias organizações. A inscrição no curso é gratuita e pode ser feita através do *site* do CNCS – Cidadão Ciberseguro[5].

2.1.2. Fundação para a Ciência e Tecnologia

A FCT[6] apoia, desde 1987, a comunidade cientifica e académica de Portugal. É a agência pública nacional de apoio à investigação em ciência, tecnologia e inovação em todas as áreas do conhecimento e é tutelada pelo Ministério da Ciência e Tecnologia e Ensino Superior. Sucedeu a UMIC desde 2012 e em 2013 assumiu as competências da FCCN. A FCT desenvolve vários projetos e promove o avanço do conhecimento científico e tecnológico em Portugal, de modo a atingir os mais elevados padrões internacionais de qualidade e competitividade em todos os domínios científicos e tecnológicos, e estimular a sua difusão e contribuição para a sociedade e o tecido produtivo.

2.1.3. Plataforma NAU

A Plataforma NAU – Sempre a Aprender[7], é uma infraestrutura técnica de publicação e serviços de acompanhamento de cursos para grandes audiências, orientado para a Administração Pública e Ensino Superior. É uma iniciativa nacional, liderada pela FCT, para construção e operação de uma infraestrutura técnica e operacional de suporte à publicação e dinamização de conteúdos para grandes audiências, nomeadamente, em formato MOOC (Massive Open Online Courses). Esta iniciativa, transversal a diversos ministérios e aberta à sociedade, permitirá desenvolver ações de formação para um maior número de funcionários e cidadãos. Esta plataforma foi criada no âmbito do Projeto NAU[8], iniciado em 1 de Outubro 2017 com os parceiros: Fundação para a Ciência e a Tecnologia (FCT), Direção-Geral da Educação (DGE), Direção-Geral da Saúde (DGS), Direção-Geral da Qualificação dos trabalhadores em Funções Públicas (INA), Instituto do Emprego e Formação Profissional (IEFP), Secretaria-Geral da Educação e Ciência (SGMEC) e Projeto NAU.

2.1.4. Seguranet

No *site* da Seguranet[9], podemos encontrar conteúdos desenvolvidos para um público variado: crianças, jovens, pais, professores e escolas.

Existem vários recursos[10] divididos em várias categorias: nível escolar, tipo de público e temas. Também é possível escolher o tipo de recurso e o formato de disponibilização: apresentações, áudio e vídeo.

Existe o programa eSafety Label[11][12] dirigido às escolas, as quais podem participar através do preenchimento de um questionário de autoavaliação sobre as infraestruturas, políticas e práticas de segurança digital. Depois recebem um plano de ação de acordo com o questionário que preencheram. O plano de ação é um guia para melhorar as práticas de segurança digital da escola, obtido de acordo com o resultado do diagnóstico efetuado. No final, recebe-se um certificado, como reconhecimento das melhorias nas práticas, em bronze, prata ou ouro, dependendo do resultado. Pode depois consultar-se o *ranking* das escolas.

2.1.5. Projeto Internet Segura

O Projeto Internet Segura[13], fruto da parceria entre várias entidades: FCT, Direção Geral da Educação, Instituto Português do Desporto e Juventude, Fundação PT e Microsoft; promove a utilização da *Internet* e a consciencialização da sociedade para os riscos associados.

Este projeto tem por objetivo o combate a conteúdos ilegais, a minimização dos efeitos de conteúdos ilegais e lesivos nos cidadãos, a promoção de uma utilização segura da *Internet* e a consciencialização da sociedade para os riscos associados à sua utilização. Integra o canal Seguranet e possui uma página no Facebook. Apresenta, ainda, alguns recursos para divulgação de conteúdos.

A Comissão Europeia lançou em 1999 o programa Safer Internet, a que se seguiu em 2005 o programa Safer Internet Plus, com o objetivo de dinamizar projetos dos Estados Membros de promoção da utilização segura da *Internet*.

No âmbito do programa Safer Internet, a Direção Geral de Inovação e Desenvolvimento Curricular, através da Equipa de Missão Computadores, Redes e *Internet* (DGIDC-CRIE) do Ministério da Educação, desenvolveu, em 2004, o projeto Seguranet, para a promoção de

uma utilização esclarecida, crítica e segura da *Internet* junto dos estudantes do ensino básico e secundário.

Uma das orientações estratégicas do programa de ação LigarPortugal, adotado pelo Governo em julho de 2005, era "Assegurar a Segurança e a Privacidade no Uso da *Internet*", mais especificamente "garantir que todos, e em particular as famílias, dispõem de instrumentos para proteção de riscos que possam ocorrer no uso da *Internet* e têm informação sobre como os utilizar".

O projeto Internet Segura contribui para a concretização desta orientação estratégica. Este projeto é da responsabilidade de um consórcio coordenado pela FCT - Fundação para a Ciência e Tecnologia, e que também envolve a DGE - Direção Geral da Educação do Ministério da Educação, a Fundação para a Computação Científica Nacional – FCCN, IPDJ - Instituto Português do Desporto e Juventude, e a Microsoft Portugal.

Após avaliação e aprovação da candidatura do projeto apresentada ao programa europeu Safer Internet Plus, o respetivo contrato entre o consórcio e a Comissão Europeia foi assinado em junho de 2007.

A janeiro de 2011, a então Fundação para a Divulgação das Tecnologias de Informação (atualmente integrada no IPDJ) passou a integrar o Consórcio Internet Segura, ficando responsável pela Linha Ajuda - serviço que iniciou funções em 1 de junho de 2011.

A integração e implementação da *helpline* nos serviços já disponibilizados pelo Consórcio, resulta da candidatura em 2010 ao Programa Safer Internet com a proposta "Centro Internet Segura Portugal".

2.1.6. Miúdos Seguros na Net

Este projeto nasceu pela mão do Tito de Morais[14], para ajudar as famílias, escolas e comunidades a promover a segurança *online*, de crianças e jovens. Pretende promover a utilização responsável e segura das novas tecnologias de informação e comunicação por crianças e jovens. Disponibiliza, no seu *site*, uma série de recursos, dicas e a subscrição de uma *newsletter*.

2.1.7. Associação Portuguesa para a Promoção da Segurança da Informação

A AP2SI é uma Associação Portuguesa para a Promoção da Segurança da Informação, foi fundada em janeiro de 2012. É uma associação sem fins lucrativos e de natureza privada. Tem como objetivo contribuir para o desenvolvimento da Segurança da Informação em Portugal, de forma ativa, através da sensibilização para o valor e necessidade de proteção da Informação, e do desenvolvimento e promoção de orientações que visem reforçar o conhecimento e a qualificação dos indivíduos e organizações.

Desenvolveu um estudo apoiado pelo ISCTE/IUL, que procurou auscultar não apenas os responsáveis de IT ou de segurança nas organizações, mas também todos os outros colaboradores, em cargos de direção ou não, para ter uma perceção da realidade atualmente, 72 colaboradores e 59 diretores. As questões abordadas estão agrupadas segundo as seguintes temáticas: a Segurança da Informação (SI), a política de SI, o programa de formação em SI, a organização de SI, as auditorias à SI e os incidentes de SI.

O inquérito cobriu diversos aspetos fundamentais para a criação de uma cultura de segurança de informação eficaz nas instituições, nomeadamente:

- O compromisso da gestão de topo;
- A formação de competências;
- A existência de uma unidade organizacional dedicada;
- O papel da auditoria e controlo;
- A gestão de incidentes de segurança.

Adicionalmente houve necessidade de aprofundar alguns dos temas com o ponto de vista da camada diretiva e da gestão, mais especificamente sobre:

- A gestão do orçamento para Segurança da Informação;
- A gestão dos recursos humanos com funções na Segurança de Informação;
- A existência de incidentes e eventuais perdas relacionadas;
- As preocupações de segurança dos órgãos de topo;
- A perceção da exposição da instituição às ameaças.

Pretende-se, assim, ter uma ideia generalizada de que modo as organizações entendem o tema da Segurança da Informação e de que modo o colocam em prática, sendo o objetivo que o trabalho possa ajudar a entender a realidade em Portugal e sirva como referência para

o aumento da consciencialização para o tema da Segurança da Informação nas instituições a operar no nosso país.

Os resultados do Inquérito estão divididos em dois documentos:

- Um Sumário[15] onde são apresentadas as principais conclusões;
- A Análise de Resultados[16], levada a cabo pelo Departamento de Matemática, da Escola de Tecnologias e Arquitetura do ISCTE-IUL.

Ambos os documentos estão disponíveis gratuitamente no *site* da AP2SI.

2.2. Entidades Internacionais

No panorama internacional, foram escolhidas as entidades que regulamentam ou aconselham os países acerca destas matérias. As entidades europeias mais relevantes que focam assuntos de *security awareness* são a Europol através da EC3[17] e a ENISA[1]. Para além destas duas, faço referência ao Instituto SANS e ao PCI Standard.

2.2.1. Centro Europeu de Cibercriminalidade

O Centro Europeu de Cibercriminalidade[17] (EUROPOL – EC3) criado em 2013 para reforçar a resposta da polícia ao cibercrime na UE, ajudando a proteger os cidadãos, as empresas e os governos. Desde a sua criação, o EC3 deu um contributo significativo para a luta contra a cibercriminalidade: esteve envolvida em muitas operações de alto nível, resultando em centenas de prisões, e analisou centenas de milhares de ficheiros apreendidos, a grande maioria dos quais provaram ser maliciosos. Publica alguns guias sobre segurança da informação em diversos cenários, *mobile*, *Internet*.

2.2.2. Agência Europeia para a segurança das Redes e da Informação

A Agência Europeia para a Segurança das Redes e da Informação (European Network and Information Security Agency (ENISA))[2], é uma agência da União Europeia (UE) que trabalha desde 2004 para tornar a Europa mais segura. É o centro de excelência para os membros da Comunidade Europeia e para as instituições Europeias em segurança de redes e informações, dando conselhos e recomendações, agindo como um painel de troca de informação de boas práticas, facilitando os contatos entre as instituições europeias, os Estados-Membros, as empresas privadas e os atores da indústria.

Através da ENISA podemos obter um leque variado de publicações[18], orientações e programas de *security awareness* para promover o conhecimento e a consciencialização dos utilizadores, como é disso exemplo o NIZ Quiz[19], questionário promovido *online* sobre o tema "NIS in Education".

Esta agência europeia, existe desde 2004 e é um centro de especialização em *cybersecurity* na Europa. A ENISA contribui ativamente para a segurança das redes e da informação na União Europeia, para aumentar a sensibilização para estas matérias.

Desde que foi criada, trabalha em estreita colaboração com os estados membros e com o sector privado, fornecendo conselhos e soluções. Inclui os exercícios pan-europeus de *cybersecurity*, o desenvolvimento de estratégias nacionais de *cybersecurity*, cooperação com os Centros de Coordenação de Resposta a Incidentes (CSIRTs) e a sua capacitação.

Inclui, na sua atividade, estudos sobre a adoção da nuvem segura, abordando as questões da proteção de dados, privacidade em tecnologias emergentes, identificar o cenário de ameaças de *cybersecurity,* entre outras. A ENISA também apoia o desenvolvimento e a implementação da política e do direito da União Europeia em questões relacionadas com a Segurança das Redes e Informações (SRI).

A abordagem da ENISA dá-se em três áreas (Figura 2.1):

- Recomendações;
- Atividades que apoiam a criação e implementação de políticas;
- *Hands on work*, onde a ENISA colabora diretamente com as equipas operacionais de toda a Europa.

Figura 2.1 – Áreas de intervenção da ENISA

2.2.3. PCI Security Standard Council

O PCI Security Standard Council[20], é um fórum global para o desenvolvimento, aprimoramento, armazenamento, disseminação e implementação contínuo de padrões de segurança para proteção de dados de contas e pagamentos bancários. Esta entidade, permite aos seus membros usufruírem de alguns benefícios, entre eles a oferta de duas ações de formação sobre *awareness* e descontos noutras sessões de formação em *e-Learning*. Segundo um dos documentos de boas práticas[21] que produziu, numa organização todos sabem qual o seu papel em relação à segurança da informação (Figura 2.2).

Figura 2.2 – Papeis desempenhados numa organização, segundo o PCI Security Standard Council

2.2.4. SysAdmin, Audit, Network, Security Institute

O SysAdmin Audit Network Security Institute (SANS Institute)[22], é o instituto que mais confiança oferece e é a maior fonte de formação em segurança da informação do mundo. Tem uma oferta de formação presencial, *online* ou por *webcast*. Os cursos de segurança de computadores são desenvolvidos por líderes do setor em vários campos, incluindo a formação em segurança da informação e informática forense, auditoria, liderança em segurança e segurança de aplicações. Também possuem certificação via GIAC, uma parceria do SANS Institute com mais de 35 certificações práticas de segurança da informação, um curso de mestrado pela escola de pós-graduação do SANS Technology Institute, além de inúmeros recursos de segurança gratuitos, entre os quais boletins, *white papers* e *webcasts*.

2.3. Normas e Recomendações

Existem algumas normas que fazem recomendações, das quais surgem alguns guias de boas práticas. De entre essas normas, destaca-se a International Organization for Standardization (ISO) e o National Institute of Standards and Technology (NIST).

2.3.1. International Organization for Standardization

A ISO desenvolve e publica padrões internacionais. É uma organização independente e não governamental. Tem mais de 160 membros e mais de 45.000 especialistas. A organização cria documentos que fornecem requisitos, especificações, diretrizes ou características que podem ser usadas de forma consistente para garantir que os materiais, produtos, processos e serviços sejam adequados à sua finalidade. Publicaram mais de vinte mil *standards* que podem ser comprados.

Uma das normas mais populares é a ISO/IEC 27001, lançada em 2005 pela ISO e pelo IEC's Joint Technical Committee (JTC), referente aos riscos da gestão da segurança da informação. À medida que as empresas se tornam mais dependentes dos sistemas de informação, a segurança dos mesmos tornou-se cada vez mais importante, sendo imperativo efetuar a sua proteção e minimizar os riscos a que estão expostas, a ISO 27001:2005 tornou-se um dos mais populares *standards*.

A ISO 27001:27005, cataloga as vulnerabilidades afetando-as a diferentes áreas gerais, organização, processos e procedimentos, rotinas de gestão, pessoal, ambiente físico, configuração do sistema, *hardware*, *software* e equipamentos de comunicações, e a dependência de terceiros.

Esta norma enfatiza a identificação das vulnerabilidades que podem ser exploradas por uma ameaça e que podem causar danos aos ativos da organização. Para isso, utiliza uma série de controlos que se não estiverem corretamente implementados poderão constituir, por si próprios, uma nova vulnerabilidade.

2.3.2. National Institute of Standards and Technology

O NIST, fundado em 1901, faz parte do Departamento de Comércio dos Estados Unidos da América (EUA), sendo um dos seus mais antigos laboratórios de ciências físicas. Promove a inovação e a competitividade industrial dos EUA, desenvolvendo a ciência, os padrões e a

tecnologia de medição, de maneira a melhorar a segurança económica e melhorar a qualidade de vida. A sua estrutura é de cariz voluntário e é baseada em padrões, diretrizes e práticas existentes para que as organizações possam gerir e reduzir os seus riscos.

O NIST tem uma *framework*[23] bastante popular sobre cibersegurança.

Através do NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program"[24], podemos seguir algumas recomendações para a implementação de um programa de *security awareness*.

2.4. Ferramentas de *Phishing*

No mercado de *software*, existem soluções para tudo o que se possa imaginar. O *software* é disponibilizado de acordo com o tipo de licença, esta pode ser de diversos tipos, livre em regime *open source*, licença comercial sujeita a pagamento único, mensal ou anual, existindo também ferramentas que possuem dois tipos de versões, uma mais leve em regime *open source* e a mais completa em regime comercial.

Esta pesquisa sobre ferramentas de *phishing*, procura encontrar uma ferramenta em regime *open source* (livre de encargos) e uma ferramenta comercial, que se adeque para efetuar campanhas de *phishing* e se possível de sensibilização em segurança informática.

O ideal é encontrar a ferramenta que permita ser maleável ao ponto de permitir efetuar campanhas de *phishing* completas. Fazer o envio de um *e-mail*, que possa conter anexos, *links* e que através deles se possa fazer a abertura de páginas fictícias, mas baseadas nas reais, para recolha de credenciais de acesso a um serviço, do tipo redes sociais ou outros, que permita também a recolha de resultados, com possibilidade de exportação de dados. Se possível integrando os indivíduos numa sessão de *awareness* sobre segurança informática.

Existem muitas ferramentas, umas mais simples, outras mais complexas, tanto ao nível da usabilidade como de características de pequenas funcionalidades.

Normalmente as ferramentas de *open source*, exigem um maior nível de conhecimentos, para a sua instalação e configuração, sendo a maior parte delas baseadas em Linux.

As soluções comerciais costumam disponibilizar versões de demonstração das suas ferramentas, que podemos usar durante quase 1 mês e que na maior parte dos casos poderá servir o nosso objetivo. Algumas disponibilizam em regime Software As A Service (SaaS),

sendo fáceis de utilizar, configurar, têm muitas funcionalidades e incluem relatórios detalhados.

Deixo de seguida uma lista de ferramentas, com algum detalhe das suas funcionalidades.

2.4.1. Sophos

A Sophos é um das grandes empresas de segurança, tem uma ferramenta dedicada ao *phishing,* chama-se Sophos Phish Threat[25]. Esta ferramenta é uma ferramenta comercial, que dispõe de uma versão de demonstração, que se pode testar durante 30 dias, apesar de ter algumas limitações, acerca do número de utilizadores que se podem colocar na plataforma, assim como em relação aos templates que se encontram disponíveis e outras funcionalidades que se encontram limitadas na versão de demonstração. É uma ferramenta muito fácil de utilizar, intuitiva, não sendo necessários grandes conhecimentos técnicos para a sua utilização e configuração.

2.4.2. Infosec IQ

Infosec IQ[26] inclui uma ferramenta de teste grátis de *phishing* que permite o lançamento de um ataque simulado de *phishing*, sendo que em 24 horas é possível receber na sua organização uma resposta em tempo real sobre a taxa de *phishing*.

Também temos acesso a uma simulação completa da ferramenta PhisnSlim, para executar um teste de phishing a uma organização. Esta ferramenta possui na sua biblioteca mais de 1.000 *templates* e anexos, além de páginas falsas para as campanhas. Estes templates são atualizados semanalmente. Também pode fazer a sua própria campanha.

2.4.3. Gophish

Gophish[27] é uma potente ferramenta fácil de utilizar, em regime *open source*, que ajuda a realizar campanhas de *phishing*. Possui um guia do utilizador, que mostra as capacidades desta plataforma, indicando os três simples passos para a criação de uma campanha de *phishing*. Escolher os modelos e destinatários, lançar a campanha e seguir os resultados.

Podemos iniciar uma campanha de *phishing*, escolher o grupo alvo, escolher o modelo de *e-mail* a utilizar, escolher a página fictícia de recolha de credenciais e lançar a campanha.

Fácil de instalar e configurar, corre em 3 plataformas, Windows, macOS e Linux. Atualmente vai na versão 0.8.0.

2.4.4. Lucy

A Lucy[28] um produto comercial que permite ao utilizador experimentar uma versão de demonstração funcional através de uma versão comunitária, pode ser feito o *download* em solução virtual ou em *scripts* de instalação da Debian. A versão *web* é atrativa, existem muitas ferramentas para explorar, esta é uma solução desenhada como uma ferramenta de engenharia social, mas que vai muito mais além. A parte de *awareness* encontra-se sob a forma de módulos e questionários. Na versão comunitária não estão disponíveis muitas das opções que seriam úteis para uso em modo empresarial, tais como a exportação de dados, o status das campanhas, ataques de *phishing* com ficheiros em anexo, assim como campanhas com calendarização de eventos.

2.4.5. Phishing Frenzy

Esta solução Phishing Frenzy[29] em formato *open source* Ruby on Rails, foi desenhada para testes de penetração e tem muitas funcionalidades para efetuar campanhas de *phishing* interno. A funcionalidade mais importante é a de poder mostrar em detalhe as campanhas de *phishing* e de poder exportar os resultados para PDF ou XML. A parte menos simpática é que sendo uma instalação Linux, não é simples de implementar.

2.4.6. King Phisher

Através desta solução King Phisher[30] *open source* da SecureState, estamos perante um *software* mais sofisticado. As funcionalidades disponíveis são muitas e incluem a possibilidade de poder efetuar várias campanhas de *phishing* ao mesmo tempo, localizando os utilizadores, efetua clonagem de páginas da *Internet*, contém um repositório de templates para o envio de *e-mails* e para as páginas de *Internet*, tem uma interface simples e clara, no entanto a instalação e configuração desta ferramenta só é suportada pelo sistema Linux e são necessários passos adicionais para a sua instalação.

2.4.7. SpeedPhishing Framework (SPF)

A ferramenta SpeedPhishing Framework[31] criada por Adam Compton em Python, inclui muitas funcionalidades que permitem rapidamente configurar ataques de *phishing* incluindo

dados de três entradas, existindo três *templates* com possibilidade de customização. Apesar de esta ferramenta possibilitar a elaboração de campanhas de *phishing* ela é principalmente uma ferramenta de testes de penetração, com funcionalidades interessantes, como a de recolha endereços de *e-mail*.

2.4.8. Social Engineer Toolkit (SET)

Esta ferramenta da Trustedsec[32], foi desenhada para efetuar vários ataques de engenharia social. Ela permite enviar *e-mails* de *spear phishing,* campanhas com envio de *e-mails* em massa, assim como efetuar a sinalização de mensagens de importância alta. SET é baseado em Python sem uma GUI. Como ferramenta de testes de penetração, é muito eficaz. Como ferramenta de *phishing* é mais limitada e não inclui nenhuma ferramenta de reporte e gestão de campanhas de *phishing*.

2.4.9. SpearPhisher BETA

A ferramenta SpearPhisher BETA[33] desenvolvida pela TrustedSec, é uma ferramenta simples de envio de *e-mails* de *phishing*. Foi desenhada para pessoal não técnico sendo um programa para Windows. Permite que rapidamente seja feita uma campanha de *phishing* com customização do *e-mail* do remetente, nome do remetente, assunto, incluindo um editor de HTML e opção para envio de um anexo. O *e-mail* pode ser enviado utilizando os campos PARA, CC e BCC. Este programa encontra-se em versão beta desde 2013.

3. Planeamento de um Programa de *Security Awareness*

Security Awareness, é o conhecimento e a atitude que os indivíduos de uma organização possuem em relação à proteção dos seus ativos físicos e principalmente informativos dessa organização, e que permite que possam ser a primeira linha de defesa de uma organização.

Definido pelo NIST 800-16[34] como "*Awareness* não é formação, é apenas colocar o foco da atenção na segurança da informação, levar a que o utilizador reconheça essas preocupações e reaja de acordo com elas." Na Figura 3.1 –Promoção de conhecimento[22] da SANS, podemos ver as três fases da promoção do conhecimento.

Figura 3.1 –Promoção de conhecimento

De seguida apresento o modelo de maturidade proposto pela SANS[35] que está representado na Figura 3.2 – SANS *Security Awareness* Maturity Model.

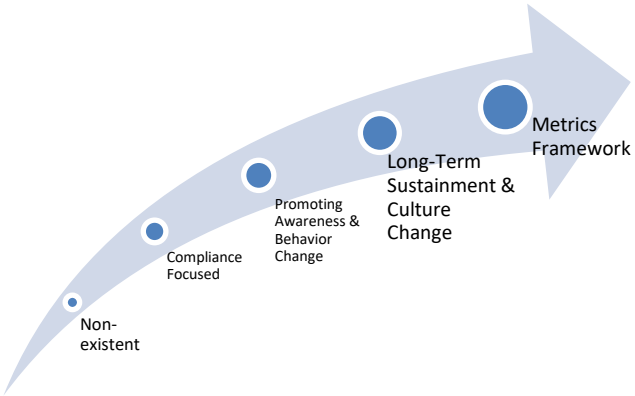


Figura 3.2 – SANS *Security Awareness* Maturity Model

Este modelo, desenvolvido em 2011 por mais de 200 elementos, permite identificar o nível de maturidade de consciência para a segurança.

Este modelo é composto por cinco níveis de *security awareness*:

- **Não existente** - A organização não possui um programa de s*ecurity awareness*, os utilizadores não têm a consciência de que são alvos e que as suas ações podem ter impacto direto na segurança da organização, desconhecem as políticas de segurança da organização caso existam, sendo alvos fáceis de ataque;
- **Focado na conformidade** - Existe um programa de *security awareness* desenhado para alcançar métricas ou indicadores específicos. O treino é reduzido. O conhecimento das políticas de segurança é fraco, assim como o seu papel na implementação das medidas de segurança da organização;
- **Promoção da consciência e mudança de comportamento** – Existe um programa de *security awareness* desenhado e implementado que identifica de forma clara os tópicos de segurança a abordar, por forma a garantir a existência de comportamentos de segurança que potenciem a continuidade do negócio da organização. São feitas múltiplas formações ao longo do ano e é encorajada a mudança de comportamento, quer em casa quer no trabalho, levando a que os colaboradores percebam e cumpram as políticas de segurança da organização, reconhecendo, prevenindo e reportando ativamente incidentes;
- **Sustentabilidade a longo prazo e mudança cultural** - O programa existente contempla processos, recursos e mecanismos de liderança necessários para que exista uma revisão com periodicidade mínima anual, garantindo também uma adequação permanente do programa às evoluções tecnológicas e à identificação de novas ameaças e vulnerabilidades. A *security awareness* é parte integrante da cultura da organização;
- **Estrutura robusta de métricas** - O programa contempla uma estrutura de métricas que permite medir a evolução das medidas definidas e aplicadas, contribuindo para a melhoria contínua do programa, evidenciando o retorno do investimento feito.

Segundo Dan Lohrmann[36], especialista em *cybersecurity*, existem dez recomendações para implementar um programa de *security awareness*, cinco a implementar e cinco a evitar.

Medidas a implementar:

- Assegurar que existe apoio por parte da direção, se houver participação direta, como exemplo, é meio caminho andado para o sucesso;
- Tornar o programa divertido, usar jogos na aprendizagem se possível;
- Incluir posters, *newsletters*, dicas por *e-mail*, *blogs* e lembretes. Pessoas diferentes, aprendem de forma diferente;
- Focar-se nas alterações de comportamento. Relativamente à vida familiar e privada.

Medidas a evitar:

- Não ficar agarrado às coisas antigas, um programa de *security awareness* tem de ser constantemente atualizado;
- Não acreditar que vídeos e apresentações fazem milagres, sendo única e exclusivamente os canais de comunicação principais do programa de *security awareness*;
- Não confundir programas de formação com programas de *security awareness*;
- Não esquecer ninguém, e não colocar a *security awareness* como um extra;
- Não se focar apenas no que deve ser feito, podemos ter de improvisar.

Solicitar aos utilizadores finais ideias e encorajar o seu feedback, para poder medir o sucesso do crescimento do programa. Quantos utilizadores terminaram o programa? O que eles gostaram? Aprenderam alguma coisa? O seu comportamento alterou-se? Perguntar por sugestões e novas ideias. Encorajar a criatividade. Providenciar mecanismos em tempo real para recolha de dados do *staff*.

Passo a descrever de seguida, a metodologia e as etapas de conceção de um programa de *security awareness*, com base maioritariamente nas orientações da ENISA[37], mas de forma simples e mais sucinta, dado que no guia da ENISA encontramos todos os pormenores em detalhe, tabelas de recolha de informação, sugestão de questionários, intervenientes.

3.1. Metodologia

A conceção de um programa de *security awareness,* envolve a colaboração de todas as partes interessadas de uma organização. Planear um programa de *security awareness* numa organização, implica avaliar o nível de conhecimento atual dos vários indivíduos sobre a

segurança da informação no contexto da organização, conhecer o grupo alvo, estabelecer uma meta de conhecimentos a atingir, analisar os resultados obtidos e implementar as medidas que sejam necessárias para melhorar esse nível de *awareness*. No final voltamos a medir esse conhecimento e tudo recomeça se for necessário.

O foco da consciencialização da segurança da informação, deve ser, o de alcançar uma mudança de longo prazo na atitude dos indivíduos em relação à segurança, ao mesmo tempo que se promove uma mudança cultural e comportamental dentro da organização.

As políticas de segurança devem ser encaradas como facilitadores essenciais para a organização, não como uma série de regras que restrinjam o funcionamento eficiente do negócio.

Figura 3.3 - Ciclo de vida de um Programa de *SecurityAwareness*

3.2. Métricas

É essencial que um programa de *security awareness* possa medir o seu impacto. Sem esta medição, não se consegue perceber, se o programa obteve sucesso ou se falhou e necessita de reforço.

Para medir o nível de conhecimento existente, assim como, o resultado obtido com a aplicação de um programa de *security awareness*, a medição pode ser efetuada através da implementação de sondagens ou questionários para recolha da informação necessária.

Numa primeira fase há que perceber o que se pretende medir. O que preocupa as empresas ao nível do comportamento humano? O que deverá ser alterado?

Será possível prevenir a engenharia social? O *phishing*? O roubo de *passwords*?

Para medir algo, é necessário ter uma tabela de valores. Em termos de conhecimento, importa definir qual a grelha de conhecimentos que se vai utilizar para essa medição e qual ou quais os seus níveis.

Tomemos como exemplo, o Europass. Quando afirmamos que sabemos falar, escrever e compreender inglês, podemos medir esse conhecimento através da grelha de níveis das línguas.

Desta forma, podemos elaborar ou utilizar uma grelha já existente (exemplo Anexo A – Competências Digitais, pág. 54), com níveis de conhecimento em segurança da informação e TIC.

Se definirmos que o grupo alvo tem 60% de *awareness* no nível 1 e se definirmos como objetivo, aumentar o *awareness* para 100%, no final ao voltar a efetuar a medição podemos avaliar se o programa está a funcionar ou se é necessário proceder a alterações.

3.3. Grupo Alvo

O grupo alvo, é uma das peças chave, de um programa de *security awareness*. A sua constituição e divisão em pequenos grupos é importante, tanto mais que daí pode depender o sucesso ou fracasso de um programa de *security awareness.*

Importa conhecer, o seu nível de conhecimento, e reconhecer as suas necessidades em termos de *security awareness*. A divisão do grupo alvo em pequenos grupos, é uma medida facilitadora de medição, avaliação e disseminação de conhecimento.

Os grupos podem ser divididos por funções ou responsabilidades na organização tal como se pode ver na Figura 2.2 – Papeis desempenhados numa organização, segundo o PCI Security Standard Council, além das suas necessidades em *security awareness*.

Independentemente dos papéis desempenhados na organização, é recomendado que o nível de conhecimento base seja igual para todos.

Vejamos como exemplo, os riscos de segurança do Departamento de Recursos Humanos, não são os mesmos que os riscos do Departamento de Sistemas Informáticos ou do Departamento da Área Financeira e Contabilidade, como tal, importa customizar a disseminação de *awareness* pelo grupo alvo, para que o interesse e a recetividade sejam os melhores na promoção de boas práticas.

Cada indivíduo como ser único que é, quando incluído num grupo com as mesmas necessidades de *awareness*, pode ter um desempenho diferente na aquisição de novas aprendizagens, devido ao seu nível cognitivo e facilidade de aprendizagem.

É relevante a preferência por algum tipo de aprendizagem por parte de alguns indivíduos, dado que uns preferem aulas com professor em modo presencial, outros preferem cursos em formato *e-learning*, outros preferem ver vídeos ou assistir a conferências e *workshops*. É importante enquadrar o grupo alvo nos vários tipos de aprendizagem.

3.4. Comportamentos de Risco

Nesta etapa e após a definição do grupo alvo, há que ter em consideração os seus hábitos dentro da organização, identificando comportamentos de riscos e promovendo as boas práticas, para minimizar os riscos de segurança.

Importa realçar as boas práticas e a mudança de hábitos e comportamentos de risco.

Apesar de existirem normas, regulamentos e políticas de segurança nas organizações as boas práticas nem sempre são cumpridas por parte dos indivíduos, sendo os comportamentos de risco uma constante, estando diretamente ligados às ameaças e riscos do momento, exemplo disso é o lançamento de campanhas direcionadas para um determinado setor ou empresa, por exemplo: *ransomware*, *phishing* ou *spam*.

Um exemplo comum é a receção de *e-mails* com ofertas de iPhones por 1€, bastando para tal, clicar num *link* e preencher o número de telemóvel, nome e *e-mail*. Costuma dizer-se que "quando a esmola é muita o pobre desconfia", mas mesmo assim existe sempre alguém que cai nesta oferta.

Se pretendemos que os indivíduos de uma organização saibam como proceder em determinadas situações, devemos identificar essas situações, indicar os comportamentos esperados, através da elaboração de uma lista de boas práticas. Pode ser uma espécie de guia prático. Algo que o individuo encontre facilmente e possa esclarecer as suas dúvidas.

3.5. Medidas

Nesta etapa são elaboradas as medidas a tomar para mitigar o risco e facilitar a mudança de comportamentos. Aqui decidimos o que fazer com os riscos que foram identificados nas etapas anteriores.

As medidas podem ter várias formas, guias, políticas, normas, regulamentos, *software* para lidar com informação classificada, politica de alteração de passwords.

3.6. Canais de Divulgação

Na etapa da divulgação, encontramos um dos grandes problemas de um programa de *security awareness,* é como disseminar a informação para o grupo alvo e como medir a sua eficácia.

Podem ser efetuadas propostas diversas de transmissão de conhecimento, nomeadamente através da formação, do treino e da criação de canais para divulgação de informação, para toda a empresa, envolvendo todos os seus intervenientes.

Para consciencializar o grupo alvo, saliento os seguintes canais:

- Convencionais em papel
    - Folhetos e posters, com *slogans* atrativos, cartazes com tópicos relevantes (ex: *passwords*), colocados em zonas de passagem ou locais de reunião;
    - *Newsletters* periódicas, mensais ou trimestrais, que podem ser eletrónicas ou impressas em papel, servem para distribuir duma só vez, várias mensagens;
    - Existe o inconveniente de não se garantir a leitura por parte do grupo alvo.
- Formação em sala de aula
    - Seminários ou *workshops*, permitem alguma interação entre o formador e o grupo alvo, permitindo a elaboração de questões e dúvidas e a

imediata resposta por parte do formador. Também permitem a partilha de experiências entre o grupo alvo.

- Formação *online*
  - Envio de *e-mail*, para uso mais sensível e importante, pode ser rapidamente direcionado a um grupo alvo
  - *Blogs*, Fórums e *Chats*
  - Cursos em *e-Learning* ou PC através de CD, de preferência com jogos ou multimédia de forma a serem menos monótonos e mais atrativos.
- Formação baseada em jogos
  - Formação através de jogos
- Formação baseada em vídeos
  - Este método tem o inconveniente de não permitir saber se a audiência está atenta, mas permite que aprendam ao seu próprio ritmo.
- Formação baseada na simulação
  - O grupo alvo pode viver a experiência simulada e após isso ser alvo de seguimento através de panfletos.

Segundo J. Abawajy[38], as preferências dos indivíduos acerca dos métodos mais escolhidos são a disseminação através de vídeos e papel.

A disseminação de informação é uma das peças mais importantes na melhoria da consciencialização da segurança da informação, importa escolher o método mais adequado ao grupo alvo. A escolha de vários métodos ajuda a que a abrangência ao grupo alvo seja maior.

3.7.Materiais

Nesta etapa são elaborados os materiais a disseminar pelo grupo alvo, que podem ser tão variados como a diversidade do grupo alvo e podem ter a forma de: cartazes, folhetos, *newsletters* em papel ou em formato digital, *screensaver* corporativo, apresentações em PowerPoint, publicações em PDF, entre outros materiais.

Os materiais desenvolvidos deverão poder dar resposta às necessidades do grupo alvo, em relação aos comportamentos de risco, o seu papel será o de facilitar a mudança de comportamento, para os hábitos desejados e as boas práticas.

3.8. Awareness

Thomas R. Peltier[39] afirma que a aprendizagem é composta por três elementos: consciencialização, formação e educação.

Nesta etapa, deve ser efetuada a consciencialização dos indivíduos através dos canais de divulgação que se julguem ser os mais adequados de acordo com o grupo alvo.

O grupo alvo pode ser constituído por toda a organização, ou pode ser dividido em pequenos grupos, sendo essa uma opção de estratégia da empresa.

Deverá utilizar-se mais do que um canal de divulgação em simultâneo, está comprovado que através de diferentes meios, será mais fácil atingir o mesmo objetivo. Nem todas os indivíduos possuem as mesmas capacidades cognitivas, sendo a diversidade de meios a usar, um facilitador da aprendizagem.

A quantidade de informação a distribuir deverá ser curta e frequente, facilitando a memorização e evitando o excesso de informação. Os canais de divulgação referidos na secção 3.6, podem ser adaptados a esta realidade.

Uma ação de *awareness*, pode ser complementada por sessões de formação ou de educação para o grupo alvo.

Após as medidas de *awareness* deverá ser avaliado e medido o seu impacto no grupo alvo, voltando à seção 3.2 (Métricas), para realização de novo ciclo se necessário, só assim podemos avaliar e melhorar o nosso programa de *security awareness*.

4. Caso de Estudo

Elaborei um caso de estudo com o objetivo de implementar um programa de *security awareness* na Polícia Judiciária, organização cuja atividade principal é a investigação criminal, mas que possui nas suas instalações uma escola de formação.

O programa foi aplicado a um universo de cerca de 100 pessoas, que voluntariamente aceitaram fazer parte deste projeto. Por questões de confidencialidade, o nome dos participantes foi mantido em sigilo, em relação aos dados recolhidos no âmbito do programa.

O objetivo do programa de *security awareness*, é o de aumentar o conhecimento dos indivíduos sobre a utilização das TIC com mais segurança, nomeadamente melhorar a sua sensibilidade acerca das seguintes temáticas:

- Utilização de passwords;
- Receção/envio de *e-mails*;
- Engenharia social;
- *Phishing.*

4.1. Metodologia Utilizada

Para aplicação do Programa de S*ecurity Awareness*, efetuei uma breve análise ao grupo alvo e à organização em questão. O foco do programa centrou-se nas fragilidades humanas em relação às *passwords*, à engenharia social e redes sociais.

Foi estabelecido qual o nível de conhecimento que deveria ser atingido, foram aplicadas medidas de avaliação desse conhecimento, através de um questionário.

Após essa avaliação, foram elaboradas e propostas, medidas de promoção do conhecimento em *security awareness*.

Foram elaboradas métricas e retiradas as conclusões acerca do caso de estudo efetuado, as suas limitações e trabalho futuro.

4.2. Estrutura e Implementação do Programa de *Security Awareness*

Para poder implementar este caso de estudo, foi solicitada autorização superior ao dirigente da signatária. Após existir concordância e interesse, demonstrado pela pertinência do tema em causa, deu-se início ao trabalho de campo.

Para aplicação da metodologia descrita no capítulo 3, o plano de trabalho foi dividido nas etapas descritas nas seções seguintes.

4.2.1. Análise do grupo alvo

O grupo alvo cingiu-se a uma amostra de cem voluntários, oriundos de várias áreas de trabalho, diferentes departamentos, sexo, idade e formação académica.

A organização estava ciente, de que para a implementação deste programa ser um sucesso, seria fundamental envolver toda a hierarquia dirigente da organização.

Do universo total de cem pessoas, apenas oitenta, participaram ativamente no caso de estudo, sendo, 47,5% do sexo masculino e 52,5% do sexo feminino.

As faixas etárias mais numerosas situaram-se nos 42,5% entre os 46 e 55 anos e 31,3% entre os 36 a 45 anos. Mais de metade dos intervenientes possuem licenciatura, 51,2% e 22,5% possuem mestrado.

4.2.2. Metas a atingir e nível de conhecimento

Dada a diversidade de funções que cada um desempenha na organização e sendo esta uma experiência piloto, optei por ter como objetivo, nivelar o conhecimento, no nível básico.

Utilizei a componente de Segurança, referente à grelha de Competências Digitais disponível no Anexo A – Competências Digitais, utilizada no âmbito do Europass - Passaporte Europeu de Competências[40]. O nível básico refere o seguinte:

> "Sei como aplicar medidas de base para proteger o meu equipamento (ex: utilizar antivírus e palavras-passe). Sei que nem toda a informação *online* é fiável. Estou ciente de que as ninhas credenciais (nome de utilizador e palavra-passe) podem ser roubadas. Sei que não devo divulgar informação pessoal *online*. Estou ciente que a utilização excessiva de tecnologia informática pode afetar a minha saúde. Eu tomo medidas simples para economizar energia."

4.2.3. Avaliação do nível de conhecimento

A avaliação dos conhecimentos de cada individuo do grupo alvo, foi efetuada através da aplicação de um questionário, presente no Anexo C – Questionário aos Hábitos e Conhecimentos sobre Segurança da Informação, que foi realizado através do serviço da Google Forms, sendo o seu acesso disponibilizado através de um *link* enviado para a caixa de correio de todo o grupo alvo.

Do universo de cem indivíduos do grupo alvo, apenas 80% respondeu ao questionário.

As respostas obtidas podem ser consultadas no Anexo F – Resultados do 1º Questionário.

No final do preenchimento do questionário, foi proposto ao individuo que frequentasse um Curso sobre Segurança da Informação.

Apenas 67,5% responderam que pretendiam frequentar esse curso.

4.2.4. Medidas de promoção do conhecimento em *security awareness*

Uma das medidas realizadas para promoção do conhecimento, foi a realização de um Curso sobre Segurança da Informação, cujo conteúdo pode ser consultado em detalhe no Anexo D – Curso Segurança da Informação.

Este curso pretende dar a conhecer alguns dos perigos das novas tecnologias, promovendo a utilização das TIC de uma forma mais segura e consciente, dando a conhecer as boas práticas, sugeridas por algumas instituições e organizações nacionais e internacionais, organizações essas, que produzem materiais educativos e de sensibilização na área da cibersegurança.

Para além da elaboração do Curso, foi elaborada uma campanha de *phishing*, cujo foco foi centrado na engenharia social e credenciais de acesso a serviços *online*, tais como serviços de *e-mail* e redes sociais.

Para realizar a campanha de *phishing*, foi necessário utilizar uma plataforma de *phishing*. No entanto, optei por utilizar duas plataformas, para poder explorar melhor as suas capacidades. Foram assim escolhidas as plataformas, GoPhish e a Sophos. A primeira é uma plataforma em *open source*, sendo a segunda, uma plataforma comercial de uma conceituada empresa no mercado, em matéria de segurança, no entanto foi utilizada a versão de demonstração, disponível durante um mês.

A escolha da plataforma GoPhish recaiu na sua versatilidade de ambiente, podendo ser utilizada em ambiente Windows, macOS e Linux, para além da facilidade de personalização das campanhas de phishing. Na página da GoPhish são disponibilizados manuais e guias explicativos da sua utilização.

Quanto à ferramenta Phish Threat da Sophos, apesar de ser uma ferramenta comercial, é possível a sua utilização na versão de demonstração, durante um mês, apesar de algumas limitações a nível de personalização das campanhas. Se optarmos por adquirir licenças, podemos adquirir apenas para o universo que se pretenda testar, ao invés de, adquirir para toda a empresa.

Podemos encontrar no Anexo I – Plataformas GoPhish e SOPHOS, uma comparação entre as duas plataformas, relativamente às suas vantagens e desvantagens.

Através da plataforma GoPhish, efetuei uma campanha que faz o envio de um *e-mail*, cujo conteúdo, continha *links* sobre a publicação de um artigo de um utilizador do Linkedin (rede social profissional), cujo clique no *link*, levava à abertura de uma página para introdução das credenciais do utilizador referentes à sua conta do Linkedin, página essa elaborada para este teste de *phishing*.

O detalhe completo desta campanha de *phishing* pode ser consultado no Anexo J – Campanha de *Phishing* da GoPhish

O resultado desta ação de *phishing* pode ser visto na Figura 4.1, onde dos 97 *e-mails* enviados, apenas dois indivíduos abriram os *e-mails* e clicaram nos *links* enviados, tendo apenas um individuo introduzido as suas credenciais, como se pode ver na Tabela 4.1.

Figura 4.1 – Resultado da campanha de *phishing* da plataforma GoPhish

A plataforma regista, a abertura do *e-mail*, o clique nos *links* e a introdução de credenciais (*user name* e *password*). Deteta qual o tipo de dispositivo que efetuou o clique no *link*, se é feito através de um PC ou de um dispositivo móvel, registando o sistema operativo e o

browser ou o modelo do dispositivo móvel e o *browser* utilizado, como se pode ver na Figura 4.2 e na Figura 4.3.

Figura 4.2 – Identificação do PC

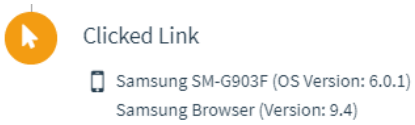


Figura 4.3 – Identificação do dispositivo móvel

Caso o individuo introduza as suas credenciais, as mesmas ficam guardadas na plataforma, podendo até ser reutilizadas para introdução noutra página de *Internet*.

Tabela 4.1 – Credenciais de acesso

session_key	paula@gmail.com
session_password	123456

Através da plataforma da SOPHOS, realizaram-se duas campanhas de *phishing*, uma orientada para a rede social Linkedin e a outra para os eventos de calendário, neste caso o serviço Gmail.

As duas campanhas realizadas através da plataforma da SOPHOS, foram divididas em quatro grupos para o envio de *e-mails*, o que fez com que os resultados também ficassem divididos em quatro grupos. Esta condicionante, deveu-se ao facto de, na versão de testes, a plataforma não permitiu o envio de *e-mails* ao grupo alvo por completo, devido a restrições com os endereços do domínio @gmail.com.

Na campanha de *phishing* 1, que consistia no envio de *e-mails* com um evento de calendário do Gmail, o individuo recebia um *link* com um convite de uma marcação no Hospital dos

Lusíadas. Ao clicar nesse *link,* era remetido para uma página falsa de inserção de credenciais do Gmail. No final e caso o utilizador inserisse as suas credenciais, iria perceber que não se tratava da página oficial do Gmail.

O detalhe completo desta campanha de *phishing* pode ser consultado no Anexo K – Campanha de *Phishing* 1 da SOPHOS.

O resultado desta campanha foi o seguinte:

Dos 56 *e-mails* enviados, 18 indivíduos abriram os *e-mails*, tendo 9 clicado no *link* que abria a página falsa de inserção de credenciais, sendo que 3 inseriram as credenciais.

Figura 4.4 – Resultados campanha *phishing* 1 SOPHOS

Na campanha de *phishing* 2, que consistia no envio de *e-mails* sobre o Linkedin, o individuo recebia um texto sobre como poderia promover o seu perfil, nessa rede social. Ao clicar, em qualquer um desses *links* era remetido para uma página falsa de inserção de credenciais do Linkedin. No final e caso o utilizador inserisse as suas credenciais, iria perceber que não se tratava da página oficial do Linkedin.

O detalhe completo desta campanha de *phishing* pode ser consultado no Anexo L – Campanha de *Phishing* 2 da SOPHOS.

O resultado desta campanha foi o seguinte:

Dos 55 *e-mails* enviados, 6 indivíduos abriram os *e-mails*, sendo que nenhum clicou nos *links* enviados que abriam a página falsa de inserção de credenciais.

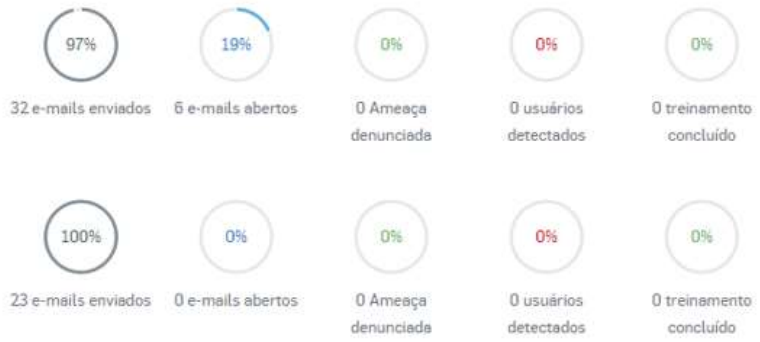


Figura 4.5 – Resultados da campanha de *phishing* 2 da SOPHOS

Estas campanhas de *phishing* poderiam ter na sua sequência, a obrigatoriedade de inscrição do utilizador num minicurso de *awareness*, mais fácil de implementar através da plataforma da SOPHOS do que na GoPhish.

4.2.5. Medição do resultado obtido

Para medir o sucesso das medidas de promoção da consciencialização, efetuei um novo questionário constante do Anexo E – Questionário Final aos Hábitos e Conhecimentos sobre Segurança da Informação.

Este questionário foi distribuído após a frequência do Curso sobre Segurança da Informação, ou passados 15 dias sobre a data da elaboração do primeiro questionário.

4.2.6. Análise dos questionários

Para efetuar a análise dos questionários, é utilizada a análise qualitativa dos dados obtidos através da realização dos dois questionários. O nível de conhecimento terá aumentado, se o número de respostas corretas aumentar entre a realização do primeiro e do último questionário.

Ao utilizar a estatística descritiva, que consiste na recolha, apresentação, análise e interpretação dos dados numéricos através da criação de quadros, gráficos e indicadores numéricos[41], pode interpretar-se os resultados obtidos.

Foi elaborado um quadro para cada questionário, com duas variáveis de estudo, as respostas corretas, e as incorretas ou menos corretas. Na Tabela 4.2 – Análise das respostas ao Questionário 1 e na Tabela 4.3 – Análise das respostas ao Questionário 2, pode ver-se o

número de respostas "corretas" e "incorretas" em percentagem, relacionado com o número de elementos que escolheu esse valor.

Os questionários, têm vinte e uma perguntas em que os indivíduos têm de escolher uma opção que se adeque à situação proposta. Esta escolha pode estar "correta", ou "incorreta ou menos correta". Na tabela seguinte, podemos ver a contabilização das respostas dadas ao questionário sobre os hábitos e conhecimentos sobre segurança da informação.

Apresentação de dados

Em relação ao género em ambos os questionários, encontram-se bem distribuídos como se pode ver na Figura 4.6 - Gráfico da Distribuição do Género.

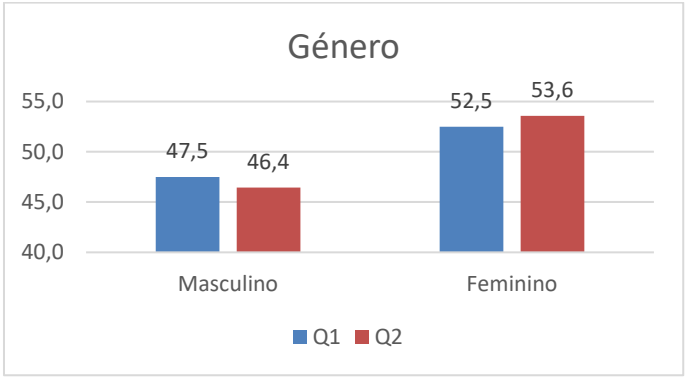


Figura 4.6 - Gráfico da Distribuição do Género

Em relação à Faixa Etária em ambos os questionários, as mais participativas situam-se entre os "36 a 45 anos" e entre os "46 a 55 anos", como se pode ver na Figura 4.7 – Gráfico da Distribuição da Faixa Etária.

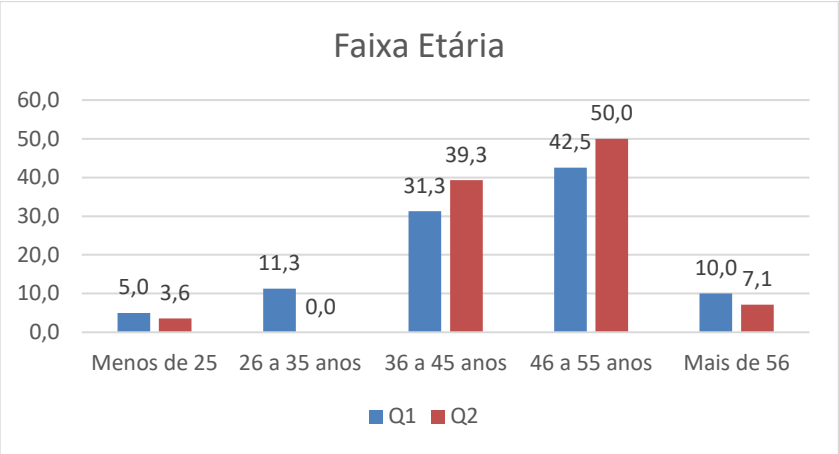


Figura 4.7 – Gráfico da Distribuição da Faixa Etária

Em relação às Habilitações elas distribuem-se por três grandes opções, "Mestrado", "Licenciatura" e "Ensino Secundário, 12º ano", como se pode ver na Figura 4.8 – Gráfico da distribuição das Habilitações

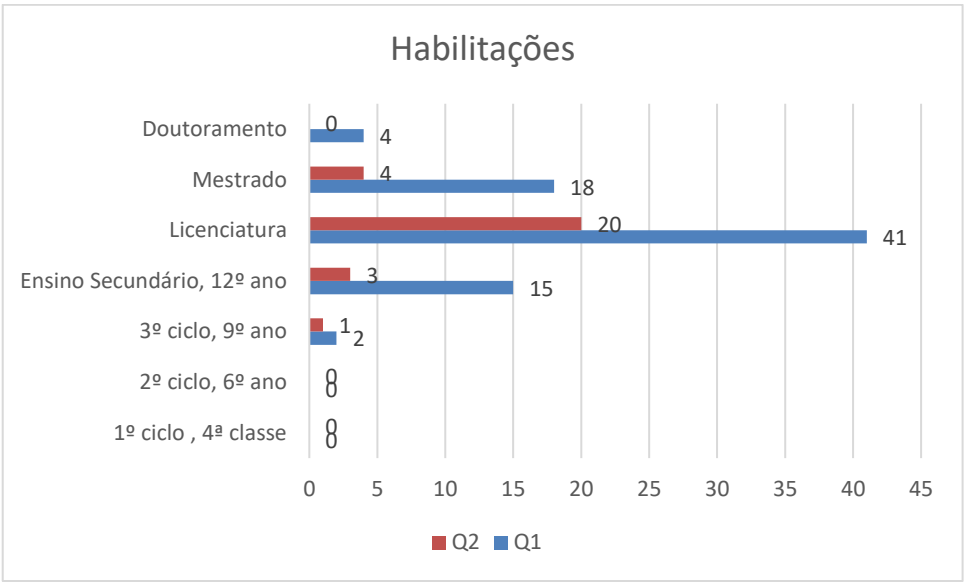


Figura 4.8 – Gráfico da distribuição das Habilitações

Na Tabela 4.2 – Análise das respostas ao Questionário 1, podemos observar as respostas que foram recolhidas e verificar a percentagem de respostas corretas em relação às incorretas. A amostra para este questionário foi de oitenta respostas.

Tabela 4.2 – Análise das respostas ao Questionário 1

Nº	Pergunta	Resposta correta	% Resposta correta	% Resposta incorreta
1	Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?	d. seja difícil de memorizar e tenha caracteres variados (com pelo menos 16 caracteres e sem nexo)	8,8	91,3
2	Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?	c. G0$t0DeGel@d0$29	88,8	11,3
3	Com que frequência altera as suas palavras passe?	a. Uma vez por mês	8,8	91,3
4	Qual o método que utiliza para guardar ou memorizar as suas palavras passe?	c. Utilizo um gestor de palavras passe com encriptação	20,0	80,0
5	Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de *e-mail* e de nos autenticar. Como procede em relação a este problema?	d. Utilizo um gestor de palavra passe que também tem a funcionalidade de gerador de palavras passe com um algoritmo aleatório	3,8	96,3
6	No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?	c. Fica bloqueado com palavra passe	85,0	15,0
7	Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?	c. Deixo o equipamento bloqueado e utilizo o dispositivo com encriptação	7,5	92,5
8	Quando subscreve um serviço online (ex: cria uma caixa de *e-mail*, conta de Facebook), está a concordar com as regras e políticas desse fornecedor de serviços, em relação ao tratamento dos seus dados pessoais. Qual a sua opinião?	a. Apenas subscrevo serviços, após ler minuciosamente os termos da política de privacidade	11,3	88,8
9	Ao enviar um *e-mail* para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatários, qual a linha de preenchimento dos endereços que mais se adequa?	c. BCC	96,3	3,8

Nº	Pergunta	Resposta correta	% Resposta correta	% Resposta incorreta
10	Acede ao seu *e-mail* pessoal/profissional em computadores públicos?	a. Não acedo	76,3	23,8
11	Quando recebe *e-mails* de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?	d. Não abro a mensagem se o contato for suspeito	57,5	42,5
12	Quando tem necessidade de preencher formulários online, o que tem em atenção?	c. Só forneço dados pessoais se estiver clara a sua utilização, a cedência a terceiros, assim como a sua atualização e direito ao esquecimento	6,3	93,8
13	Quando navega na *Internet* sabe se existem dados que ficam guardados no computador localmente?	a. Sim, as cookies, os ficheiros transferidos e o histórico de navegação	68,8	31,3
14	Quando navega na *Internet* tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?	a. Sim	98,8	1,3
15	Acede às suas contas de redes sociais em computadores públicos?	b. Não acedo	82,5	17,5
16	Já foi alguma vez alvo de *Phishing*?	a. Sim, já fui	17,5	82,5
17	Já foi afetado por malware no seu dispositivo (ex: pc, smartphone)?	a. Sim.	43,8	56,3
18	Quando navega na *Internet* existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?	a. Tenho um bloqueador de pop ups para estes casos	42,5	57,5
19	Utiliza um antivírus no seu computador?	a. Sim	90,0	10,0
20	Encontra uma Pen Drive USB no chão, o que faz de seguida?	a. Entrego nos perdidos e achados	52,5	47,5
21	Habitualmente procura estar informado sobre a atualidade do mundo informático?	d. Sim, procuro informação quando necessito de fontes diversas (cursos, *Internet*, revistas)	52,5	47,5

Na Tabela 4.3 – Análise das respostas ao Questionário 2Tabela 4.3 – Análise das respostas ao Questionário 2, podemos observar as respostas que foram recolhidas através do questionário final. Neste questionário apenas se obteve um total de vinte e oito respostas.

Tabela 4.3 – Análise das respostas ao Questionário 2

Nº	Pergunta	Resposta correta	% Resposta correta	% Resposta incorreta
1	Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?	d. seja difícil de memorizar e tenha caracteres variados (com pelo menos 16 caracteres e sem nexo)	3,6	96,4
2	Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?	c. G0$t0DeGel@d0$29	85,7	15,3
3	Com que frequência altera as suas palavras passe?	a. Uma vez por mês	53,6	46,4
4	Qual o método que utiliza para guardar ou memorizar as suas palavras passe?	c. Utilizo um gestor de palavras passe com encriptação	42,9	57,1
5	Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de *e-mails* e de nos autenticar. Como procede em relação a este problema?	d. Utilizo um gestor de palavra passe que também tem a funcionalidade de gerador de palavras passe com um algoritmo aleatório	25,0	75,0
6	No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?	c. Fica bloqueado com palavra passe	82,1	17,9
7	Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?	c. Deixo o equipamento bloqueado e utilizo o dispositivo com encriptação	17,9	82,1
8	Quando subscreve um serviço online (ex: cria uma caixa de *e-mail*, conta de Facebook), está a concordar com as regras e políticas desse fornecedor de serviços, em relação ao tratamento dos seus dados pessoais. Qual a sua opinião?	a. Apenas subscrevo serviços, após ler minuciosamente os termos da política de privacidade	7,1	92,9
9	Ao enviar um *e-mail* para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatários, qual a linha de preenchimento dos endereços que mais se adequa?	c. BCC	100,0	0,0

Nº	Pergunta	Resposta correta	% Resposta correta	% Resposta incorreta
10	Acede ao seu *e-mail* pessoal/profissional em computadores públicos?	a. Não acedo	75,0	25,0
11	Quando recebe *e-mails* de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?	d. Não abro a mensagem se o contato for suspeito	46,4	53,6
12	Quando tem necessidade de preencher formulários online, o que tem em atenção?	c. Só forneço dados pessoais se estiver clara a sua utilização, a cedência a terceiros, assim como a sua atualização e direito ao esquecimento	67,9	32,1
13	Quando navega na *Internet* sabe se existem dados que ficam guardados no computador localmente?	a. Sim, as cookies, os ficheiros transferidos e o histórico de navegação	82,1	17,9
14	Quando navega na *Internet* tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?	a. Sim	100,0	0,0
15	Acede às suas contas de redes sociais em computadores públicos?	b. Não acedo	85,7	14,3
16	Já foi alguma vez alvo de *Phishing*?	a. Sim, já fui	28,6	71,4
17	Já foi afetado por malware no seu dispositivo (ex: pc, smartphone)?	a. Sim.	35,7	64,3
18	Quando navega na *Internet* existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?	a. Tenho um bloqueador de pop ups para estes casos	21,4	78,6
19	Utiliza um antivírus no seu computador?	a. Sim	92,9	7,1
20	Encontra uma Pen Drive USB no chão, o que faz de seguida?	a. Entrego nos perdidos e achados	78,6	21,4
21	Habitualmente procura estar informado sobre a atualidade do mundo informático?	d. Sim, procuro informação quando necessito de fontes diversas (cursos, *Internet*, revistas)	57,1	42,9

Na Tabela 4.4 – Tabela de Comparação dos Questionários, podemos observar as respostas que foram recolhidas em ambos os questionários e verificar a percentagem de respostas corretas no Q1 e no Q2.

Tabela 4.4 – Tabela de Comparação dos Questionários

Nº	Pergunta	Resposta correta	Q1 % Resposta correta	Q2 % Resposta correta	Média
1	Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?	d. seja difícil de memorizar e tenha caracteres variados (com pelo menos 16 caracteres e sem nexo)	8,8	3,6	6,2
2	Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?	c. G0$t0DeGel@d0$29	88,8	85,7	87,2
3	Com que frequência altera as suas palavras passe?	a. Uma vez por mês	8,8	53,6	31,2
4	Qual o método que utiliza para guardar ou memorizar as suas palavras passe?	c. Utilizo um gestor de palavras passe com encriptação	20,0	42,9	31,4
5	Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de *e-mail* e de nos autenticar. Como procede em relação a este problema?	d. Utilizo um gestor de palavra passe que também tem a funcionalidade de gerador de palavras passe com um algoritmo aleatório	3,8	25,0	14,4
6	No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?	c. Fica bloqueado com palavra passe	85,0	82,1	83,6
7	Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?	c. Deixo o equipamento bloqueado e utilizo o dispositivo com encriptação	7,5	17,9	12,7
8	Quando subscreve um serviço online (ex: cria uma caixa de *e-mail*, conta de Facebook), está a concordar com as regras e políticas desse fornecedor de serviços, em relação ao tratamento dos seus dados pessoais. Qual a sua opinião?	a. Apenas subscrevo serviços, após ler minuciosamente os termos da política de privacidade	11,3	7,1	9,2
9	Ao enviar um *e-mail* para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatários, qual a linha de preenchimento dos endereços que mais se adequa?	c. BCC	96,3	100,0	98,1

Nº	Pergunta	Resposta correta	Q1 % Resposta correta	Q2 % Resposta correta	Média
10	Acede ao seu *e-mail* pessoal/profissional em computadores públicos?	a. Não acedo	76,3	75,0	75,6
11	Quando recebe *e-mails* de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?	d. Não abro a mensagem se o contato for suspeito	57,5	46,4	52,0
12	Quando tem necessidade de preencher formulários online, o que tem em atenção?	c. Só forneço dados pessoais se estiver clara a sua utilização, a cedência a terceiros, assim como a sua atualização e direito ao esquecimento	6,3	67,9	37,1
13	Quando navega na *Internet* sabe se existem dados que ficam guardados no computador localmente?	a. Sim, as cookies, os ficheiros transferidos e o histórico de navegação	68,8	82,1	75,4
14	Quando navega na *Internet* tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?	a. Sim	98,8	100,0	99,4
15	Acede às suas contas de redes sociais em computadores públicos?	b. Não acedo	82,5	85,7	84,1
16	Já foi alguma vez alvo de *Phishing*?	a. Sim, já fui	17,5	28,6	23,0
17	Já foi afetado por malware no seu dispositivo (ex: pc, smartphone)?	a. Sim.	43,8	35,7	39,7
18	Quando navega na *Internet* existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?	a. Tenho um bloqueador de pop ups para estes casos	42,5	21,4	32,0
19	Utiliza um antivírus no seu computador?	a. Sim	90,0	92,9	91,4
20	Encontra uma Pen Drive USB no chão, o que faz de seguida?	a. Entrego nos perdidos e achados	52,5	78,6	65,5
21	Habitualmente procura estar informado sobre a atualidade do mundo informático?	d. Sim, procuro informação quando necessito de fontes diversas (cursos, *Internet*, revistas)	52,5	57,1	54,8

Através da análise do primeiro e do último questionário efetuado, podemos concluir o seguinte, referindo as percentagens dos dois questionários entre parêntesis (Q1 e Q2) ou mediante a média dos dois questionários:

- **Género** – A distribuição de respostas por ambos os sexos foi uniforme e manteve-se com o género feminino em minoria (47,5% e 46,4%) contra (52,5% e 53,6%) do género masculino;
- **Faixa etária** – O maior número de respostas centrou-se nas idades compreendidas entre os 36 a 45 anos com (31,3% e 42,5,3%) e entre os 46 a 55 anos com (39,3% e 50%) respetivamente;
- **Habilitações** – Mais de 50% dos inquiridos possui licenciatura;
- ***Passwords*** – Cerca de 45% e 32,1%, consideram importante a escolha de uma *password* que possam "memorizar"; 40% e 57,1% considera importante que "tenha caracteres variados"; 88,8% e 85,7% considera "G0$t0DeGel@d0$29" uma palavra passe segura; A maioria dos utilizadores considera alterar a *password* "quando entender" (38,7% e 17,9%) ou "quando for obrigado a tal" (43,8% e 25%), tendo no segundo questionário havido um acréscimo em relação à resposta "uma vez por mês" (de 8,8% para 53,6%), ainda existem utilizadores que "nunca alteram a *password*" (2,5% no Q1); Para guardar ou memorizar as *passwords* o método escolhido em maioria foi "memorizo" (43,8% no Q1), "utilizo um gestor de *passwords*" (20% e 42,9%), "guardo num papel num local seguro" (16,3% e 25%) e "guardo no telemóvel" (11,2% e 17,9%). Ainda existem utilizadores a guardar as *passwords* em "*post-it* em locais de fácil acesso" (1,3% e 7,1%); ao utilizar outros serviços *online* a maior parte dos utilizadores usa *passwords* diferentes (47,5% e 42,9%), sendo que (23,7% e 21,4%) utilizam a mesma *password*;
- **Bloqueio do PC e dispositivos (tablet ou smartphone)** – Mais de 80% bloqueia o seu PC quando se ausenta do mesmo, sendo que no questionário 1 ainda existia 5% que deixava desbloqueado; quanto a restantes dispositivos mais de 75% bloqueia os mesmos;
- **Políticas de privacidade (aplicações)** – Cerca de 60% lê as condições por alto, sendo que mais de 20% não lê e cerca de 10% lê na integra.
- **Envio de *e-mails* em massa** – 3,8% ainda colocava os endereços na linha "Para:", mas após o segundo questionário 100% já utilizava a linha "BCC";

- **Acesso ao *e-mail* em computadores públicos** – cerca de 75% não acede;
- **Receção de *e-mail*** – Mais de 55% não abre o *e-mail* se o contacto for suspeito e não constar na sua lista de endereços, 25% analisam o remetente da mensagem, ainda 3,8% abre o *e-mail* e clica nos *links* recebidos;
- **Privacidade no preenchimento de formulários online** – Mais de 70% dos indivíduos, já se certifica sobre qual o fim a que se destinam os seus dados pessoais, o seu tratamento e o direito ao esquecimento;
- **Privacidade dos dados e ao navegar na *Internet*** – (98,8% e 100%) dos indivíduos tem consciência que os seus dados podem ser alvo de recolha por terceiros, ao navegar na *Internet*, mais de (68% e 82,1%) tem consciência que os seus dados não são completamente privados, e cerca de 20% têm consciência que minimiza esse problema utilizando a navegação anónima;
- ***Phishing*** – Alguns indivíduos já foram alvo de *phishing* (17,5% e 28,6%), mais de 10% não sabe o que é o *phishing* e menos de 53,6% nunca foi alvo de *phishing*;
- ***Malware*** – Cerca de (7,5% e 14,3%) não sabe o que é *malware*, cerca de (45% e 46,4%) nunca foi afetado por *malware*, cerca de (43,8% e 35,7%) já foi afetado por *malware* sendo que (3,7% e 3,6%) foi afetado por *ransomware*;
- **Antivírus** – Mais de 90% já utiliza antivírus no seu dispositivo;
- ***Pen Drive USB* perdida** – (52,5% e 78,6%) entrega a *pen usb* nos perdidos e achados, no entanto ainda há uma pequena percentagem que liga a *pen usb* ao seu PC para ver o conteúdo (11,3% e 14,3%);
- **Atualização de conhecimentos** – (20% e 7,1%) não demonstram interesse pela atualidade do mundo informático, cerca de 15% procura ler revistas e ver programas de tv, cerca de 10% apenas se atualiza quando tem necessidade a nível profissional, sendo que a maioria se mantém atualizada com (52,5 e 57,1%);
- **Frequência do Curso sobre Segurança Informática** – 32,5% responderam não ter interesse e 67,5% responderam que tinham interesse.

Após a realização do segundo questionário verificou-se que:

- O número de indivíduos, que ponderam **alterar a *password*** uma vez por mês e que pretendem utilizar um gestor de *passwords* aumentou;
- Existe ainda uma grande percentagem de indivíduos, que utiliza a **mesma *password*** para vários serviços *online,* mais de 20%;

- Mais de 80% dos individuos, **bloqueia o seu PC**, *tablet* ou *smartphone*, quando se ausenta do mesmo;
- Todos os indivíduos têm cuidados com a privacidade no **envio de *e-mails*** em massa, sendo que apenas 25% abre os seus *e-mail*s em computadores públicos;
- Mais de 70% dos indivíduos, já se certifica sobre qual o fim a que se destinam os seus **dados pessoais**, o seu tratamento e o direito ao esquecimento, aquando do preenchimento de formulários ou consentimento de uso sobre os mesmos;
- Mais de 90% dos indivíduos, utiliza um **antivírus** no(s) seu(s) dispositivo(s);
- Mais de 70% dos indivíduos, se encontrar uma ***pen usb* perdida**, afirma entregar a mesma nos perdidos e achados, no entanto ainda existe uma pequena percentagem que coloca a a *pen usb* no seu PC para ver o seu conteúdo;
- Metade dos individuou afirma que se **mantém atualizado**, 10% apenas se necessário por questões profissionais e 7% não demonstra interesse.

Foi avaliada a taxa de frequência do curso sobre segurança da informação, assim como a alteração dos hábitos dos indivíduos.

- Frequência do **Curso sobre Segurança Informática** – dos 67,5% que responderam ter interesse em frequentar o curso, apenas 61,5% afirma ter concluído o curso, o que corresponde a cerca de 8 pessoas (menor número de respostas no segundo questionário, fazem com que este resultado seja inferior). 28,8% afirma que não se lembra do que respondeu no questionário anterior. Dos 38,5% que responderam que "não concluíram o curso", 83,3% afirmaram que não o fizeram por "falta de tempo", 8,3% por "desinteresse na matéria" e 8,3% por "ainda não tive tempo";
- Para os indivíduos que **não frequentaram o curso** sobre segurança da informação, apenas 25% afirmou ter "procurado informação sobre estas matérias através de outros meios".

4.2.7. Medidas alternativas

Como trabalho futuro de promoção do conhecimento não adquirido e de passagem a outra etapa com maior grau de complexidade, em relação aos conhecimentos dos indivíduos, sugere-se:

- A elaboração de *newsletters* quinzenais;

- A realização de *workshops* temáticos 1 vez por mês;
- A elaboração de jogos temáticos;
- A colocação de cartazes (ver o Anexo B – Cartazes) em zonas estratégicas;
- A elaboração de campanhas de *phishing* com obrigatoriedade de frequência de ações de *awareness* sobre essa temática.

4.2.8. Conclusão

Neste caso de estudo, pretendeu-se testar a viabilidade de implementação de um programa de *security awareness* em larga escala que abranja todo o universo da PJ.

Durante a sua implementação, verifico que é muito positiva a realização de qualquer projeto que se efetue nesta área, no entanto houve algumas limitações e deixo a sugestão de algum trabalho futuro a realizar.

Os indivíduos que habitualmente não têm possibilidade de frequentar ações de formação, ficam bastante agradados com os conhecimentos adquiridos nas ações de sensibilização. Infelizmente, nem todas as organizações incluem formação obrigatória nos seus objetivos anuais. Dado o carácter mais informal das ações de sensibilização é possível envolver todos os indivíduos sem efetuar grandes investimentos, vejamos como exemplo, a difusão de *newsletters* ou cartazes. Existe outro tipo de iniciativas de maior custo, como *workshops* ou ações de sensibilização em *e-learning*.

Apesar de alguns indivíduos afirmarem ter dificuldade em realizar o curso e responder ao segundo questionário, devido à falta de tempo, a iniciativa realizada foi muito bem recebida pelos participantes. As matérias abordadas no questionário, apesar de atuais e pertinentes, nem todos os indivíduos estavam familiarizados com as mesmas.

O Curso sobre Segurança Informática, abordou as matérias de *security awareness*, utilizando uma linguagem simples e de fácil leitura, levando o individuo a colocar-se em três espaços físicos de utilização das TIC bastante familiares, em casa, no trabalho e no exterior. Este Curso foi uma das medidas implementadas, além da campanha de *phishing* efetuada a todos os participantes. Através de alguns vídeos podia ter-se acesso a uma versão de sensibilização mais rápida.

Após a implementação destas medidas, realizou-se a avaliação, através da análise dos questionários, tendo sido utilizado o método de comparação entre as respostas dadas pelos

indivíduos em ambos os questionários. Este método permitiu verificar se existiu melhoria do nível de consciencialização dos indivíduos.

Limitações

Este projeto teve algumas limitações, nomeadamente, os questionários aplicados eram de caracter anónimo, daí resultou que não foi possível identificar quem foram os indivíduos que responderam aos dois questionários e que efetuaram o curso sobre segurança da informação. Se tal tivesse sido possível, apesar das poucas respostas obtidas no segundo questionário, a conclusão acerca da evolução do nível de conhecimento dos indivíduos seria avaliada de forma correta.

Estes questionários foram distribuídos aos indivíduos em altura de férias, mais concretamente durante o mês de julho e agosto, o que contribuiu para que as respostas ao segundo questionário fossem inferiores ao do primeiro.

Podemos verificar através da análise aos questionários na seção 4.2.6, as questões onde houve evolução do nível de conhecimento dos indivíduos inquiridos.

Tendo em conta estes pressupostos, há que garantir o mesmo número de respostas em ambos os questionários, pois só assim se consegue avaliar com exatidão o nível de conhecimentos dos indivíduos.

Trabalho Futuro

Deixo como desafio a implementação de um programa de *security awareness* a toda a organização. Basta que exista um individuo que não cumpra os requisitos de segurança, para que a empresa esteja sob risco.

A organização deverá incluir nos seus objetivos anuais, formação sobre estes temas. A atualização, nesta área é fundamental, devido à sua rápida evolução. Pode solicitar-se aos indivíduos sugestões, sobre quais as formas que gostariam de obter sessões de *awareness*, encorajar o seu *feedback*.

As campanhas de *phishing* poderão ser drasticamente reduzidas, caso as sessões de sensibilização sejam eficazes.

5. Conclusão

A elaboração de um programa de *security awareness*, é uma tarefa exigente, mas necessária às organizações. Para ter sucesso na sua implementação, é necessário envolver toda a hierarquia da organização.

Para a elaboração de um programa de *security awareness* numa organização, é necessário, avaliar o nível de conhecimento do grupo alvo, conhecer o grupo alvo, identificar comportamentos de risco do grupo alvo, elaborar medidas para prevenir os comportamentos de risco, difundir essas medidas, escolher os canais de divulgação, elaborar os materiais e por fim, aplicar a consciencialização ao grupo alvo.

Para avaliar o grau de eficácia deverá analisar-se os resultados obtidos e implementar as ações necessárias para melhorar o conhecimento do grupo alvo. A mudança na atitude dos colaboradores deve ser feita a longo prazo, ao mesmo tempo que se promove a mudança cultural e comportamental dentro da organização. As políticas de segurança devem ser encaradas como facilitadores essenciais para a organização.

Na elaboração deste projeto, realizo um caso de estudo que foi implementado na Polícia Judiciária. Este projeto piloto devido à sua pequena dimensão, pretendeu testar a viabilidade de implementação de um programa de *security awareness* em larga escala que abranja todo o universo da PJ.

O Caso de Estudo apresentado, foi um desafio cumprido com algumas limitações, mas com um balanço final positivo, dado que os objetivos foram alcançados, sendo possível a implementação de um projeto desta natureza, com algumas alterações no futuro.

Um dos componentes do caso de estudo foi o Curso sobre Segurança Informática, que abordou as matérias de *security awareness*, utilizando uma linguagem simples e de fácil leitura, levando o individuo a colocar-se em três espaços físicos de utilização das TIC bastante familiares, em casa, no trabalho e no exterior. Este Curso foi uma das medidas implementadas, além da campanha de *phishing* efetuada a todos os participantes. Através de alguns vídeos podia ter-se acesso a uma versão de sensibilização mais rápida.

Após a implementação destas medidas, realizou-se a avaliação, através da análise dos questionários, tendo sido utilizado o método de comparação entre as respostas dadas pelos

indivíduos em ambos os questionários. Este método permitiu verificar se existiu melhoria do nível de consciencialização dos indivíduos.

Este projeto teve algumas limitações, nomeadamente os questionários aplicados eram de caracter anónimo, daí resultou que no questionário final foram recebidas menos respostas não tendo sido possível identificar quais os indivíduos em falta na resposta ao questionário.

Além disso, os questionários foram distribuídos em época de férias, mais concretamente durante o mês de julho e agosto, o que contribuiu para que as respostas ao segundo questionário fossem inferiores ao do primeiro.

No computo geral houve uma pequena melhoria do nível de conhecimento nas respostas dadas, como se pode verificar através da análise dos quadros comparativos na secção 4.2.6.

Tendo em conta estes pressupostos, há que garantir o mesmo número de respostas em ambos os questionários, pois só assim se consegue avaliar com exatidão o nível de conhecimentos.

Conclui-se que no seu todo o objetivo de implementação do programa de *security awareness* foi cumprido, apesar de não ter sido possível alcançar uma melhoria de conhecimentos para todos os indivíduos em todos os itens.

5.1. Principais Contribuições

Este projeto contribuiu para que dentro do universo da PJ, se possa encarar a segurança da informação e a dos seus indivíduos no papel de cidadão, trabalhador e utilizador de recursos externos. O fator humano é o elemento chave da organização e apresenta um risco elevado pois é suscetível de contaminar ou ser contaminado pelas mais diversas formas a segurança informática da organização.

Não é necessário despender de muito investimento, para se poder implementar um programa de *security awareness*, haja disponibilidade de alguns elementos, autorização da chefia, tempo disponível para a elaboração dos materiais de divulgação, meios humanos e recursos técnicos para implementar as soluções através das ferramentas que se encontram disponíveis em regime de *open source*, nascendo assim um programa de *security awareness low cost,* que em nada fica atrás de uma solução paga a peso de ouro.

5.2. Trabalho Futuro

Como trabalho futuro, sugere-se que o projeto de *security awareness*, seja implementado a todo o universo da PJ, com as devidas adaptações, aos seus vários departamentos e realidades locais.

As sessões de *awareness* deverão passar a fazer parte dos objetivos da organização, enquadradas com outras sessões de formação dentro da temática da segurança da informação.

Deve ser elaborada uma grelha de conhecimentos mais exigente e complexa de acordo com os comportamentos de risco.

Tendo em conta a diferença de respostas obtidas nos dois questionários, sugere-se que é necessário garantir o mesmo número de respostas em ambos os questionários, só assim se consegue avaliar com exatidão o nível de conhecimentos de cada individuo, permitindo assim, elaborar medidas de correção à medida de cada um, refiro como exemplo, uma campanha de *phishing*, em que o individuo alvo de *phishing*, pode reportar o *e-mail* recebido como *phishing*, ou no caso de clicar em links e ser ludibriado, pode ser alvo imediato de uma ação de sensibilização sobre *phishing*.

Referências Bibliográficas

[1] A. L. B. Donald L. Evans, Phillip J. Bond, "NIST Special Publication 800-50," no. October, p. 40, 2003.

[2] ENISA, "About ENISA — ENISA." [Online]. Available: https://www.enisa.europa.eu/about-enisa. [Accessed: 11-Sep-2019].

[3] M. Antunes and B. Rodrigues, *Introdução à Cibersegurança - A Internet, os Aspetos Legais e a Análise Digital Forense*, 2018th ed. Leiria: FCA, 2018.

[4] CNCS, "Centro Nacional de Cibersegurança." [Online]. Available: www.cncs.pt. [Accessed: 11-Sep-2019].

[5] CNCS, "Cidadão Ciberseguro." [Online]. Available: https://lms.nau.edu.pt/courses/course-v1:CNCS+CC101+2018_T1/about. [Accessed: 11-Sep-2019].

[6] FCT, "FCCN | Computação Cientifica Nacional." [Online]. Available: https://www.fccn.pt/. [Accessed: 11-Sep-2019].

[7] NAU, "NAU." [Online]. Available: https://lms.nau.edu.pt/. [Accessed: 11-Sep-2019].

[8] Projeto NAU, "NAU." [Online]. Available: https://www.fccn.pt/projeto-nau/. [Accessed: 11-Sep-2019].

[9] Seguranet, "Início | SeguraNet." [Online]. Available: http://www.seguranet.pt/pt/. [Accessed: 11-Sep-2019].

[10] Seguranet, "Seguranet, Recursos." [Online]. Available: https://www.seguranet.pt/pt/recursos. [Accessed: 11-Sep-2019].

[11] esafety, "Como participar? | SeguraNet." [Online]. Available: http://www.seguranet.pt/como-participar. [Accessed: 11-Sep-2019].

[12] eSafety EU, "Home - eSafety label." [Online]. Available: http://www.esafetylabel.eu/web/guest. [Accessed: 11-Sep-2019].

[13] Internetsegura.pt, "InternetSegura." [Online]. Available: http://www.internetsegura.pt/. [Accessed: 11-Sep-2019].

[14] Tito de Morais, "Tito de Morais, fundador do site Miúdos Seguros Na .Net." [Online]. Available: http://www.miudossegurosna.net/sobre/titodemorais.html. [Accessed: 11-Sep-2019].

[15] E. Familiares, "Sumário - Inquérito Aberto à Segurança da Informação nas Instituições em Portugal."

[16] E. Familiares, "Análise - Inquérito Aberto à Segurança da Informação nas Instituições em Portugal," vol. 1ª edição, 2016.

[17] Eurpopol-EC3, "European Cybercrime Centre - EC3 | About Europol | Europol." [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. [Accessed: 11-Sep-2019].

[18] ENISA, "Material — ENISA." [Online]. Available: https://www.enisa.europa.eu/media/multimedia/material. [Accessed: 11-Sep-2019].

[19] ENISA, "ENISA Quiz," 2019. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education. [Accessed: 11-Sep-2019].

[20] P. S. S. Council, "PCI Security Standard Council," 2019. [Online]. Available: https://www.pcisecuritystandards.org/. [Accessed: 11-Sep-2019].

[21] PCI Security Standards Council, "Best Practices for Implementing a Security Awareness Program," *PCI Data Security Standard (PCI DSS)*, no. October, p. 12, 2014.

[22] SANS, "SANS." [Online]. Available: https://www.sans.org/. [Accessed: 11-Sep-2019].

[23] "NIST Cybersecurity Framework." [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: 11-Sep-2019].

[24] J. (2003) Wilson, M., & Hash, "Building an Information Architecture Checklist," *Organization*, vol. 2, no. 2, pp. 1–70, 2003.

[25] "Email Phishing Attack Simulation for Employees | Sophos Phish Threat." [Online]. Available: https://www.sophos.com/pt-br/products/phish-threat.aspx. [Accessed: 11-Sep-2019].

[26] "Security Awareness Training & Phishing Simulator – Infosec IQ." [Online]. Available: https://securityiq.infosecinstitute.com/. [Accessed: 11-Sep-2019].

[27] "Gophish - Open Source Phishing Framework." [Online]. Available: https://getgophish.com/. [Accessed: 11-Sep-2019].

[28] "Homepage | Lucy Security | Awareness Training." [Online]. Available: https://lucysecurity.com/. [Accessed: 11-Sep-2019].

[29] "Home - Phishing Frenzy - Manage Email Phishing Campaigns - Penetration Testing." [Online]. Available: https://www.phishingfrenzy.com/. [Accessed: 11-Sep-2019].

[30] "GitHub - securestate/king-phisher: Phishing Campaign Toolkit." [Online]. Available: https://github.com/securestate/king-phisher. [Accessed: 11-Sep-2019].

[31] "GitHub - tatanus/SPF: SpeedPhishing Framework." [Online]. Available: https://github.com/tatanus/SPF. [Accessed: 11-Sep-2019].

[32] T. Sec, "TrustedSec." [Online]. Available: https://www.trustedsec.com/social-engineer-toolkit-set/. [Accessed: 11-Sep-2019].

[33] "SpearPhisher - A simple phishing email generation tool." [Online]. Available: https://www.trustedsec.com/2013/09/introducing-spearphisher-simple-phishing-email-generation-tool/. [Accessed: 11-Sep-2019].

[34] M. Wilson, D. E. De Zafra, S. I. Pitcher, D. Tiressler, and J. B. Ippolito, *Training Requirements : Role- and Performance-Based Model*. 1998.

[35] P. Honeynet, "Lance Spitzner," pp. 22–23.

[36] D. Lohrmann, "Ten Recommendations for Security Awareness Programs." [Online]. Available: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/Ten-Recommendations-for-Security-Awareness-Programs.html. [Accessed: 11-Sep-2019].

[37] I. Santa, "The new users' guide: How to raise information security awareness.," *Information Security*, pp. 1–140, 2010.

[38] J. Abawajy, "User preference of cyber security awareness delivery methods.: SearchPoint for Cranfield University," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 236–247, 2014.

[39] T. R. Peltier, "Implementing an information security awareness program," *Information Systems Security*, vol. 14, no. 2, pp. 37–49, 2005.

[40] Europass, "Competencias Digitais." [Online]. Available: https://europass.cedefop.europa.eu/pt/resources/digital-competences. [Accessed: 11-Sep-2019].

[41] E. Reis, *Estatística Descritiva*. 2008.

[42] P. Joaquim, "Curso Segurança da Informação," 2019. [Online]. Available: https://drive.google.com/file/d/1US2eVv_31DwC0voPrWCKYDQ47ELfrW-4/view?usp=sharing. [Accessed: 11-Sep-2019].

Anexo A – Competências Digitais

Competências digitais - Grelha de auto-avaliação

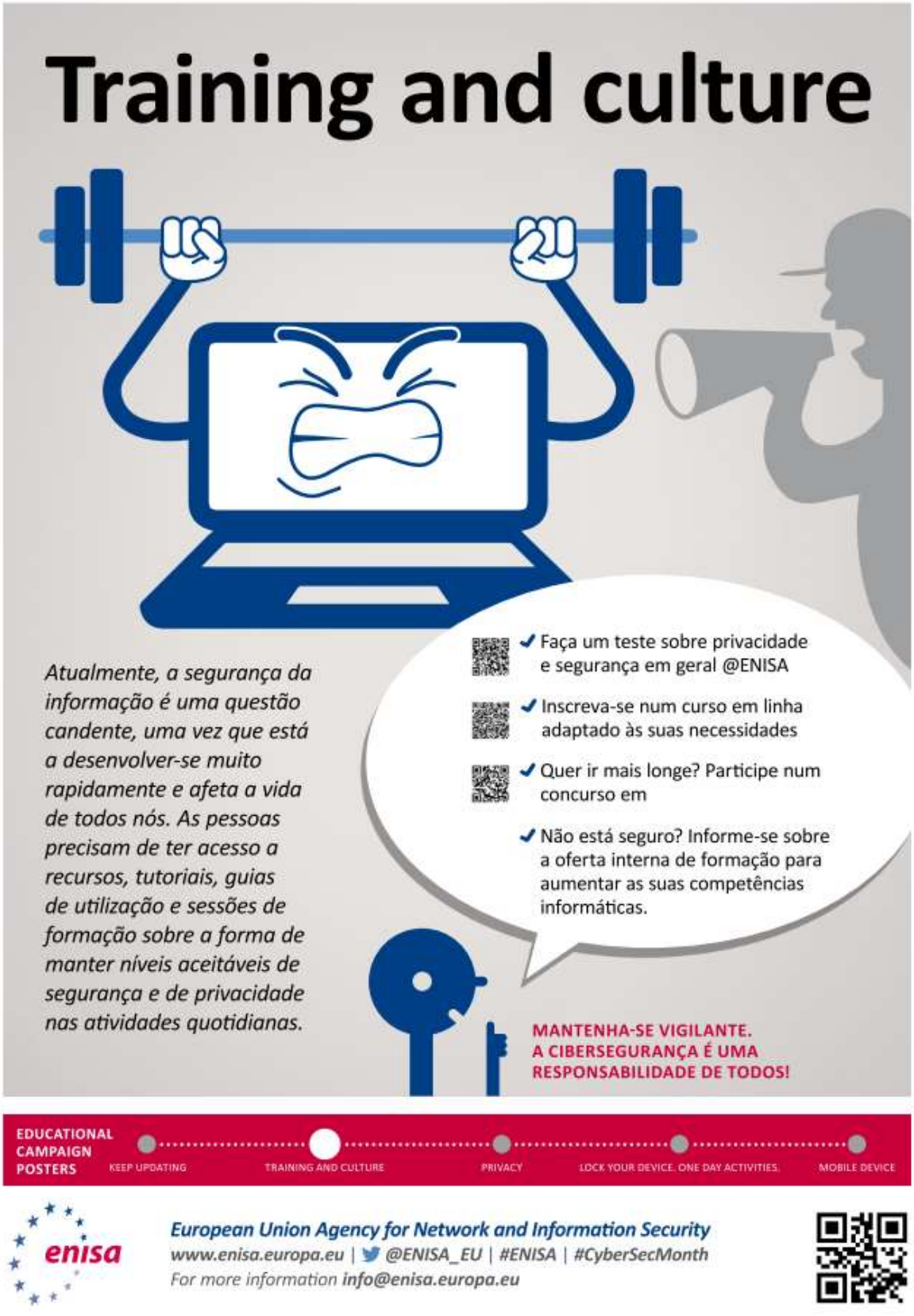
	Utilizador básico	Utilizador independente	Utilizador avançado
Processamento de informação	Sei pesquisar informação online utilizando um motor de busca. Sei que nem toda a informação online é fiável. Sei guardar e arquivar ficheiros ou conteúdos (ex. texto, imagens, músicas, vídeos, páginas web) e recuperá-los uma vez guardados e arquivados.	Sei utilizar diferentes motores de busca para pesquisar informação. Quando pesquiso sei utilizar alguns filtros (ex. pesquisar apenas imagens, vídeos, mapas). Comparo diferentes fontes para avaliar a fiabilidade da informação que encontro. Organizo a informação metodicamente através de ficheiros e pastas de forma a encontrá-los mais facilmente. Faço cópias de segurança da informação ou dos ficheiros que guardei.	Sei utilizar estratégias de pesquisa avançadas (ex. utilizando operadores de pesquisa) para encontrar informação fiável na internet. Sei utilizar feeds da web (ex.RSS) para poder ser atualizado sobre conteúdos em que estou interessado. Sei avaliar a legitimidade e fiabilidade da informação pela aplicação de uma série de critérios. Tenho conhecimento sobre os novos progressos nas áreas da pesquisa, armazenamento e acesso de informação. Sei guardar a informação encontrada na internet em diferentes formatos. Sei utilizar os serviços de armazenamento de informação em núvem.
Comunicação	Sei comunicar com os outros por telemóvel, Voz sobre IP (ex. Skype), correio eletrónico ou chat – utilizando funções básicas (ex. mensagem de voz, SMS, enviar e receber correio eletrónico, texto). Sei partilhar ficheiros e conteúdos utilizando ferramentas básicas. Sei que posso utilizar tecnologias digitais para interagir com serviços (serviços públicos, bancos, hospitais). Tenho conhecimento de sites de redes sociais e de ferramentas de colaboração online. Sei que deverão ser respeitadas determinadas regras de comunicação, quando utilizo ferramentas digitais (ex. em comentários, ao partilhar informação pessoal).	Sei utilizar as funções avançadas de várias ferramentas de comunicação (ex. utilizar Voz sobre IP e partilha ficheiros). Sei utilizar ferramentas de colaboração e intervir em, por ex., documentos/ficheiros partilhados criados por outrém. Sei utilizar algumas funções de serviços online(ex. serviços públicos, bancários, comerciais). Transmito ou partilho conhecimento online com outras pessoas (ex. através de ferramentas de redes sociais ou em comunidades online). Tenho conhecimento e sei aplicar as regras de comunicação online ("Netiqueta").	Utilizo ativamente uma grande variedade de ferramentas de comunicação (correio eletrónico, chat, SMS, mensagem instantânea, blogues, microblogues, redes sociais) para comunicar online. Sei criar e gerir conteúdos com ferramentas de colaboração (ex. calendários eletrónicos, sistemas de gestão de projetos, revisão online, folhas de cálculo online). Participo ativamente em espaços virtuais e utilizo vários serviços online(ex. serviços públicos, bancários, comerciais). Sei utilizar funções avançadas de ferramentas de comunicação (ex. vídeo conferência, partilha de dados, partilha de aplicações).
Criação de conteúdos	Sei produzir conteúdo digital simples (ex. texto, tabelas, imagens, ficheiros de som) com ferramentas digitais em, pelo menos, um tipo de formato. Sei fazer modificações de base em conteúdos produzidos por outros. Sei que o conteúdo pode ser protegido por direitos de autor. Sei aplicar e modificar funções e configurações de base de software e aplicações que utilizo (ex. alteração de configurações padrão).	Sei produzir conteúdo digital sofisticado em diferentes formatos (ex. texto, tabelas, imagens, ficheiros de som). Sei utilizar ferramentas ou editores para criar uma página web ou um blogue usando modelos (p.ex. WordPress). Sei aplicar formatação de base (ex. inserir notas de rodapé, gráficos, tabelas) em conteúdos que criei ou criados por outrém. Sei como fazer referência e reutilizar conteúdos protegidos por direitos de autor. Tenho conhecimentos básicos de uma linguagem de programação.	Sei criar ou modificar conteúdo multimédia sofisticado em diferentes formatos, utilizando várias plataformas, ferramentas e ambientes digitais. Sei criar um website utilizando uma linguagem de programação. Sei utilizar funções de formação avançadas de diferentes ferramentas (ex. impressão em série, fusão de documentos de diferentes formatos, utilização de fórmulas e macros avançadas). Sei como aplicar licenças e direitos de reprodução. Sei utilizar várias linguagens de programação. Sei como projetar, criar e modificar bases de dados com uma ferramenta informática.
Segurança	Sei como aplicar medidas de base para proteger o meu equipamento (ex. utilizar antivírus e palavras-passe). Sei que nem toda a informação online é fiável. Estou ciente de que as minhas credenciais (nome de utilizador e palavra-passe) credenciais (username and password) podem ser roubadas. Sei que não devo divulgar informação pessoal online. Estou ciente que a utilização excessiva de tecnologia informática pode afetar a minha saúde. Eu tomo medidas simples para economizar energia.	Instalei programas para proteger o(s) equipamento(s) que utilizo para aceder à internet (ex. antivírus, firewall). Executo e atualizo estes programas regularmente. Tenho diferentes palavras-passe para aceder a equipamentos, dispositivos e serviços digitais e altero-as regularmente. Sei identificar websites e mensagens de correio eletrónico que podem ser usados para defraudar. Sei identificar mensagens phishing. Sei configurar a minha identidade digital online e acompanhar o meu rasto digital. Estou ciente dos riscos para a saúde que a utilização de tecnologia informática pode acarretar. (ex. ergonomia, risco de dependência). Compreendo o impacto, positivo e negativo, da tecnologia sobre o meio ambiente.	Verifico, regularmente, as configurações de segurança e dos sistemas dos meus equipamentos e/ou das aplicações que utilizo. Sei como proceder se o meu computador for infetado por um vírus. Sei como configurar ou modificar as definições dos sistemas de firewall e de segurança dos meus equipamentos informáticos. Sei como cifrar correios eletrónicos e ficheiros. Sei filtrar mensagens de spam. Sei como utilizar moderadamente a tecnologia de informação e comunicação, de modo a evitar problemas de saúde (físicos e psicológicos). Estou claramente informado sobre o impacto das tecnologias informáticas na vida quotidiana, no consumo online e no meio ambiente.
Resolução de problemas	Sei como encontrar ajuda e assistência quando surgem problemas técnicos ou ao utilizar um novo equipamento, programa ou aplicação. Sei como resolver problemas habituais (ex. encerrar um programa, reiniciar o computador, reinstalar/atualizar um programa, verificar a ligação à internet). Sei que as ferramentas informáticas podem ajudar-me a resolver problemas, mas estou ciente, igualmente, que têm os seus limites. Sempre que me deparo com um problema tecnológico ou não tecnológico, utilizo as ferramentas informáticas para resolvê-lo. Estou ciente que tenho de atualizar as minhas competências informáticas regularmente.	Sei como resolver a maioria dos problemas mais frequentes relacionados com a utilização de tecnologias informáticas. Sei utilizar tecnologias informáticas para resolver problemas não técnicos. Sei selecionar uma ferramenta informática que se adeque às minhas necessidades e avaliar a sua eficácia. Sei resolver problemas tecnológicos pesquisando as definições e opções de programas ou ferramentas. Atualizo regularmente as minhas competências informáticas. Sei quais são os meus limites e tento corrigi-los.	Sei resolver quase todos os problemas que surgem quando utilizo tecnologias informáticas. Sei escolher a ferramenta, equipamento, aplicação, software ou serviço adequados para resolver problemas não técnicos. Estou informado sobre os progressos tecnológicos. Compreendo como é que as novas ferramentas funcionam. Atualizo frequentemente as minhas competências informáticas.

Anexo B – Cartazes

Para o desenvolvimento de uma campanha mais próxima do utilizador, deixa-se como exemplo os cartazes seguintes, retirados da ENISA, sobre:

- Mantenha-se atualizado;
- Treino e cultura;
- Privacidade;
- Bloqueie o seu dispositivo no seu dia de trabalho;
- Dispositivos móveis.


Keep updating
Quantas vezes por semana utiliza a Internet? É extremamente importante proteger os seus dados pessoais na vida quotidiana, no trabalho ou nos tempos livres.
1+1=
?
✓ Utilize um gestor de palavras-passe
✓ Utilize a autenticação bi-fatorial para as contas em linha
✓ Utilize um antivírus
✓ Instale as atualizações de software
✓ Ligue-se a sítios com URL https://
MANTENHA-SE VIGILANTE. A CIBERSEGURANÇA É UMA RESPONSABILIDADE DE TODOS!
EDUCATIONAL CAMPAIGN POSTERS
KEEP UPDATING
TRAINING AND CULTURE
PRIVACY
LOCK YOUR DEVICE. ONE DAY ACTIVITIES.
MOBILE DEVICE
enisa
European Union Agency for Network and Information Security
www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth
For more information info@enisa.europa.eu


Training and culture
Atualmente, a segurança da informação é uma questão candente, uma vez que está a desenvolver-se muito rapidamente e afeta a vida de todos nós. As pessoas precisam de ter acesso a recursos, tutoriais, guias de utilização e sessões de formação sobre a forma de manter níveis aceitáveis de segurança e de privacidade nas atividades quotidianas.
✓ Faça um teste sobre privacidade e segurança em geral @ENISA
✓ Inscreva-se num curso em linha adaptado às suas necessidades
✓ Quer ir mais longe? Participe num concurso em
✓ Não está seguro? Informe-se sobre a oferta interna de formação para aumentar as suas competências informáticas.
MANTENHA-SE VIGILANTE.
A CIBERSEGURANÇA É UMA RESPONSABILIDADE DE TODOS!
EDUCATIONAL CAMPAIGN POSTERS
KEEP UPDATING
TRAINING AND CULTURE
PRIVACY
LOCK YOUR DEVICE, ONE DAY ACTIVITIES.
MOBILE DEVICE
enisa
European Union Agency for Network and Information Security
www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth
For more information info@enisa.europa.eu


Privacy
Sempre que utilizar um dispositivo digital e, por exemplo, navegar na Internet e visitar sítios Web, vai deixando um pequeno rasto das suas atividades. Estas atividades podem ser armazenadas tanto no seu dispositivo como nos sítios Web visitados. Este rasto constitui a sua pegada digital.
Direito ao apagamento de dados? Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito - direito da UE *
YAWNN
✓ Dedique algum tempo a verificar os parâmetros de privacidade dos serviços
✓ Utilize a cifragem e encripte os ficheiros que partilha
✓ Se receber uma mensagem eletrónica «surpresa» de uma fonte desconhecida, não a abra e informe o seu serviço informático
* A UE estabeleceu normas comuns para garantir um nível elevado de proteção dos dados pessoais de cada cidadão em todo o seu território. Tem o direito de apresentar queixa e de obter reparação, caso os seus dados sejam utilizados de forma abusiva em qualquer lugar na UE.
MANTENHA-SE VIGILANTE.
A CIBERSEGURANÇA É UMA RESPONSABILIDADE DE TODOS!
EDUCATIONAL CAMPAIGN POSTERS
KEEP UPDATING
TRAINING AND CULTURE
PRIVACY
LOCK YOUR DEVICE. ONE DAY ACTIVITIES.
MOBILE DEVICE
enisa
European Union Agency for Network and Information Security
www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth
For more information info@enisa.europa.eu


Lock your device
One day activities
✓ A caminho do trabalho nos transportes públicos? Tenha cuidado com os olhares indiscretos.
✓ Uma pausa para tomar café? Bloqueie o seu computador. Prima Control ALT DELETE
✓ Vai voltar para casa após um dia de trabalho? Encerre a sua sessão.
MANTENHA-SE VIGILANTE.
A CIBERSEGURANÇA É UMA
RESPONSABILIDADE DE TODOS!
EDUCATIONAL CAMPAIGN POSTERS
KEEP UPDATING
TRAINING AND CULTURE
PRIVACY
LOCK YOUR DEVICE. ONE DAY ACTIVITIES.
MOBILE DEVICE
enisa
European Union Agency for Network and Information Security
www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth
For more information info@enisa.europa.eu


Mobile device
Considera-se um utilizador experiente das tecnologias móveis. Tem um dispositivo pessoal com o qual navega na Internet e utiliza várias aplicações para obter atualizações dos serviços locais, a meteorologia, etc., e encontrar serviços adicionais, por exemplo localizar os melhores restaurantes da zona.
✓ Ligue-se apenas a redes Wi-Fi seguras
✓ Examine os pedidos de autorização ao utilizar ou instalar aplicações
✓ Bloqueie o seu dispositivo quando não está a utilizá-lo
MANTENHA-SE VIGILANTE. A CIBERSEGURANÇA É UMA RESPONSABILIDADE DE TODOS!
EDUCATIONAL CAMPAIGN POSTERS
KEEP UPDATING
TRAINING AND CULTURE
PRIVACY
LOCK YOUR DEVICE. ONE DAY ACTIVITIES.
MOBILE DEVICE
enisa
European Union Agency for Network and Information Security
www.enisa.europa.eu | @ENISA_EU | #ENISA | #CyberSecMonth
For more information info@enisa.europa.eu

Anexo C – Questionário aos Hábitos e Conhecimentos sobre Segurança da Informação

Este questionário é constituído por 24 perguntas, das quais, 3 são sobre a caracterização do individuou, 21 são acerca dos seus hábitos e conhecimentos sobre a segurança da informação, finalizando com 1 pergunta sobre a sugestão da frequência de um curso sobre segurança da informação. Todas as questões são de resposta obrigatória. Todo o questionário é anónimo, salvaguardado qualquer questão mais sensível.

O questionário foi enviado aos indivíduos por *e-mail*, no qual se explicava o teor do Projeto *Security Awareness*. O texto que acompanhava o questionário era o seguinte:

> "Projeto *Security Awareness*
> Questionário aos hábitos e conhecimentos sobre segurança da informação - *Link* Questionário (disponível durante os próximos 5 dias)
> No âmbito da dissertação do Mestrado em Cibersegurança e Informática Forense, estou a desenvolver o Projeto de *Security Awareness*, que pretende consciencializar o cidadão para os perigos das Tecnologias de Informação e Comunicação (TIC).
> Este projeto é composto por um questionário aos hábitos e conhecimentos sobre a segurança da informação.
> Após o preenchimento do questionário, o cidadão pode frequentar o Curso Segurança da Informação, para complementar os seus conhecimentos na área da segurança da informação.
> O Curso Segurança da Informação, é disponibilizado em formato PDF, através de um *link*, no final do preenchimento do Questionário aos hábitos e conhecimentos sobre segurança da informação, tem a duração média de 12 horas e tem uma versão rápida de 3 horas de duração.
> Após o término do curso, ou passados 7 dias desde o seu início, será solicitado ao cidadão que volte a preencher o questionário de segurança da informação.
> Pretende-se assim aferir, se de alguma forma os seus conhecimentos foram solidificados nesta área.
> Todo este processo decorre de forma anónima, os dados que são solicitados ao cidadão, são apenas para tratamento estatístico, não permitindo a sua caracterização como indivíduo isolado.
> Face ao exposto, solicito uns breves minutos da sua atenção para o preenchimento do questionário.
> Para que este projeto tenha alguma pertinência a nível de resultados, necessito de obter pelo menos 50 respostas ao questionário para obter dados conclusivos para o estudo em causa.
> Desde já o meu obrigado pela atenção.
> Paula Joaquim"

Projeto Security Awareness (MCIF)

*Obrigatório

Projeto Security Awareness

A sua colaboração é muito importante na resposta a este questionário.
Após o seu preenchimento é convidado a obter mais informações sobre a segurança da informação, se assim pretender.

Este questionário é anónimo.
Pretende aferir os hábitos e conhecimentos sobre a segurança da informação do cidadão.

Responda às questões, com a máxima sinceridade refletindo as ações praticadas por si no dia a dia.

Desde já agradeço os 5 minutos da sua atenção para o preencher.

Dados estatisticos

1. **Qual o seu género?** * *Marcar apenas uma oval.*
   - ◯ Feminino
   - ◯ Masculino

2. **Qual a sua faixa etária?** *
   Marcar apenas uma oval.
   - ◯ Menos de 25
   - ◯ 26 a 35 anos
   - ◯ 36 a 45 anos
   - ◯ 46 a 55 anos
   - ◯ Mais de 56

3. **Quais as suas habilitações?** *
   Marcar apenas uma oval.
   - ◯ 1º ciclo , 4ª classe
   - ◯ 2º ciclo, 6º ano
   - ◯ 3º ciclo, 9º ano
   - ◯ Ensino Secundário, 12º ano
   - ◯ Licenciatura
   - ◯ Mestrado
   - ◯ Doutoramento

Questionário

Responda de acordo com os seus comportamentos habituais.

4. **Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?** * *Marcar apenas uma oval.*

   - a. seja fácil de memorizar
   - b. seja suficientemente grande
   - c. tenha caracteres variados
   - d. seja difícil de memorizar e tenha caracteres variados (com pelo menos 16 caracteres e sem nexo)

5. **Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?** * *Marcar apenas uma oval.*

   - a. Borboleta65
   - b. 210967000
   - c. G0$t0DeGel@d0$29
   - d. zxcvbn

6. **Com que frequência altera as suas palavras passe?** * *Marcar apenas uma oval.*

   - a. Uma vez por mês
   - b. Nunca
   - c. Quando a palavra passe é descoberta por alguém
   - d. Quando sou obrigado pelo fornecedor do serviço associado
   - e. Sem prazo definido, quando entender que devo trocar

7 **Qual o método que utiliza para guardar ou memorizar as suas palavras passe?** * *Marcar apenas uma oval.*

   - a. Guardo num papel num local seguro
   - b. Guardo num ficheiro no disco do computador
   - c. Utilizo um gestor de palavras passe com encriptação
   - d. Guardo num post-it de fácil acesso
   - e. Guardo no telemóvel
   - f. Memorizo
   - Outra: _____

8. **Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de email e de nos autenticar. Como procede em relação a este problema?** *
Marcar apenas uma oval.

- a. Utilizo uma palavra passe diferente para cada serviço
- b. Utilizo sempre a mesma palavra passe
- c. Utilizo a autenticação de outros serviços (Facebook, Google, etc)
- d. Utilizo um gestor de palavra passe que também tem a funcionalidade de gerador de palavras passe com um algoritmo aleatório.
- Outra: _____

9. **No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?** *
Marcar apenas uma oval.

- a. Fica desbloqueado
- b. Fica bloqueado com palavra passe, mas a minha colega tem conhecimento da palavra palavra passe
- c. Fica bloqueado com palavra passe
- d. Dependendo do tempo que me ausento, fica desbloqueado

10. **Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?** * *Marcar apenas uma oval.*

- a. Deixo o equipamento desbloqueado
- b. Deixo o equipamento bloqueado
- c. Deixo o equipamento bloqueado e utilizo o dispositivo com encriptação
- d. Não tenho smartphone ou tablet
- Outra: _____

11. **Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com as regras e políticas desse fornecedor de serviços, em relação ao tratamento dos seus dados pessoais. Qual a sua opinião?** *
Marcar apenas uma oval.

- a. Apenas subscrevo serviços, após ler minuciosamente os termos da política de privacidade
- b. Não costumo ler os termos e políticas de privacidade, mas subscrevo o serviço
- c. Leio na diagonal e subscrevo os serviços
- d. Não leio e não subscrevo o serviço

12. **Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatários, qual a linha de preenchimento dos endereços que mais se adequa?** *
Marcar apenas uma oval.

- a. Para
- b. CC
- c. BCC
- d. Qualquer uma das anteriores

13. **Acede ao seu email pessoal/profissional em computadores públicos?** * *Marcar apenas uma oval.*

- a. Não acedo
- b. Acedo ao email pessoal
- c. Acedo ao email profissional
- d. Acedo ao email pessoal e profissional

14. **Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?** * *Marcar apenas uma oval.*

- a. Leio a mensagem, clico nos links e abro os anexos
- b. Leio a mensagem, mas não clico nos links e não abro os anexos
- c. Leio o assunto e verifico o endereço do remetente da mensagem e só depois abro a mensagem para ler o seu conteúdo, verifico os links antes de clicar e verifico se os anexos têm vírus antes de os abrir.
- d. Não abro a mensagem se o contato for suspeito

15 **Quando tem necessidade de preencher formulários online, o que tem em atenção?** *
Marcar apenas uma oval.

- a. Forneço os dados que me são pedidos mediante o fim a que se destinam
- b. Forneço os dados que me são pedidos mediante a garantia do tratamento dos dados posteriormente e o fim a que se destinam
- c. Só forneço dados pessoais se estiver clara a sua utilização, a cedência a terceiros, assim como a sua atualização e direito ao esquecimento
- d. Forneço os dados que me são pedidos

16. **Quando navega na internet sabe se existem dados que ficam guardados no computador localmente?** * *Marcar apenas uma oval.*

- a. Sim, as cookies, os ficheiros transferidos e o histórico de navegação
- b. Sim, mas se usar a navegação privada minimizo os dados que ficam guardados
- c. Não fica nada guardado no computador
- d. Sim, apenas as cookies
- e. Não sei responder

17. **Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?** * *Marcar apenas uma oval.*

- a. Sim
- b. Não

18. **Acede às suas contas de redes sociais em computadores públicos?** * *Marcar apenas uma oval.*

- a. Acedo
- b. Não acedo
- c. Não tenho contas de redes sociais

19. **Já foi alguma vez alvo de Phishing?** * *Marcar apenas uma oval.*

- a. Sim, já fui
- b. Não, nunca fui
- c. Não sei o que é phishing

20. **Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):** * *Marcar apenas uma oval.*

- a. Sim.
- b. Sim, por Ransomware
- c. Não
- d. Não sei o que é malware

21. **Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?** * *Marcar apenas uma oval.*

- a. Tenho um bloqueador de pop ups para estes casos
- b. Fecho de imediato as janelas que foram abertas
- c. Vejo o conteúdo das janelas e clico nos links se o conteúdo for fidedigno
- d. O meu navegador de internet pergunta se quero abrir a janela (pop-up)

22. **Utiliza um antivírus no seu computador?** * *Marcar apenas uma oval.*

- a. Sim
- b. Não
- c. Não sei o que é antivírus.

23. **Encontra uma Pen Drive USB no chão, o que faz de seguida?** * *Marcar apenas uma oval.*

- a. Entrego nos perdidos e achados
- b. Ligo ao meu computador para ver o que tem
- c. Procuro a ajuda de um colega mais experiente em informática
- d. Fico com a Pen Drive para mim
- Outra: _____

24 **Habitualmente procura estar informado sobre a atualidade do mundo informático?** * *Marcar apenas uma oval.*

- a. Sim, leio revistas e vejo programas de tv sobre a temática
- b. Sim, recebo emails temáticos
- c. Sim, mas apenas quando sou obrigado profissionalmente a frequentar cursos
- d. Sim, procuro informação quando necessito de fontes diversas (cursos, internet, revistas)
- e. Não, pois não tenho interesse pela área.

Chegou ao fim do questionário.

25. **Aceita o desafio de frequentar um pequeno curso sobre segurança da informação, com a duração de apenas 12 horas? Este curso é constituído por 3 pequenos módulos e 3 mini questionários no final de cada módulo.** * *Marcar apenas uma oval.*

- Sim *Passe para "Guarde o atalho para acesso ao curso segurança da informação. Caso perca este link solicite-o por email.."*
- Não *Pare de preencher este formulário.*

Pare de preencher este formulário.

Guarde o atalho para acesso ao curso segurança da informação. Caso perca este link solicite-o por email.

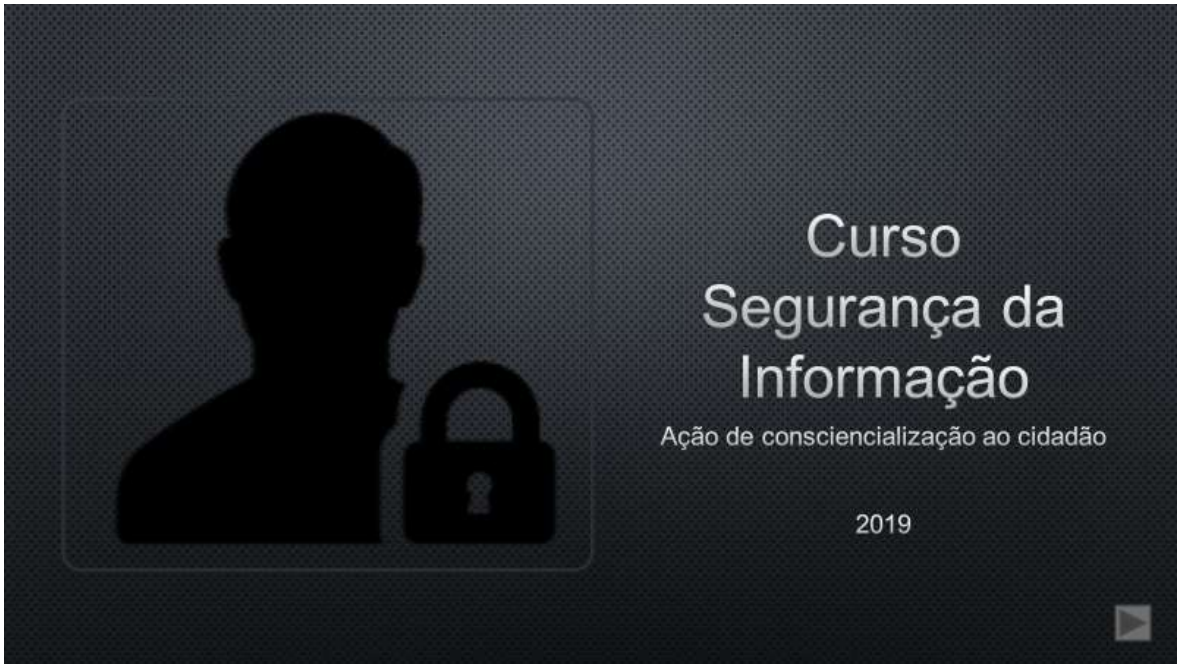
https://drive.google.com/open?id=1US2eVv_31DwC0voPrWCKYDQ47ELfrW-4

Passe para "Obrigado pela sua participação.."

Obrigado pela sua participação.

https://drive.google.com/open?id=1US2eVv_31DwC0voPrWCKYDQ47ELfrW-4

Anexo D – Curso Segurança da Informação



O Curso Segurança da Informação[42], pretende consciencializar o cidadão para os perigos das novas tecnologias, promovendo a utilização das TIC de uma forma mais segura e consciente, mostrando, as boas práticas sugeridas por algumas instituições e organizações nacionais e internacionais que produzem materiais educativos e de sensibilização na área da cibersegurança.

Através das próximas páginas, vão ser abordados vários assuntos relacionados com as novas tecnologias, nomeadamente a ciberhigiene que o indivíduo deverá ter, que lhe permitam fazer uso das TIC de uma forma segura, enquanto seu utilizador nos meios envolventes, em casa, no trabalho e no exterior.

Pretende-se, com esta ação, sensibilizar os participantes para a utilização segura e consciente das TIC, utilizando as boas práticas sugeridas ao longo do Curso, reduzindo a sua exposição aos riscos do ciberespaço.

A carga horária, é de 12 horas divididas em 3 módulos, 4 horas cada módulo, ou, Versão rápida, 3 horas para ver os vídeos, recursos e questionários.

O Curso está organizado em 3 módulos, cujos temas principais são: Casa, Trabalho e Exterior, que por sua vez estão divididos em 4 módulos: Identidade, Redes e Navegação,

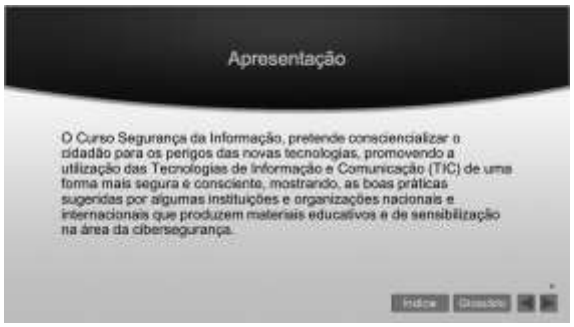
Comportamento Social e Posto de Trabalho/Posto Doméstico/Passaporte. Cada tópico contém textos e vídeos com conteúdos específicos sobre esse tópico.

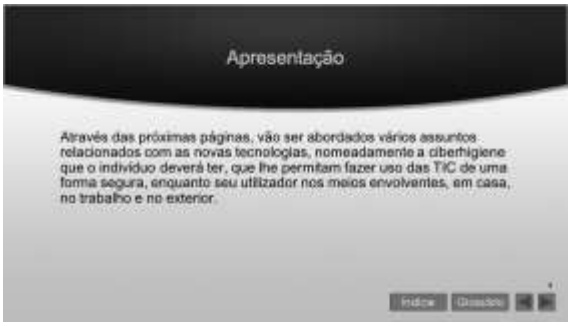
O Curso está no formato PDF. Existem *links* (atalhos assinalados a laranja) para recursos externos na *Internet*, sob a forma de PDF ou vídeos.

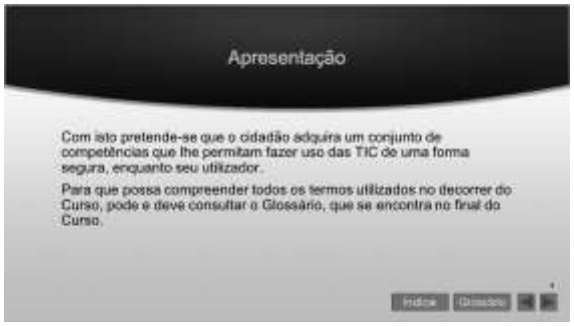
Este Curso é de frequência livre e anónimo, mas permite que faça a sua autoavaliação através do preenchimento dos questionários no final de cada módulo. Só deverá passar ao módulo seguinte após responder ao questionário final de cada módulo. No final do Curso há uma avaliação final onde tem a oportunidade de testar os conhecimentos adquiridos e verificar se é um cidadão ciberseguro. Os recursos utilizados referem algumas entidades e estão assinalados no final de cada página. Foram disponibilizados ao abrigo da licença de partilha de forma gratuita, cujo fim se destine à disseminação da informação sem fins lucrativos.

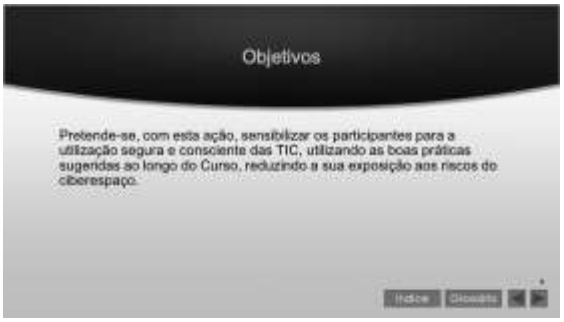
Nas próximas 16 páginas, podemos ver parte do conteúdo do curso.


Curso
Segurança da
Informação
Ação de consciencialização ao cidadão
2019


Apresentação
O Curso Segurança da Informação, pretende consciencializar o cidadão para os perigos das novas tecnologias, promovendo a utilização das Tecnologias de Informação e Comunicação (TIC) de uma forma mais segura e consciente, mostrando, as boas práticas sugeridas por algumas instituições e organizações nacionais e internacionais que produzem materiais educativos e de sensibilização na área da cibersegurança.
Índice
Glossário


Apresentação
Através das próximas páginas, vão ser abordados vários assuntos relacionados com as novas tecnologias, nomeadamente a ciberhigiene que o indivíduo deverá ter, que lhe permitam fazer uso das TIC de uma forma segura, enquanto seu utilizador nos meios envolventes, em casa, no trabalho e no exterior.
Índice
Glossário


Apresentação
Com isto pretende-se que o cidadão adquira um conjunto de competências que lhe permitam fazer uso das TIC de uma forma segura, enquanto seu utilizador.
Para que possa compreender todos os termos utilizados no decorrer do Curso, pode e deve consultar o Glossário, que se encontra no final do Curso.
Índice
Glossário


Objetivos
Pretende-se, com esta ação, sensibilizar os participantes para a utilização segura e consciente das TIC, utilizando as boas práticas sugeridas ao longo do Curso, reduzindo a sua exposição aos riscos do ciberespaço.
Índice
Glossário

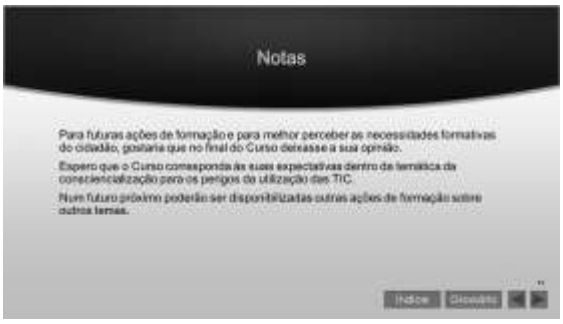

Destinatários / Carga Horária
Destinatários
O Curso destina-se a todos os cidadãos.
Carga horária
12 horas divididas em 3 módulos, 4 horas cada módulo
ou
Versão rápida, 3 horas para ver os vídeos, recursos e questionários
Índice
Glossário


Estrutura e Conteúdos
Estrutura
O Curso está organizado em 3 módulos, cujos temas principais são:
1. Casa
2. Trabalho
3. Exterior
Conteúdo
Cada módulo tem quatro tópicos:
1. Identidade
2. Redes e Navegação
3. Comportamento Social
4. Posto de Trabalho/Posto Doméstico/Passaporte.
Cada tópico contem textos e vídeos com conteúdos específicos sobre esse tópico.
Índice
Glossário


Navegação
Para uma melhor experiência, aconselho que efetue o download do ficheiro do Curso para o seu computador ou dispositivo móvel.
O Curso está no formato PDF.
Existem links (atalhos assinalados a laranja) para recursos externos na Internet sob a forma PDF ou vídeos.
Quando visualiza o documento PDF através da Internet em modo de pré-visualização os links não ficam disponíveis, terá de descarregar o ficheiro PDF.
Índice
Glossário


Avaliação
Este Curso é de frequência livre e anónimo, mas permite que faça a sua autoavaliação através do preenchimento dos questionários no final de cada módulo.
Só deverá passar ao módulo seguinte após responder ao questionário final de cada módulo.
No final do Curso há uma avaliação final onde tem a oportunidade de testar os conhecimentos adquiridos e verificar se é um cidadão ciberseguro.
Índice
Glossário


Autor
Este Curso, foi elaborado no âmbito da dissertação do Mestrado em Ciberssegurança e Informática Forense.
Os recursos utilizados referem algumas entidades e estão assinalados no final de cada página. Foram disponibilizados ao abrigo da licença de partilha de forma gratuita, cujo fim se destina à disseminação da informação sem fins lucrativos.
O presente conteúdo é propriedade de Paula Joaquim, estando protegido nos termos da legislação da propriedade intelectual aplicável. O utilizador pode copiar, importar ou usar gratuitamente parte ou a totalidade da informação, para uso pessoal ou público, desde que não tenha finalidades lucrativas ou ofensivas e seja referida a fonte de informação.
Índice
Glossário


Notas
Para futuras ações de formação e para melhor perceber as necessidades formativas do cidadão, gostaria que no final do Curso deixasse a sua opinião.
Espero que o Curso corresponda às suas expectativas dentro da temática da consciencialização para os perigos da utilização das TIC.
Num futuro próximo poderão ser disponibilizadas outras ações de formação sobre outros temas.
Índice
Glossário


Curso Segurança da Informação
Índice
Glossário


Curso Segurança da Informação
Módulo 1
Ação de consciencialização ao cidadão
2019


Curso Segurança da Informação
Bem vindo ao Curso Segurança da Informação
O Curso foi elaborado de forma transversal, tendo em conta que todos nós, enquanto cidadãos, trabalhadores de uma organização, ou até mesmo apenas como utilizadores da internet, devemos saber os cuidados a ter para nos prevenirmos de todo e qualquer perigo que possa existir no ciberespaço.
Índice
Glossário


Curso Segurança da Informação
Aqui encontrará noções sobre os perigos e as boas práticas para lidar com eles.
De seguida pode ver um pequeno vídeo sobre os perigos a que estamos sujeitos.
Versão Rápida
Caso não disponha de tempo suficiente para fazer o Curso na sua totalidade, poderá visionar todos os vídeos, aceder aos recursos disponibilizados e fazer os questionários de avaliação no seguinte link – Versão Rápida.
Índice
Glossário

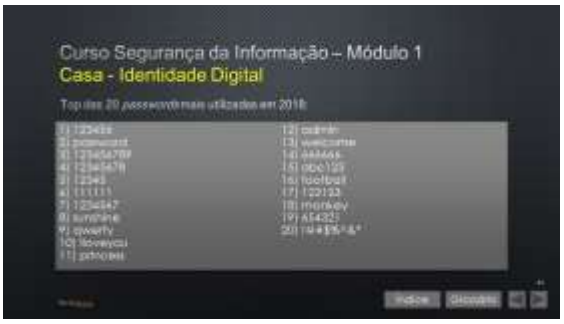

Curso Segurança da Informação
Índice
Casa
Identidade
Redes e Navegação
Comportamento Social
Posto de Trabalho
Questionário
Glossário
Trabalho
Identidade
Redes e Navegação
Comportamento Social
Posto de Trabalho
Questionário
Versão Rápida – Vídeos, Recursos, Questionários
Exterior
Identidade
Redes e Navegação
Comportamento Social
Passaporte
Questionário
Questionário Final
Questionários Selecção
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Vamos começar com algumas questões!
Tem Wi-Fi em casa?
Dispositivos ligados à Internet?
Costuma receber amigos ou família em casa?
E por fim... tem a certeza que está seguro na sua casa?
Não precisa responder já! No final deste módulo poderá ter uma resposta melhor.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
A sua identidade digital é composta pelo conjunto de dados que o/a identificam, permitindo o seu reconhecimento no mundo digital.
Quando falamos na nossa identidade digital, esta é relativa à nossa presença no Mundo Digital. Por exemplo:
o cartão de cidadão
o nosso cartão multibanco
o cartão bancário de crédito
nome de utilizador/palavra-passe no Google, Facebook, Instagram, e Twitter
a nossa identificação (nome de utilizador/palavra-passe) para aceder à conta bancária, para lojas e comprar online, plataformas de jogos
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Para proteger a sua identidade digital deve ter em atenção algumas questões acerca das passwords (palavras-passe) e das credenciais de acesso.
Password
As passwords são a principal chave para aceder a dados e a informação protegida.
O uso de passwords associada ao nome do utilizador (username) é um meio de autenticação simples e seguro, que permite ao utilizador autenticar-se e aceder aos serviços (ex. acesso à sua rede Wi-Fi em casa).
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
As passwords escolhidas pelos utilizadores devem, não só, conter alguma complexidade, mas também necessitam de ser alteradas periodicamente.
Desta forma, se ocorrer algum acesso não autorizado por um desconhecido, este será temporariamente limitado, reduzindo a possibilidade de interferências indevidas.
Quando falamos em passwords, referimo-nos a uma sequência de caracteres ou palavras que uma pessoa utiliza para se autenticar.
Estas, garantem-nos alguma proteção contra fraudes e perda de informações confidenciais, contudo, muitas vezes as passwords escolhidas pelos utilizadores são pouco seguras.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Top dos 20 passwords mais utilizadas em 2018:
1) 123456
2) password
3) 12345678
4) 12345679
5) 12345
6) 111111
7) 1234567
8) sunshine
9) qwerty
10) iloveyou
11) princess
12) admin
13) welcome
14) 666666
15) abc123
16) football
17) 123123
18) monkey
19) 654321
20) !@#$%^&*
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Para aumentar a força das passwords, deve privilegiar-se a dimensão face à complexidade, ou até mesmo optar por frases complexas, mas fáceis de memorizar (ex. "Nomedacasadeinfância"). (...)
Deve usar diferentes tipos de caracteres.
Incluir números, sinais de pontuação, símbolos e letras maiúsculas e minúsculas.
Em dispositivos móveis que não são projetados para facilitar a entrada de caracteres especiais, considere o uso de passwords mais longas com caracteres diferentes.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Recomendações
Não utilize a mesma password para várias contas.
Use passwords complexas com 8 ou mais caracteres, que contenha números, letras e caracteres especiais.
Se a password for roubada, deve alterá-la imediatamente.
Uma password longa não significa que seja difícil de memorizar. Quatro palavras comuns misturadas com caracteres especiais fazem uma password longa e fácil de memorizar.
Altere regularmente as passwords dos seus serviços online.
Utilize um gestor de passwords.
Prefira os serviços que oferecem a possibilidade de utilizar dois fatores de autenticação ou multifator fatores.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Não use palavras, nomes próprios ou nomes de lugares facilmente encontrados em dicionários.
Isto porque os atacantes utilizam sistemas que permitem testar todas as palavras existentes no dicionário, de forma automática, conseguindo decifrar as suas ultimas passwords de acesso.
Não utilize informações pessoais.
É provável que outras pessoas saibam informações sobre si, como o dia de aniversário, o nome do parceiro ou filhos, o número de telefone e podem adivinhar que usou estas referências como password.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Não use o nome próprio, é demasiado óbvio!
Não opte por uma password que seja igual ao seu nome de utilizador ou número de conta bancária.
Escolha passwords difíceis de identificar à medida que as digita.
Não use caracteres repetidos nem deixe as passwords escritas em locais visíveis junto ao computador, monitor ou teclado.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Com o objetivo de simplificar, o técnico que instala o serviço de Internet[1] (rede informática utilizada para interligar computadores a nível mundial, à qual pode aceder qualquer tipo de utilizador, e que possibilita o acesso a toda a espécie de informação) na sua casa, muitas vezes escreve a password em texto claro num post-it.
Não deixe esse post-it em local visível e assim que possível altere a password por uma escolhida por si e que só você a saiba.
password
123456
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Não menos importante é não armazenar backups de passwords no seu computador pessoal, especialmente em ficheiros que não estão protegidos com password.
Alternativamente, pode usar software de gestão de passwords.
Estes softwares são baseados em bases de dados cifradas e geralmente mais seguros.
Exemplo o LastPass, é um dos mais populares.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Credenciais de acesso
Para além da password existem outros meios para aceder aos serviços, que asseguram algum nível de segurança.
Com recurso a um smart card eletrónico (ex. cartão de cidadão), o utilizador pode autenticar-se e aceder a um serviço, utilizando um certificado digital.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Mesmo que recorra a um sistema de autenticação de dois fatores de segurança (two factor authentication ou 2FA) para aceder a um serviço, ou seja, a password e um código numérico de segurança (recebido por SMS no seu telemóvel ou por mensagem no seu e-mail[1] (correio eletrónico, sistema que permite a troca de correspondência a partir de equipamento ligado em rede)), não partilhe os seus códigos de acesso com terceiros, mesmo que estes lhe sejam solicitados por um técnico que lhe assegura um serviço em casa.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Autenticação de dois fatores (2FA) ou multiplos fatores (MFA)
Esta autenticação é utilizada para complementar a segurança da sua conta, pois além do seu password, vai lhe ser solicitado outro elemento que só você tem na sua posse.
Esta funcionalidade tem de ser ativada.
Nem todos os serviços que utiliza possuem esta funcionalidade.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Exemplos de 2FA
Após a inserção da password, é-lhe solicitado outro elemento que esteja na sua posse:
Um SMS é-lhe enviado com um código que terá de inserir após colocar as suas credenciais de autenticação (utilizador e a sua password).
Envio de código através de chamada telefónica.
Geração de um código através de uma aplicação no telemóvel.
Colocação dos seus dados biométricos.
Colocação de uma security key (pen usb especial) na porta usb do computador.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
A Autenticação de dois fatores ou multi-fator deve ser utilizada para os serviços que são mais críticos.
Pode ver aqui alguns serviços que estão disponíveis em relação a 2FA.
Alguns exemplos de serviços disponíveis para as suas contas:
Índice
Glossário

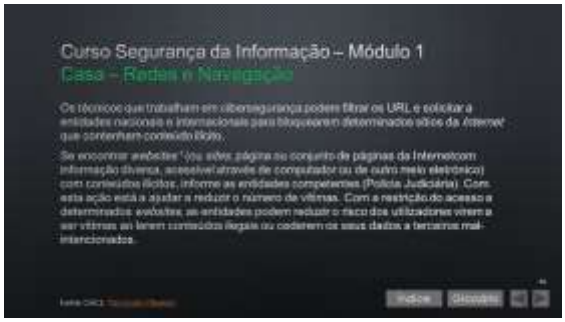

Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Convém manter os seus equipamentos eletrónicos com todas as atualizações de segurança em dia e o sistema de proteção de vírus ativo, de forma a evitar que a segurança do equipamento possa vir a ser comprometida e, eventualmente, as credenciais de acesso possam ser identificadas antes mesmo de serem enviadas para os servidores do serviço em causa.
Evite a utilização de equipamentos de terceiros ou cuja segurança possa levantar dúvidas para aceder a plataformas ou serviços que impliquem a introdução de credenciais de acesso.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Existe um local na Internet onde pode consultar se a sua conta de acesso a um serviço online foi comprometida.
Este site é o ';--have i been pwned?
Introduza o seu endereço de e-mail e fique a saber os serviços que subscreve com essa conta que foram alvo de quebra de segurança e qual o tipo de exposição.
';--have i been pwned?
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa - Identidade Digital
Se não tiver outra opção e utilizar equipamentos de terceiros, como o do técnico que pretende estabelecer ligação entre o seu dispositivo e os seus eletrodomésticos, é recomendável que questione sempre a intervenção do técnico e assegure que é uma pessoa credenciada pela empresa contratada.
Visualize o seguinte vídeo e fique com mais algumas sugestões para proteger a sua identidade
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Na sua casa pode navegar na Internet e realizar uma infinidade de atividades.
Pode procurar informação sobre qualquer assunto, fazer pagamentos online, procurar receitas de culinária, procurar um eletricista ou um canalizador, fazer compras online, comprar um detergente ou até mesmo chamar um médico.
Como pode observar, existe uma vasta gama de serviços e produtos em sítios da Internet mas antes de os utilizar, tenha alguns cuidados para se proteger quando navega no ciberespaço.
online shopping
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
URL
O endereço de rede (URL - Uniform Resource Locator) é um endereço onde os documentos e outros recursos são disponibilizados na Internet, através da ajuda de um programa de navegação (ex. Google).
O URL integra caracteres identificadores do protocolo (http, https, ftp), do domínio que é o endereço do servidor, da porta onde se estabelece a ligação com o servidor e do caminho para se conseguir chegar ao recurso que se encontra no servidor.
URL: http://www.xpto.com
Índice
Glossário

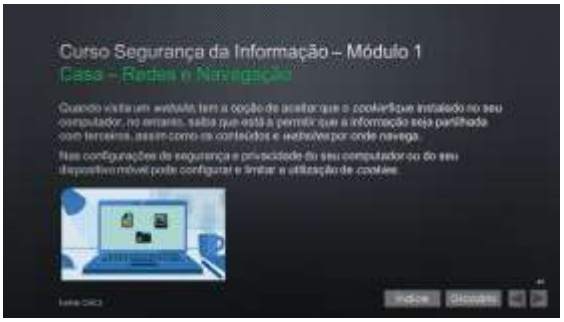

Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Os técnicos que trabalham em cibersegurança podem filtrar os URL e solicitar a entidades nacionais e internacionais para bloquearem determinados sítios da Internet que contenham conteúdo ilícito.
Se encontrar websites (ou sites: página ou conjunto de páginas da Internet com informação diversa, acessível através de computador ou de outro meio eletrónico) com conteúdos ilícitos, informe as entidades competentes (Polícia Judiciária). Com esta ação está a ajudar a reduzir o número de vítimas. Com a restrição do acesso a determinados websites, as entidades podem reduzir o risco dos utilizadores virem a ser vítimas ao lerem conteúdos ilegais ou cederem os seus dados a terceiros mal-intencionados.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Pop-ups
É normal que, quando acede a determinados websites a partir do seu computador pessoal, lhe apareça uma janela com publicidade, o que muitas vezes dificulta a leitura do próprio website que pretende consultar.
Essa janela é um pop-up.
A publicidade que lhe aparece é, geralmente, sobre os itens que mais procura na Internet (ex. produtos para a casa, serviços de limpeza, roupas, sapatos ou outros objetos).
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Saiba que pode configurar o seu navegador de Internet para bloquear pop-ups.
Normalmente, em websites pouco fidedignos os pop-ups podem conter software malicioso (malware) com informações ou outros endereços que enganam e manipulam o utilizador.
Portanto, deve verificar se o sítio da Internet ao qual acede é fidedigno e estar com atenção a situações pouco habituais ou que lhe exigem os seus dados pessoais para outros serviços que não pretende.
Índice
Glossário

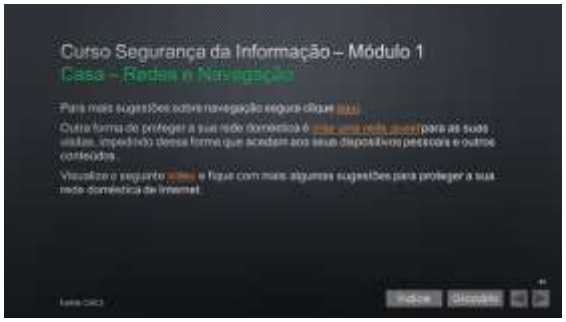

Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Cookies
Cookies são etiquetas de software instaladas no seu computador através de navegadores – ex. Google Chrome, Internet Explorer, Firefox, Opera – que armazenam informação sobre as suas preferências e pesquisas online.
Essas etiquetas, depois de instaladas no seu computador, partilham informação, sempre que o navegador estabelece comunicação com o servidor.
Tenha cuidado com esta atividade.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Os cookies podem ser úteis quando nos indicam as páginas web mais consultadas e nos mostram informações relacionadas com as nossas pesquisas.
Contudo, alerta-se para o facto dos cookies poderem ser uma ameaça à sua privacidade, nos casos em que sejam instalados ficheiros de texto sem o seu consentimento, sendo que podem recolher informações sobre os seus interesses de navegação na Internet.
Essas informações podem ser partilhadas ou até vendidas a outros sites da Internet, como por exemplo, o número de vezes que acedeu a uma hiperligação ou a uma notícia.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Quando visita um website tem a opção de aceitar que o cookie/que instalado no seu computador, no entanto, saiba que está a permitir que a informação seja partilhada com terceiros, assim como os conteúdos e websites por onde navega.
Nas configurações de segurança e privacidade do seu computador ou do seu dispositivo móvel pode configurar e limitar a utilização de cookies.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Histórico de navegação
Quando visita páginas na Internet os seus navegadores (ex. Google Chrome, Internet Explorer) guardam o seu histórico de navegação.
Todas as informações ficam armazenadas no seu computador, como por exemplo, os dados que forneceu num determinado website de compras através do preenchimento de formulários, as suas credenciais de acesso como as passwords e códigos pessoais introduzidos, as ligações que acedeu, o tempo que despendeu em determinados websites e conteúdos.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Não deve guardar o histórico de navegação, eliminar websites que possam ter conteúdo indevido e que sejam suspeitos. Periodicamente, deve eliminar o histórico de todos os navegadores que utiliza no seu computador ou dispositivo móvel. Desta forma, está a proteger a sua privacidade.
Lembre-se que os seus dados podem ser facilmente acedidos por terceiros quando se encontram gravados de forma automática no seu navegador.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Redes e Navegação
Para mais sugestões sobre navegação segura clique aqui.
Outra forma de proteger a sua rede doméstica é criar uma rede guest para as suas visitas, impedindo dessa forma que acedam aos seus dispositivos pessoais e outros conteúdos.
Visualize o seguinte vídeo e fique com mais algumas sugestões para proteger a sua rede doméstica de Internet.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Quando utilizamos o ciberespaço, por vezes esquecemo-nos dos perigos.
Um deles é a engenharia social, um método para manipular os indivíduos com o intuito de obter informação e dados que permitam aceder, de forma não autorizada, aos seus serviços ou dispositivos móveis.
Exemplos desses dados são: dados bancários, contactos, fotografias, documentos pessoais, números de cartões de crédito ou palavras-passe.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Os engenheiros sociais obtêm a informação e os dados que pretendem, através de um conjunto de técnicas que lhes permitem obter informações indevidamente:
• aproveitando-se da ingenuidade das pessoas;
• observando comportamentos, rotinas e partilhas das vítimas.
O engenheiro social procura dar credibilidade a certas interações, explorando a ingenuidade das pessoas, obtendo informações através da proximidade à vítima com um discurso convincente, recorrendo a falsas histórias e informações e a aplicações maliciosas (malware).
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Atualmente, a engenharia social é considerada um dos maiores riscos de segurança das pessoas e das organizações. As técnicas de ataque são cada vez mais sofisticadas e a vítima muitas vezes não tem a devida noção do ataque.
Se for vítima deste tipo de ataque, que geralmente se traduz na violação de dados ou de privacidade na Internet, reporte-o às autoridades competentes, neste caso a Polícia Judiciária.
Você confia em quem está ao seu lado?
Engenharia Social
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Correio eletrónico
O correio eletrónico, mais conhecido por e-mail, é o meio de comunicação mais utilizado no ciberespaço.
Atualmente, torna-se fundamental termos em conta alguns fatores úteis para proteger as nossas contas de e-mail.
Índice
Glossário


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
BCC
Em caso de enviar um e-mail para vários destinatários do correio eletrónico, deverá colocar os endereços no campo BCC (Black Carbon Copy)
Esta funcionalidade faz com que quem receba o e-mail apenas visualize o remetente, não causando incómodo, em caso de não partilha do e-mail com terceiros.
Evitando assim a propagação de SPAM (Stupid Pointless Annoying Messages) que em português é sinónimo de correio eletrónico para o lixo.
SPAM designa o envio em massa de e-mails


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
SPAM é uma das formas de propagação de vírus e de phishing
Verifique se o remetente da mensagem que recebeu, é de confiança.
No caso de se tratar de um remetente desconhecido, não abra o e-mail. Não clique nas ligações, nem abra os anexos.
Não clique em links que promovam propaganda ou publicidade enganosa, pois pode colocar o seu computador em risco, através da instalação de malware.


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Anexos
Ao abrir anexos que recebe num e-mail, cujo remetente se desconhece, é necessário ter algum cuidado.
Um anexo descarregado pode ser, ou até conter, um software malicioso proveniente de uma fonte não fidedigna.
Verifique sempre o formato do anexo que recebe no e-mail e seja prudente com os ficheiros executáveis, que possam permanecer no seu computador ou dispositivo móvel.


Curso Segurança da Informação – Módulo 1
Casa – Comportamento Social
Para aprofundar um pouco este tema clique aqui.
Nos seguintes vídeos, pode consultar algumas dicas para proteger a sua identidade e os seus dispositivos eletrónicos de diversos tipos de ataques, entre eles, a engenharia social.
Pode aqui ver também um pequeno documentário sobre SPAM. (fonte: RTP)
Veja o vídeo sobre comportamento social.
Veja o vídeo para proteger os seus dispositivos eletrónicos.


Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
Tanto o computador como os dispositivos móveis trazem vantagens e auxiliam na realização de diversas tarefas, incluindo as tarefas de casa, facilitando a nossa vida.
Isto permite-nos partilhar a agenda com os nossos filhos, ver receitas nos vídeos do YouTube (serviço de disponibilização de vídeos através da Internet), programar as máquinas de lavar roupa e de lavar louça através de programas instalados no computador ou até observar os nossos filhos a brincar no quarto.
No entanto, a disponibilização imediata de informação e a comunicação entre vários dispositivos carece de medidas de segurança.

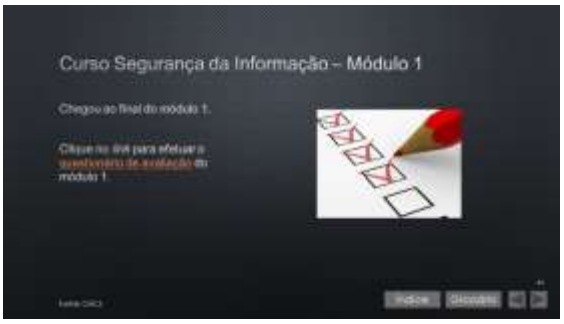

Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
A ligação desses dispositivos deverá respeitar algumas regras, principalmente quando os dispositivos contêm informação sensível.
Com a proliferação de dispositivos inteligentes em casa é difícil controlar a troca de dados.
No entanto, são os próprios utilizadores que decidem o nível de segurança dos seus equipamentos.


Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
Além disso, deve-se proibir ou evitar a ligação desses dispositivos a uma rede desconhecida e automaticamente estabelecida, que suporta todas as comunicações e informações que ocorrem dentro de casa.
É ainda necessário ter atenção e cuidado, na seleção das aplicações que são descarregadas nos dispositivos, pois podem conter malware e aceder à sua informação pessoal, assim como interferir no funcionamento dos seus equipamentos eletrónicos.
Descarregue as aplicações apenas de fontes fidedignas.


Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
Para assegurar um maior nível de cibersegurança, utilize uma rede privada virtual (VPN) em casa, especialmente para realizar tarefas que impliquem a disponibilização de informação sensível (quer seja sua ou da sua organização).
A rede privada virtual (VPN) recorre a uma infraestrutura pública para a transmissão de informação protegida, cifrando os dados.
Desta forma, a VPN possibilita uma ligação segura, cifrando os dados que fluem na rede.

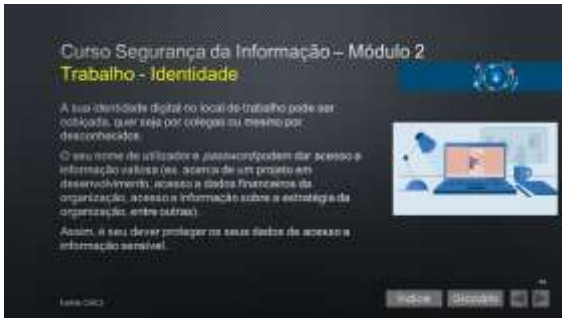

Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
A cifra (algoritmo de complexidade variável que permite a transformação de um texto claro num texto ilegível) protege os dados nos dispositivos eletrónicos e plataformas informáticas, nomeadamente nos serviços de e-mail, ficheiros de rede, armazenamento em nuvem (cloud) e na comunicação com outros dispositivos.
As informações que se encontram protegidas desta forma só podem ser cedidas com a inserção de credenciais.

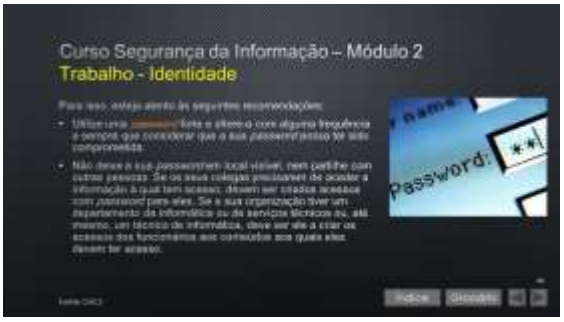

Curso Segurança da Informação – Módulo 1
Casa – Posto Doméstico
Existem soluções de criptografia que, além de fazerem a gestão de chaves, podem ser configuradas para que os dados sejam automaticamente desencriptados. Desse modo, não é necessário inserir uma palavra-passe para se ter acesso às informações.
Para uma melhor segurança dos dados deve proteger as suas informações confidenciais e não permitir que as credenciais sejam gravadas automaticamente.
Visualize o seguinte vídeo e fique com mais algumas sugestões para proteger o seu computador pessoal.


Curso Segurança da Informação – Módulo 1
Chegou ao final do módulo 1.
Clique no link para efetuar o questionário de avaliação do módulo 1.
Índice
Glossário

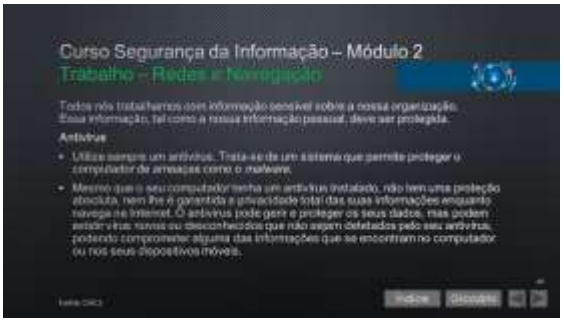

Curso Segurança da Informação
Módulo 2
Ação de consciencialização ao cidadão
2019

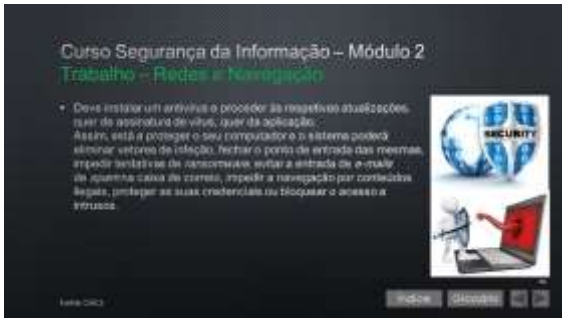

Curso Segurança da Informação – Módulo 2
Índice
Glossário

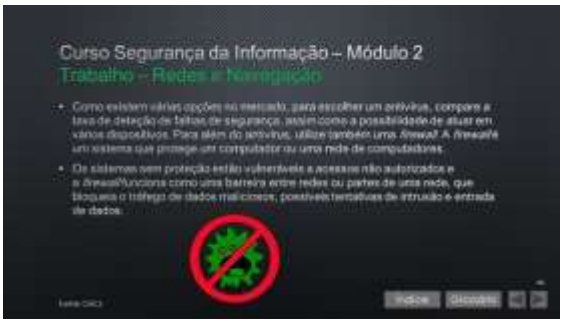

Curso Segurança da Informação – Módulo 2
Trabalho - Identidade
A sua identidade digital no local de trabalho pode ser colhida, quer seja por colegas ou mesmo por desconhecidos.
O seu nome de utilizador e password podem dar acesso a informação valiosa (ex. acerca de um projeto em desenvolvimento, acesso a dados financeiros da organização, acesso a informação sobre a estratégia da organização, entre outras).
Assim, é seu dever proteger os seus dados de acesso a informação sensível.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho - Identidade
Para isso, esteja atento às seguintes recomendações:
Utilize uma password forte e altere-a com alguma frequência e sempre que considerar que a sua password possa ter sido comprometida.
Não deixe a sua password em local visível, nem partilhe com outras pessoas. Se os seus colegas precisarem de aceder a informação à qual tem acesso, devem ser criados acessos com password para eles. Se a sua organização tiver um departamento de informática ou de serviços técnicos ou, até mesmo, um técnico de informática, deve ser ele a criar os acessos dos funcionários aos computadores aos quais eles devem ter acesso.
Password:
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho - Identidade
Sempre que se ausentar do seu posto de trabalho, bloqueie o computador, mesmo que seja por um período muito curto.
Quando sair do local de trabalho no final do dia, desligue o computador.
Faça todas as atualizações que o sistema lhe sugere.
Não deixe o seu cartão de acesso à organização (cartão de abertura de portas) longe da sua vista, transporte-o sempre consigo. Este cartão também é parte da sua identidade digital na organização.
Password
No seguinte vídeo, pode consultar algumas sugestões para proteger a sua identidade no local de trabalho:
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
Todos nós trabalhamos com informação sensível sobre a nossa organização. Essa informação, tal como a nossa informação pessoal, deve ser protegida.
Antivírus
Utilize sempre um antivírus. Trata-se de um sistema que permite proteger o computador de ameaças como o malware.
Mesmo que o seu computador tenha um antivírus instalado, não tem uma proteção absoluta, nem lhe é garantida a privacidade total das suas informações enquanto navega na Internet. O antivírus pode gerir e proteger os seus dados, mas podem existir vírus novos ou desconhecidos que não sejam detetados pelo seu antivírus, podendo comprometer alguns dos seus dados que se encontram no computador ou nos seus dispositivos móveis.
Índice
Glossário

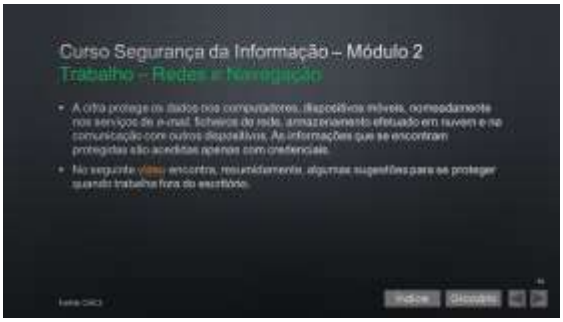

Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
Deve instalar um antivírus e proceder às respetivas atualizações, quer da assinatura de vírus, quer da aplicação.
Assim, está a proteger o seu computador e o sistema poderá eliminar vetores de infeção, fechar o ponto de entrada das mesmas, impedir tentativas de ransomware, evitar a entrada de e-mails de spam na caixa de correio, impedir a navegação por conteúdos ilegais, proteger as suas credenciais ou bloquear o acesso a intrusos.
SECURITY
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
Como existem várias opções no mercado, para escolher um antivírus, compare a taxa de deteção de falhas de segurança, assim como a possibilidade de atuar em vários dispositivos. Para além do antivírus, utilize também uma firewall. A firewall é um sistema que protege um computador ou uma rede de computadores.
Os sistemas sem proteção estão vulneráveis a acessos não autorizados e a firewall funciona como uma barreira entre redes ou partes de uma rede, que bloqueia o tráfego de dados maliciosos, possíveis tentativas de intrusão e entrada de dados.
Índice
Glossário

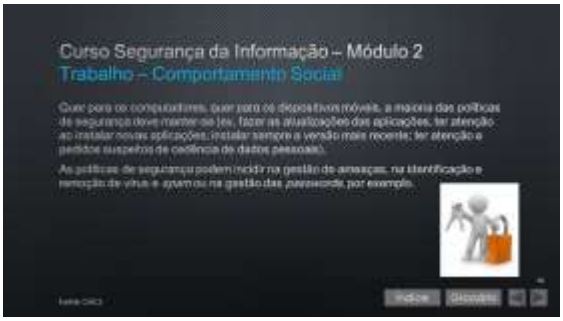

Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
Firewall vs VPN
FIREWALL
VPN
INTERNET
Índice
Glossário

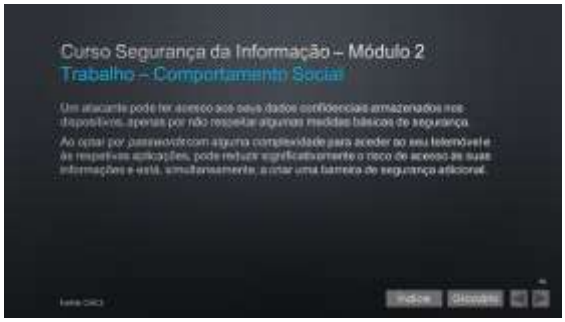

Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
Firewall
• Quando a firewall está instalada no seu computador, esta pode avisá-lo sempre que um programa tenta estabelecer uma ligação e questioná-lo se a ligação deve ser permitida ou bloqueada.
• Desta forma, a firewall pode controlar ligações realizadas ao seu computador a partir de outros computadores com acesso à rede da Internet do seu trabalho. Deve evitar que sistemas desconhecidos tenham controlo sobre a sua porta de rede.
Índice
Glossário

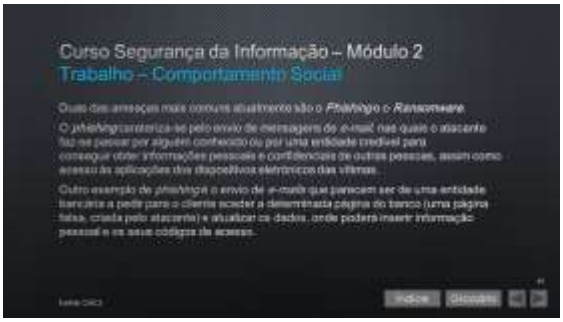

Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
VPN
• Quando trabalha fora do escritório, deve ter especial cuidado com as redes de Internet às quais se liga e com que informação trabalha. Nestes casos, utilize sempre uma rede privada virtual (VPN).
• Esta garante-lhe a proteção dos seus dados, através da sua encriptação, o que impede os hackers (atacantes) de observar o que está a fazer e a escrever no seu equipamento eletrónico, quando se liga à Internet em locais públicos.
Índice
Glossário

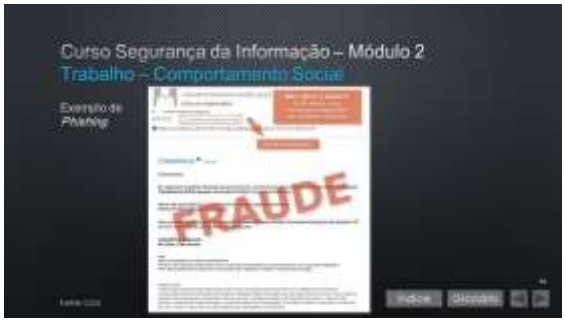

Curso Segurança da Informação – Módulo 2
Trabalho – Redes e Navegação
• A cifra protege os dados nos computadores, dispositivos móveis, nomeadamente nos serviços de e-mail, ficheiros de rede, armazenamento efetuado em nuvem e na comunicação com outros dispositivos. As informações que se encontram protegidas são acedidas apenas com credenciais.
• No seguinte vídeo encontra, resumidamente, algumas sugestões para se proteger quando trabalha fora do escritório.
Índice
Glossário

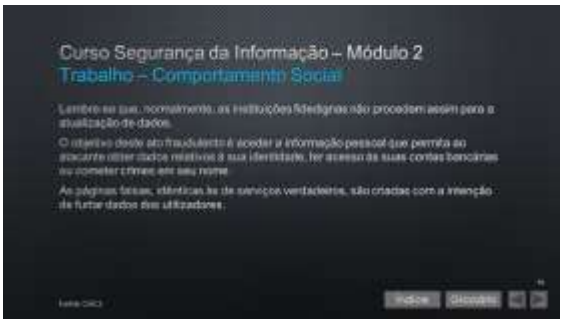

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
O utilizador dos dispositivos eletrónicos é o elemento mais importante na garantia da cibersegurança. Todos nós devemos ter hábitos e comportamentos ciberseguros.
Esses comportamentos passam pelo cumprimento de políticas, procedimentos e a utilização de ferramentas para proteger os respetivos dispositivos.
Verifique se os contratos estabelecidos com os operadores e as respetivas políticas e procedimentos estão atualizados.
Índice
Glossário

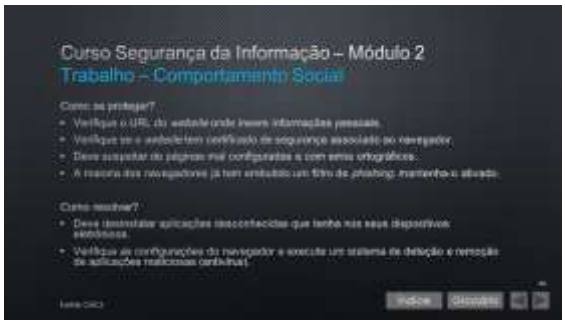

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Quer para os computadores, quer para os dispositivos móveis, a maioria das políticas de segurança deve manter-se (ex. fazer as atualizações das aplicações, ter atenção ao instalar novas aplicações, instalar sempre a versão mais recente; ter atenção a pedidos suspeitos de confiança de dados pessoais).
As políticas de segurança podem incidir na gestão de ameaças, na identificação e remoção de vírus e ajuam ou na gestão das passwords, por exemplo.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Um atacante pode ter acesso aos seus dados confidenciais armazenados nos dispositivos, apenas por não respeitar algumas medidas básicas de segurança.
Ao optar por password com alguma complexidade para aceder ao seu telemóvel e às respetivas aplicações, pode reduzir significativamente o risco de acesso às suas informações e está, simultaneamente, a criar uma barreira de segurança adicional.
Índice
Glossário

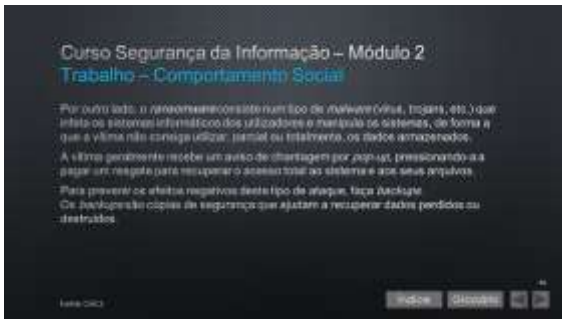

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Duas das ameaças mais comuns atualmente são o Phishing e o Ransomware.
O phishing caracteriza-se pelo envio de mensagens de e-mail nas quais o atacante faz-se passar por alguém conhecido ou por uma entidade credível para conseguir obter informações pessoais e confidenciais de outras pessoas, assim como acesso às aplicações dos dispositivos eletrónicos das vítimas.
Outro exemplo de phishing é o envio de e-mails que parecem ser de uma entidade bancária a pedir para o cliente aceder a determinada página do banco (uma página falsa, criada pelo atacante) e atualizar os dados, onde poderá inserir informação pessoal e os seus códigos de acesso.
Índice
Glossário

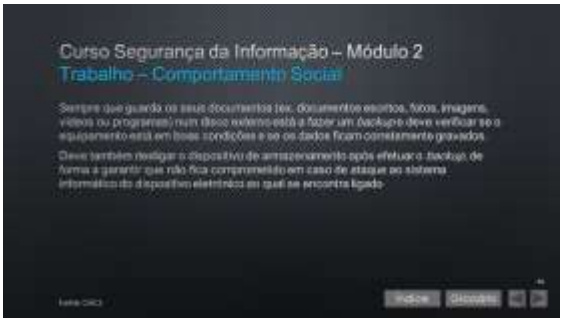

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Exemplo de Phishing
FRAUDE
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Lembre-se que, normalmente, as instituições fidedignas não procedem assim para a atualização de dados.
O objetivo deste ato fraudulento é aceder a informação pessoal que permita ao atacante obter dados relativos à sua identidade, ter acesso às suas contas bancárias ou cometer crimes em seu nome.
As páginas falsas, idênticas às de serviços vantajosos, são criadas com a intenção de furtar dados dos utilizadores.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Como se proteger?
• Verifique o URL do website onde insere informações pessoais.
• Verifique se o website tem certificado de segurança associado ao navegador.
• Deve suspeitar de páginas mal configuradas e com erros ortográficos.
• A maioria dos navegadores já tem embutido um filtro de phishing, mantenha-o ativado.
Como resolver?
• Deve desinstalar aplicações desconhecidas que tenha nos seus dispositivos eletrónicos.
• Verifique as configurações do navegador e execute um sistema de deteção e remoção de aplicações maliciosas (antivírus).
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Para diminuir a probabilidade de ataque ao seu computador ou outros dispositivos eletrónicos, deve ter cuidado com os dados pessoais que fornece, evitar aceder a conteúdos web maliciosos, não abrir documentos provenientes de endereços de e-mail desconhecidos e que possam estar infetados, não permitir a introdução no seu computador de um dispositivo USB (ex. pen USB) que desconhece e que pode estar infetado e não abrir qualquer ligação de e-mails que desconhece, porque pode estar perante e-mails de phishing.
4 GB
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Por outro lado, o ransomware consiste num tipo de malware (vírus, trojans, etc.) que infeta os sistemas informáticos dos utilizadores e manipula os sistemas, de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados.
A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando-a a pagar um resgate para recuperar o acesso total ao sistema e aos seus arquivos.
Para prevenir os efeitos negativos deste tipo de ataque, faça Backups.
Os backups são cópias de segurança que ajudam a recuperar dados perdidos ou destruídos.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Sempre que guarda os seus documentos (ex. documentos escritos, fotos, imagens, vídeos ou programas) num disco externo está a fazer um backup e deve verificar se o equipamento está em boas condições e se os dados ficam corretamente gravados.
Deve também desligar o dispositivo de armazenamento após efetuar o backup, de forma a garantir que não fica comprometido em caso de ataque ao sistema informático do dispositivo eletrónico ao qual se encontra ligado.
Índice
Glossário

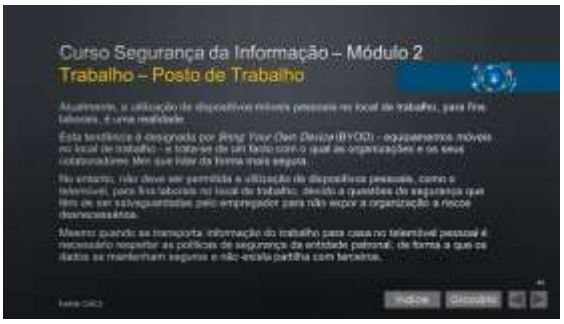

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Exemplo de Ransomware
Ransomware attack
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Se sofrer algum ataque de ransomware ou tiver algum acidente com o dispositivo eletrónico, se tiver uma cópia de segurança pode restaurar os dados do seu computador ou os seus dados pessoais.
Por esta razão, deve fazer cópias de segurança regularmente para manter os seus documentos atualizados e deve armazená-los em dispositivos diferentes.
Se quiser fazer um backup de uma grande quantidade de dados para um disco externo ou uma pen USB, assegure previamente que o equipamento tem uma grande capacidade de armazenamento.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Atualmente, pode recorrer a cópias de segurança para a nuvem (cloud), que permite o armazenamento dos seus dados e à qual pode aceder, via online, do seu computador ou outro dispositivo móvel, em qualquer lugar. No entanto, certifique-se que conhece os termos e as condições desse serviço.
Se pretende aprofundar um pouco este assunto clique aqui.
Visualize o seguinte vídeo, para mais dicas relacionadas com Ransomware.
Índice
Glossário

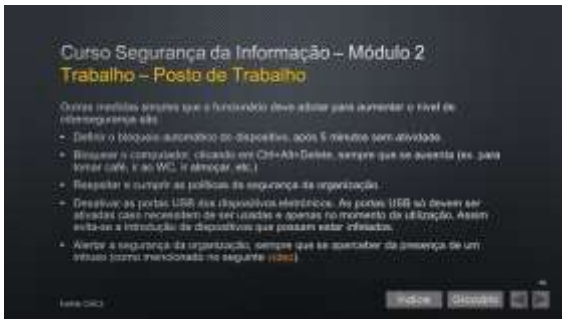

Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
Para mais informações sobre Ransomware, clique aqui. (ransomware.org)
Outro dos importantes é ter cuidado com os dispositivos eletrónicos utilizados e não ligar dispositivos de fonte desconhecida aos seus equipamentos eletrónicos, pois os mesmos podem estar infetados ou programados para realizar ações que desconhece nos seus equipamentos.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Comportamento Social
O que faria se encontrasse uma PEN USB na rua?
Veja o vídeo.
Índice
Glossário

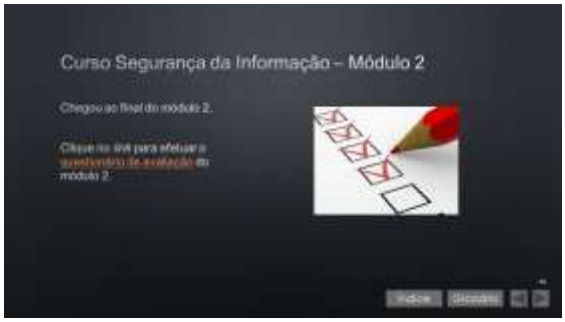

Curso Segurança da Informação – Módulo 2
Trabalho – Posto de Trabalho
Atualmente, a utilização de dispositivos móveis pessoais no local de trabalho, para fins laborais, é uma realidade.
Esta tendência é designada por Bring Your Own Device (BYOD) - equipamentos móveis no local de trabalho - e trata-se de um facto com o qual as organizações e os seus colaboradores têm que lidar da forma mais segura.
No entanto, não deve ser permitida a utilização de dispositivos pessoais, como o telemóvel, para fins laborais no local de trabalho, devido a questões de segurança que têm de ser salvaguardadas pelo empregador para não expor a organização a riscos desnecessários.
Mesmo quando se transporta informação do trabalho para casa no telemóvel pessoal é necessário respeitar as políticas de segurança da entidade patronal, de forma a que os dados se mantenham seguros e não exista partilha com terceiros.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Posto de Trabalho
Neste sentido, é essencial que conheça as políticas de segurança associadas ao BYOD e aos dispositivos móveis para uma maior segurança da informação que circula entre o dispositivo móvel pessoal e a entidade patronal.
A dificuldade de configuração dos dispositivos, a gestão de conteúdos, a dificuldade de controlo do tráfego de rede, as incompatibilidades entre sistemas, as configurações de e-mails de trabalho nos dispositivos pessoais são situações que podem dar origem a potenciais riscos de segurança da informação. Como, por exemplo, o armazenamento externo de informações confidenciais e sensíveis da organização.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Posto de Trabalho
Muitos dos aplicações que estão nos dispositivos móveis podem estabelecer ligações não seguras pela Internet, o que pode comprometer os dispositivos e os dados neles armazenados.
Sempre que possível, não utilize os seus próprios dispositivos móveis no local de trabalho. Mesmo existindo uma configuração por parte da sua entidade patronal, para que seja estabelecida uma ligação VPN segura, podem haver problemas associados à utilização de uma rede não segura que levam a riscos de ciberataques.
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Posto de Trabalho
Outras medidas simples que o funcionário deve adotar para aumentar o nível de cibersegurança são:
Definir o bloqueio automático do dispositivo, após 5 minutos sem atividade.
Bloquear o computador, clicando em Ctrl+Alt+Delete, sempre que se ausenta (ex. para tomar café, ir ao WC, ir almoçar, etc.)
Respeitar e cumprir as políticas de segurança da organização.
Desativar as portas USB dos dispositivos eletrónicos. As portas USB só devem ser ativadas caso necessitem de ser usadas e apenas no momento da utilização. Assim evita-se a introdução de dispositivos que possam estar infetados.
Alertar a segurança da organização, sempre que se aperceber da presença de um intruso (como mencionado no seguinte vídeo)
Índice
Glossário


Curso Segurança da Informação – Módulo 2
Trabalho – Posto de Trabalho
Para além dos cuidados mencionados, as organizações devem ter determinados cuidados para garantir a sua Cibersegurança (ex. a criação de uma rede Wi-Fi para visitantes).
O seguinte vídeo contém algumas sugestões para as organizações e a rede Wi-Fi.
Índice
Glossário

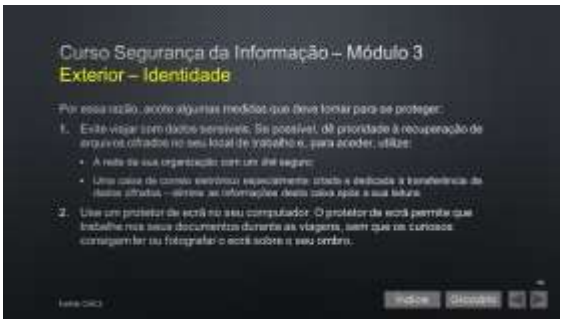

Curso Segurança da Informação – Módulo 2
Chegou ao final do módulo 2.
Clique no link para efetuar o questionário de avaliação do módulo 2.
Índice
Glossário

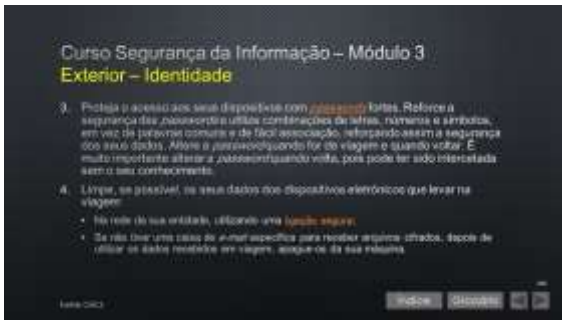

Curso Segurança da Informação
Módulo 3
Ação de consciencialização ao cidadão
2019


Curso Segurança da Informação – Módulo 3
Índice
Glossário


Curso Segurança da Informação – Módulo 3
Exterior – Identidade
As ciberameaças não tiram férias, na verdade estas podem ser mais recorrentes fora do seu ambiente de trabalho ou da sua casa.
Viagens de trabalho representam uma ameaça maior à sua segurança, porque na maioria das vezes você leva consigo material sensível, seja ele pessoal ou de trabalho, numa variedade de dispositivos, incluindo smartphones, computadores portáteis e tablets.
Índice
Glossário


Curso Segurança da Informação – Módulo 3
Exterior – Identidade
Os seus dispositivos e os seus dados podem chamar a atenção de terceiros e, nesse sentido, o utilizador deve ser cauteloso, independentemente das limitações que esse cuidado possa causar.
A internet disponibilizada em locais públicos como cafés, hotéis, aeroportos, entre outros locais, não garante a sua confidencialidade. Em muitos países estrangeiros, os sistemas políticos, os centros de negócios e as redes de comunicação são monitorizados regularmente.
FREE WiFi
Índice
Glossário


Curso Segurança da Informação – Módulo 3
Exterior – Identidade
Por essa razão, aconte algumas medidas que deve tomar para se proteger:
1. Evite viajar com dados sensíveis. Se possível, dê prioridade à recuperação de arquivos ofradios no seu local de trabalho e, para aceder, utilize:
• A rede da sua organização com um vPN seguro;
• Uma caixa de correio eletrónico especialmente criada e dedicada à transferência de dados ofradios – elimine as informações desta caixa após a sua leitura.
2. Use um protetor de ecrã no seu computador. O protetor de ecrã permite que trabalhe nos seus documentos durante as viagens, sem que os curiosos consigam ler ou fotografar o ecrã sobre o seu ombro.
Índice
Glossário


Curso Segurança da Informação – Módulo 3
Exterior – Identidade
3. Proteja o acesso aos seus dispositivos com passwords fortes. Reforce a segurança das passwords e utilize combinações de letras, números e símbolos, em vez de palavras comuns e de fácil associação, reforçando assim a segurança dos seus dados. Altere a password quando for de viagem e quando voltar. É muito importante alterar a password quando volta, pois pode ter sido interceptada sem o seu conhecimento.
4. Limpe, se possível, os seus dados dos dispositivos eletrónicos que levar na viagem:
• Na rede da sua entidade, utilizando uma ligação segura;
• Se não tiver uma caixa de e-mail específica para receber arquivos ofradios, depois de utilizar os dados recebidos em viagem, apague-os da sua máquina.
Índice
Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Identidade

5. Limpe o histórico de chamadas e pesquisas dos seus dispositivos eletrónicos. Esta é uma medida de segurança que deve aplicar diariamente e não apenas em viagem, embora seja mais importante em ambientes desconhecidos.

Visualize no seguinte vídeo, alguns dos cuidados a ter quando viaja.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Redes e Navegação

Em viagem temos a tendência para usar mais os nossos dispositivos móveis ligados à Internet, seja para consultar mapas, website de locais turísticos, partilhar fotos com os amigos e a família, entre outros, e são vários os locais públicos que disponibilizam rede Wi-Fi gratuita, como restaurantes, aeroportos, hotéis, museus, etc.

No entanto, pense numa questão importante:

Confiaria as suas informações e os seus dados a um estranho?

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Redes e Navegação

Provavelmente não... mas quando usa redes Wi-Fi públicas, é praticamente isso que está a fazer.

Está a permitir o acesso aos seus dados e aos conteúdos dos seus dispositivos eletrónicos a desconhecidos.

Não deve utilizar redes Wi-Fi públicas, especialmente se utilizar essas redes para tratar de assuntos pessoais ou de trabalho, sensíveis.

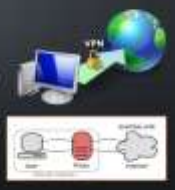
Lembre-se que não sabe quem gere e como gere essas redes.

Portanto, tal como não abre a porta da sua casa a desconhecidos, não permita o acesso de estranhos aos conteúdos dos seus dispositivos eletrónicos.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Redes e Navegação

Se tiver mesmo que usar os seus dispositivos e não tiver dados móveis disponíveis, utilize uma VPN (rede virtual privada) que age como um servidor *proxy* (cria uma ligação cifrada entre os seus dispositivos e a rede que está a utilizar).



Esta ferramenta vai tornar a sua navegação muito mais segura, pois mesmo que a sua ligação seja intercetada por *hackers*, não vão conseguir ler ou visualizar o que está a fazer.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Redes e Navegação

Pode também utilizar um software de cifra durante a viagem.

Não partilhe informações confidenciais ou sensíveis por telefone ou qualquer outro meio de transmissão de voz por canais sem cifra.

Lembre-se de limpar o histórico das suas chamadas e de navegação.

Além do histórico, apague os dados que permanecem em cache, cookies, senhas de acesso a websites e arquivos temporários.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Redes e Navegação

Também é importante que não conecte aos seus dispositivos, periféricos ou dispositivos de computação que não sejam confiáveis. Atenção à troca de documentos (ex. utilização de *pen* USB durante as apresentações de negócios ou durante conferências). Leve uma *pen* USB destinada apenas a essas trocas e descarte-a ou formate-a após utilização, em ambiente controlado.

O seguinte vídeo demonstra a importância do uso de uma VPN.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Comportamento Social

Quando vamos de férias, geralmente estamos mais descontraídos e recetivos a interagir e conversar com desconhecidos, permitindo que estranhos possam ver o que estamos a fazer nos nossos dispositivos eletrónicos (muitas vezes com a "desculpa" de que não conhecem a nossa língua).

Mas, não se descuide. Os ambientes desconhecidos apresentam mais perigos do que os habituais, para os quais já estamos preparados.

Quando interagir com desconhecidos, lembre-se de não revelar informação pessoal, pois esta pode ser usada para acederem aos seus dispositivos e contas eletrónicas.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Comportamento Social

Deve estar ter em consideração um conjunto de medidas para se proteger quando viaja:

- Utilize uma VPN quando navega na Internet, especialmente quando usa informação pessoal e/ou sensível.
- Leia e siga atentamente as normas de segurança estabelecidas pela sua organização (ex. Políticas de segurança e de utilização de equipamentos, normas internas).
- Esteja ciente das leis locais. Procure informações sobre os controlos nos aeroportos e importação ou uso de cifra.
- Antes da viagem limpe a informação dos seus dispositivos eletrónicos (ex. computadores, smartphones, discos rígidos ou cartões de memória e dispositivos de armazenamento USB). Por precaução, estes equipamentos não devem conter qualquer informação para além da que será necessária durante a viagem.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Comportamento Social

(continuação)

- Tenha os seus equipamentos e arquivos sempre consigo. Mantenha-os por perto na cabine durante a viagem. Não os deixe no escritório ou no quarto do hotel (mesmo que seja dentro de um cofre).
- Se tiver que se separar dos seus equipamentos móveis, retire as baterias e cartões SIM e mantenha-os consigo.
- Não utilize dispositivos oferecidos (USB), pois podem conter vírus ou realizar ações inesperadas nos seus equipamentos. As *pen* USB, pelas suas múltiplas vulnerabilidades, são um método privilegiado de infeção de dispositivos eletrónicos.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Comportamento Social

(continuação)

- Não carregue os seus dispositivos nos terminais elétricos self-service. Alguns destes terminais podem ter sido concebidos ou estar comprometidos de forma a copiar documentos sem o seu conhecimento. Leve os seus carregadores e utilize apenas os seus equipamentos.

Por fim, lembre-se de se proteger dos olhares de desconhecidos, como indicado no seguinte vídeo.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Passaporte

Quando vai de viagem, seja ela de lazer ou trabalho, deve ter em consideração a sua "bagagem".

- Vai levar o seu computador portátil?
- O tablet, o smartphone?
- E o smartwatch?

Considere bem o que acha essencial levar consigo quando vai para fora.

Pense na informação que cada um destes dispositivos contém!

Considere se o risco de os perder ou serem comprometidos compensa.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Passaporte

Faça uma lista dos seus dispositivos antes de viajar e não leve consigo os que não são necessários, tenha atenção às redes às quais se liga, verifique se os softwares instalados dispositivos estão atualizados, não perca os dispositivos de vista e, sempre que possível, utilize uma VPN quando se liga à Internet fora de casa ou do seu local de trabalho.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Passaporte

Lembre-se de algumas medidas para se cuidar:

- Faça *backup* dos seus dados e deixe o *backup* num local seguro. Assim, poderá recuperar a sua informação em caso de perda, roubo ou apreensão do seu equipamento.
- Marque o seu equipamento com um sinal distintivo (ex. com um autocolante). Desta forma poderá garantir que não há nenhuma troca com outros equipamentos, especialmente durante o transporte. Considere também colocar um sinal nas capas e malas de transporte.

Índice | Glossário

Curso Segurança da Informação – Módulo 3
Exterior – Passaporte

(continuação)

- Em caso de inspeção ou apreensão por parte das autoridades, caso o equipamento pertença à sua entidade patronal ou contenha informação dessa entidade, informe-a imediatamente.
- Se for forçado pelas autoridades locais a fornecer palavras-chave ou criptografia, alerte também de imediato a sua entidade patronal.
- Quando voltar de viagem, analise o equipamento. Não ligue os dispositivos à rede da sua organização sem antes ter feito um teste com antivírus e antispyware.
- Proteja-se a si, proteja a sua informação e tenha uma viagem cibersegura.

Veja o vídeo seguinte.

Índice | Glossário

Curso Segurança da Informação – Módulo 3

Chegou ao final do módulo 3.

Clique no link para efetuar o questionário de avaliação do módulo 3.

Índice | Glossário

Curso Segurança da Informação – Questionário Final

Chegou ao final do Curso.

Questionário Final

Clique no link para efetuar o questionário de avaliação final do Curso.

Índice | Glossário

Curso Segurança da Informação – Questionário Final

Questionário de Satisfação

Clique no link para efetuar o questionário de satisfação do Curso.

Índice | Glossário

Curso Segurança da Informação – Glossário

Glossário

Aqui pode consultar o Glossário do CNCS disponibilizado para este Curso.

Alguns termos mais importantes, podem ser consultados nas páginas seguintes.

Pode também consultar o Glossário da APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), um pouco mais completo.

Índice | Glossário

Curso Segurança da Informação – Glossário

AMEAÇA

Causa potencial de incidente indesejável que pode resultar em dano para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou deliberadas (com dolo) e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque.

ATAQUE

Qualquer tipo de atividade maliciosa que tenta coletar, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si.

Índice | Glossário

Curso Segurança da Informação – Glossário

BACKUP

Qualificativo de um processo, técnica ou equipamento usado para ajudar a recuperar dados perdidos ou destruídos ou para manter um sistema em funcionamento.

No contexto do *software* usado para realizar a salvaguarda de ficheiros (*software* de salvaguarda), obtemos as chamadas "cópias de segurança" (*backup copies*). No contexto de equipamento que permita redundância, temos por exemplo "fontes de alimentação de reserva" (*backup power supplies*) ou mesmo "discos de reserva" (*backup disks*).

Índice | Glossário

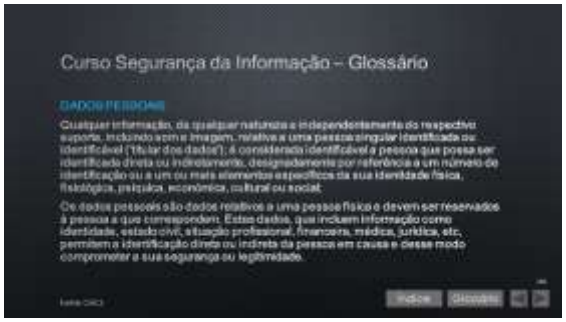

Curso Segurança da Informação – Glossário
BLUETOOTH
Tecnologia normalizada de ligação via rádio, com baixa potência de transmissão e de pequeno alcance, utilizando um sistema de mudança aleatória de frequência de transmissão, que permite o estabelecimento automático de ligação, sem fios ou cabos, de vários aparelhos eletrónicos (telemóveis, assistentes digitais pessoais (PDA), computadores, etc.) situados a pequena distância uns dos outros, constituindo assim uma pequena rede local sem fios.
Índice
Glossário


Curso Segurança da Informação – Glossário
CHAVE CRIPTOGRÁFICA
Cadeia de bits que comanda as operações de um algoritmo criptográfico. O secretismo destas chaves garante, normalmente, a segurança da transformação (cifragem/decifragem), especialmente quando o algoritmo de transformação é, como desejável, público.
CIBERATAQUE
Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente.
Índice
Glossário


Curso Segurança da Informação – Glossário
CIBERESPAÇO
Ambiente complexo, de valores e interesses materializando uma área de responsabilidade coletiva, que resulta da interação entre pessoas, informação, sistemas de informação, equipamentos tecnológicos e redes digitais, incluindo a *Internet*.
Metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela *Internet*, onde as pessoas podem comunicar de diferentes maneiras, por exemplo, através de mensagens eletrónicas, em salas de conversa ou em fóruns de discussão.
Índice
Glossário


Curso Segurança da Informação – Glossário
CIBERSEGURANÇA
Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem.
CIFRA
Algoritmo de complexidade variável que permite a transformação de um texto claro num texto ilegível, inviabilizando a leitura do texto original por pessoas que desconheçam o algoritmo.
Índice
Glossário


Curso Segurança da Informação – Glossário
CRIPTOGRAFIA
Aplicação de algoritmos matemáticos que cifram a informação, entre uma origem e um destino, para garantir atributos de segurança: autenticação, confidencialidade, integridade e não repúdio.
Índice
Glossário


Curso Segurança da Informação – Glossário
DADOS PESSOAIS
Qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.
Os dados pessoais são dados relativos a uma pessoa física e devem ser reservados à pessoa a que correspondem. Estes dados, que incluem informação como identidade, estado civil, situação profissional, financeira, médica, jurídica, etc., permitem a identificação direta ou indireta da pessoa em causa e desse modo comprometer a sua segurança ou legitimidade.
Índice
Glossário


Curso Segurança da Informação – Glossário
DISPONIBILIDADE
Em tecnologias da informação e da comunicação, capacidade de uma unidade funcional permanecer em estado de realizar uma determinada função dentro de condições determinadas, num dado instante ou num dado intervalo de tempo, supondo que estão assegurados os necessários meios exteriores.
DOMÍNIO
Grupo de computadores e dispositivos de uma rede, em particular da *Internet*, que são administrados como uma unidade, com regras e procedimentos comuns, e que partilham um nome comum (nome do domínio).
Índice
Glossário


Curso Segurança da Informação – Glossário
ENDEREÇO IP
Endereço IP (*Internet Protocol address*) de 32 bits de um computador ou outro dispositivo ligado à Internet, representado habitualmente por uma notação decimal de quatro grupos de algarismos separados por pontos.
ENGENHARIA SOCIAL
Manipulação de pessoas para obtenção de acesso às redes e aos sistemas de informação como método para cometer cibercrimes. Técnicas utilizadas para obter informações importantes ou sigilosas através de ações que enganam ou exploram a confiança das pessoas.
Índice
Glossário


Curso Segurança da Informação – Glossário
FICHEIRO DE DADOS PESSOAIS
Qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.
FIREWALL
Em tecnologias da informação e da comunicação, sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados.
Índice
Glossário


Curso Segurança da Informação – Glossário
HARDWARE
Totalidade ou parte dos componentes físicos de um sistema de processamento de dados.
HIPERLIGAÇÃO
Referência de algum ponto de um hipertexto para um ponto do mesmo ou de outro documento; uma tal referência é normalmente especificada de uma forma diferenciada do resto do hipertexto (por exemplo, usando palavras sublinhadas).
Índice
Glossário

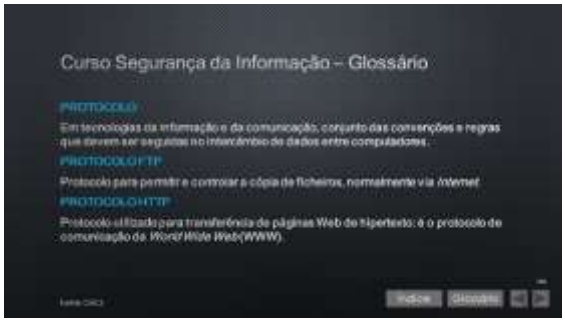

Curso Segurança da Informação – Glossário
HTML
Linguagem de marcação de hipertexto que possibilita a preparação de documentos com gráficos e hiperligações, para visualização na *World Wide Web* (WWW) ou em sistemas compatíveis.
IDENTIDADE DIGITAL
É a nossa presença no mundo digital.
INTEGRIDADE
Garantia de que os dados ou a informação não sejam alterados de modo não autorizado.
Índice
Glossário


Curso Segurança da Informação – Glossário
INTERNET
Rede de área alargada que é uma confederação de redes de computadores das universidades e de centros de pesquisa, do Governo, do comércio e da indústria, com base no protocolo TCP/IP. Proporciona acesso a sítios *Web*, correio eletrónico, bases de dados, fóruns de discussão, etc.
INTRANET
Rede corporativa baseada no protocolo TCP/IP e acessível apenas aos membros ou colaboradores de uma organização, ou a outros desde que autorizados.
Índice
Glossário


Curso Segurança da Informação – Glossário
PALAVRA-PASSE
Sequência de caracteres ou palavras que um sujeito apresenta a um sistema, como informação de autenticação.
PHISHING
Envio aos internautas de mensagens de correio eletrónico, com a aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios *Web* que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes.
Índice
Glossário


Curso Segurança da Informação – Glossário
PIRATA INFORMÁTICO (HACKER)
Pessoa que explora as falhas de segurança de um sistema com o intuito de violar a sua inviolabilidade, destruindo ou alterando a informação aí residente, ou ainda de copiar fraudulentamente os seus ficheiros.
POLÍTICA DE INFORMAÇÃO
Conjunto de orientações ou diretrizes relativas à utilização ou divulgação de informação, tais como as respeitantes à privacidade, aos direitos de cópia e à propriedade intelectual. A sua aplicação ao meio digital coloca novos desafios, tanto ao nível da redefinição de política como da sua aplicabilidade e do seu controlo.
Índice
Glossário


Curso Segurança da Informação – Glossário
PONTO DE ACESSO À INTERNET
Zona de acesso público abrangida por um nó de uma rede de área local sem fios (WLAN) que fornece ligação à *Internet*.
PRIVACIDADE DE DADOS
Característica de segurança de um sistema de informação que permite definir quais os dados que podem, ou não, ser acedidos por terceiros.
PROTEÇÃO DE DADOS PESSOAIS
Implementação de medidas para proteger dados pessoais e sensíveis de acessos públicos não autorizados, e para controlar o fluxo desses dados.
Índice
Glossário

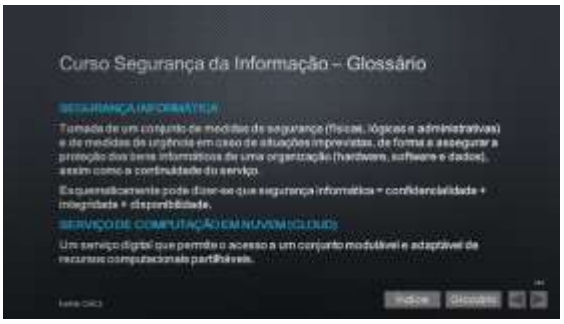

Curso Segurança da Informação – Glossário
PROTOCOLO
Em tecnologias da informação e da comunicação, conjunto das convenções e regras que devem ser seguidas no intercâmbio de dados entre computadores.
PROTOCOLO FTP
Protocolo para permitir e controlar a cópia de ficheiros, normalmente via *Internet*.
PROTOCOLO HTTP
Protocolo utilizado para transferência de páginas Web de hipertexto; é o protocolo de comunicação da *World Wide Web* (WWW).
Índice
Glossário

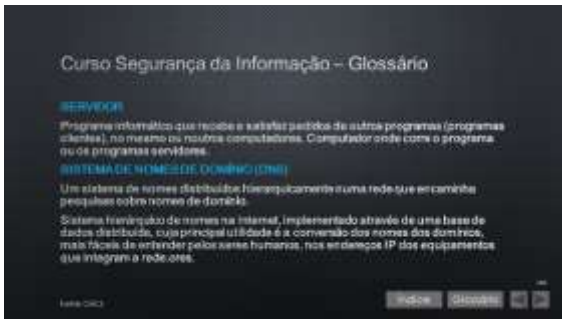

Curso Segurança da Informação – Glossário
PROTOCOLO HTTPS
Versão segura do protocolo HTTP. Foi criada pela Netscape Communications Corporation para fornecer autenticação e comunicação cifrada e é usada no comércio electrónico.
PROTOCOLO IP
Protocolo da família TCP/IP que controla a circulação de dados na Internet, fragmentando-os na origem sob a forma de pacotes de comprimento variável que incluem o endereço do destinatário, e reunindo-os na chegada.
Índice
Glossário


Curso Segurança da Informação – Glossário
RANSOMWARE
O Ransomware representa um tipo de malware (vírus, trojans, etc.) que infectam os sistemas informáticos dos utilizadores e manipulam o sistema de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos.
REDE
Conjunto formado por entidades e as suas interconexões. Em topologia de rede ou numa estrutura informática, as entidades interconectadas são pontos e as interconexões são linhas num esquema; numa rede de computadores, as entidades interconectadas são computadores ou equipamentos de comunicação de dados e as interconexões são ligações de dados.
Índice
Glossário


Curso Segurança da Informação – Glossário
REDE PRIVADA VIRTUAL (VPN)
Rede virtual de comunicação privada que utiliza uma infraestrutura pública de telecomunicações para transmitir dados que são protegidos devido à utilização de técnicas de cifragem ou de encapsulação.
Índice
Glossário


Curso Segurança da Informação – Glossário
ROUTER
Equipamento de interconexão, instalado num nó de uma rede de computadores, que se destina a otimizar a transmissão de dados, determinando qual o melhor caminho que eles devem seguir.
SEGURANÇA DA INFORMAÇÃO
Proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças.
Índice
Glossário


Curso Segurança da Informação – Glossário
SEGURANÇA INFORMÁTICA
Tomada de um conjunto de medidas de segurança (físicas, lógicas e administrativas) e de medidas de urgência em caso de situações imprevistas, de forma a assegurar a proteção dos bens informáticos de uma organização (hardware, software e dados), assim como a continuidade do serviço.
Esquematicamente pode dizer-se que segurança informática = confidencialidade + integridade + disponibilidade.
SERVIÇO DE COMPUTAÇÃO EM NUVEM (CLOUD)
Um serviço digital que permite o acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis.
Índice
Glossário

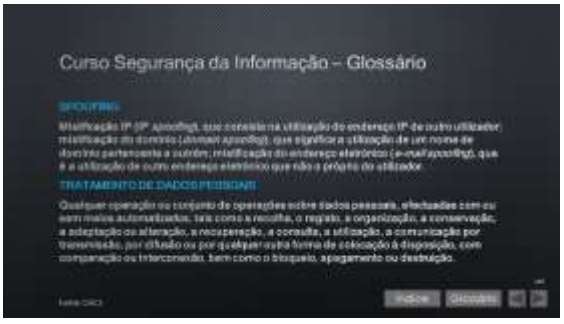

Curso Segurança da Informação – Glossário
SERVIDOR
Programa informático que recebe e satisfaz pedidos de outros programas (programas clientes), no mesmo ou noutros computadores. Computador onde corre o programa ou os programas servidores.
SISTEMA DE NOMES DE DOMÍNIO (DNS)
Um sistema de nomes distribuídos hierarquicamente numa rede que encaminha pesquisas sobre nomes de domínio.
Sistema hierárquico de nomes na Internet, implementado através de uma base de dados distribuída, cuja principal utilidade é a conversão dos nomes dos domínios, mais fáceis de entender pelos seres humanos, nos endereços IP dos equipamentos que integram a rede *ores*.
Índice
Glossário


Curso Segurança da Informação – Glossário
SISTEMA INFORMÁTICO
Significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado de dados.
Qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.
Índice
Glossário


Curso Segurança da Informação – Glossário
SISTEMA OPERATIVO
Software de base de um computador destinado a controlar a execução de programas e a comunicação entre dispositivos e programas, assegurando as operações de entrada-saída, a atribuição de recursos aos diferentes processos, o acesso às bibliotecas de programas e aos ficheiros, assim como a compatibilidade dos trabalhos.
Índice
Glossário


Curso Segurança da Informação – Glossário
SMART CARD
Cartão de circuitos integrados, normalmente com a dimensão de um cartão de crédito, provido de um microprocessador e de memória, capaz de armazenar e atualizar informação sobre o utilizador, permitindo-lhe por exemplo efetuar transações de natureza financeira.
SOFTWARE
Totalidade ou parte dos programas, dos procedimentos, das regras e da documentação associada, pertencentes a um sistema de processamento de informação.
Índice
Glossário


Curso Segurança da Informação – Glossário
SOFTWARE MALICIOSO
Programas informáticos destinados a perturbar, alterar ou destruir todos ou parte dos módulos indispensáveis ao bom funcionamento.
SPAM
Mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que, para além do incómodo provocado aos utilizadores do correio, podem comprometer o bom funcionamento dos sistemas informáticos.
Índice
Glossário


Curso Segurança da Informação – Glossário
SPOOFING
Modificação IP (IP *spoofing*), que consiste na utilização do endereço IP de outro utilizador; mistificação do domínio (*domain spoofing*), que significa a utilização de um nome de domínio pertencente a outrém; mistificação do endereço eletrónico (*e-mail spoofing*), que é a utilização de outro endereço eletrónico que não o próprio do utilizador.
TRATAMENTO DE DADOS PESSOAIS
Qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.
Índice
Glossário


Curso Segurança da Informação – Glossário
USABILIDADE
Nível de eficiência de um utilizador na realização de determinadas tarefas num produto, por exemplo um sítio Web ou uma aplicação. A usabilidade pode ser medida objetivamente através de erros de desempenho cometidos e da produtividade alcançada, e subjetivamente através da caracterização das preferências do utilizador em relação à interface.
VÍRUS
Classe de software malicioso que tem a capacidade de se autoreplicar e "infetar" partes do sistema operativo ou de outros programas, com o intuito de causar a perda ou alteração da informação.
Índice
Glossário


Curso Segurança da Informação – Glossário
VOIP
Tecnologia através da qual as informações de voz são transmitidas via protocolo IP.
VULNERABILIDADE
Insuficiência, seja de que natureza for, que possa ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional.
Fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, concepção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele.
Índice
Glossário


Curso Segurança da Informação – Glossário
WI-FI
Abreviatura de "*wireless fidelity*", termo usado para designar determinados tipos de redes locais sem fios.
Índice
Glossário


Curso Segurança da Informação – Vídeos
– Módulo 1
Vídeos
Recursos
Índice
Glossário


Curso Segurança da Informação – Vídeos
– Módulo 2
Vídeos
Recursos
Índice
Glossário


Curso Segurança da Informação – Vídeos
– Módulo 3
Vídeos
Recursos
Índice
Glossário


Curso Segurança da Informação
Obrigado pela sua participação.
Índice
Glossário

Questionário Módulo 1 - Casa

No final pode ver o resultado do seu questionário.
Não se esqueça de enviar o questionário.

*Obrigatório

1. **1.Qual das seguintes passwords é mais forte?** *
   Marcar apenas uma oval.
   - ◯ I_love_you
   - ◯ Maria
   - ◯ !L0veY0u2
   - ◯ Est0uaFrequentar0M0dul0DeC!berh!g!ene1

2. **2. O que é a identidade digital?** *
   Marcar apenas uma oval.
   - ◯ A palavra-passe
   - ◯ A informação que colocamos online
   - ◯ O conjunto de dados que nos identificam e permitem que nos reconheçam no mundo digital
   - ◯ As credenciais de acesso a plataformas digitais

3. **3. Quando tem visitas em casa e pretende dar-lhes acesso à sua rede Wi-Fi deve:** *
   Marcar apenas uma oval.
   - ◯ Fornecer a password da rede Wi-Fi
   - ◯ Criar uma rede Wi-Fi "guest" para as suas visitas acederem
   - ◯ Desligar a password para facilitar o acesso às visitas
   - ◯ Dar-lhes uma password errada

4. **4. Como é que a VPN protege a sua privacidade?** *
   Marcar apenas uma oval.
   - ◯ Faz gestão das passwords
   - ◯ Bloqueia tráfego malicioso
   - ◯ Faz backup dos seus ficheiros
   - ◯ Cifra o seu tráfego para que não seja visivel por terceiros

Pare de preencher este formulário.

Parabéns pode agora passar ao Módulo 2

Questionário Módulo 2 - Trabalho

No final pode ver o resultado do seu questionário.
Não se esqueça de enviar o questionário.

*Obrigatório

1. **1. Idealmente, com que periodicidade deve alterar a sua password?** *
   Marcar apenas uma oval.
   - ◯ Nunca, a minha password é forte
   - ◯ Só quando for vítima de um ciberataque
   - ◯ Com alguma regularidade e conforme a minha atividade na Internet
   - ◯ Uma vez por ano

2. **2. O que deve ter em atenção quando escolhe um antivirus?** *
   Marcar apenas uma oval.
   - ◯ A taxa de deteção de falhas de segurança e a possibilidade de atuar em vários dispositivos
   - ◯ O preço
   - ◯ A gratuitidade
   - ◯ A taxa de intrusão e a possibilidade de utilização em smartphones

3. **3. O que é o Phishing?** *
   Marcar apenas uma oval.
   - ◯ Ir à pesca
   - ◯ E-mails de publicidade
   - ◯ Uma ferramenta para consultar notícias na Internet
   - ◯ E-mails fraudulentos com o objectivo de recolher informações da vítima para benefício do criminoso

4. **4. Como pode verificar se uma página web está segura de modo a garantir a confidencialidade?** *
   Marcar apenas uma oval.
   - ◯ Deve iniciar com "https://..."
   - ◯ Deve iniciar com "www...."
   - ◯ Deve iniciar com "httpx://...."
   - ◯ Deve iniciar com "http://..."

5. **5. Como prevenir a perda das suas informações após um ataque de Ransomware?** *
   Marcar apenas uma oval.
   - ◯ Bloquear os pop-ups
   - ◯ Fazer backups com alguma regularidade num dispositivo de armazenamento externo
   - ◯ Guardar os ficheiros em várias pastas no seu computador
   - ◯ Basta usar um antivírus

Parabéns, pode agora passar ao Módulo 3

Questionário Módulo 3 - Exterior

No final pode ver o resultado do seu questionário.
Não se esqueça de enviar o questionário.
O Link de acesso ao Questionário Final é-lhe fornecido no final deste questionário.

*Obrigatório

1. **1.Quando está fora de casa ou do escritório e precisa de aceder à Internet, como deve fazer?** *
   Marcar apenas uma oval.
   - ◯ Acedo a redes Wi-Fi públicas (ex. cafés, hotéis, aeroportos)
   - ◯ Acedo à Internet utilizando as redes "Free"
   - ◯ Acedo à Internet através de uma VPN
   - ◯ Acedo à Internet Wi-Fi paga dos locais (com password)

2. **2. Quais os cuidados mais importantes a ter quando viaja com os seus dispositivos?** *
   Marcar apenas uma oval.
   - ◯ Levar mochilas adequadas para não os danificar
   - ◯ Instalar um antivírus
   - ◯ Não levar mais do que um dispositivo comigo
   - ◯ Usar sempre uma VPN quando aceder a redes Wi-Fi e nunca perder os meus dispositivos de vista

3. **3. Antes de viajar, qual destes cuidados com os seus dispositivos é mais importante?** *
   Marcar apenas uma oval.
   - ◯ Preparar uma refeição para a viagem
   - ◯ Fazer backups dos conteúdos do meu equipamento eletrónico
   - ◯ Adquirir um computador novo
   - ◯ Deixar as informações importantes e passwords com os colegas de trabalho

4. **4. Durante a viagem, o que deve fazer se não puder transportar consigo os seus dispositivos eletrónicos?** *
   Marcar apenas uma oval.
   - ◯ Guardo no cofre do hotel
   - ◯ Guardo no cacifo do aeroporto
   - ◯ Retiro as baterias e cartões SIM e mantenho-os comigo
   - ◯ Faço um backup de segurança

5. **5. Quando volta de viagem, idealmente o que deve fazer?** *

Marcar apenas uma oval.

- ◯ Atualizar os sistemas operativos
- ◯ Fazer backups
- ◯ Inspecionar os equipamentos antes de os ligar a outros dispositivos
- ◯ Instalar um antivírus

Pare de preencher este formulário.

Parabéns chegou ao final do questionário, pode agora fazer o questionário final.

https://drive.google.com/open?id=1vEay_ILH35Wu9K_LtzOu_edY5bfSykNDbg6pWi91Le4

Questionário Final

No final pode ver o resultado do seu questionário.
Não se esqueça de enviar o questionário.

*Obrigatório

1. **1. Qual das seguintes palavras-passe escolheria para aceder ao seu correio eletrónico?** *
   Marcar apenas uma oval.

   - ◯ Amo-te
   - ◯ qwerty
   - ◯ SapatoscomChantilly32%
   - ◯ 210497400

Ontem, quando cheguei a casa fui para o escritório e liguei o meu computador pessoal. Liguei-me à rede interna sem fios (Wi-Fi), acedi ao meu email pessoal introduzindo o nome de utilizador (username) e a palavra-passe (password) e verifiquei se tinha emails por ler na caixa de entrada. Nesse momento, verifiquei que tinha um email com a imagem do meu banco, mas desconhecia o remetente. O texto do email tinha erros ortográficos e uma ligação a dizer "clique aqui", onde cliquei e fui direcionado para uma página que me pedia o nome, número de conta bancária e palavra-passe.

2. **2. Que tipo de ciberataque é descrito no cenário descrito em cima, cujo objetivo é "pescar" os seus dados?** *
   Marcar apenas uma oval.

   - ◯ Bluetooth
   - ◯ Ransomware
   - ◯ Firewall
   - ◯ Phishing

3. **3. Se for vítima de Ransomware o que deve fazer?** *
   Marcar apenas uma oval.

   - ◯ Procurar ajuda em www.nomoreransom.org
   - ◯ Pagar a quantia que os atacantes pedem, para recuperar os dados e ficheiros
   - ◯ Ligar para o 112
   - ◯ Atualizar o anti-vírus

4. **4. Qual destes comportamentos é mais ciberseguro?** *
Marcar apenas uma oval.

- ◯ Quando me ausento do posto de trabalho, deixo o computador desbloqueado para que os meus colegas possam ver o que necessitam enquanto eu não estou lá.
- ◯ Antes de ir de viagem deixo as minhas palavras-passe escritas em post-its para que os meus colegas possam aceder ao meu computador, pois posso precisar de alguma informação enquanto estiver fora.
- ◯ Não atualizo o software e sistemas informáticos porque podem conter vírus.
- ◯ Quando me ausento do posto de trabalho bloqueio o computador. Não partilho as minhas palavras-passe com ninguém e atualizo o software dos meus equipamentos informáticos.

5. **5. Deve atualizar os sistemas informáticos para:** *
Marcar apenas uma oval.

- ◯ Continuar a usar os sistemas operativos sem pagar.
- ◯ Tornar o computador mais rápido.
- ◯ Corrigir problemas ou vulnerabilidades do sistema operativo e torná-lo mais seguro.
- ◯ Ficar com a versão que está na moda.

6. **6. Como pode proteger a confidencialidade dos seus dados pessoais?** *
Marcar apenas uma oval.

- ◯ Guardando os dados em diferentes pastas.
- ◯ Cifrando os dados.
- ◯ Colocando os dados na cloud.
- ◯ Fazendo backup dos dados.

7. **7. O que deve fazer para memorizar passwords?** *
Marcar apenas uma oval.

- ◯ Escrevê-las num papel.
- ◯ Utilizar um gestor de passwords.
- ◯ Utilizar sempre a mesma password.
- ◯ Partilhá-las com um colega.

8. **8. Qual destes softwares garante que os seus dados são cifrados enquanto navega na Internet?** *
Marcar apenas uma oval.

- ◯ Antivírus
- ◯ Firewall
- ◯ VPN (Virtual Private Network).
- ◯ Microsft Office.

9. **9. O que deve fazer se vir alguém que não pertence à sua organização dentro do seu local de trabalho?** *

Marcar apenas uma oval.

- ◯ Ajudar essa pessoa.
- ◯ Avisar a segurança local.
- ◯ Ignorar.
- ◯ Oferecer-lhe um café.

10. **10. Qual é o principal efeito de um ataque de ransomware?** *

Marcar apenas uma oval.

- ◯ Envio de Spam
- ◯ Computador lento
- ◯ Cifrar os dados das vítimas a troco de dinheiro
- ◯ Roubar fotografias das vítimas

Pare de preencher este formulário.

Parabéns chegou ao final do Curso

Muito obrigado pela sua colaboração

Questionário de satisfação

1. **Quais os motivos que o/a levaram a frequentar o curso?**

2. **Qual o interesse/utilidade dos conteúdos?**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada adequados	◯	◯	◯	◯	◯	Muito adequados

3. **Os conteúdos, métodos e meios audiovisuais utilizados foram adequados aos temas abordados?**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada adequados	◯	◯	◯	◯	◯	Muito adequados

4. **A carga horária do curso foi adequada?**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada adequada	◯	◯	◯	◯	◯	Muito adequada

5. **Facilidade de navegação e funcionalidades**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada adequado	◯	◯	◯	◯	◯	Muito adequado

6. **Interactividade com o utilizador?**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada adequada	◯	◯	◯	◯	◯	Muito adequada

7. **O curso correspondeu às suas expectativas?**
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Outra: _____

8. **Qual o nivel de clareza na apresentação dos temas?**
Marcar apenas uma oval.

	1	2	3	4	5	
Sem clareza	◯	◯	◯	◯	◯	Muita clareza

9. **Qual a utilidade prática deste curso?**
Marcar apenas uma oval.

- ◯ Desenvolvimento pessoal
- ◯ Desenvolvimento profissional
- ◯ Utilidade no trabalho diário
- ◯ Nenhuma
- ◯ Outra: _____

10. **Apreciação geral**
Marcar apenas uma oval.

	1	2	3	4	5	
Nada satisfeito	◯	◯	◯	◯	◯	Muito satisfeito

11. **Gostaria de ver outros temas desenvolvidos?**
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Outra: _____

12. **Se respondeu SIM na questão anterior quais os temas que gostaria de ver abordados num próximo curso?**

_____

_____

_____

_____

_____

13. **Deixe aqui sugestões/observações:**

_____

_____

_____

_____

_____

14. **Recomendaria este curso a outras pessoas?**
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Outra: _____

Obrigado pela sua participação. Os dados recolhidos serão tratados estatisticamente.

Anexo E – Questionário Final aos Hábitos e Conhecimentos sobre Segurança da Informação

Este questionário é constituído por 28 perguntas, das quais, 3 são sobre a caracterização do individuou, 4 sobre a formação sugerida no 1º questionário, 21 são acerca dos seus hábitos e conhecimentos sobre a segurança da informação. Todas as questões são de resposta obrigatória. Todo o questionário é anónimo, salvaguardado qualquer questão mais sensível. O questionário foi enviado aos indivíduos por *e-mail*, no qual se explicava o teor do Projeto *Security Awareness*. O texto que acompanhava o questionário era o seguinte:

> O Projeto *Security Awareness*, termina com o preenchimento de um questionário final - (disponível durante os próximos 2 dias)
> Pretende-se assim aferir, se de alguma forma os seus conhecimentos foram solidificados nesta área, quer tenha frequentado o Curso Segurança da Informação ou não.
> Todo este processo decorre de forma anónima, os dados que são solicitados ao cidadão, são apenas para tratamento estatístico, não permitindo a sua caracterização como indivíduo isolado.
> Face ao exposto, solicito uns breves 5 minutos da sua atenção para o preenchimento do referido questionário.
> Para que este projeto tenha alguma pertinência a nível de resultados, necessito de obter pelo menos 50 respostas ao questionário para obter dados conclusivos para o estudo em causa.
> Desde já o meu obrigado pela atenção. Este questionário é constituído por 24 perguntas, das quais,

Projeto Security Awareness - Fim do Projeto (MCIF)

*Obrigatório

Projeto Security Awareness - Fim do Projeto

A sua colaboração é muito importante na resposta a este questionário.

Este questionário é anónimo.
Pretende aferir os hábitos e conhecimentos sobre a segurança da informação do cidadão, após a frequência do Curso Segurança da Informação. Caso não tenha feito o curso, agradecemos que efetue o preenchimento do questionário novamente.

Responda às questões, com a máxima sinceridade refletindo as ações praticadas por si no dia a dia.

Desde já agradeço os 5 minutos da sua atenção para o preencher.

Dados estatisticos

1. **Qual o seu género?** * *Marcar apenas uma oval.*

   - ◯ Feminino
   - ◯ Masculino

2. **Qual a sua faixa etária?** *
   Marcar apenas uma oval.

   - ◯ Menos de 25
   - ◯ 26 a 35 anos
   - ◯ 36 a 45 anos
   - ◯ 46 a 55 anos
   - ◯ Mais de 56

3 **Quais as suas habilitações?** * *Marcar apenas uma oval.*

- ◯ 1º ciclo , 4ª classe
- ◯ 2º ciclo, 6º ano
- ◯ 3º ciclo, 9º ano
- ◯ Ensino Secundário, 12º ano
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento

4. **No 1º questionário do Projeto Security Awareness, (acerca dos hábitos e conhecimentos sobre a segurança da informação do cidadão) respondeu que pretendia fazer o Curso Segurança da Informação?** * *Marcar apenas uma oval.*

- ◯ Sim *Passe para a pergunta 5.*
- ◯ Não *Passe para a pergunta 6.*
- ◯ Não me lembro do que respondi *Passe para a pergunta 8.*

Curso Segurança da Informação

5. **Concluiu o Curso Segurança da Informação?** * *Marcar apenas uma oval.*

- ◯ Sim *Passe para a pergunta 8.*
- ◯ Não *Passe para a pergunta 6.*

Caso não tenha concluido o Curso Segurança da Informação

6. **Qual o motivo porque não concluiu o Curso?** * *Marcar apenas uma oval.*

- ◯ Falta de tempo
- ◯ Desinteresse pela matéria
- ◯ Outra: _____

7. **Procurou outra forma de adquirir mais conhecimentos sobre estas matérias?** * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Outra: _____

Questionário

Responda de acordo com os seus comportamentos habituais.

8. **Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?** * *Marcar apenas uma oval.*

   a. seja fácil de memorizar
   b. seja suficientemente grande
   c. tenha caracteres variados
   d. seja difícil de memorizar e tenha caracteres variados (com pelo menos 16 caracteres e sem nexo)

9. **Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?** * *Marcar apenas uma oval.*

   a. Borboleta65
   b. 210967000
   c. G0$t0DeGel@d0$29
   d. zxcvbn

10. **Com que frequência altera as suas palavras passe?** * *Marcar apenas uma oval.*

    a. Uma vez por mês
    b. Nunca
    c. Quando a palavra passe é descoberta por alguém
    d. Quando sou obrigado pelo fornecedor do serviço associado
    e. Sem prazo definido, quando entender que devo trocar

11 **Qual o método que utiliza para guardar ou memorizar as suas palavras passe?** * *Marcar apenas uma oval.*

    a. Guardo num papel num local seguro
    b. Guardo num ficheiro no disco do computador
    c. Utilizo um gestor de palavras passe com encriptação
    d. Guardo num post-it de fácil acesso
    e. Guardo no telemóvel
    f. Memorizo
    Outra: _____

12. **Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de email e de nos autenticar. Como procede em relação a este problema?** *
Marcar apenas uma oval.

- a. Utilizo uma palavra passe diferente para cada serviço
- b. Utilizo sempre a mesma palavra passe
- c. Utilizo a autenticação de outros serviços (Facebook, Google, etc)
- d. Utilizo um gestor de palavra passe que também tem a funcionalidade de gerador de palavras passe com um algoritmo aleatório.
- Outra: _____

13. **No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?** *
Marcar apenas uma oval.

- a. Fica desbloqueado
- b. Fica bloqueado com palavra passe, mas a minha colega tem conhecimento da palavra palavra passe
- c. Fica bloqueado com palavra passe
- d. Dependendo do tempo que me ausento, fica desbloqueado

14. **Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?** * *Marcar apenas uma oval.*

- a. Deixo o equipamento desbloqueado
- b. Deixo o equipamento bloqueado
- c. Deixo o equipamento bloqueado e utilizo o dispositivo com encriptação
- d. Não tenho smartphone ou tablet
- Outra: _____

15. **Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com as regras e políticas desse fornecedor de serviços, em relação ao tratamento dos seus dados pessoais. Qual a sua opinião?** * *Marcar apenas uma oval.*

- a. Apenas subscrevo serviços, após ler minuciosamente os termos da política de privacidade
- b. Não costumo ler os termos e políticas de privacidade, mas subscrevo o serviço
- c. Leio na diagonal e subscrevo os serviços
- d. Não leio e não subscrevo o serviço

16. **Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatários, qual a linha de preenchimento dos endereços que mais se adequa?** *
Marcar apenas uma oval.

- a. Para
- b. CC
- c. BCC
- d. Qualquer uma das anteriores

17. **Acede ao seu email pessoal/profissional em computadores públicos?** * *Marcar apenas uma oval.*

- a. Não acedo
- b. Acedo ao email pessoal
- c. Acedo ao email profissional
- d. Acedo ao email pessoal e profissional

18. **Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?** * *Marcar apenas uma oval.*

- a. Leio a mensagem, clico nos links e abro os anexos
- b. Leio a mensagem, mas não clico nos links e não abro os anexos
- c. Leio o assunto e verifico o endereço do remetente da mensagem e só depois abro a mensagem para ler o seu conteúdo, verifico os links antes de clicar e verifico se os anexos têm vírus antes de os abrir.
- d. Não abro a mensagem se o contato for suspeito

19 **Quando tem necessidade de preencher formulários online, o que tem em atenção?** *
Marcar apenas uma oval.

- a. Forneço os dados que me são pedidos mediante o fim a que se destinam
- b. Forneço os dados que me são pedidos mediante a garantia do tratamento dos dados posteriormente e o fim a que se destinam
- c. Só forneço dados pessoais se estiver clara a sua utilização, a cedência a terceiros, assim como a sua atualização e direito ao esquecimento
- d. Forneço os dados que me são pedidos

20. **Quando navega na internet sabe se existem dados que ficam guardados no computador localmente?** * *Marcar apenas uma oval.*

- a. Sim, as cookies, os ficheiros transferidos e o histórico de navegação
- b. Sim, mas se usar a navegação privada minimizo os dados que ficam guardados
- c. Não fica nada guardado no computador
- d. Sim, apenas as cookies
- e. Não sei responder

21. **Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?** * *Marcar apenas uma oval.*

- a. Sim
- b. Não

22 **Acede às suas contas de redes sociais em computadores públicos?** * *Marcar apenas uma oval.*

- a. Acedo
- b. Não acedo
- c. Não tenho contas de redes sociais

23. **Já foi alguma vez alvo de Phishing?** * *Marcar apenas uma oval.*

- a. Sim, já fui
- b. Não, nunca fui
- c. Não sei o que é phishing

24. **Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):** * *Marcar apenas uma oval.*

- a. Sim.
- b. Sim, por Ransomware
- c. Não
- d. Não sei o que é malware

25. **Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?** * *Marcar apenas uma oval.*

- a. Tenho um bloqueador de pop ups para estes casos
- b. Fecho de imediato as janelas que foram abertas
- c. Vejo o conteúdo das janelas e clico nos links se o conteúdo for fidedigno
- d. O meu navegador de internet pergunta se quero abrir a janela (pop-up)

26. **Utiliza um antivírus no seu computador?** * *Marcar apenas uma oval.*

- a. Sim
- b. Não
- c. Não sei o que é antivírus.

27. **Encontra uma Pen Drive USB no chão, o que faz de seguida?** * *Marcar apenas uma oval.*

- a. Entrego nos perdidos e achados
- b. Ligo ao meu computador para ver o que tem
- c. Procuro a ajuda de um colega mais experiente em informática
- d. Fico com a Pen Drive para mim
- Outra: _____

28 **Habitualmente procura estar informado sobre a atualidade do mundo informático?** * *Marcar apenas uma oval.*

- a. Sim, leio revistas e vejo programas de tv sobre a temática
- b. Sim, recebo emails temáticos
- c. Sim, mas apenas quando sou obrigado profissionalmente a frequentar cursos
- d. Sim, procuro informação quando necessito de fontes diversas (cursos, internet, revistas)
- e. Não, pois não tenho interesse pela área.

Chegou ao fim do questionário.

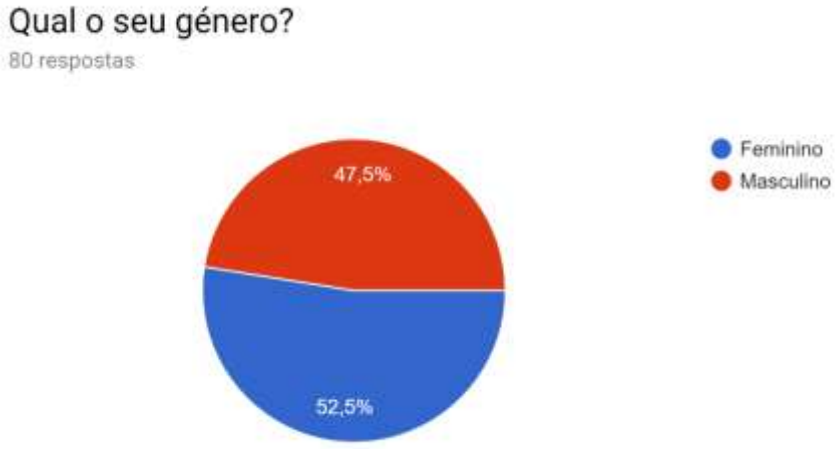
Pare de preencher este formulário.

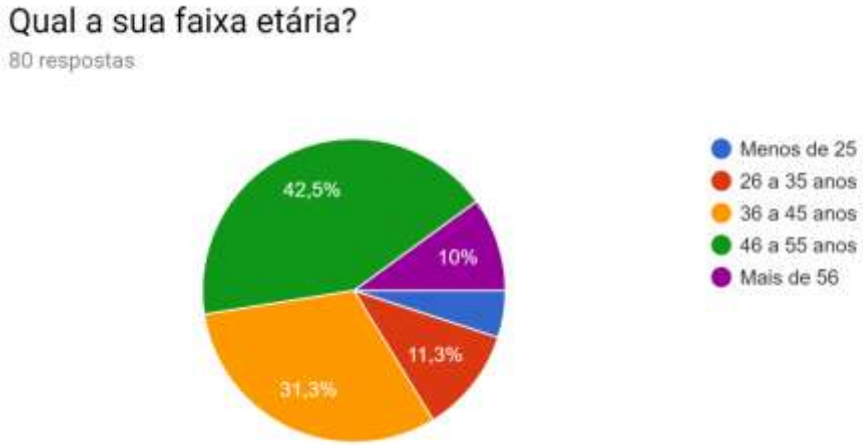
Obrigado pela sua participação.

Anexo F – Resultados do 1º Questionário

Resumo das respostas obtidas aos inquiridos.

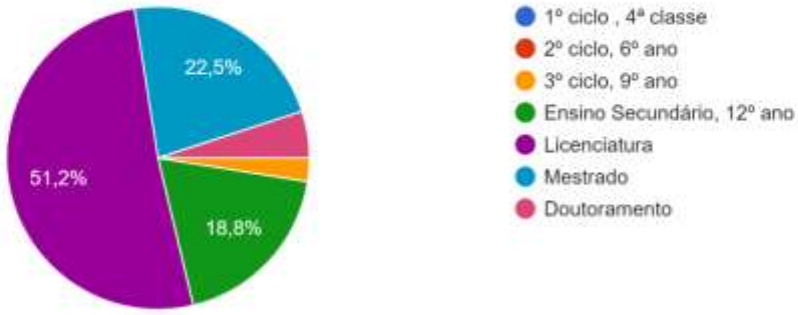
Dados Estatísticos





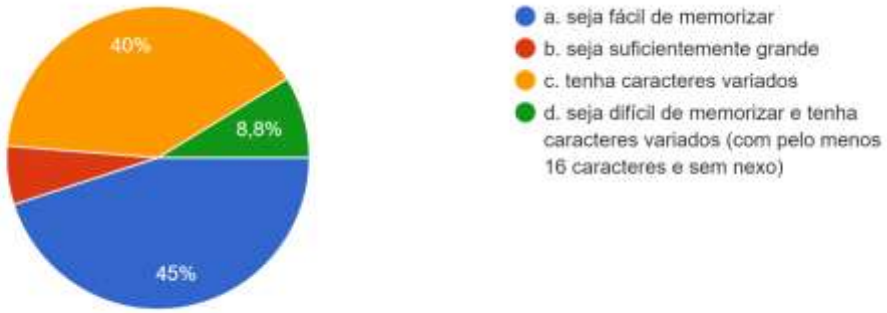
Quais as suas habilitações?

80 respostas



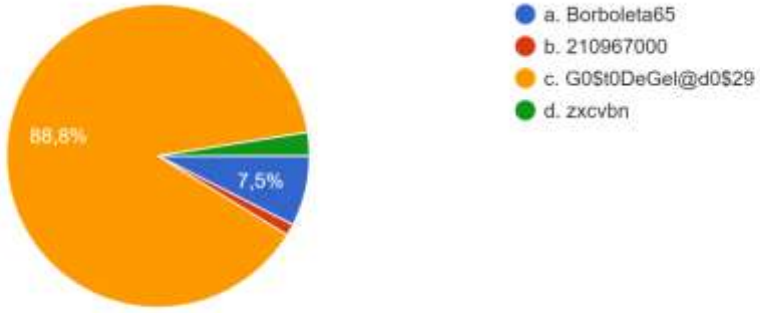
1. Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?

80 respostas



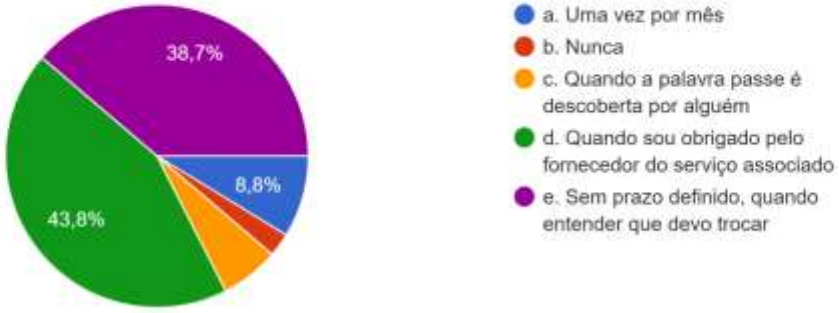
2. Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?

80 respostas



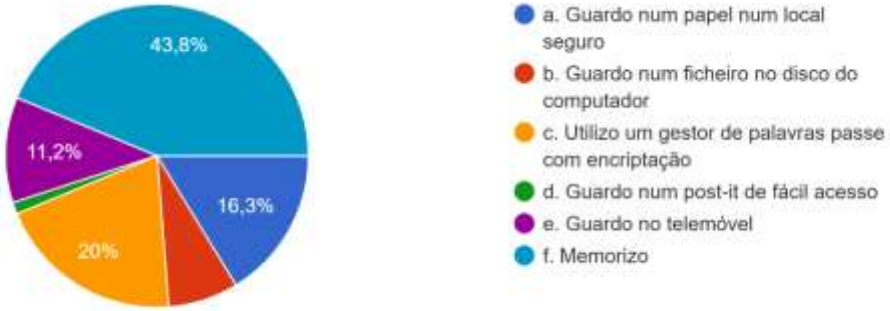
3. Com que frequência altera as suas palavras passe?

80 respostas



4. Qual o método que utiliza para guardar ou memorizar as suas palavras passe?

80 respostas

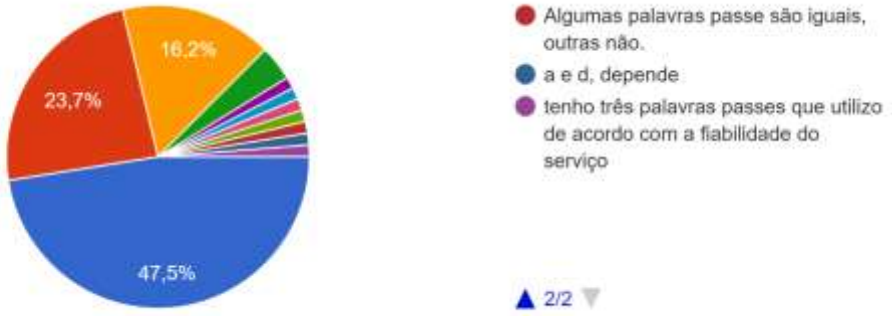


5. Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de emai... procede em relação a este problema?

80 respostas

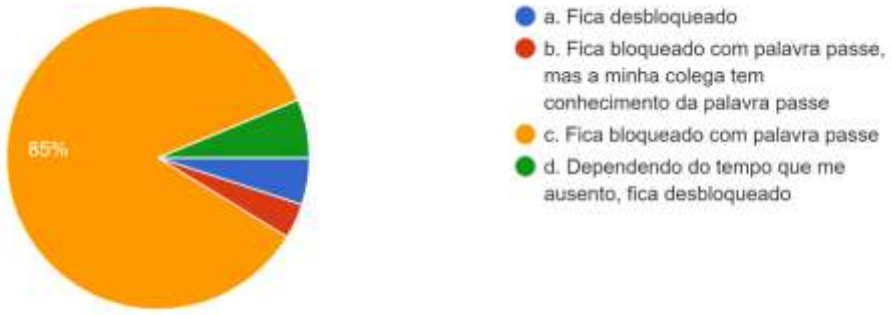
5. Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de emai... procede em relação a este problema?

80 respostas



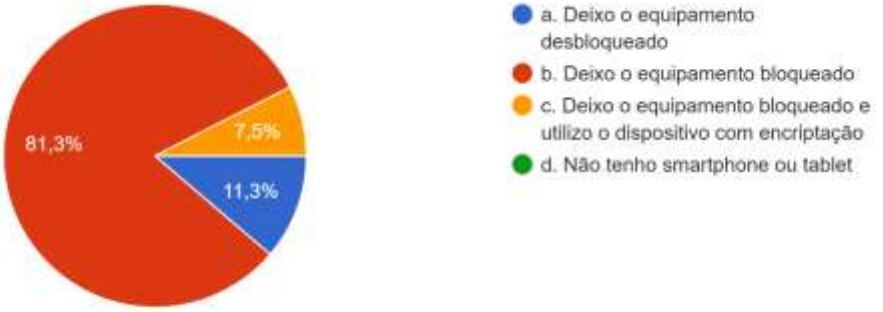
6. No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?

80 respostas



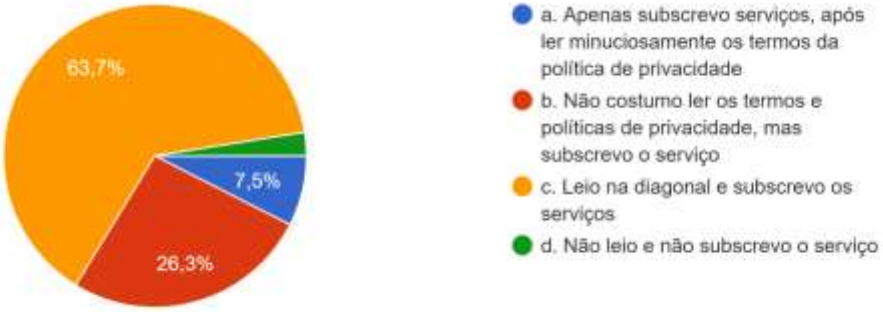
7. Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?

80 respostas



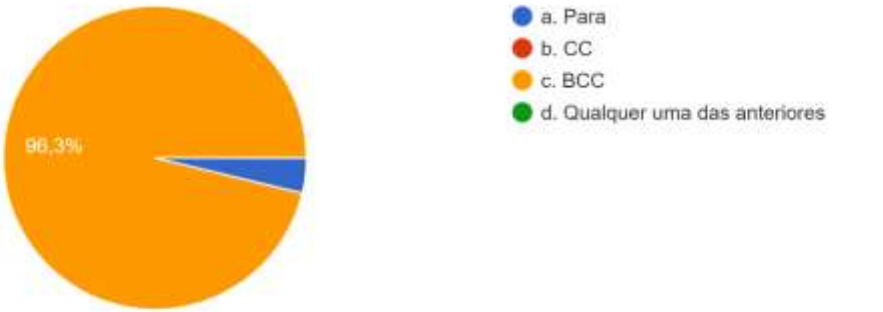
8. Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com as... dados pessoais. Qual a sua opinião?

80 respostas



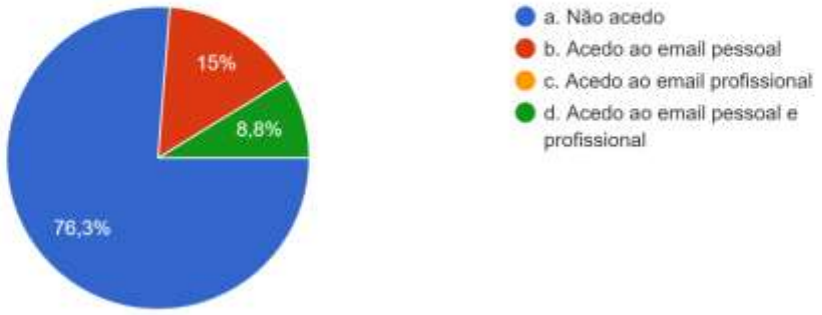
9. Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatári...to dos endereços que mais se adequa?

80 respostas



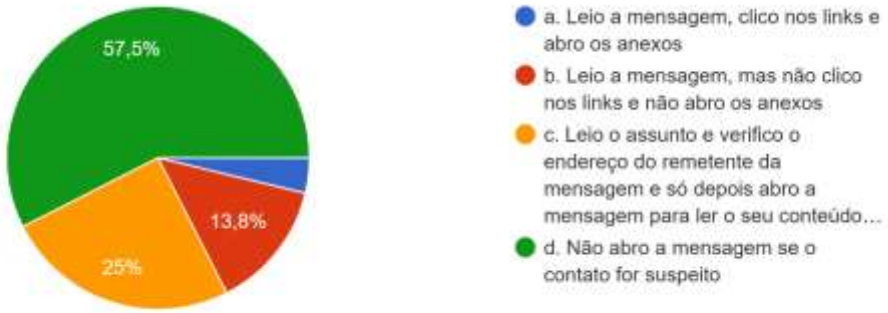
10. Acede ao seu email pessoal/profissional em computadores públicos?

80 respostas



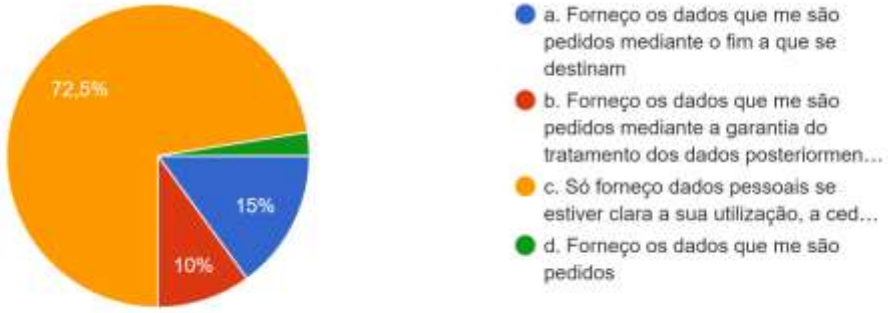
11. Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?

80 respostas



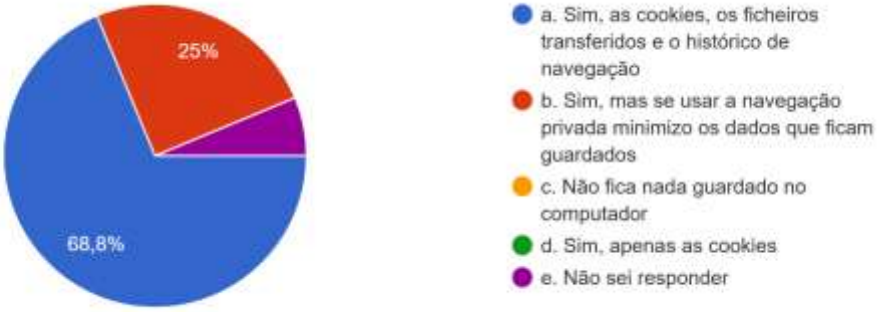
12. Quando tem necessidade de preencher formulários online, o que tem em atenção?

80 respostas



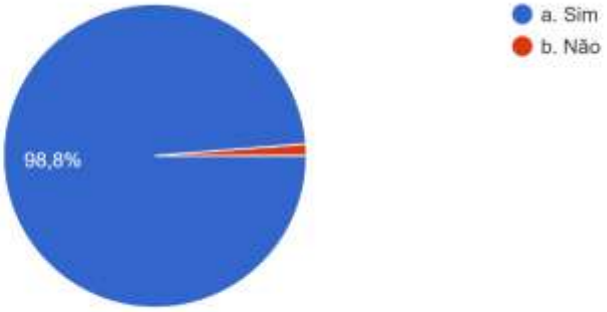
13. Quando navega na internet sabe se existem dados que ficam guardados no computador localmente?

80 respostas



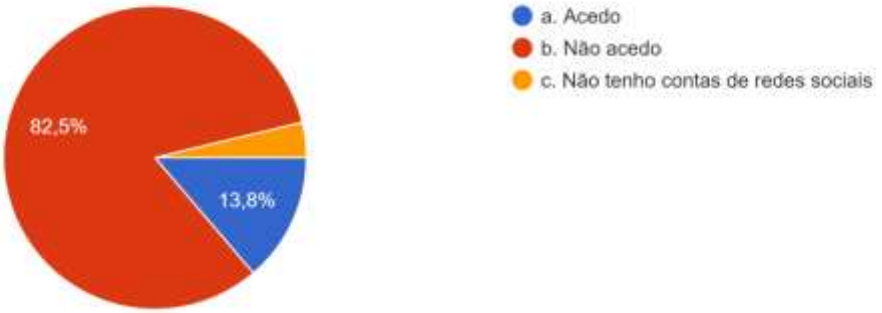
14. Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?

80 respostas



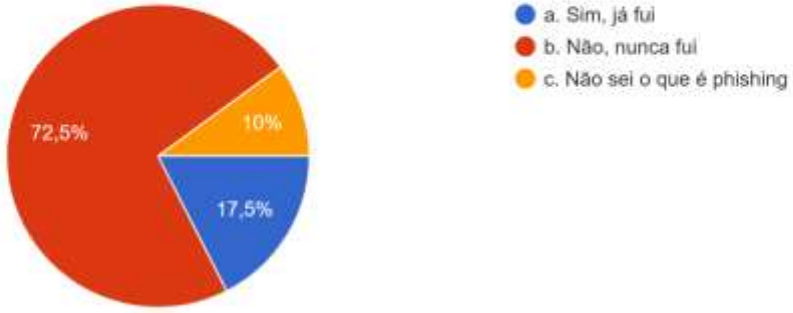
15. Acede às suas contas de redes sociais em computadores públicos?

80 respostas



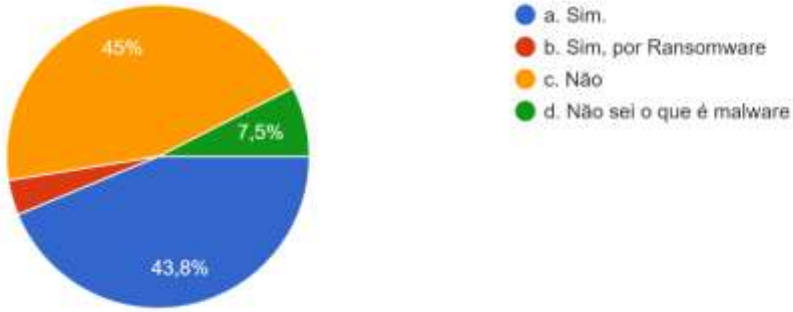
16. Já foi alguma vez alvo de Phishing?

80 respostas



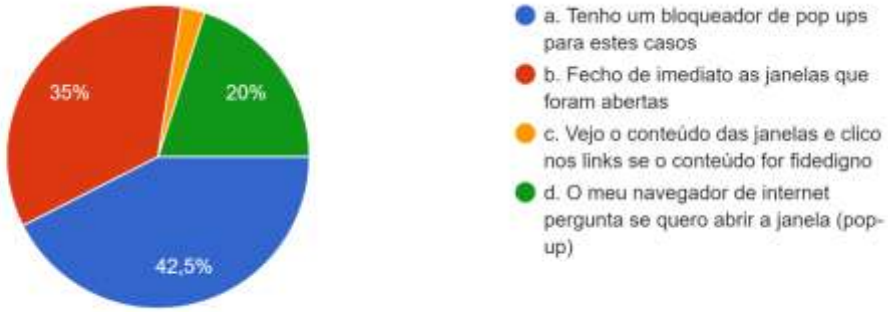
17. Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):

80 respostas



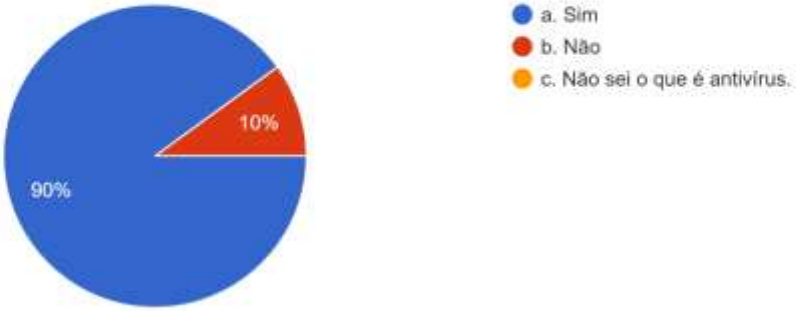
18. Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?

80 respostas



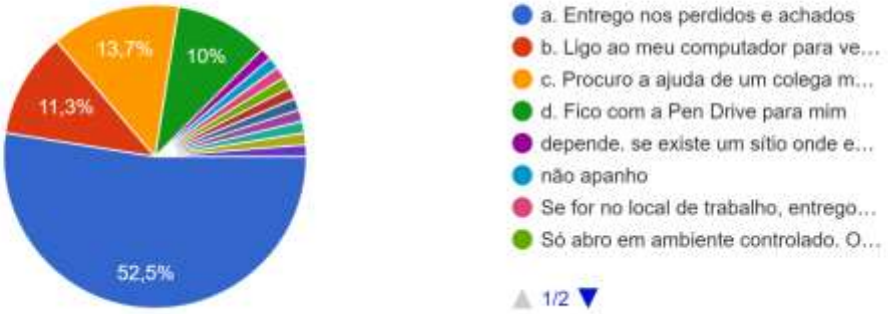
19. Utiliza um antivírus no seu computador?

80 respostas



20. Encontra uma Pen Drive USB no chão, o que faz de seguida?

80 respostas

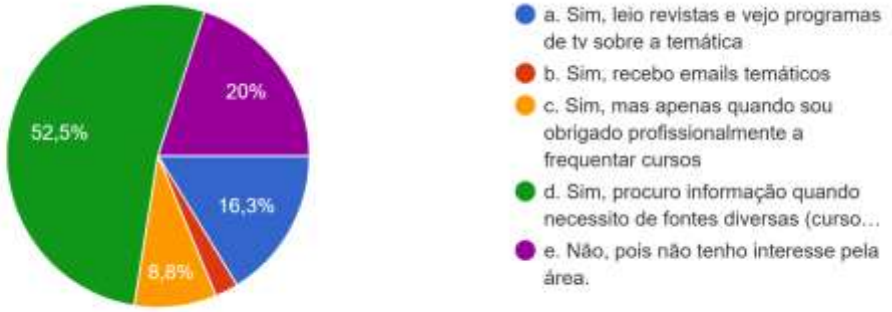


20. Encontra uma Pen Drive USB no chão, o que faz de seguida?

80 respostas

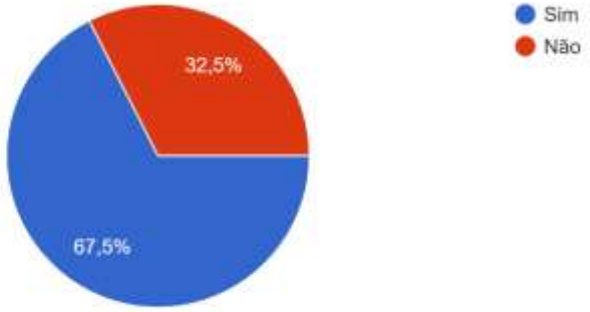
20. Habitualmente procura estar informado sobre a atualidade do mundo informático?

80 respostas



Aceita o desafio de frequentar um pequeno curso sobre segurança da informação, com a duração de apenas 1...estionários no final de cada módulo.

80 respostas

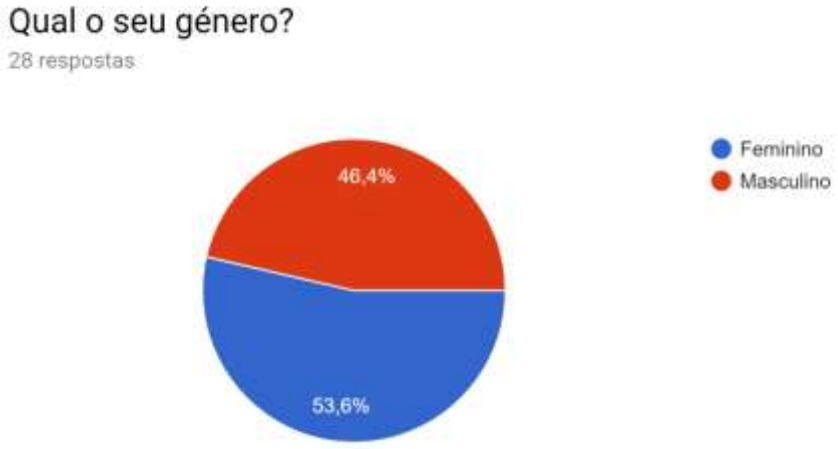


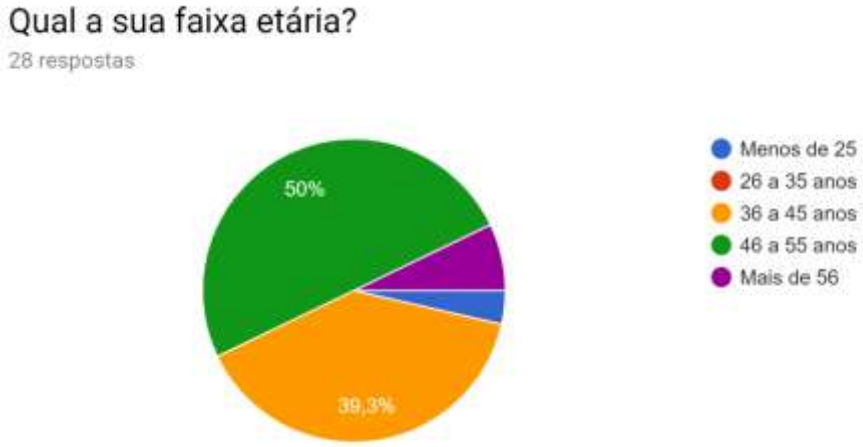
Nota: O resultado do questionário está disponível através de ficheiro *.csv,

Anexo G – Resultados do 2º Questionário

Resumo das respostas obtidas aos inquiridos.

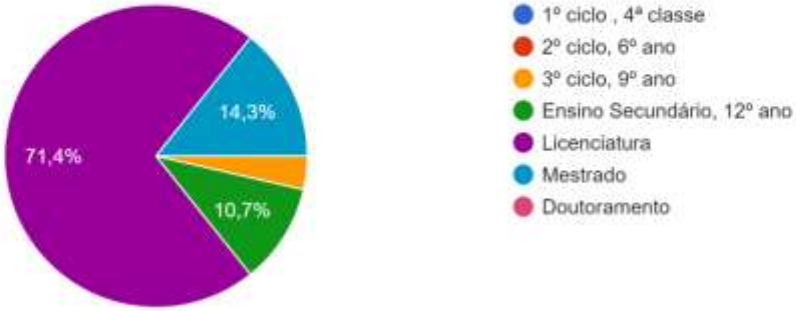
Dados Estatísticos





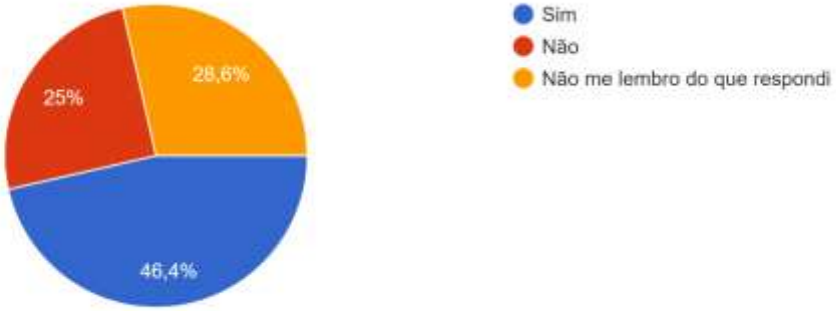
Quais as suas habilitações?

28 respostas



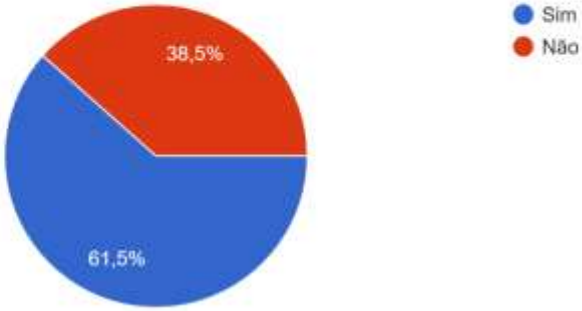
No 1º questionário do Projeto Security Awareness, (acerca dos hábitos e conhecimentos sobre a segurança da i...r o Curso Segurança da Informação?

28 respostas



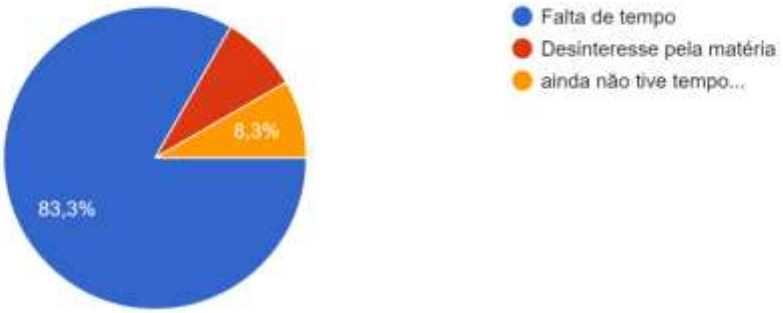
Concluiu o Curso Segurança da Informação?

13 respostas



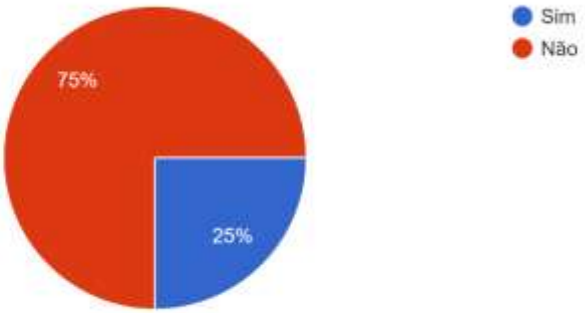
Qual o motivo porque não concluiu o Curso?

12 respostas



Procurou outra forma de adquirir mais conhecimentos sobre estas matérias?

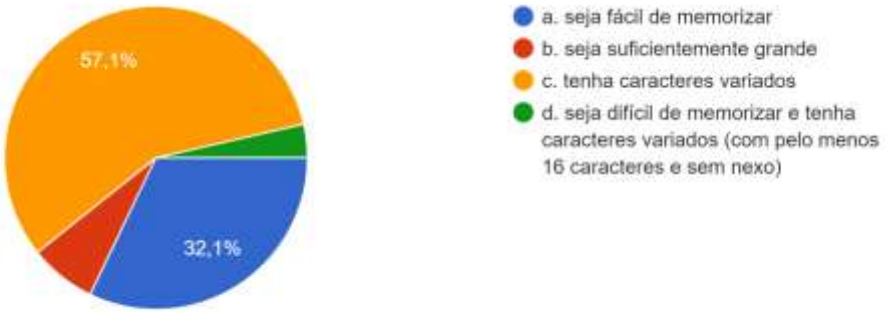
12 respostas



Questionário – Repetição

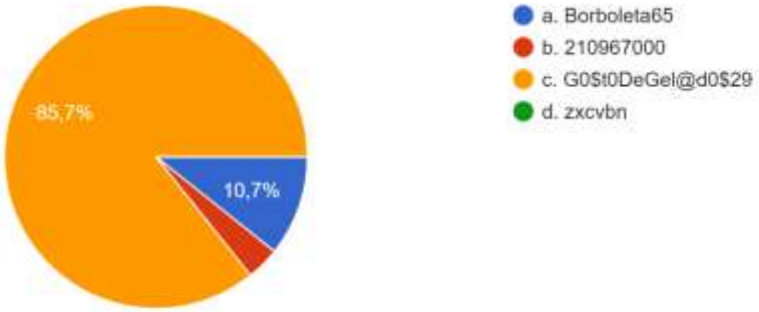
1. Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?

28 respostas



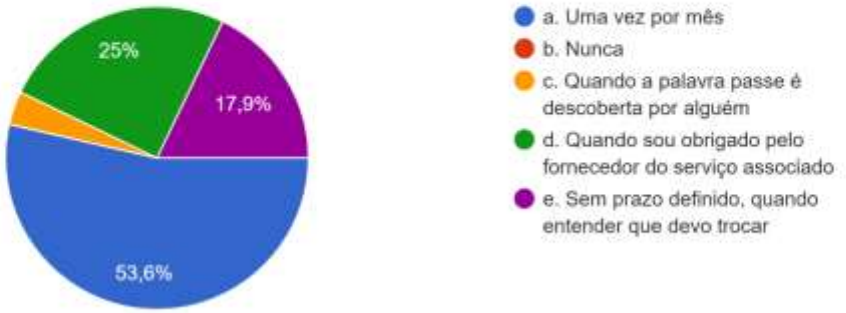
2. Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?

28 respostas



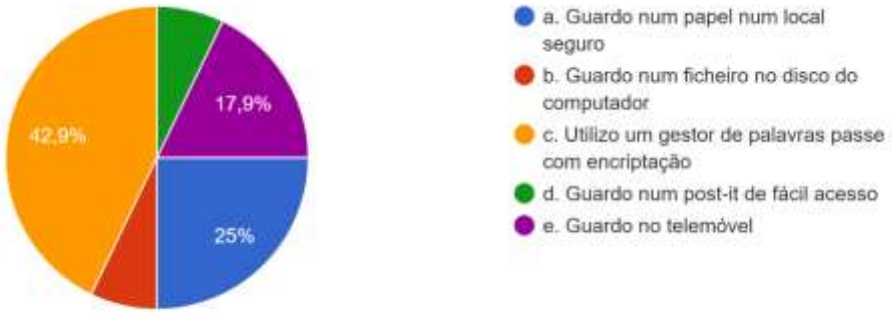
3. Com que frequência considera que deve alterar as suas palavras passe?

28 respostas



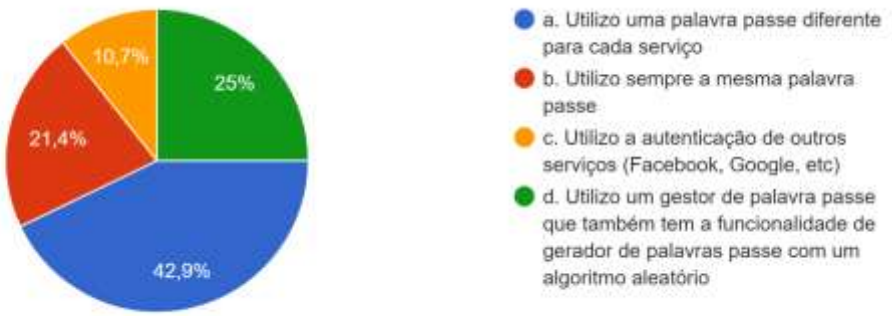
4. Qual o método que utiliza para guardar ou memorizar as suas palavras passe?

28 respostas



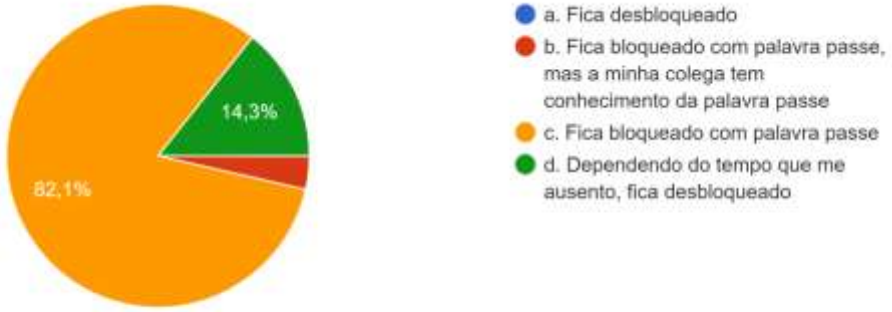
5. Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de emai... procede em relação a este problema?

28 respostas



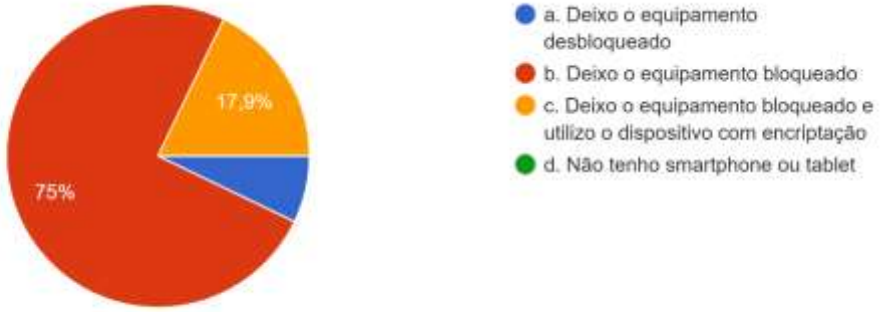
6. No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?

28 respostas



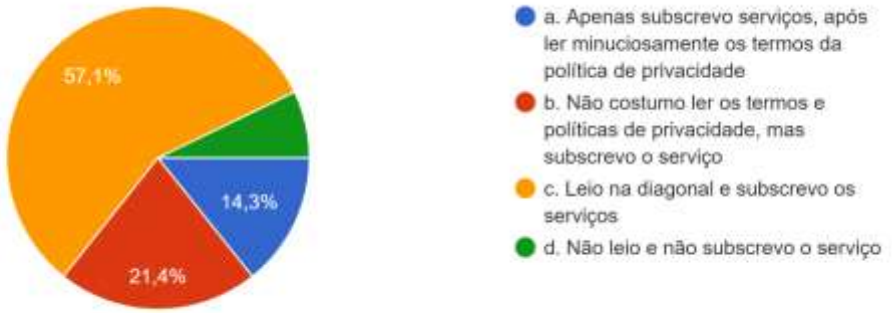
7. Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?

28 respostas



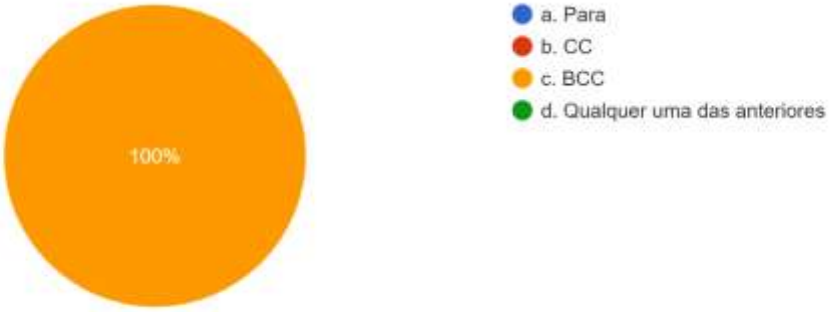
8. Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com a ... dados pessoais. Qual a sua opinião?

28 respostas



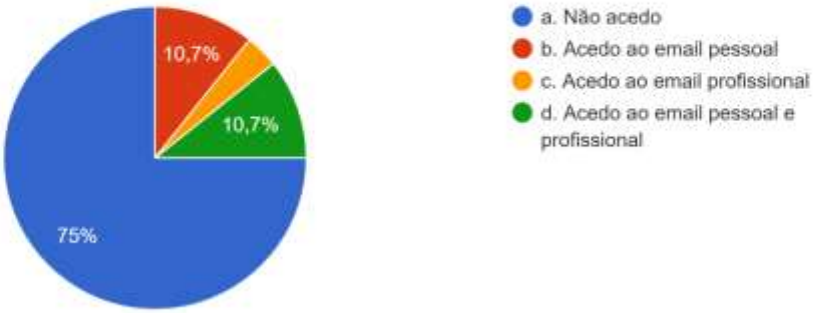
9. Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatári...to dos endereços que mais se adequa?

28 respostas



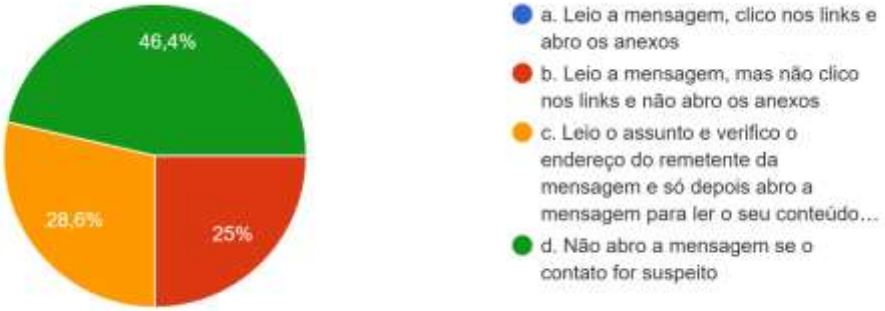
10. Acede ao seu email pessoal/profissional em computadores públicos?

28 respostas



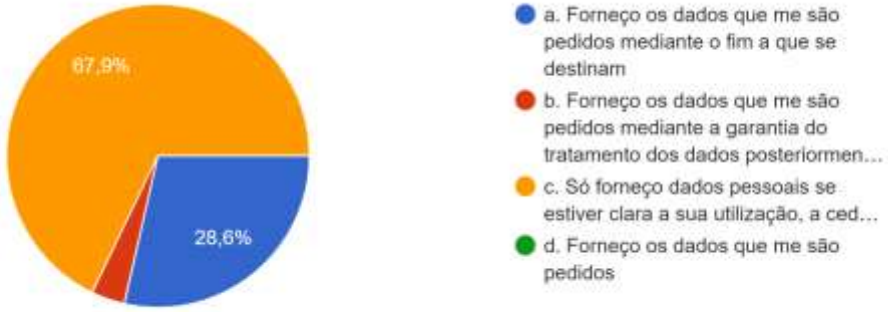
11. Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?

28 respostas



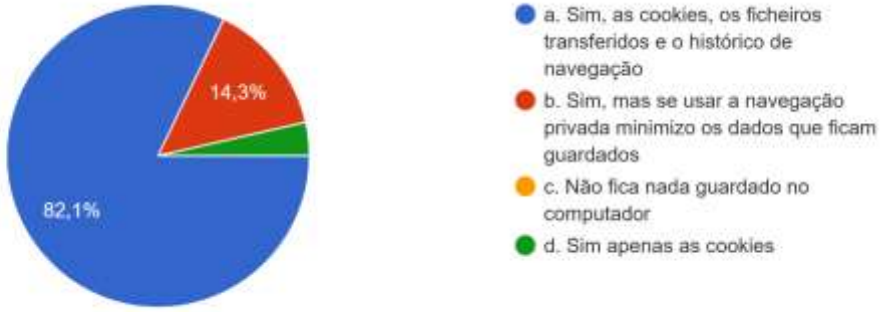
12. Quando tem necessidade de preencher formulários online, o que tem em atenção?

28 respostas



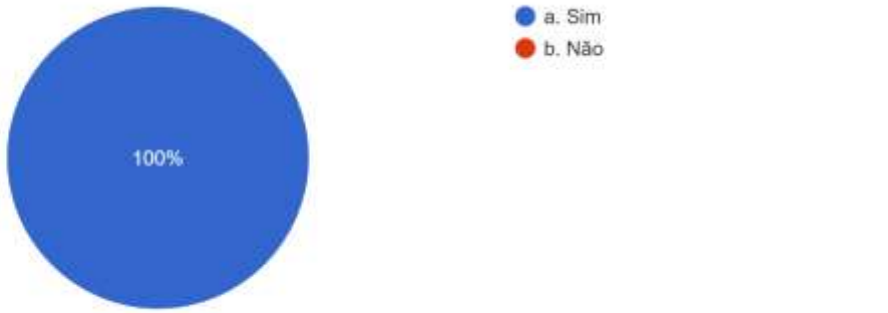
13. Quando navega na internet sabe que existem dados que ficam guardados no computador localmente?

28 respostas



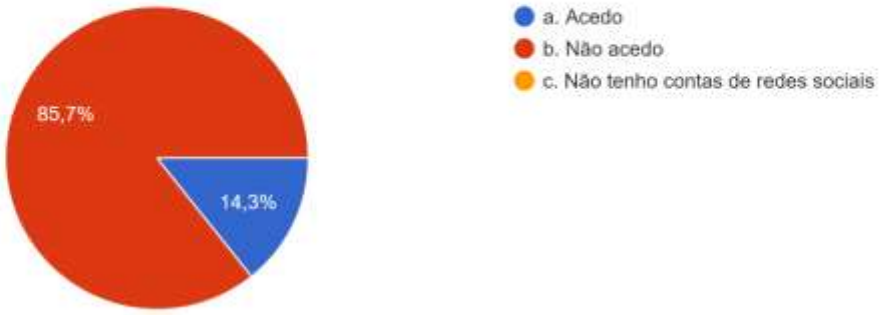
14. Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?

28 respostas



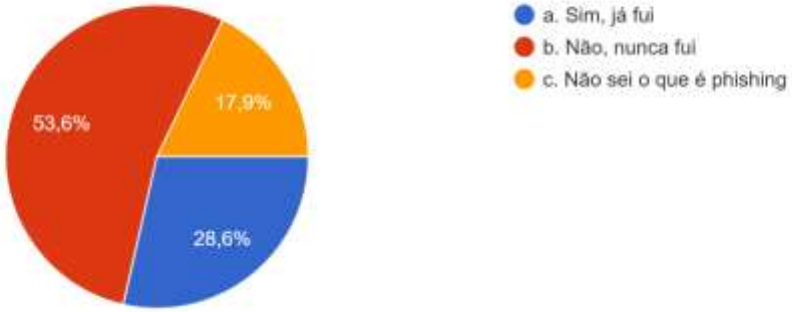
15. Acede às suas contas de redes sociais em computadores públicos?

28 respostas



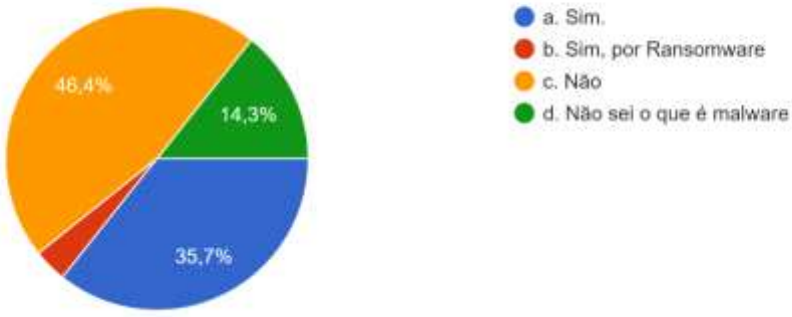
16. Já foi alguma vez alvo de Phishing?

28 respostas



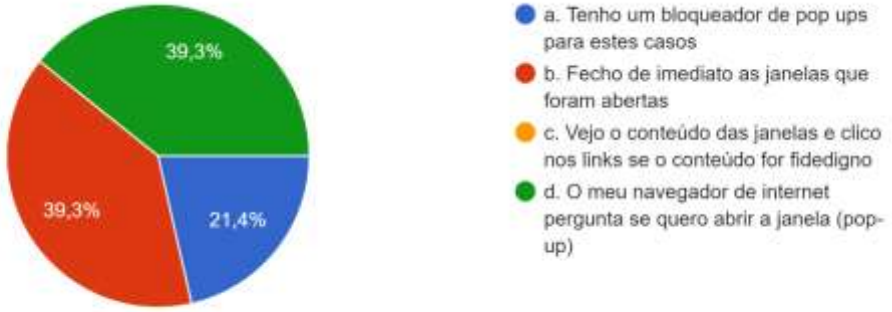
17. Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):

28 respostas



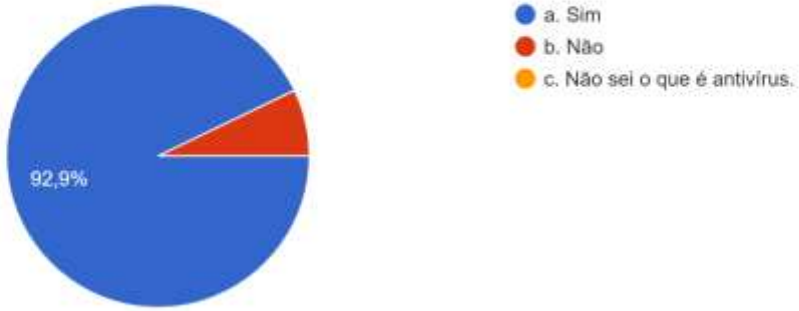
18. Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?

28 respostas



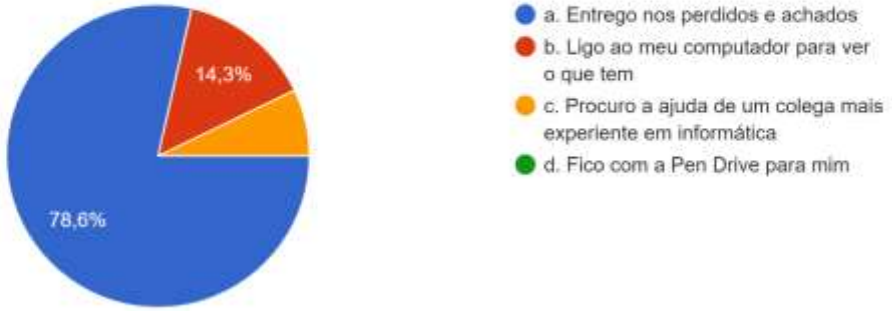
19. Utiliza um antivírus no seu computador?

28 respostas



20. Encontra uma Pen Drive USB no chão, o que faz de seguida?

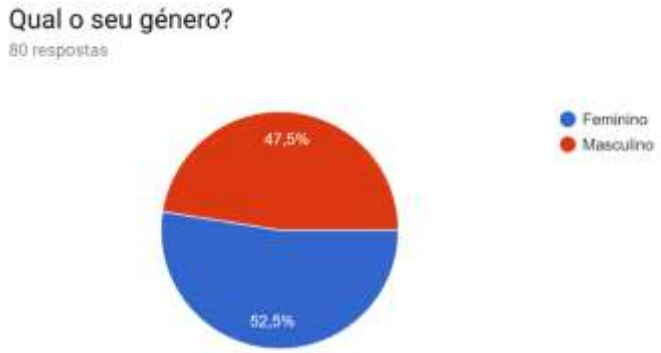
28 respostas



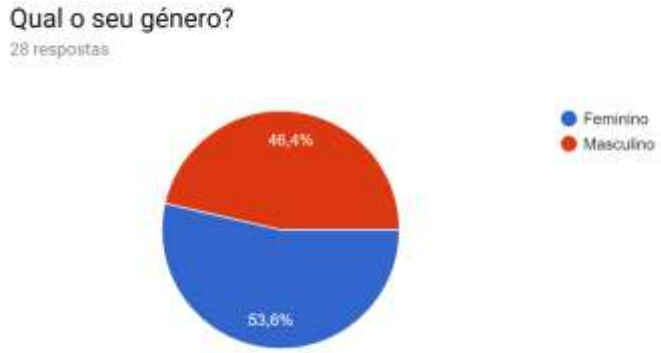
Nota: O resultado do questionário está disponível através de ficheiro *.csv,

Anexo H – Comparação de Respostas aos Questionários

1º Questionário



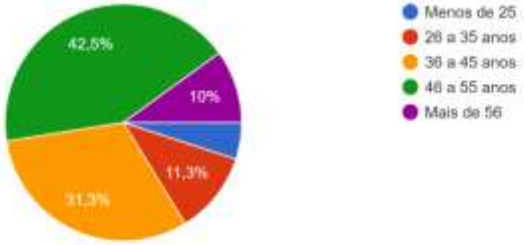
2º Questionário



1º Questionário

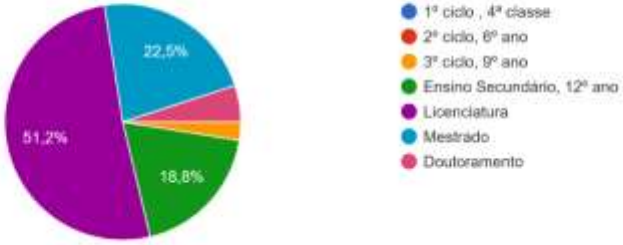
Qual a sua faixa etária?

80 respostas



Quais as suas habilitações?

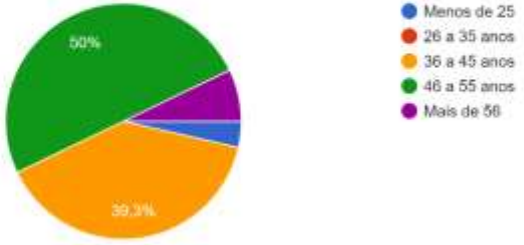
80 respostas



2º Questionário

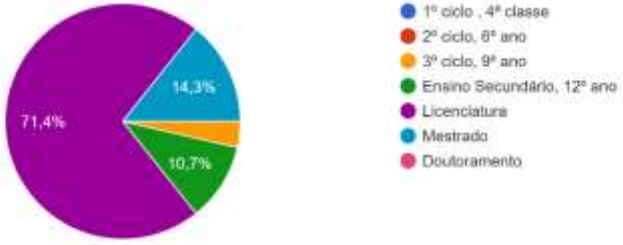
Qual a sua faixa etária?

28 respostas



Quais as suas habilitações?

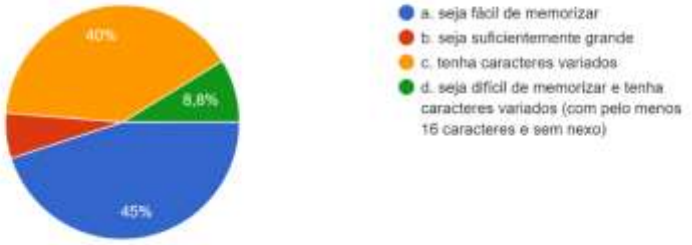
28 respostas



1º Questionário

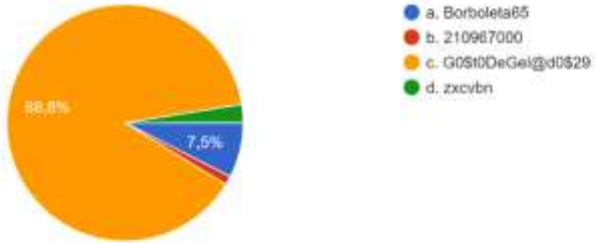
1. Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?

80 respostas



2. Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?

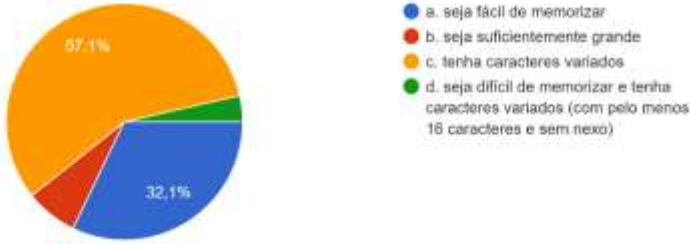
80 respostas



2º Questionário

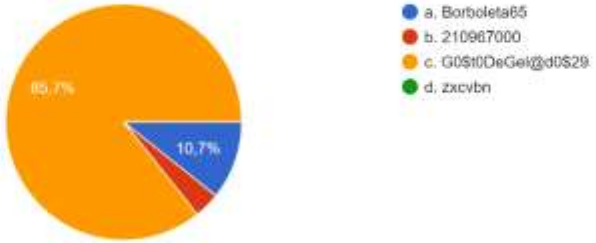
1. Quando tem necessidade de escolher uma palavra passe (password) o que considera mais importante na sua construção?

28 respostas



2. Dos exemplos seguintes escolha qual a palavra passe que acha mais segura?

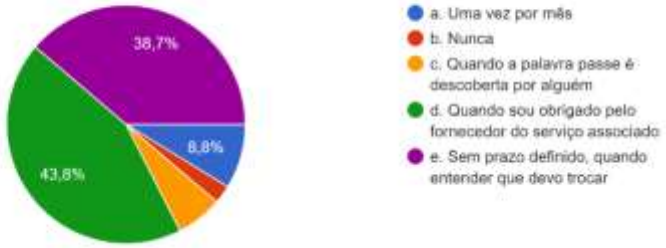
28 respostas



1º Questionário

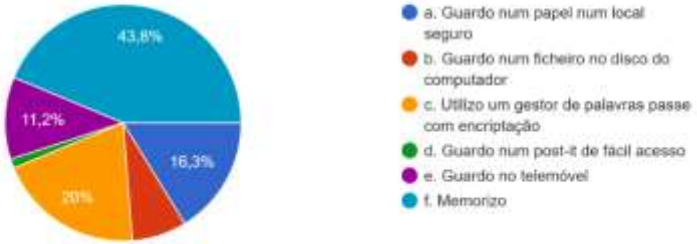
3. Com que frequência altera as suas palavras passe?

60 respostas



4. Qual o método que utiliza para guardar ou memorizar as suas palavras passe?

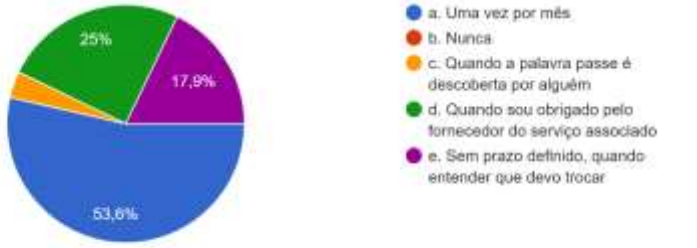
80 respostas



2º Questionário

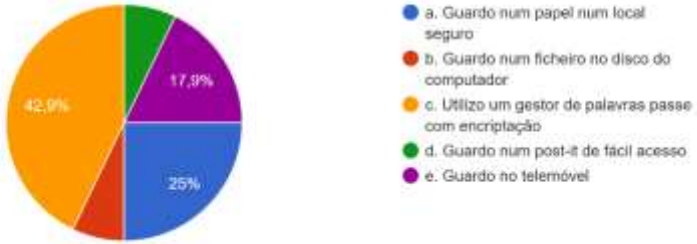
3. Com que frequência considera que deve alterar as suas palavras passe?

28 respostas



4. Qual o método que utiliza para guardar ou memorizar as suas palavras passe?

28 respostas



1º Questionário

5. Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de emai... procede em relação a este problema?

80 respostas

2º Questionário

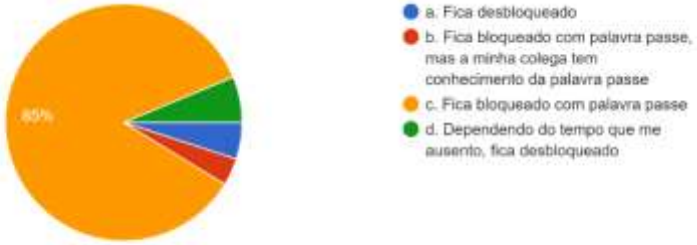
5. Para aceder aos vários serviços e entidades online, hoje em dia necessitamos de criar contas de emai... procede em relação a este problema?

28 respostas

1º Questionário

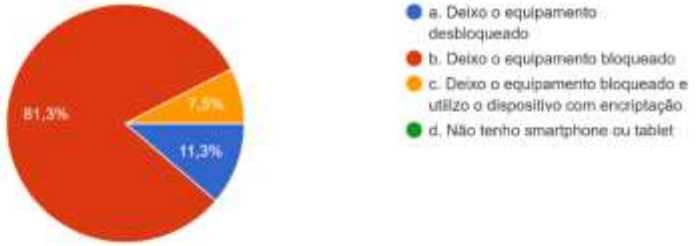
6. No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?

80 respostas



7. Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?

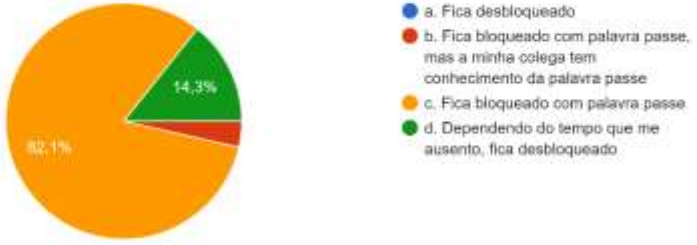
80 respostas



2º Questionário

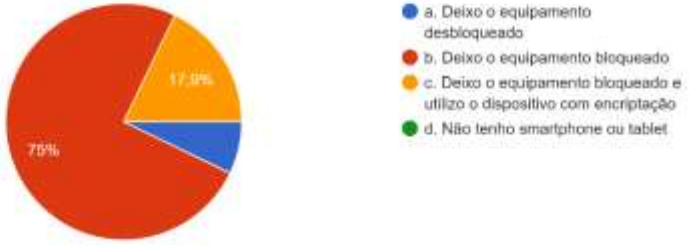
6. No seu local de trabalho, quando se ausenta do seu posto de trabalho, como deixa o computador pessoal?

28 respostas



7. Ao utilizar o seu dispositivo digital como um smartphone ou tablet, o que costuma fazer quando não está a utilizar o equipamento?

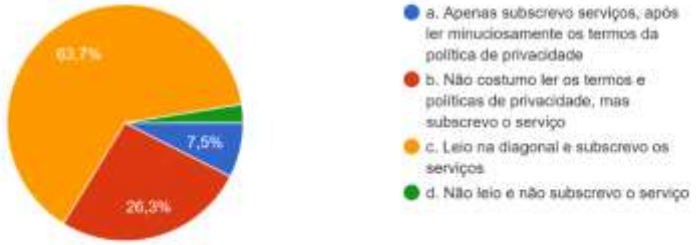
28 respostas



1º Questionário

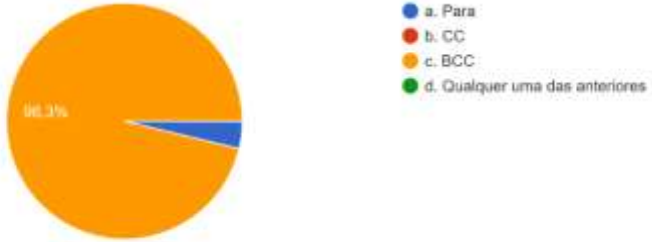
8. Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com as... dados pessoais. Qual a sua opinião?

80 respostas



9. Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatári...to dos endereços que mais se adequa?

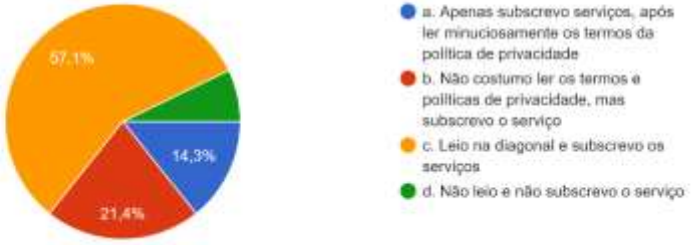
80 respostas



2º Questionário

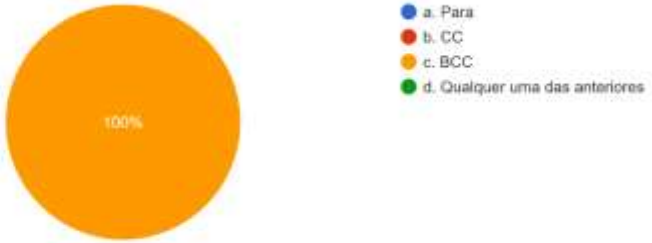
8. Quando subscreve um serviço online (ex: cria uma caixa de email, conta de Facebook), está a concordar com a ... dados pessoais. Qual a sua opinião?

28 respostas



9. Ao enviar um email para um grupo de pessoas em que pretende manter o anonimato sobre todos os destinatári...to dos endereços que mais se adequa?

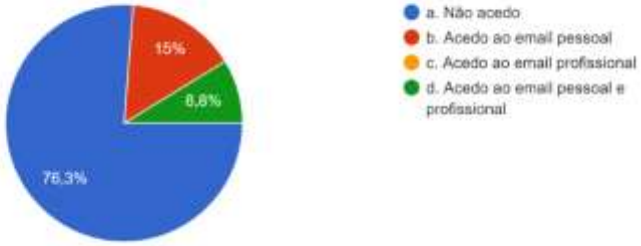
28 respostas



1º Questionário

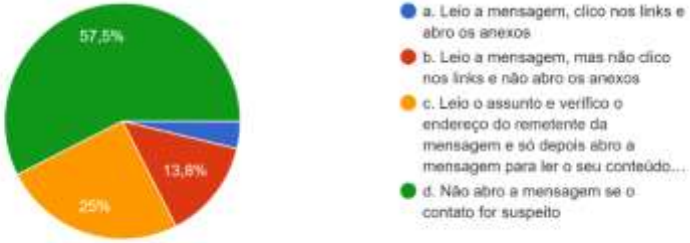
10. Acede ao seu email pessoal/profissional em computadores públicos?

80 respostas



11. Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?

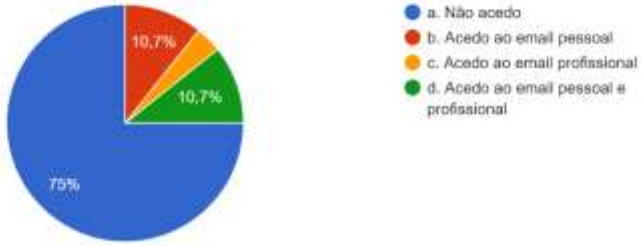
80 respostas



2º Questionário

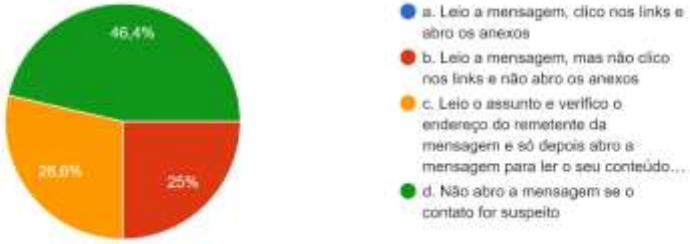
10. Acede ao seu email pessoal/profissional em computadores públicos?

28 respostas



11. Quando recebe emails de contactos que não estão na sua lista de endereços, que cuidados tem habitualmente?

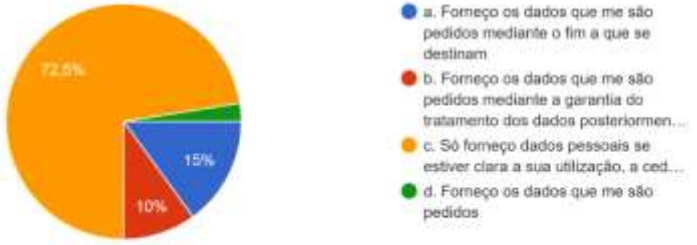
28 respostas



1º Questionário

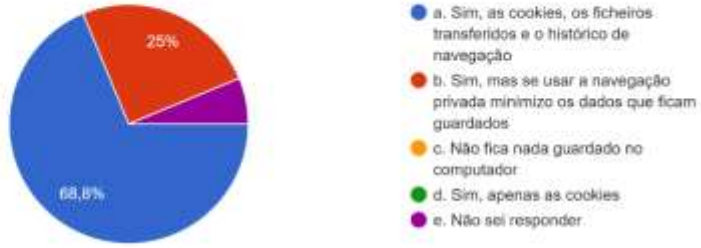
12. Quando tem necessidade de preencher formulários online, o que tem em atenção?

80 respostas



13. Quando navega na internet sabe se existem dados que ficam guardados no computador localmente?

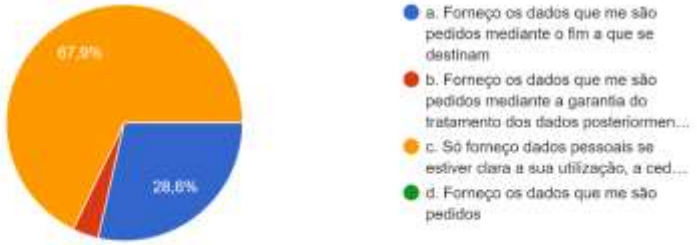
80 respostas



2º Questionário

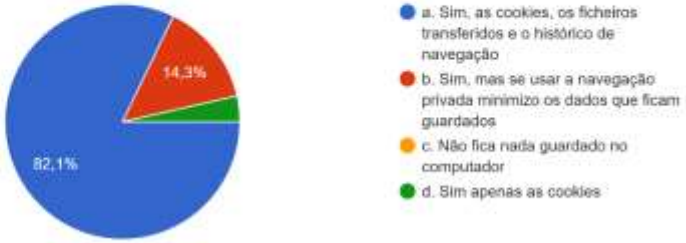
12. Quando tem necessidade de preencher formulários online, o que tem em atenção?

28 respostas



13. Quando navega na internet sabe que existem dados que ficam guardados no computador localmente?

28 respostas



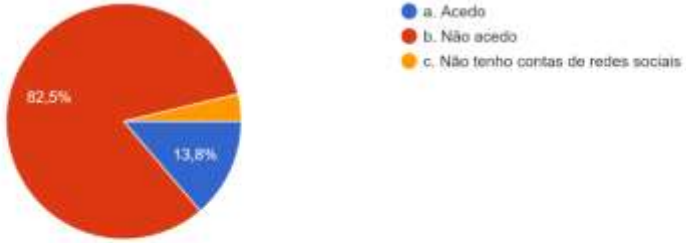
1º Questionário

14. Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?

60 respostas

15. Acede às suas contas de redes sociais em computadores públicos?

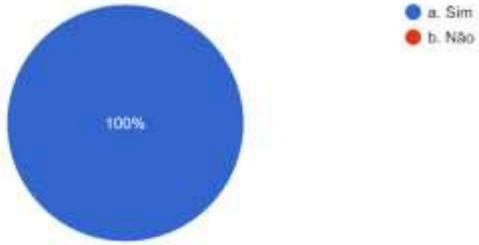
60 respostas



2º Questionário

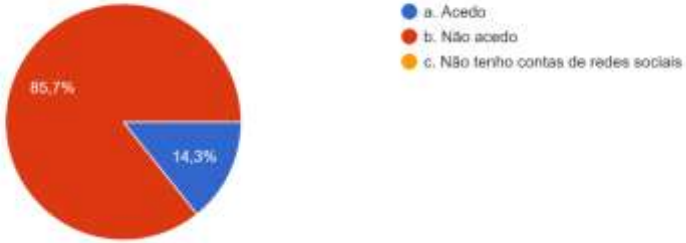
14. Quando navega na internet tem consciência que os seus dados podem ser alvo de registo e recolha por terceiros?

28 respostas



15. Acede às suas contas de redes sociais em computadores públicos?

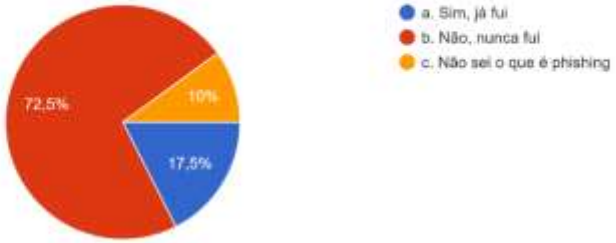
28 respostas



1º Questionário

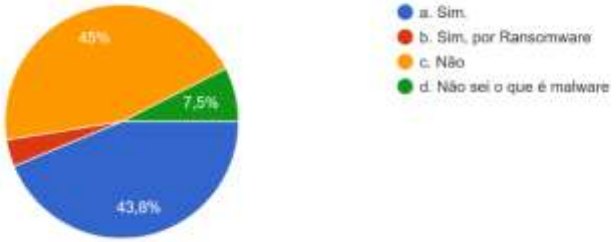
16. Já foi alguma vez alvo de Phishing?

80 respostas



17. Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):

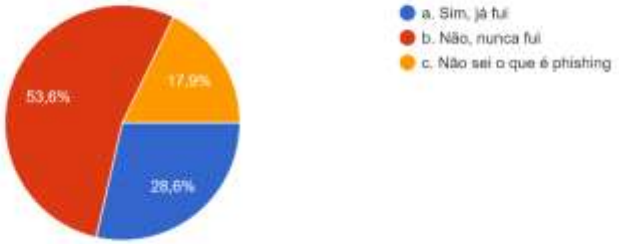
80 respostas



2º Questionário

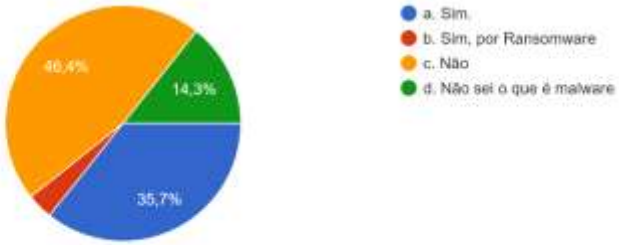
16. Já foi alguma vez alvo de Phishing?

28 respostas



17. Já foi afetado por malware no seu dispositivo (ex: pc, smartphone):

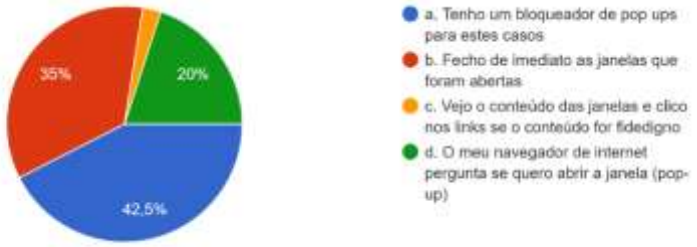
28 respostas



1º Questionário

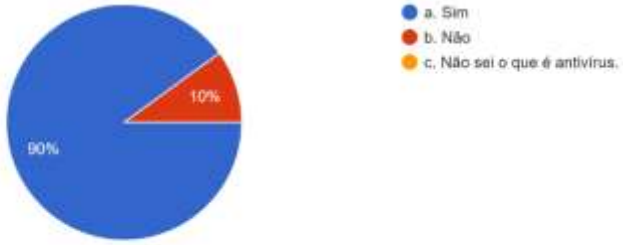
18. Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?

80 respostas



19. Utiliza um antivírus no seu computador?

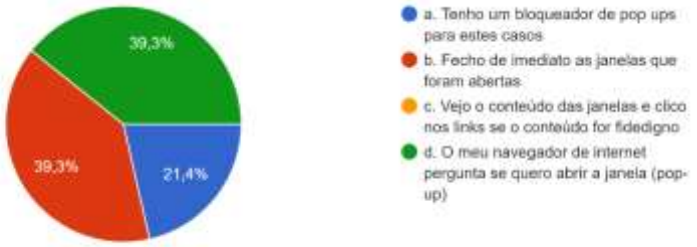
80 respostas



2º Questionário

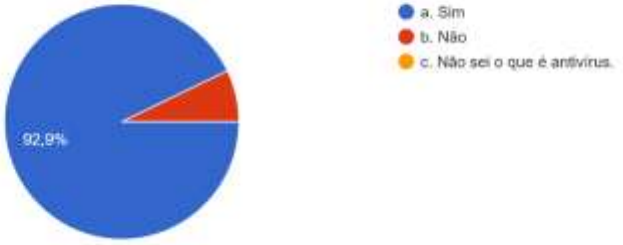
18. Quando navega na internet existem páginas que abrem outras páginas (pop-ups) sem que as tenha solicitado. O que costuma fazer?

28 respostas



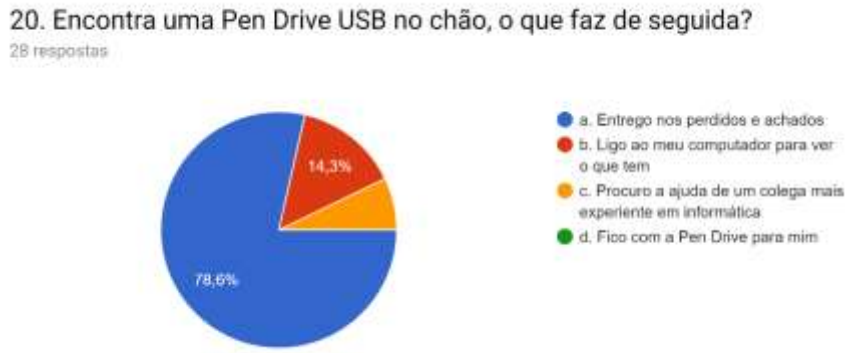
19. Utiliza um antivírus no seu computador?

28 respostas



1º Questionário

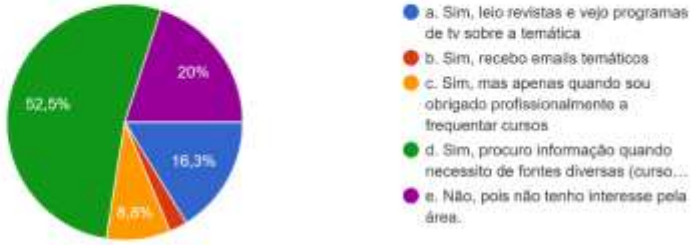
2º Questionário



1º Questionário

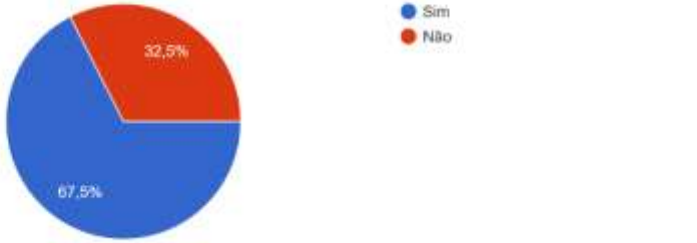
20. Habitualmente procura estar informado sobre a atualidade do mundo informático?

60 respostas



Aceita o desafio de frequentar um pequeno curso sobre segurança da informação, com a duração de apenas 1...estionários no final de cada módulo.

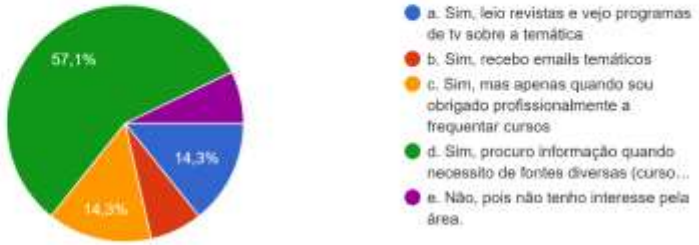
60 respostas



2º Questionário

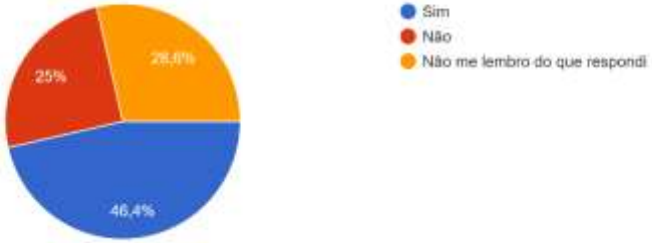
20. Habitualmente procura estar informado sobre a atualidade do mundo informático?

28 respostas



No 1º questionário do Projeto Security Awareness, (acerca dos hábitos e conhecimentos sobre a segurança da i...r o Curso Segurança da Informação?

28 respostas



1º Questionário

-

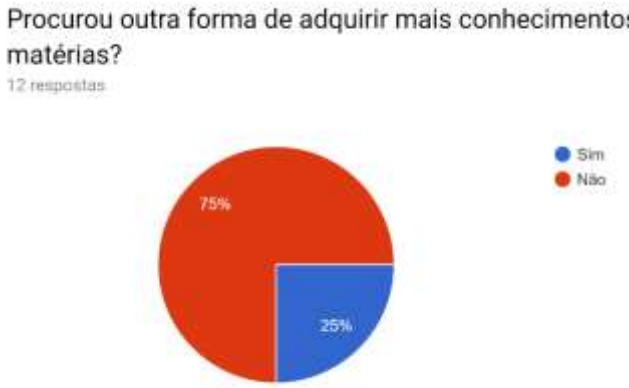
-

2º Questionário

1º Questionário

-

2º Questionário



Anexo I – Plataformas GoPhish e SOPHOS

Foram testadas duas plataformas de *phishing*, a GoPhish e a SOPHOS Phish Threat. Ambas cumprem o objetivo de enviar *e-mails* a um grupo de utilizadores com uma simulação de *phishing*, no entanto são bastante diferentes, na sua configuração, facilidade de instalação e configuração, facilidade de manuseamento e custo final por utilizador.

Tabela comparativa:

	Gophish ***Open Source Phishing*** **Platform**	**SOPHOS** **Sophos Phish Threat**
Plataforma		
Endereço	https://getgophish.com/	https://www.sophos.com/en-us/products/phish-threat.aspx
Requisitos prévios	*Server* Windows/Linux/iOS *Browser* e *Internet*	*Browser* e *Internet*
Facilidade de instalação (1 a 5)	2	5
Criação e upload de utilizadores e grupos	Sim	Sim
Ligação Active Directory	Não	Sim
Templates em Português	Não, mas podem ser criados pelo utilizador	Sim, tem biblioteca
Criação/Importação de templates	Sim	Sim

	Gophish ***Open Source Phishing*** **Platform**	**SOPHOS** **Sophos Phish Threat**
Personalização *Template* com variáveis (Nome, Apelido, *e-mail*)	Sim	Sim
Multilinguagem	Sim (utilizador escolhe o que adiciona)	Sim (English, Spanish, French, German, Italian, Brazilian Portuguese, Japanese, Korean, and Traditional Chinese)
Redireccionamento páginas	Sim, *link* externo	Sim
Redireccionamento para Formação	Não, mas pode ser feito, requer serviço externo	Sim
Marcação de *e-mail* como inseguro	Não	Sim (Exchange Outlook)
Reports por utilizador e grupo	Sim	Sim
Exportação Resultados (*.csv)	Sim	Sim
Documentação	Sim	Sim

<u>Vantagens:</u>

Gophish - *Open Source Phishing* Platform

- Preço = 0€
- Multilinguagem (utilizador escolhe a linguagem que adiciona)

SOPHOS - Sophos Phish Threat

- Facilidade de instalação
- Ligação Active Directory

- Templates vários e em português, pode criar-se novos templates
- Redireccionamento dos *links* do *e-mail* para Formação, seguimento do utilizador
- Marcação de *e-mail* como inseguro através do Exchange

Desvantagens:

Gophish - *Open Source Phishing* Platform

- Dificuldade de instalação
- Não tem ligação ao Active Directory
- Templates são criados de raiz ou importados
- Não tem redireccionamento automático para formação, mas pode ser feito manualmente, através de outros serviços
- Não permite marcar automaticamente um *e-mail* como inseguro

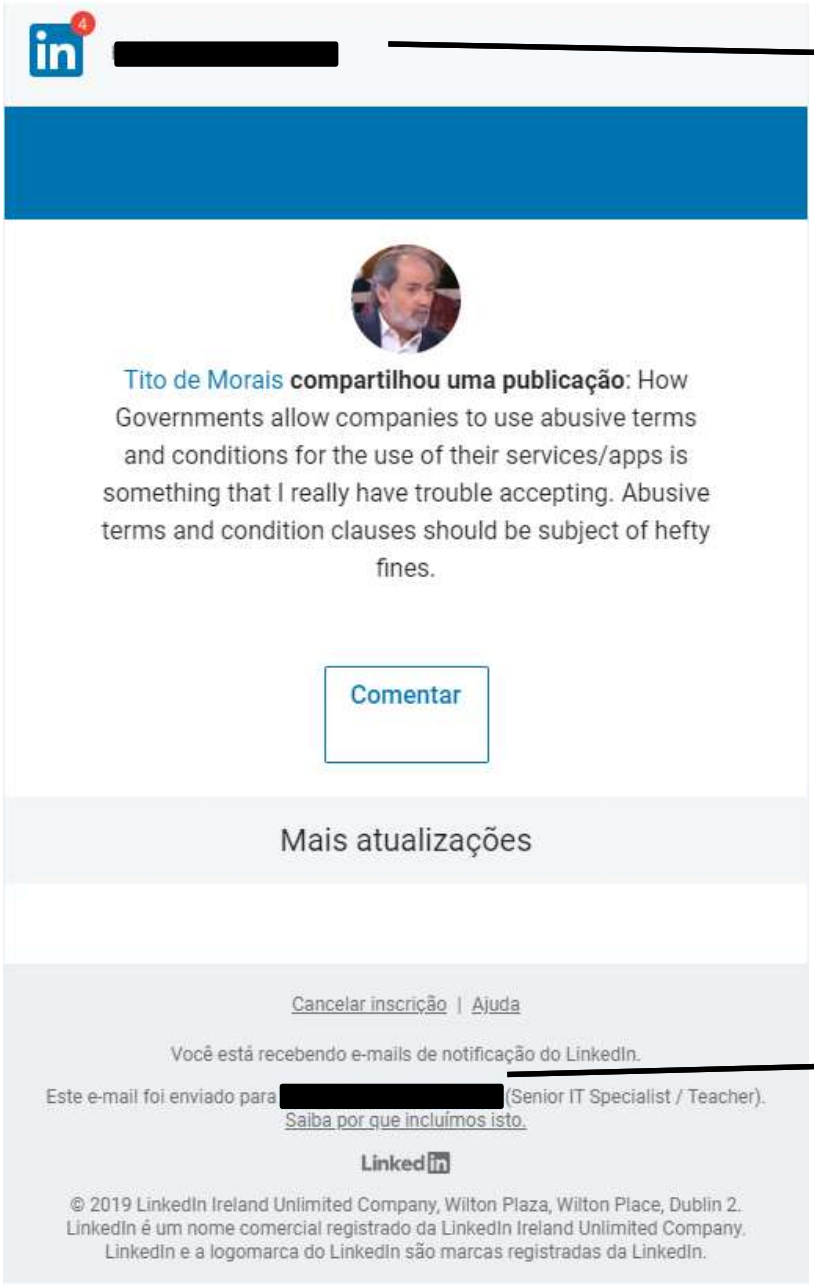
SOPHOS - Sophos Phish Threat

- Preço varia de acordo com o número de utilizadores (ex: 2.500 utilizadores cerca de 15.000€)

Anexo J – Campanha de *Phishing* da GoPhish

Campanha de *phishing* através do envio de um *e-mail*, personalizado com o nome e *e-mail* do destinatário, onde qualquer *link* clicável, dá acesso a uma página fictícia de pedido de colocação das credenciais do Linkedin.

***E-mail* enviado:**



Personalização do nome do destinatário

Personalização do email do destinatário

Parte do cabeçalho técnico do *e-mail* da campanha enviado:

```
Delivered-To: <e-mail_do_destinatário>
```

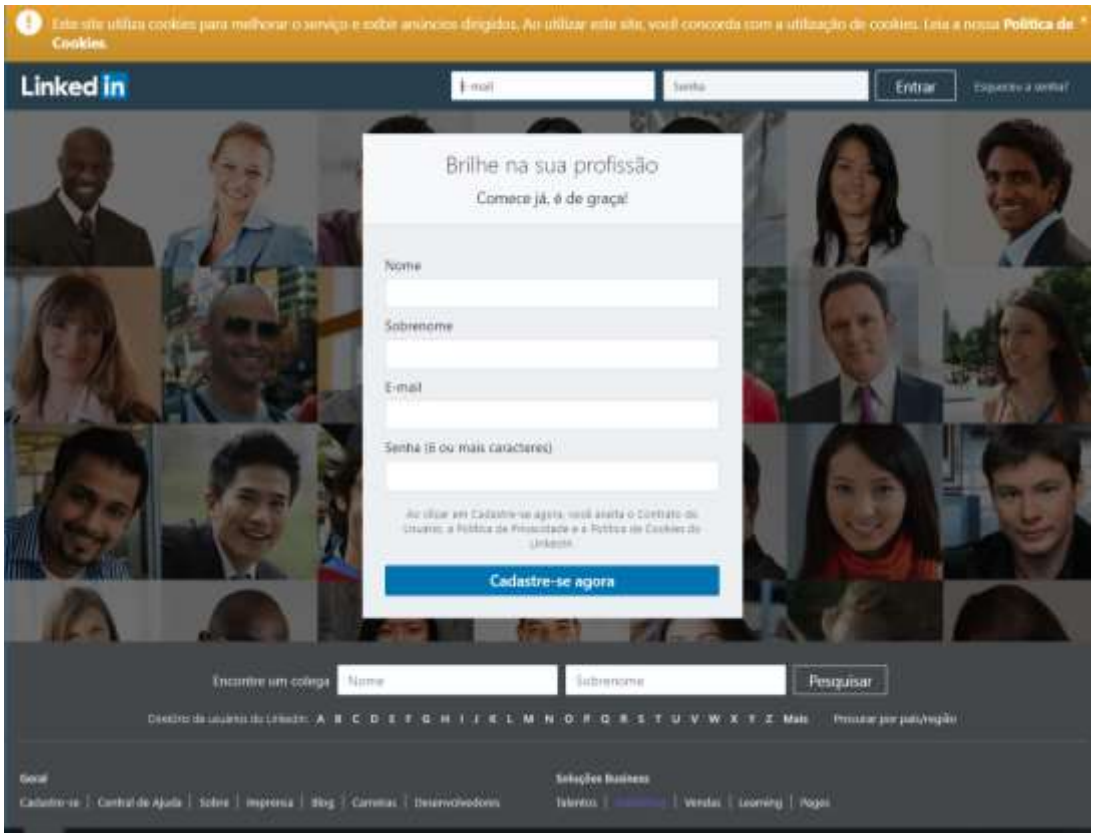
```
Received: by 2002:a67:e00b:0:0:0:0:0 with SMTP id c11csp1144538vsl;
        Wed, 11 Sep 2019 10:24:57 -0700 (PDT)
X-Received: by 2002:a17:902:202:: with SMTP id 2mr37025112plc.96.1568222457386;
        Wed, 11 Sep 2019 10:20:57 -0700 (PDT)
X-Received: by 2002:a17:902:202:: with SMTP id 2mr37025049plc.96.1568222456504;
        Wed, 11 Sep 2019 10:20:56 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1568222456; cv=none;
        d=google.com; s=arc-20160816;
        b=k/kRkFrwHAp4J3Ydk3DMxRD1BsMFUHhSwhTmAP8x/3cfCRBQrCWxni33RZ0vCIu60T
         0Ij4MFjVnv/qh50x97ghr0PGuwt5lXU6/uviKPcMb++Uyj+D9I+juw6fKA3jV7QpchxM
         LiocVQHToQDVSdlDdXou5xzMpZWIEPaey/vJAJxXGY0+JzdqWYYwG+qxMhi/byHjfP3s
         tC7OQ+k5uQEqEUlfn3kRPUzvmZwsukBqbWB6sIjaAg0DiSToaYF5JOOIo7rhlM5fXbIx
         cxOseMnry2VasUn668JW+SSYaBIeHUTFf1cuZdmOwgJgOGxXc0T71A9KnNg955UuoDoW
         nd0Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:from:date:mime-version:message-id:dkim-signature;
        bh=DKQ4kpIa4egi8Ivqlr9jte02WCLoubJKhCjuKQG/6ak=;
        b=NTBfLRcL4DzzLYDm/BvsdYPgI/LtA17sasZInKYXLloCKLOZJ/mu2ZOTfhto2JOqXW
         sSDTNTEfIkFvWA78AjBW8TBXdGkUrHULh9K+0TeTyWykUX4SWPDkfJC9VW4laJQMG9ZI
         MkLJ2tDdnJniYw6nXoi9RFYgzEI3d+7AaBARDJjLm7vJS7tidyJHlNHjUTV7JmNZWzlM
         HugEWqp6QOlEm3kF8dOAPup3g66e0EwiaUUeS6ao9tz8/BPk4+qpv9zW2F5ODcv2p72A
         8bVDZ08djh5H6wXduAg7Oqct9lnii14Elpq5zcDKFnWlfVlTsXFf/6ZDp6klY3YOV8Ci
         eEVw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20161025 header.b=blJUsaR3;
       spf=pass (google.com: domain of marketing.notifications.noreply@gmail.com designates
209.85.220.65 as permitted sender) smtp.mailfrom=marketing.notifications.noreply@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <marketing.notifications.noreply@gmail.com>
Received: from mail-sor-f65.google.com (mail-sor-f65.google.com. [209.85.220.65])
        by mx.google.com with SMTPS id s24sor3181956pji.26.2019.09.11.10.20.56
        for <<e-mail_do_destinatário>>
        (Google Transport Security);
        Wed, 11 Sep 2019 10:20:56 -0700 (PDT)
Received-SPF: pass (google.com: domain of marketing.notifications.noreply@gmail.com designates
209.85.220.65 as permitted sender) client-ip=209.85.220.65;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20161025 header.b=blJUsaR3;
       spf=pass (google.com: domain of marketing.notifications.noreply@gmail.com designates
209.85.220.65 as permitted sender) smtp.mailfrom=marketing.notifications.noreply@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=message-id:mime-version:date:from:subject:to;
        bh=DKQ4kpIa4egi8Ivqlr9jte02WCLoubJKhCjuKQG/6ak=;
        b=blJUsaR3JEpwy2xIyRoZUgSVkDMXfSF6KPTZy3C3QG6YY+poXPeH1c/VeDJI77JMpk
         udrHyJ9ol3v0lDfduVQPkzqhngpN75FjKHqDr7FCOmPJo0htQ0GxCerRok2dCqrbfAwd
         sncG3Fy2D19Uv9ywvNDLG2J3TcyXaPkwRsVIBXBIsG1JymsN0HRdNweFiW1WDxvlFu9y
         7JEkz6icBw9ESp734uW3epvAsz2Npl8pvmH2M0QVY43bBQcCaizMyV40UuTzbyTQhqCG
         DVz/vtP4sqprFSbrtDHX1lJkw2K3WVuUI69YTnKSEfpNuvrypS7H6eMRpxchcux62Kwe
         Wp5w==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20161025;
        h=x-gm-message-state:message-id:mime-version:date:from:subject:to;
        bh=DKQ4kpIa4egi8Ivqlr9jte02WCLoubJKhCjuKQG/6ak=;
        b=VL2KyvuOxgF8Hiz4zxPi4iItUjutVEIV8kQ76+HGNZAWEinQk3dWx2eGVA0wN5f9gE
         91/OSEMQ90bfv6znXnqMuibIz/jz2p9gIoKniWDFv8t8i1YYHc/cVK033txr0/8GHjts
         /2phVxZBxx/QN/e1G/vL5E51ZpsWVjc0Xfwlax16MDsqte7aiQnRT6bVXS2bh7+6OUIv
         Pr3I9vpX7ONd8mGo+85Yb5nkwsiR5lWSweEtVGAD49CsNc6jggOZuc0EPwTNy2rQ0qVP
         H2uO45FDb/m6D0Sg4fNNyw6vWYkyJsDzdbg+FYK0DoLAECqIk07RGOYUoFXRi2ec/F+D
         MGcw==
X-Gm-Message-State: APjAAAWgHWaUF3/ZbiVPLUQhX59xwQQi5dLeqJCM0qiR4UruPl921AN2
0EoslpgJj4EvU9oRhRGnpRRdQY1kYvk=
X-Google-Smtp-Source: APXvYqz8VB9MMbSBZC/+zcXBHzdABzrsYwcR+fO72MLolZEv8c+vOJc9dD0/1NOpM9dhsVzZDu5/lg==
X-Received: by 2002:a17:90b:d98:: with SMTP id bg24mr6279456pjb.74.1568215380719;
        Wed, 11 Sep 2019 08:23:00 -0700 (PDT)
Return-Path: <marketing.notifications.noreply@gmail.com>
Received: from Ubunto ([167.99.78.232])
        by smtp.gmail.com with ESMTPSA id b10sm2056299pfo.123.2019.09.11.08.22.59
        for <<e-mail_do_destinatário>>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 11 Sep 2019 08:22:59 -0700 (PDT)
Message-ID: <5d791153.1c69fb81.17fdc.41c0@mx.google.com>
Mime-Version: 1.0
Date: Wed, 11 Sep 2019 15:22:59 +0000
From: marketing.notifications.noreply@gmail.com
X-Mailer: gophish
Subject: Tito de Morais compartilhou uma...
To: Paula Joaquim <<e-mail_do_destinatário>>
Content-Type: multipart/alternative;
boundary=49453c02961a55ef88cd00a6661d3ce6165648c57d4f009392bcf64f8923

--49453c02961a55ef88cd00a6661d3ce6165648c57d4f009392bcf64f8923
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset=UTF-8

Isto =C3=A9 o que voc=C3=AA est=C3=A1 perdendo no LinkedIn
```

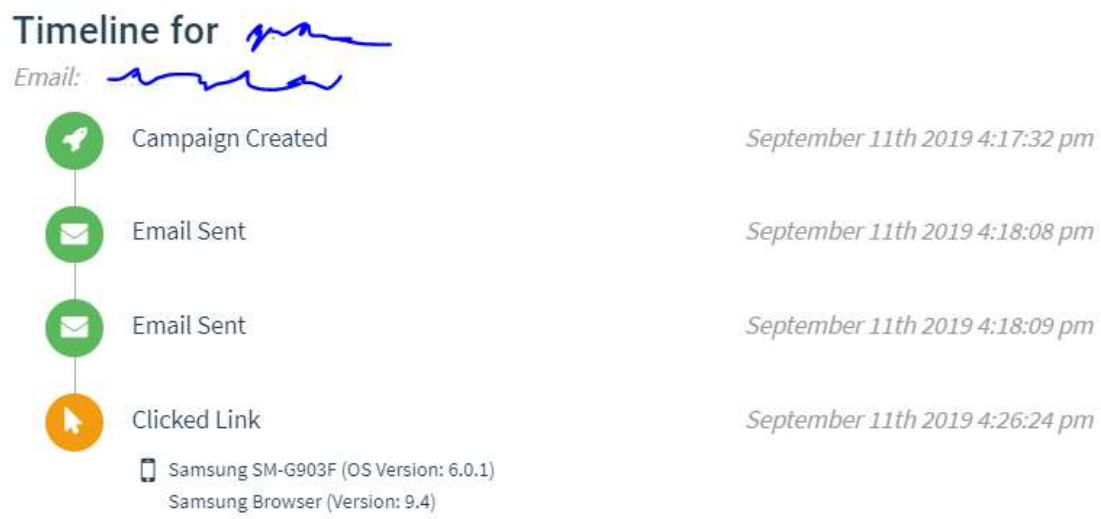
```
----------------------------------------
 https://www.linkedin.com/comm/in/titodemorais?midToken=3DAQHDN4tAmLTqqw&am=
p;trk=3Deml-e-mail_notification_digest_01-notifications-4-prof_photo&amp;trk=
E-mail=3Deml-e-mail_notification_digest_01-notifications-4-prof_photo-null-2t=
53n2%7Ejye93pqe%7Eu0-null-neptune%2Fprofile%7Evanity%2Eview&amp;lipi=3Durn%=
3Ali%3Apage%3Ae-mail_e-mail_notification_digest_01%3B%2BUHzPgT8QLyJi2ZR6P0dVw=
%3D%3D
```

Página fictícia de introdução das credenciais:

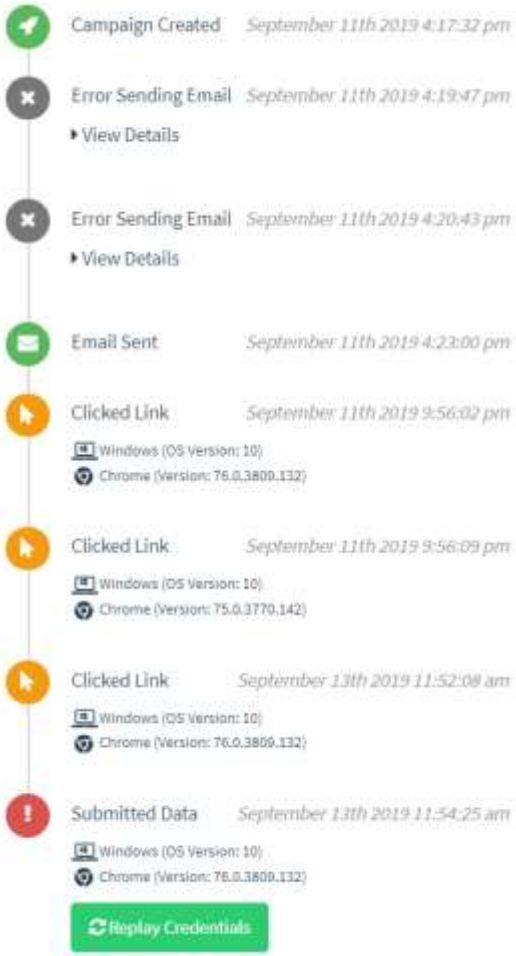


Resumo da campanha:

Detalhe obtido de um utilizador que apenas fez um clique num dos *links* do *e-mail* recebido:



Detalhe obtido de um utilizador que introduziu as suas credenciais após o clique num dos links do *e-mail* recebido:



Detalhe das credenciais inseridas pelo utilizador:

__original_url	https://www.linkedin.com/uas/login-submit?loginSubmitSource=GUEST_HOME
isJsEnabled	false
loginCsrfParam	434ab0ec-5639-423d-8c14-079f788a2a09
session_key	paula@gmail.com
session_password	123456

É possível exportar para um ficheiro CSV os resultados da campanha. Na tabela seguinte podemos ver o conteúdo desse ficheiro, sem as 3 últimas colunas devido à confidencialidade dos dados pessoais (*e-mail*, nome e apelido).

id	status	ip	latitude	longitude	send_date	reported	modified_date
Uyodqsh	Sending		0	0	11/09/2019 16:16	FALSO	11/09/2019 16:17
QLjAmKn	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
SOtpcle	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
TsplCS5	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
iZxp2Vf	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
jk5WKBY	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
GY5QZ7T	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
6s5zSHJ	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
iAk4y2Q	Email Sent		0	0	11/09/2019 16:17	FALSO	11/09/2019 16:17
EW4Aecz	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
6H2BusP	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
DkapM3n	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
ISsSr4o	Clicked Link	62.28.68.50	38.7139	-9.1394	11/09/2019 16:18	FALSO	11/09/2019 16:26
MSkryik	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
jhk5va9	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
TdEb80X	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
JeKvy77	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
h3iXjXo	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
onLDpJH	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
6YX8XmH	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
8oUSGLd	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
CYyztp7	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
WDUx2Xl	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
zU048ch	Email Sent		0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18

MdufPJQ	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
Td538FW	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
yCvg3xt	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
f1f2myQ	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
EePttnM	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
8orBiI2	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
ZcKikJd	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
cAbNXAn	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
oyNR6fK	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
BOMPnj8	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
3jfxGgp	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
4zow7TD	Email Sent	0	0	11/09/2019 16:18	FALSO	11/09/2019 16:18
vAJnilU	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
45yX2LP	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
J8wacLr	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
em2fxv6	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
QVBeC44	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
Hlpo7j9	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
CMI5LsY	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
0NAvgeh	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
NEcxQvG	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
BpNyp65	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
gvVGyL4	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
yrQOnMC	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
zgXh6hw	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
FQ59utr	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
HXNmHHy	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
O7da5m0	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
QuZEAis	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
i3zacW8	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
so4ss9y	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
UfAlMFq	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
KBcHtEX	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
VWWtnx5	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
l4acijA	Email Sent	0	0	11/09/2019 16:19	FALSO	11/09/2019 16:19
SXBuGwc	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
8oxyPF3	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
jyylK84	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
wxxlKZ6	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
Kk1GOTk	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
fuILmvu	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
HnzvQ0O	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
Dt9zd72	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
2bOKom8	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
IZ9yHVv	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
8ZbJhUk	Email Sent	0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22

jwgCdpB	Email Sent		0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
ux3Gu5B	Email Sent		0	0	11/09/2019 16:22	FALSO	11/09/2019 16:22
U21tfVi	Submitted Data	148.63.76.198	38	-97	11/09/2019 16:23	FALSO	13/09/2019 11:54
LohhGXi	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
zDDEmVO	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
X9qLCib	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
86zDNKu	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
uCpF5u4	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
r5zm0ka	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
GS8H3OP	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
Kb1WAH5	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
Vee2SYe	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
9vq2Fji	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
Bu34rFu	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
s1lwxIq	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
eVHkzKh	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
uWfnuIX	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
IO8cGHl	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
YYH3Fly	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
aAOgMBJ	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
wO5Rqx3	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
UKjubEh	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
M06liUv	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
rGzfdK9	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
pPlRrkn	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
hNstXYj	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
RWK0HoB	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23
LLhDYRu	Email Sent		0	0	11/09/2019 16:23	FALSO	11/09/2019 16:23

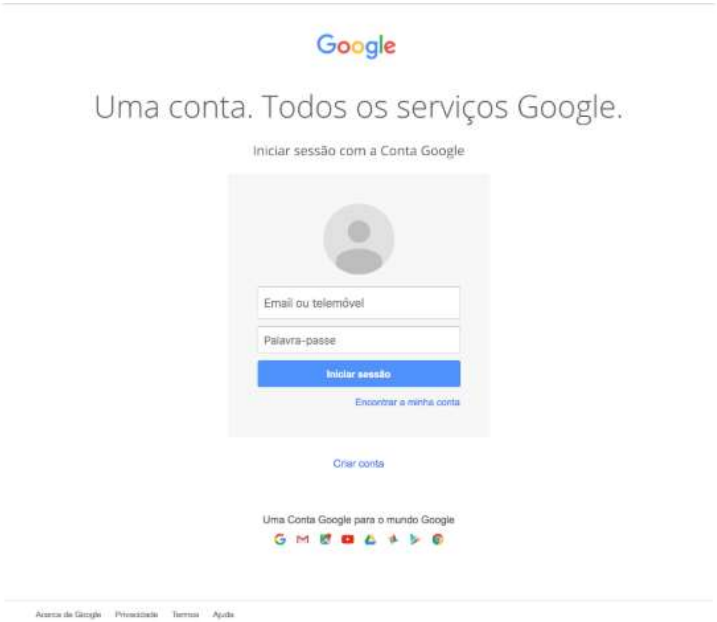
Anexo K – Campanha de *Phishing* 1 da SOPHOS

Campanha de *phishing* 1 – Evento de calendário.

Esta campanha consiste no envio de um agendamento de calendário com o nome Hospital Lusíadas, cujo clique em cima de qualquer *link* abre uma página fictícia que solicita a inserção das credenciais de uma conta do Gmail.

***E-mail* enviado:**

Página fictícia de introdução das credenciais:



Ecrã de resumo da campanha:

Os *e-mails* enviados seguiram em 2 grupos diferentes.

Total de *e-mails* enviados: 56 equivalente a 100%

Total de *e-mails* abertos: 18 equivalente a 32%

Total de *links* clicados: 9 equivalente a 16%

Total de credenciais inseridas: 3 equivalente a 5%

Ecrã de detalhe da ação dos utilizadores:

O SOPHOS Phish Threat, permite obter resultados sobre os parâmetros: *e-mail*, nome, *e-mail* enviado, *e-mail* aberto, *link* clicado, credenciais inseridas, formação iniciada e formação concluída (treinamento).

Por questões de privacidade não estão listados o *e-mail* e o nome de cada utilizador, devido a não ter sido testada a parte da formação (não estão visíveis as colunas da formação iniciada e concluída).

Na campanha do envio do evento de calendário os resultados foram:

É possível exportar para um ficheiro CSV os resultados da campanha. Na tabela seguinte podemos ver o conteúdo desse ficheiro, sem as colunas referentes a: dados pessoais (*e-mail*, nome e apelido), dados sobre reporte de *e-mail* suspeito, formação (iniciada e terminada).

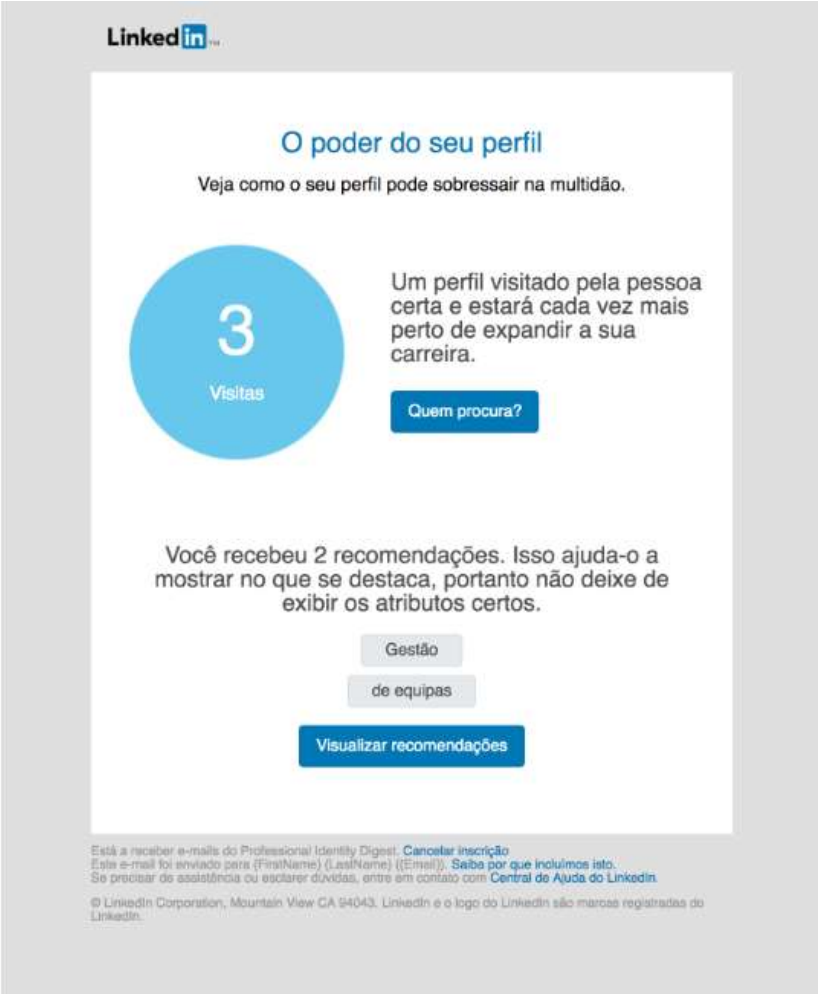
ID	Sent	Sent Date	Opened	Opened Date	Clicked	Clicked Date	Entered Credentials	Entered Credentials Date	Attachment Opened	Attachment Opened Date	IP
1	Yes	10/09/2019 16:31	No		No		No		No		
2	Yes	10/09/2019 16:31	No		No		No		No		
3	Yes	10/09/2019 16:31	No		No		No		No		
4	Yes	10/09/2019 16:31	No		No		No		No		
5	Yes	10/09/2019 16:31	No		No		No		No		
6	Yes	10/09/2019 16:31	No		No		No		No		
7	Yes	10/09/2019 16:31	Yes	11/09/2019 19:22	No		No		No		89.115.124.58
8	Yes	10/09/2019 16:31	No		No		No		No		
9	Yes	10/09/2019 16:31	No		No		No		No		
10	Yes	10/09/2019 16:31	No		No		No		No		
11	Yes	10/09/2019 16:31	Yes	10/09/2019 19:21	Yes	10/09/2019 19:21	No		No		193.47.185.124
12	Yes	10/09/2019 16:31	No		No		No		No		
13	Yes	10/09/2019 16:31	No		No		No		No		
14	Yes	10/09/2019 16:31	No		No		No		No		
15	Yes	10/09/2019 16:31	No		No		No		No		
16	Yes	10/09/2019 16:31	No		No		No		No		
17	Yes	10/09/2019 16:31	No		No		No		No		
18	Yes	10/09/2019 16:31	No		No		No		No		
19	Yes	10/09/2019 16:31	Yes	10/09/2019 16:36	No		No		No		172.22.105.81, 195.234.134.115
20	Yes	10/09/2019 16:31	No		No		No		No		
21	Yes	10/09/2019 16:31	No		No		No		No		
22	Yes	10/09/2019 16:31	No		No		No		No		
23	Yes	10/09/2019 16:31	Yes	12/09/2019 14:31	No		No		No		212.82.108.32
24	Yes	10/09/2019 16:31	No		No		No		No		
25	Yes	10/09/2019 16:31	Yes	10/09/2019 17:32	Yes	10/09/2019 17:33	No		No		82.154.46.245
26	Yes	10/09/2019 16:31	No		No		No		No		
27	Yes	10/09/2019 16:31	No		No		No		No		
28	Yes	10/09/2019 16:31	Yes	10/09/2019 16:57	Yes	10/09/2019 16:57	Yes	10/09/2019 16:57	No		31.22.203.68
29	Yes	10/09/2019 16:31	Yes	10/09/2019 16:59	No		No		No		46.50.4.57
30	Yes	10/09/2019 16:31	Yes	10/09/2019 16:34	No		No		No		82.154.46.245
31	Yes	10/09/2019 16:31	No		No		No		No		
32	Yes	10/09/2019 16:31	Yes	11/09/2019 15:12	Yes	11/09/2019 15:12	No		No		89.115.229.222
33	Yes	10/09/2019 16:31	No		No		No		No		
34	Yes	11/09/2019 18:54	No		No		No		No		
35	Yes	11/09/2019 18:54	Yes	12/09/2019 10:48	No		No		No		62.28.150.162
36	Yes	11/09/2019 18:54	No		No		No		No		
37	Yes	11/09/2019 18:54	No		No		No		No		
38	Yes	11/09/2019 18:54	Yes	12/09/2019 10:38	Yes	12/09/2019 10:38	No		No		62.28.150.162
39	Yes	11/09/2019 18:54	No		No		No		No		
40	Yes	11/09/2019 18:54	No		No		No		No		
41	Yes	11/09/2019 18:54	Yes	12/09/2019 14:46	No		No		No		62.28.150.162
42	Yes	11/09/2019 18:54	Yes	12/09/2019 09:56	No		No		No		62.28.150.162
43	Yes	11/09/2019 18:54	No		No		No		No		
44	Yes	11/09/2019 18:54	Yes	17/09/2019 12:00	Yes	17/09/2019 12:00	Yes	17/09/2019 12:01	No		66.249.93.33
45	Yes	11/09/2019 18:54	Yes	12/09/2019 09:58	Yes	12/09/2019 09:58	No		No		62.28.150.162
46	Yes	11/09/2019 18:54	Yes	12/09/2019 17:25	Yes	12/09/2019 17:25	No		No		62.28.150.162
47	Yes	11/09/2019 18:54	No		No		No		No		
48	Yes	11/09/2019 18:54	No		No		No		No		
49	Yes	11/09/2019 18:54	No		No		No		No		
50	Yes	11/09/2019 18:54	No		No		No		No		
51	Yes	11/09/2019 18:54	Yes	12/09/2019 10:03	Yes	12/09/2019 10:03	Yes	12/09/2019 10:04	No		62.28.150.162
52	Yes	11/09/2019 18:54	No		No		No		No		
53	Yes	11/09/2019 18:54	Yes	13/09/2019 11:24	Yes	13/09/2019 11:24	No		No		62.28.150.162
54	Yes	11/09/2019 18:54	No		No		No		No		
55	Yes	11/09/2019 18:54	No		No		No		No		
56	Yes	11/09/2019 18:54	No		No		No		No		

Anexo L – Campanha de *Phishing* 2 da SOPHOS

Campanha de *phishing* 2 – Linkedin o poder do seu perfil.

Esta campanha consiste no envio de uma notificação, sobre como pode um perfil de Linkedin sobressair na multidão e as recomendações que recebeu. Após um clique em qualquer um dos *links* do *e-mail* recebido, é remetido para uma página de inserção de credenciais fictícia do Linkedin.

***E-mail* enviado:**



Página fictícia de introdução das credenciais:

Ecrã de resumo da campanha:

Os *e-mails* enviados seguiram em 2 grupos diferentes.

Total de *e-mails* enviados: 55 equivalente a 100% (total 56, 1 não foi enviado)

Total de *e-mails* abertos: 6 equivalente a 11%

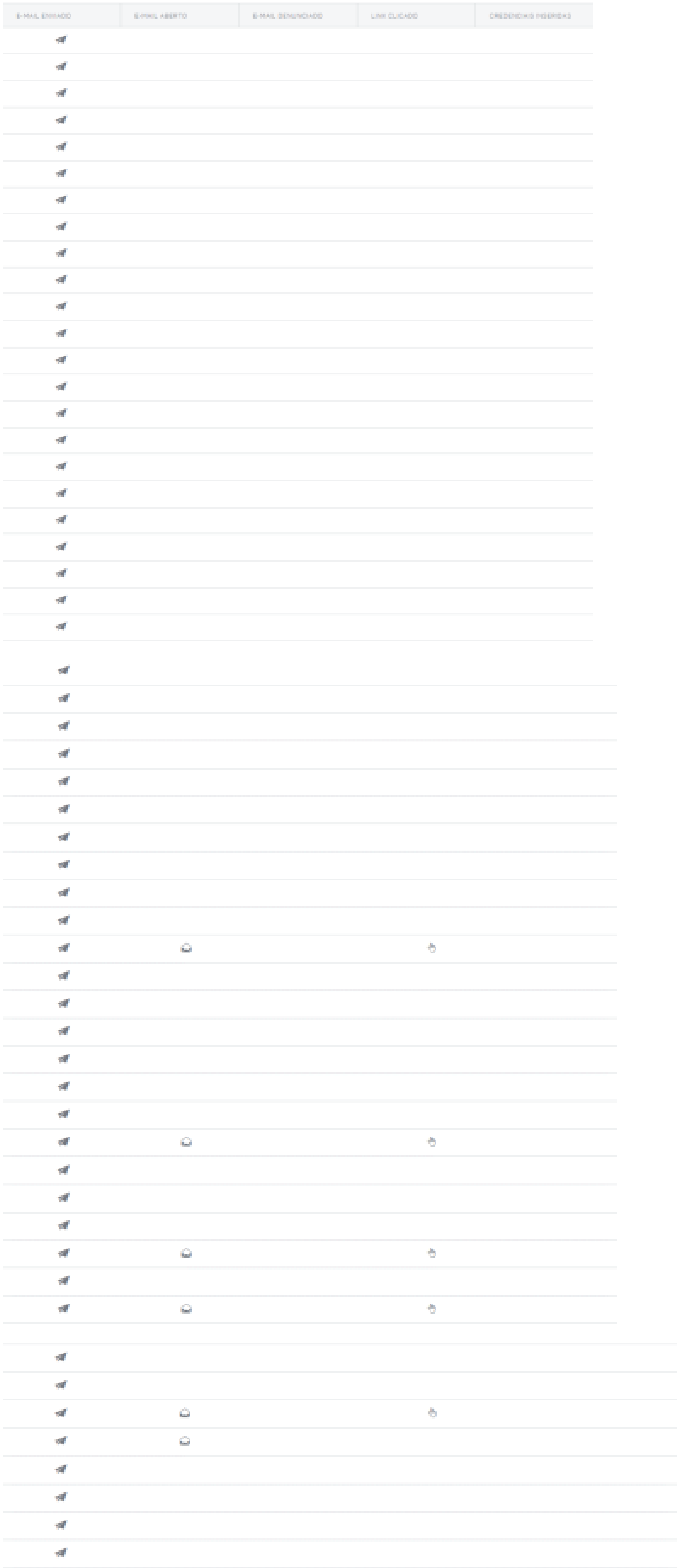
Total de *links* clicados: 5 equivalente a 19%

Total de credenciais inseridas: 0 equivalente a 0%

Ecrã de detalhe da ação dos utilizadores:

O SOPHOS permite obter resultados sobre os parâmetros, "*e-mail*, nome, *e-mail* enviado, *e-mail* aberto, *link* clicado, credenciais inseridas, treinamento iniciado e treinamento concluído.

Por questões de privacidade não serão listados o *e-mail* e o nome de cada utilizador e por não ter sido testada a parte da formação (treinamento), não estão visíveis as colunas do treinamento iniciado e concluído.


E-MAIL ENVIADO
E-MAIL ABERTO
E-MAIL DENUNCIADO
LINK CLICADO
CREDENCIAIS INSERIDAS

É possível exportar para um ficheiro CSV os resultados da campanha. Na tabela seguinte podemos ver o conteúdo desse ficheiro, sem as colunas referentes aos dados pessoais (*e-mail*, nome e apelido).

id	Sent	Sent Date	Opened	Opened Date	Clicked	Clicked Date	Entered Credentials	Entered Credentials Date	Attachment Opened	Attachment Opened Date	IP
1	Yes	10/09/2019 16:09	No		No		No		No		
2	Yes	10/09/2019 16:09	No		No		No		No		
3	Yes	10/09/2019 16:09	No		No		No		No		
4	No		No		No		No		No		
5	Yes	10/09/2019 16:09	No		No		No		No		
6	Yes	10/09/2019 16:09	No		No		No		No		
7	Yes	10/09/2019 16:09	No		No		No		No		
8	Yes	10/09/2019 16:09	No		No		No		No		
9	Yes	10/09/2019 16:09	No		No		No		No		
10	Yes	10/09/2019 16:09	No		No		No		No		
11	Yes	10/09/2019 16:09	No		No		No		No		
12	Yes	10/09/2019 16:09	Yes	10/09/2019 17:30	Yes	10/09/2019 17:30	No		No		94.63.112.193
13	Yes	10/09/2019 16:09	No		No		No		No		
14	Yes	10/09/2019 16:09	No		No		No		No		
15	Yes	10/09/2019 16:09	No		No		No		No		
16	Yes	10/09/2019 16:09	No		No		No		No		
17	Yes	10/09/2019 16:09	No		No		No		No		
18	Yes	10/09/2019 16:09	No		No		No		No		
19	Yes	10/09/2019 16:09	Yes	10/09/2019 16:20	Yes	10/09/2019 16:20	No		No		195.234.134.115
20	Yes	10/09/2019 16:09	No		No		No		No		
21	Yes	10/09/2019 16:09	No		No		No		No		
22	Yes	10/09/2019 16:09	No		No		No		No		
23	Yes	10/09/2019 16:09	Yes	12/09/2019 14:31	Yes	12/09/2019 14:31	No		No		213.228.154.29
24	Yes	10/09/2019 16:09	No		No		No		No		
25	Yes	10/09/2019 16:09	Yes	10/09/2019 19:54	Yes	10/09/2019 19:54	No		No		82.154.46.245
26	Yes	10/09/2019 16:09	No		No		No		No		
27	Yes	10/09/2019 16:09	No		No		No		No		
28	Yes	10/09/2019 16:09	Yes	10/09/2019 16:12	Yes	10/09/2019 16:13	No		No		31.22.203.68
29	Yes	10/09/2019 16:09	Yes	10/09/2019 16:59	No		No		No		46.50.4.57
30	Yes	10/09/2019 16:09	No		No		No		No		
31	Yes	10/09/2019 16:10	No		No		No		No		
32	Yes	10/09/2019 16:09	No		No		No		No		
33	Yes	10/09/2019 16:09	No		No		No		No		
34	Yes	11/09/2019 18:50	No		No		No		No		
35	Yes	11/09/2019 18:50	No		No		No		No		
36	Yes	11/09/2019 18:50	No		No		No		No		
37	Yes	11/09/2019 18:50	No		No		No		No		
38	Yes	11/09/2019 18:50	No		No		No		No		
39	Yes	11/09/2019 18:50	No		No		No		No		
40	Yes	11/09/2019 18:50	No		No		No		No		
41	Yes	11/09/2019 18:50	No		No		No		No		
42	Yes	11/09/2019 18:50	No		No		No		No		
43	Yes	11/09/2019 18:50	No		No		No		No		
44	Yes	11/09/2019 18:50	No		No		No		No		
45	Yes	11/09/2019 18:50	No		No		No		No		
46	Yes	11/09/2019 18:50	No		No		No		No		
47	Yes	11/09/2019 18:50	No		No		No		No		
48	Yes	11/09/2019 18:50	No		No		No		No		
49	Yes	11/09/2019 18:50	No		No		No		No		
50	Yes	11/09/2019 18:50	No		No		No		No		
51	Yes	11/09/2019 18:50	No		No		No		No		
52	Yes	11/09/2019 18:50	No		No		No		No		
53	Yes	11/09/2019 18:50	No		No		No		No		
54	Yes	11/09/2019 18:50	No		No		No		No		
55	Yes	11/09/2019 18:50	No		No		No		No		
56	Yes	11/09/2019 18:50	No		No		No		No		