



Módulo de aprendizagem Cibersegurança

Projeto: B-SAFE

Número: 2018-1CZ01-KA204-048148

Nome do autor: EDIT VALUE®

Última data de processamento: 28.10.2020

Funded by the
Erasmus+ Programme
of the European Union



"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."



Cibersegurança

Introdução

Alguma vez experienciaste um ataque malicioso no qual, por exemplo, houve uma tentativa de obtenção de um documento importante ou informação privada através de um *link* presente num *email*? Se sim, foste vítima de cibersegurança.

Hoje em dia, a cibersegurança é uma grande preocupação. **A cibersegurança envolve prevenir e detetar ataques digitais, proteger sistemas, *hardware* e *software*.** A cibersegurança também está relacionada com a prevenção, deteção, resposta e recuperação de incidentes de cibersegurança que podem ou não ser intencionais. Normalmente, os ciberataques objetivam o **acesso, modificação, roubo ou destruição de dados/informações, extorquir dinheiro ou interromper a normalidade do negócio** e das infraestruturas críticas. Sabias que, de acordo com estudos recentes, o custo total do cibercrime para cada empresa é cerca de 12.000.000€? Portanto, a cibersegurança é um debate atual que precisa de incorporar a sociedade como um todo, dado que cada indivíduo desempenha um papel importante no que toca à proteção da sua própria informação digital.



Relevância Prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

Os ciberataques estão sempre a acontecer, o que significa que manter o *software*, o *hardware*, e os dados protegidos e seguros é mais importante agora do que nunca. Apesar disto, o número de pessoas com estas competências é limitado, pelo que aprender o básico da segurança cibernética pode ser útil para garantir a segurança pessoal na Internet.

Depois de aprender esta unidade de conteúdo, terás contacto com o termo “cibersegurança” e reconhecerás a sua importância hoje em dia. Adicionalmente, nesta unidade de conteúdo aprenderás algumas medidas de cibersegurança que poderás aplicar à tua vida quotidiana.



1.Desenvolver conhecimento - Cibersegurança – definição e legislação

A proteção de dados e cibersegurança estão a tornar-se valores cada vez mais importantes para a sociedade. Devido a isso, estas duas áreas sofreram recentemente um desenvolvimento jurídico significativo e estão agora mais consolidadas na UE. Contudo, a eliminação permanente de ameaças e ataques cibernéticos é quase impossível, pelo que a implementação de medidas de cibersegurança e o reforço das capacidades de cibersegurança são obrigatórios.



A implementação de medidas eficazes de cibersegurança é particularmente desafiante atualmente, porque existem mais dispositivos do que pessoas e os *hackers* estão a tornar-se mais inovadores. No mundo conectado em que vivemos, todos beneficiamos de medidas avançadas de cibersegurança. A nível individual, um ciberataque pode resultar em tudo, desde roubo de identidade, a tentativas de extorsão, até à perda de dados importantes.

Mas o que é exatamente a “cibersegurança”?

Definição

Cibersegurança é a prática de **defender computadores, servidores, dispositivos móveis, sistemas eletrónicos, programas, redes e dados de ataques maliciosos, danos ou acessos não autorizados**. Não há uma definição padrão universalmente aceite do conceito de cibersegurança. Por outras palavras, a cibersegurança está ligada a todas as salvaguardas e medidas adotadas para defender os sistemas de informação e a sua utilização contra acessos não autorizados, ataques e danos, por forma a assegurar a confidencialidade, integridade e disponibilidade dos dados.

1.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_01_01



Situação: Qual é o significado de cibersegurança?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

- Cibersegurança inclui a defesa de *hardware* e *software*.
- Os ciberataques estão a aumentar e todos são atualmente mais vulneráveis a este tipo de incidentes.
- Medidas de cibersegurança eficazes incluem a aplicação de várias medidas de cibersegurança.
- Formação em cibersegurança deve ser ministrada o mais cedo possível devido à necessidade de aplicação de múltiplas ações de cibersegurança.

2.Desenvolver conhecimento – Cibersegurança – segurança de palavras-passe



Sabes qual é a maneira mais fácil para um cibercriminoso ganhar acesso aos teus dados do banco, redes sociais, *email* e outras informações privadas? Através de uma **password fraca**. De facto, a maioria das palavras-passe são descobertas num “piscar de olhos”. Segundo o Centro Nacional de Cibersegurança, as cinco *passwords* mais comuns em 2019 foram “123456”, “123456789”, “qwerty”, “password” e “111111”. Ou seja, se tiveres alguma dessas palavras-passe, ou outras semelhantes, por favor repara no exemplo em baixo.

Exemplo	
Quantidade de tempo para quebrar uma palavra-passe	
	
123456	0,29 milisegundos (ms)
potato	1,37 ms
Potato	3,28 s
P0tat0	1h 23m.27s 0.10ms
P0tat0!	1 mês, 3 semanas, 5 dias and 21h 54min, 40s 8ms
lAtE27P0taT0s!	47623938 milénios, 8 séculos, 73 anos and 8 meses

Um dos problemas mais comuns com as palavras-passe é que são geralmente fáceis de adivinhar. Muitas pessoas pensam que uma senha curta com muitos tipos de caracteres diferentes é segura



quando, de facto, a realidade é que a única maneira de garantir que uma senha é verdadeiramente segura é dando-lhe uma dimensão de, pelo menos, 14 caracteres e torná-la um pouco arbitrária. Além disso, como se pode ver, quanto mais complexa a *password*, mais difícil é de adivinhar. Uma palavra-passe forte é uma combinação de letras (maiúsculas e minúsculas), números e símbolos. Uma boa maneira de nunca esquecer a *password* é escolher uma frase em vez de palavras, misturando letras com caracteres alfanuméricos – a maioria dos *websites* até permitem espaços entre palavras!

Não obstante, há mais aspetos a considerar aquando da criação de novas contas e perfis digitais, por forma a maximizar plenamente a segurança e proteção cibernética. Abaixo podem ser encontradas algumas recomendações comuns do que fazer e o que não fazer no que toca às palavras-passe. Quando estas “regras de ouro” são seguidas, as palavras-passe tornam-se quase indecifráveis para os *hackers*.

NÃO FAÇAS: Usar a mesma palavra-passe para todas as contas

FAZ: Criar *passwords* únicas para contas e perfis únicos

Todos sabemos que hoje em dia quase todos os *websites* requerem uma conta e quase toda a gente usa a mesma palavra-passe para diferentes contas. Contudo, as pessoas esquecem-se frequentemente que estas contas contêm informações identitária e financeira sobre os próprios, as quais podem ser roubadas ou comprometidas e, usando apenas uma *password* para tudo, os indivíduos tornam-se alvos mais fáceis para ciberataques.

NÃO FAÇAS: Guardar a tua *password* noutra fonte

FAZ: Memorizar as tuas palavras-passe e configurar questões de segurança nas tuas contas

Uma maneira fácil que é frequentemente utilizada para lembrar palavras-passe é registá-las numa planilha, num disco rígido ou num bloco de notas pessoais. **Tenta memorizar as tuas palavras-passe!** Também podes registar as questões de segurança das suas contas, como precaução. No entanto, em vez de definir perguntas comuns como "Qual é o nome da tua mãe?" ou "De onde és?", usa perguntas que só tu sabes responder.

NÃO FAÇAS: Partilhar palavras-passe com outros

FAZ: Ser sigiloso com as tuas *passwords*

A par de usar a mesma palavra-passe para cada conta, outro erro comum está relacionado com o facto de as pessoas partilharem as suas palavras-passe com outros, através de *email*, mensagens de texto ou redes sociais.

Por forma a manter a segurança das palavras-passe, deve **alterar-se as mesmas com regularidade**. Lembra-te que, algures no mundo, há um *hacker* que continua a tentar roubar as senhas dos utilizadores e, quanto mais tempo tem para fazê-lo, maiores as hipóteses de ser bem sucedido.

NÃO FAÇAS: Escolher uma palavra-passe forte e manteres-te fiel a ela

FAZ: Mudar as senhas a cada três meses



Co-funded by the
Erasmus+ Programme
of the European Union

A maioria dos *browsers* e aplicações permitem aos utilizadores guardar as suas credenciais para que não tenham de as inserir sempre que quiserem iniciar sessão. Apesar de ser muito conveniente, tem em mente que se perderes os teus dispositivos e um estranho conseguir decifrar a tua senha de acesso, toda essa informação torna-se acessível a essa pessoa.

NÃO FAÇAS: Usar um fator de autenticação
FAZ: Acrescentar autenticação de dois fatores para cada conta digital

Se utilizares a **autenticação de dois fatores** nas tuas contas digitais, isso acrescentará uma camada extra de segurança às mesmas. Quando alguém entra na tua conta a partir de um novo local, dispositivo ou navegador, receberás uma **palavra-passe**, que precisa de ser introduzida para entrares na tua conta. Para além disso, outro tipo de autenticação de dois fatores é uma **impressão digital, uma impressão de voz ou um código enviado** para o teu telefone. Muitas pessoas pensam que isto consome muito tempo, mas se estiveres seriamente preocupado com a tua privacidade, deverás utilizar uma autenticação de dois fatores para as tuas contas digitais quando esta opção for possível. Quando não tiveres a opção de usar uma autenticação de dois fatores, deverás seguir as recomendações que foram mencionadas anteriormente.



2. Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Medidas de cibersegurança_O2_01

Situação: Selecionar de entre as frases seguintes a frase certa.

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Recomenda-se a escolha de uma senha simples para melhor memorizá-la.
- Algumas senhas únicas são compostas por alcunhas, nomes de membros da família ou de animais de estimação.
- Quanto mais caracteres especiais e símbolos a palavra-passe contém, menos difícil é de adivinhar.
- Uma *password* forte contém uma combinação de letras maiúsculas e minúsculas, símbolos e números, e pelo menos oito caracteres de comprimento.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_O2_02

Situação: Quais são algumas das regras de proteção das contas digitais de possíveis ciberataques?

Tarefa: Escolher a(s) opção(ões) certa(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Utilizar a mesma palavra-passe em múltiplos *websites*/contas.
- Alterar as palavras-passe regularmente.
- Guardar as credenciais de *login* no *browser* ou aplicação de um computador particular.
- Uma impressão digital, impressão de voz ou código PIN são boas opções para uma autenticação com dois fatores.
- Quando se cria uma nova *password*, é aconselhável evitar palavras encontradas no dicionário, pronomes, nomes de utilizador e outros termos pré-definidos, bem como palavras-passe comumente utilizadas.

3. Desenvolver conhecimento – Compras *online*

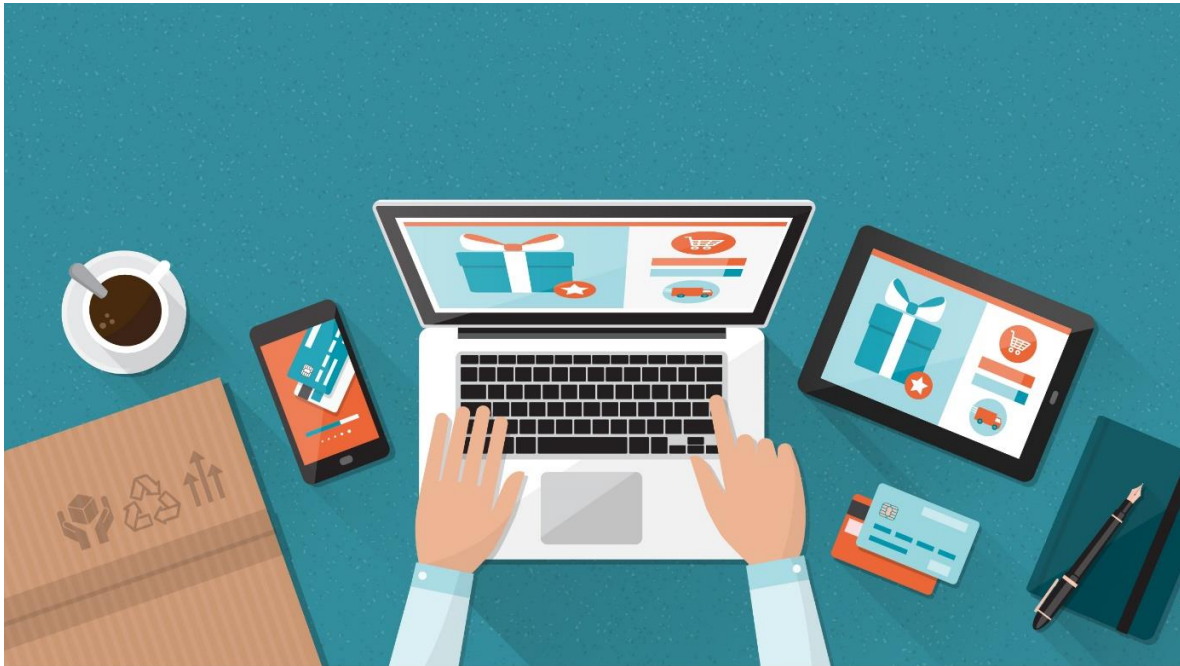
Como vimos anteriormente, a cibersegurança desenvolve a conexão entre as pessoas e a aplicação de práticas que visam proteger a informação de ataques maliciosos.

Em 2019, o comércio eletrónico foi responsável por cerca de 3,5 biliões de dólares em vendas, e espera-se que atinja 4,9 biliões de dólares até 2021. Adicionalmente, 21,8% da população mundial faz compras *online* e as marcas estão a tornar-se cada vez mais ativas nas redes sociais, o que significa que estão a interagir mais com as pessoas através de diferentes meios digitais.

Hoje em dia, cada vez mais pessoas preferem fazer compras *online* em vez de recorrer aos meios convencionais. Algumas das vantagens estão relacionadas com a conveniência, comparações de preços, conforto e acessibilidade. Normalmente, quando se compra *online*, é necessário criar uma conta. Consequentemente, há uma obrigatoriedade de ceder algumas informações privadas como “nome”, “endereço”, “número de telefone”, “*email*” e método de pagamento.

Tendo isto em mente, e dado que tudo na Internet é rastreado, não é surpresa que todos os dados que resultam da enorme quantidade de comércio eletrónico e interações nas redes sociais signifiquem que é importante conhecer mais profundamente as potenciais consequências destas ações.

Para evitar fraudes na Internet enquanto se faz compras *online* é necessário tomar algumas precauções. Abaixo encontram-se algumas sugestões:



Saber com quem se está a lidar: Lê as críticas e vê se outros consumidores tiveram uma experiência positiva ou negativa com o *site*. Certifica-te que o *website* está habilitado em termos de segurança.

Monitorizar as contas financeiras: Verifica as tuas declarações regularmente, para garantir que estas refletem os pagamentos que autorizaste

Pagar com cartão de crédito ou de débito: Os cartões de crédito são geralmente a opção mais segura, uma vez que permitem aos compradores procurar um crédito junto do emissor, se o produto não for entregue ou não corresponder à encomenda feita. Considera usar um cartão de crédito virtual de uso único. Os cartões de crédito virtuais são cartões únicos que permitem transacionar através da conta de crédito principal sem usar ou expor o número da conta principal de cartão de crédito. Podes usar, por exemplo, o Capital One para criar este tipo de cartões.

Verificar a política de privacidade: A política de privacidade descreve como as informações pessoais são recolhidas, utilizadas e partilhadas quando se visita ou faz uma compra numa loja *online*. Deves ler a política de privacidade para perceber se concordas com a privacidade da empresa.

O barato pode sair caro: Fundos de ecrã gratuitos, *e-cards* ou outros podem transportar vírus perigosos. Mantém o teu software antivírus e anti-*spyware* atualizado juntamente com a tua *firewall*.

Não enviar informação financeira por email: As empresas legítimas não pedem informações financeiras via *email* ou mensagem *pop-up*.

3. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_O3_O1



Situação: Quais são as informações que nunca se deve fornecer enquanto se faz compras *online*?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Número de segurança social.
- Código de segurança do cartão de crédito - PIN
- Número do cartão de débito.
- Número da conta bancária.
- Endereço de *email*.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_O3_O2

Situação: Da seguinte lista, escolher os comportamentos corretos de maneira a evitar ser uma vítima de um cibercrime.

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Antes de ceder informação sobre o cartão de crédito, é necessário tirar algum tempo para estudar o *website*.
- Comprar de *websites* que tenham encriptação.
- Ler a política de devoluções e outros termos e condições do *site*, bem como a política de segurança do *website* antes de encomendar alguma coisa.
- Pagar com um cartão de débito, dinheiro, ou transferência bancária.
- Usar um “*hotspot*” para proteger a confidencialidade.

4.Desenvolver conhecimento – Computação na *cloud*

Longe vão os dias quando os ficheiros eram guardados num CD ou numa *pen drive*, sempre com a terrível sensação de que eventualmente esses seriam perdidos e nunca mais encontrados de novo. Hoje em dia, os ficheiros são acessíveis a partir de qualquer computador e, de facto, as soluções em *cloud* estão a tornar-se cada vez mais usadas mundialmente nas atividades do dia-a-dia.

Interagimos constantemente com algum tipo de soluções em *cloud* quando verificamos o nosso *email* ou quando usamos os telemóveis para verificar informações de trânsito. **Com as soluções “na nuvem”, os nossos dados são armazenados junto de um fornecedor e acedidos através da Internet.**

Portanto, a questão que se impõe neste contexto é se os nossos dados estão seguros e protegidos na *cloud*? Devido a isso, é importante saber mais sobre o conceito de computação na *cloud*.



Definição

Computação na *cloud* pode ser definida como a **entrega de recursos informáticos mediante solicitação** - tais como armazenamento, capacidade computacional ou capacidade de partilha de dados – via Internet, através do alojamento em servidores remotos.

Por outras palavras, a computação na *cloud* significa armazenar e aceder a dados e programas através da Internet, em vez do disco rígido do computador. Estes recursos incluem ferramentas e aplicações como armazenamento de dados, servidores, bases de dados, redes e *software*. As soluções “na nuvem” são uma opção muito popular para pessoas e negócios, por variadas razões, entre as quais a poupança de custos, aumento da produtividade, velocidade e eficiência, desempenho e segurança.

A *cloud*, os megadados e a digitalização da indústria são acompanhados por um crescimento na exposição das vulnerabilidades, permitindo a pessoas maliciosas lesar ainda mais vítimas. A variedade dos tipos de ataques e a sua crescente sofisticação tornam verdadeiramente difícil acompanhar o seu ritmo. Por causa disso, **é importante implementar algumas precauções diárias por forma a evitar o roubo, fuga e/ou eliminação de informações importantes.**

Consulta em baixo um breve resumo de algumas medidas a aplicar de modo a melhorar a segurança da computação em *cloud*.

Usar uma autenticação multi-factor	A combinação tradicional de nome de utilizador e <i>password</i> é muitas vezes insuficiente na proteção de contas de utilizadores de <i>hackers</i>, e o roubo de credenciais é uma das principais formas através das quais os <i>hackers</i> acedem aos dados/informações. Por causa disso, deve usar-se não só uma palavra-passe forte mas também uma autenticação multi-factor – também conhecida como autenticação de dois fatores – para assegurar que apenas o pessoal autorizado possa entrar nas suas aplicações na <i>cloud</i> e aceder a esses dados sensíveis. Uma autenticação multi-factor é uma das formas mais eficazes de impedir os <i>hackers</i> de aceder às aplicações na <i>cloud</i>. Alguns exemplos de autenticações multi-
---	---



	factor são uma senha combinada com um código enviado por SMS ou com um número gerado por uma aplicação. Também é importante lembrar sempre de terminar sessão e nunca guardar credenciais.
Gerir o acesso dos utilizadores para melhorar a segurança da computação em cloud	A maioria das pessoas não necessitam de acesso a todas as informações, todas as aplicações ou todos os ficheiros. Por conseguinte, estipular níveis adequados de autorização garante que cada pessoa só pode visualizar ou manipular as aplicações ou os dados/informações aos quais necessitam de aceder. Se alguém tiver acesso a tudo, e for enganado por um <i>email</i> de <i>phishing</i> que o leve a ceder a sua informação de <i>login</i>, o <i>hacker</i> terá acesso a toda a informação muito facilmente.
Monitorizar, registar e analisar atividades de utilizadores com soluções automatizadas para detetar intrusos	A monitorização e análise em tempo real das atividades dos utilizadores pode ser útil para se detetarem eventuais irregularidades que se desviam dos comportamentos/padrões normais. Estas atividades invulgaes podem indicar uma violação no sistema, pelo que descobri-las cedo pode travar os <i>hackers</i> e permitir que se resolvam os problemas de segurança antes que as coisas corram mal. É possível encontrar variadas soluções para esta monitorização e gestão automatizada e constante das redes, bem como adotar soluções avançadas de cibersegurança. Uma vez que cada empresa/pessoa tem diferentes necessidades correspondentes a diferentes níveis de cibersegurança, é pertinente obter uma avaliação de terceiros antes de fazer um grande investimento.
Formação anti-<i>phishing</i>	Os <i>hackers</i> conseguem aceder a informações seguras através do roubo de credenciais, recorrendo a técnicas como <i>phishing</i>, <i>websites</i> falsificados e espionagem de redes sociais. É, por isso, necessário manter em mente que, por exemplo, a formação <i>anti-phishing</i> deve ser um processo contínuo gerido por alguém interino à organização, a fim de o tornar eficaz.
Fazer cópias de segurança de ficheiros em diferentes contas da cloud	Independentemente da escala, indústria, região e/ou pessoa, assegurar a disponibilidade dos dados é uma prioridade para todos. Adicionalmente, a probabilidade de se perderem dados/informação devido a erro humano é muito alta, por isso é pouco recomendável que se ponham todos os dados importantes num só lugar. Quer estejas a proteger e a aceder aos ficheiros no teu portátil pessoal ou sejas um fornecedor de serviços de gestão responsável por uma carteira de negócios (e a sua crescente quantidade de dados), as aplicações na “nuvem” são essenciais no mundo digital moderno. Por isso, é essencial encontrar mais do que uma solução de <i>backup</i> “<i>cloud-to-cloud</i>” (guardar cópias de segurança do conteúdo de uma cloud numa outra cloud) por forma a garantir que existe uma cópia dos dados criados, armazenados e



partilhados num local seguro.

4. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_O4_O1

Situação: Relativamente à computação em *cloud*, qual das seguintes afirmações é verdadeira?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Numa Plataforma como um Serviço (*Platform as a Service – PaaS*), uma empresa paga por serviços tais como o armazenamento, redes e virtualização.
- Infraestrutura como um Serviço (*Infrastructure as a Service – IaaS*) é um modelo de computação em *cloud* no qual um terceiro fornecedor providencia ferramentas de *hardware* e *software*.
- *Software* como um Serviço (*Software as a Service – SaaS*) é um modelo de licenciamento e entrega de *software* em que o *software* é licenciado com base em subscrições e é alojado centralmente.
- Enquanto usam computadores em *cloud*, os utilizadores e empresas têm de gerir servidores físicos.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Medidas de cibersegurança_O4_O2

Situação: Da seguinte lista, escolher os comportamentos corretos de maneira a evitar ser uma vítima de um cibercrime.

Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Guardar informações como moradas, números de telefone, informações bancárias, etc., em diferentes *clouds*.
- Criar uma *password* única exclusivamente para o serviço *cloud*.
- Enquanto se usam soluções da *cloud*, não é relevante ter um antivírus.
- Graças à sua conveniência, sugere-se que se guardem credenciais de *login* nas aplicações correspondentes.

Fontes

Alexandra, Susan (04 de abril de 2019). 10 Tips for Keeping Your Personal Data Safe on Social Media. Retirado de <https://securitytoday.com/Articles/2019/04/04/10-Tips-for-Keeping-Your-Personal-Data-Safe-on-Social-Media.aspx?Page=2>

Cucu, Paul (21 de dezembro de 2016). 17 Underused Online Shopping Security Tips. Retirado de <https://heimdalsecurity.com/blog/online-shopping-security-tips/>

European Commission (março de 2019). Briefing Paper: Challenges to effective EU cybersecurity policy, Briefing paper. European Court of Auditors.



Federal Trade Commission (n.d.). 9 Online Shopping Tips. Retirado de <https://www.yumpu.com/en/document/read/4010016/nine-online-shopping-tips-federal-trade-commission>

Kapiswe, Subham (23 de abril de 2019). NCSC Reveals List Of World's Most Hacked Passwords. Retirado de https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#cite_note-NCSCList-15

Kaspersky (n.d.). Safer Online Shopping. Retirado de <https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping>

National Cybersecurity Alliance (n.d.). Online Safety Basics: Online Shopping. Retirado de <https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/>

Acronis (n.d.). Case study: The Benefits of Cloud-to-Cloud Backup Solutions from Acronis. Retirado de <https://www.acronis.com/en-us/articles/cloud-to-cloud-backup/>

D'Silva, Frank (15 de junho de 2020). 6 Tips for Improving Cloud Computing Security. Retirado de <https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security>

Guardar conhecimento

Resumo

A era da Internet concedeu-nos o superpoder da onnipresença. Reduziu o poço entre pessoas, empresas e lugares, permitindo que as pessoas estivessem em qualquer lugar e com qualquer pessoa, com apenas um clique.

Como foi demonstrado ao longo desta unidade de conteúdo, **a privacidade online e a segurança de informações pessoais é uma responsabilidade partilhada por todas as entidades:** governo, programadores de *software*, fornecedores de serviços de *cloud*, empresas e utilizadores finais.

Com a implementação do RGPD, os utilizadores finais ganharam mais confiança na proteção dos seus dados, uma vez que este regulamento visa salvaguardar a privacidade dos indivíduos na Internet. Contudo, há muitos comportamentos que os utilizadores finais devem adotar para cumprirem com a sua parte. Esses comportamentos são comuns a todas as atividades na Internet – desde as regras sociais até à *cloud* – e são geralmente referidos como “as regras de ouro da Internet”.

A primeira regra refere-se às palavras-passe: **ter senhas únicas e fortes com autenticação de dois fatores quando do login e mudá-las a cada três meses.**

A segunda regra está relacionada com informação privada: **não é recomendado guardar ou partilhar informação sensível através da Internet**, especialmente quando se fazem compras *online*; além disso, quando existe informação privada na *cloud*, **é sempre sensato garantir que não se agrega toda a informação numa só “nuvem”!**

A terceira regra é praticar uma navegação inteligente: **não guardar credenciais de login** em nenhum *browser*, *website* ou aplicação, e terminar a sessão sempre que sair de um *website*. Do mesmo modo, **não é aconselhável clicar em qualquer ligação duvidosa** ou introduzir informação privada em *websites* não seguros.

Em geral, devemos reconhecer que são os nossos dados que podem eventualmente ser comprometidos por ciberataques e, consequentemente, devemos garantir que cumprimos a nossa parte na privacidade e segurança dos dados na Internet.



As respostas corretas estão assinaladas a negrito

Situação: Qual é o significado de cibersegurança?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

- Cibersegurança inclui a defesa de **hardware e software**.
- Os ciberataques estão a aumentar e todos são atualmente mais vulneráveis a este tipo de incidentes.
- Medidas de cibersegurança eficazes incluem a aplicação de várias medidas de cibersegurança.
- Formação em cibersegurança deve ser dada o mais cedo possível devido à necessidade de aplicação de múltiplas ações de cibersegurança.

Situação: Seleccionar de entre as frases seguintes a frase certa.

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Recomenda-se a escolha de uma senha simples para melhor memorizá-la.
- Algumas senhas únicas são compostas por alcunhas, nomes de membros da família ou de animais de estimação.
- Quanto mais caracteres especiais e símbolos a palavra-passe contém, menos difícil é de adivinhar.
- **Uma password forte contém uma combinação de letras maiúsculas e minúsculas, símbolos e números, e pelo menos oito caracteres de comprimento.**

Situação: Quais são algumas das regras de proteção das contas digitais de possíveis ciberataques?

Tarefa: Escolher a(s) opção(ões) certa(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Utilizar a mesma palavra-passe em múltiplos *websites*/contas.
- **Alterar as palavras-passe regularmente.**
- Guardar as credenciais de *login* no *browser* ou aplicação de um computador particular.
- **Uma impressão digital, impressão de voz ou código PIN são boas opções para uma autenticação com dois fatores.**
- Quando se cria uma nova *password*, é aconselhável evitar palavras encontradas no dicionário, pronomes, nomes de utilizador e outros termos pré-definidos, bem como palavras-passe comumente utilizadas.

Situação: Quais são as informações que nunca se deve fornecer enquanto se faz compras *online*?

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Número de segurança social.**
- **Código de segurança do cartão de crédito - PIN**
- **Número do cartão de débito.**
- **Número da conta bancária.**
- Endereço de *email*.

Situação: Da seguinte lista, escolher os comportamentos corretos de maneira a evitar ser uma vítima de um cibercrime.

Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.



- Antes de ceder informação sobre o cartão de crédito, é necessário tirar algum tempo para estudar o *website*.
- Comprar a partir de *websites* que tenham encriptação.
- Ler a política de devoluções e outros termos e condições do *site*, bem como a política de segurança do *website* antes de encomendar alguma coisa.
- Pagar com um cartão de débito, dinheiro, ou transferência bancária.
- Usar um “*hotspot*” para proteger a confidencialidade.

Situação: Relativamente à computação em *cloud*, qual das seguintes afirmações é verdadeira?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Numa Plataforma como um Serviço (*Platform as a Service – PaaS*), uma empresa paga por serviços tais como o armazenamento, redes e virtualização.
- Infraestrutura como um Serviço (*Infrastructure as a Service – IaaS*) é um modelo de computação em *cloud* no qual um terceiro fornecedor providencia ferramentas de *hardware* e *software*.
- ***Software* como um Serviço (*Software as a Service – SaaS*) é um modelo de licenciamento e entrega de *software* em que o *software* é licenciado com base em subscrições e é alojado centralmente.**
- Enquanto usam computadores em *cloud*, os utilizadores e empresas têm de gerir servidores físicos.

Situação: Da seguinte lista, escolher os comportamentos corretos de maneira a evitar ser uma vítima de um cibercrime.

Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Guardar informações como moradas, números de telefone, informações bancárias, etc., em diferentes *clouds*.**
- **Criar uma *password* única exclusivamente para o serviço *cloud*.**
- Enquanto se usam soluções da *cloud*, não é relevante ter um antivírus.
- Graças à sua conveniência, sugere-se que se guardem credenciais de *login* nas aplicações correspondentes.