Módulo de aprendizagem

Proteção de dados pessoais nas redes sociais

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

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

Proteção de dados pessoais nas redes sociais

Introdução

Em 2010, o famoso programa televisivo de comédia *Saturday Night Live* fez um *sketch* sobre as redes sociais. Durante o programa, este ator fez-se passar por Julian Assange (fundador da plataforma WikiLeaks) e declarou, de forma alegre e sarcástica: "Eu dou-vos informações privadas sobre grandes empresas de graça e sou um vilão. O criador do Facebook Mark Zuckerberg dá a vossa informação às grandes empresas, em troca de dinheiro, e depois é considerado o Homem do Ano [pela revista Time]". É possível compreender a ligação entre este *sketch* de comédia e a realidade? Como te sentes ao ceder gratuitamente os teus dados a uma empresa enquanto esta ganha dinheiro com isso? Será que os nossos dados estão seguros enquanto utilizamos as redes sociais?

Obviamente, hoje em dia, a proteção de dados pessoais nas redes sociais é um tema muito importante. A utilização das redes sociais está a crescer exponencialmente e é, atualmente, uma parte essencial da vida quotidiana da maioria das pessoas em todo o mundo. Desde o nosso colega do escritório até à nossa avó, quase todos usam as redes sociais para partilhar fotografias, vídeos e conversas com amigos ou familiares, publicando informação pessoal em geral e criando uma sensação de proximidade.

No entanto, como a utilização das redes sociais está tão enraizada nos nossos hábitos como indivíduos e sociedade, a maioria das pessoas baixou a guarda quando se trata de cibersegurança, o que pode ter consequências graves a longo prazo.

Quem mais terá acesso a estes dados?

Assim sendo, há muito a aprender sobre a proteção de dados e informações pessoais enquanto se utiliza as redes sociais, como se verá neste módulo de aprendizagem.

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

Com as aprendizagens concretizadas neste módulo, será possível identificar os riscos de privacidade mais relevantes associados à utilização de redes sociais, bem como saber como se proteger adequadamente.

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

1.Desenvolver conhecimento - Proteção de dados pessoais nas redes sociais

Definição
As **redes sociais** são tecnologias interativas mediadas por computadores que facilitam a **criação ou partilha** de informação, ideias, interesses de carreira e outras formas de expressão através da criação de comunidades e redes virtuais. O objetivo das redes sociais é possibilitar a **conexão e partilha de informação com qualquer pessoa na Terra ou com muitas pessoas simultaneamente**. Podem ser usadas como uma forma de interagir com amigos e familiares ou como uma ferramenta de marketing pelas empresas. As redes sociais são uma digital que permite aos utilizadores criar e partilhar rapidamente conteúdos com outras pessoas.

Na caixa acima é apresentada uma definição ampla das redes sociais. A realidade é que, como existem 3,5 mil milhões de utilizadores ativos das redes sociais em todo o mundo, estas evoluíram de uma forma que, atualmente, permite a divisão em diferentes categorias, consoante os interesses e intenções do utilizador. A seguir, é apresentada uma lista dos 10 tipos de redes sociais, de acordo com o seu intuito:

	Propósito	Exemplo
Redes sociais	Conectar pessoas e marcas *online*	Facebook; Twitter; LinkedIN
Redes de partilha de conteúdo multimédia	Encontrar e partilhar imagens, vídeos, vídeos ao vivo, e outros tipos de conteúdo multimédia *online*	Instragram; Youtube; Tik Tok
Fóruns de debate	Encontrar, discutir e partilhar notícias, informações e opiniões	Reddit; Quora
Redes de partilha de conteúdo	Descobrir, guardar, partilhar e discutir conteúdos e material multimédia viral	Pinterest; Flipboard
Redes de opiniões de clientes	Encontrar e partilhar opiniões e informações sobre marcas, produtos e serviços, bem como restaurantes, destinos de viagem, etc	Yelp; Zomato, Tripadvisor
Blogs e redes de publicação editorial	Publicar, descobrir e comentar conteúdos *online*	Wordpress; Tumblr
Redes de compras e vendas comunitárias	Detetar tendências, seguir marcas, partilhar grandes descobertas e fazer compras	Etsy
Redes baseadas em interesses	Conectar com outras pessoas que partilham dos mesmos interesses ou hobbies	Goodreads; Last.Fm

Redes de economia partilhada	Anunciar, encontrar, partilhar, comprar, vender e trocar produtos e serviços entre pares	Airbnb; Uber; Glovo
Redes sociais anónimas	Para fofocar, desabafar e bisbilhotar	Whisper; Ask.fm

Não há dúvidas que vivemos na era das redes sociais. Por causa disso, existem **múltiplas questões legais** que surgem quando as pessoas partilham conteúdos *online* através de diferentes plataformas, tais como o Instagram, Pinterest, Facebook, entre outros. Os direitos mais importantes das redes sociais estão relacionados com **quem é o proprietário do conteúdo a ser partilhado, quando e onde se considera que a partilha é adequada e que limites podem ser impostos às partilhas**. Estes direitos levantam frequentemente questões relacionadas com a **violação de marcas registadas, violação de direitos de autor, marketing nas redes sociais, relações laborais** e muito mais. Encontra-se em baixo uma breve lista sobre os direitos mais importantes dos meios de comunicação social para o Instagram, Whatsapp, Youtube e Facebook.

1. Oficialmente, os utilizadores são proprietários das fotografias e/ou vídeos que postam, mas é possível que outros paguem para usar esses conteúdos e o Instagram não paga ao proprietário por esse uso
2. Cada um é responsável por todas as ações que toma enquanto usa o Instagram e por todas as publicações feitas
3. Ainda que cada indivíduo seja responsável pela informação divulgada nesta rede social, o Instagram pode guardar, usar e partilhar informação pessoal com outras empresas ligadas ao Instagram
4. Cada um pode apagar a sua conta do Instagram mas, apesar de as fotos, *posts* e perfil desaparecerem da conta apagada, quaisquer conteúdos afetos à conta apagada (fotos, informação pessoal) partilhados ou utilizados por outrem, para qualquer fim, podem continuar a aparecer nesta rede social

1. Um utilizador do Whatsapp pode mudar o nome de perfil, fotografia e mensagem de estado sempre que quiser
2. O número de telemóvel, nome de perfil, foto, estado, mensagem de estado, último uso da aplicação e recibos de mensagem podem ser visíveis para qualquer outra pessoa que use o Whatsapp. Isto pode ser alterado nas configurações, onde também é possível bloquear pessoas e controlar com quem se conversa
3. Depois de as mensagens serem entregues, são apagadas do sistema e ficam armazenadas apenas no próprio telemóvel ou dispositivo. As mensagens são encriptadas, o que significa que a empresa proprietária do Whatsapp não as consegue ler
4. Outras empresas não têm autorização para colocar anúncios na aplicação do Whatsapp a menos que estejam conectadas com o próprio utilizador

1. Quando se cria uma conta do YouTube, os dados gerados são recolhidos pelo Google. É

possível determinar quais as informações que o YouTube pode recolher através do "controlo de atividade" (opção *activity control*) da conta Google. Adicionalmente, a informação pessoal é partilhada pelas várias empresas da Google sem o consentimento dos utilizadores
2. É possível requisitar ao YouTube um relatório sobre as informações que contem sobre o próprio utilizador e pedir à empresa que retifique ou elimine essas informações
3. É possível pedir ao YouTube que elimine uma aparição indesejada do próprio num vídeo: basta enviar o URL à empresa, dizer o minuto exato em que o próprio ou a informação pessoal aparece no vídeo e explicar como é que esse conteúdo se destaca de outras pessoas ou informações alheias no vídeo
4. Se alguém reclamar de um vídeo num canal e o YouTube der razão ao queixoso, o dono do canal será notificado sobre a reclamação, e terá de eliminar o vídeo ou editar os detalhes pessoais

1. Mesmo que um perfil seja privado, convém manter em mente que outras pessoas podem ver e partilhar informação divulgada por terceiros sobre o próprio. As outras pessoas também podem guardar informação pessoal publicada pelo próprio nos seus telemóveis e dispositivos
2. Algumas empresas vão partilhar informação pessoal sobre utilizadores do Facebook com o próprio Facebook e o Facebook também vai partilhar informações pessoais com outras empresas
3. Quando se consente o uso de uma aplicação dentro do Facebook, essa aplicação pode ser capaz de usar, partilhar e armazenar a informação partilhada pelo próprio no Facebook
4. Quando se apaga uma conta do Facebook, as publicações feitas são apagadas, mas as partilhas alheias afetas ao perfil apagado não serão eliminadas

1.1. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de dados pessoais nas redes sociais_01_01

Situação: O que são as 'redes sociais'?
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.

- *Websites* e aplicações que permitem às pessoas enviar mensagens e fotografias.
- As redes sociais são uma forma de comunicação eletrónica (como *websites* para relacionamentos sociais).
- *Websites* e programas de computador que permitem às pessoas comunicar e partilhar informações na Internet utilizando um computador ou telemóvel.
- As redes sociais referem-se a *websites* e aplicações que são concebidos para partilhar conteúdos rapidamente.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Proteção de dados pessoais nas redes sociais_01_02

Situação: Quais são os direitos de proteção de dados pessoais que se aplicam no Whatsapp?
Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: apenas uma resposta está errada.

- O direito de encriptação das mensagens, o que significa que o WhatsApp não pode ler as mensagens enviadas a outras pessoas.

- O direito de eliminar a própria conta do Whatsapp, sem que haja a eliminação das mensagens entregues a outras pessoas.
- Se se apagar simplesmente a aplicação Whatsapp no próprio dispositivo, sem apagar a conta, a informação pessoal será mantida.
- O WhatsApp guarda e armazena informações sobre cada um de nós, e nós não podemos voltar a utilizar essas informações em mais nenhum lado do mundo.

2.Desenvolver conhecimentos - Os riscos mais comuns das redes sociais

Hoje em dia, é do conhecimento geral que as redes sociais integram os nossos interesses e atividades diárias. No entanto, será que todos partilhamos os mesmos hábitos e comportamentos relativos à utilização das redes sociais? Para compreender a relevância das redes sociais na nossa sociedade, é importante que estejamos a par das mais recentes estatísticas relativamente às redes sociais. Apresentamos de seguida as 10 estatísticas mais relevantes sobre redes sociais:

AS 10 ESTATÍSTICAS MAIS RELEVANTES SOBRE AS REDES SOCIAIS

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

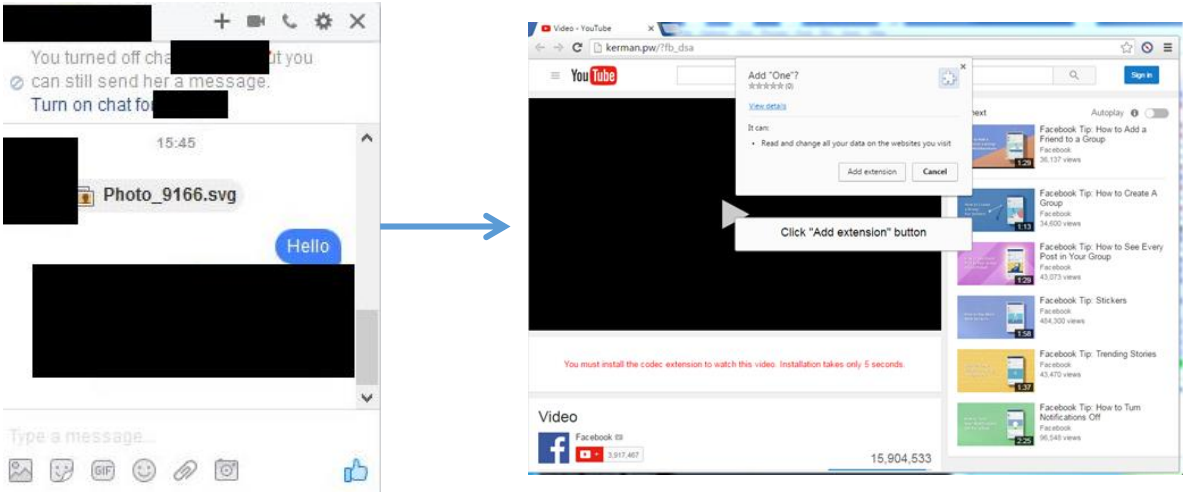
81% das Pequenas e Médias Empresas utilizam atualmente as redes sociais para impulsionar o crescimento dos seus negócios e 9% planeiam utilizá-las no futuro (LinkedIN, 2014)

Em média, as pessoas têm 7,6 contas nas redes sociais (Clement, 2019)

Com este tipo de estatísticas, não é de admirar que as redes sociais se estejam a tornar uma das plataformas mais usadas para a recolha de dados dos utilizadores quer perpetuadas pela própria rede de forma legal quer por *hackers* com intenções maliciosas.
O risco mais preeminente das redes sociais é o *malware* que pode comprometer todos os dados pessoais. Existem diferentes tipos de *malware* com diferentes propósitos, como se pode ver abaixo:

1. ***Ransomware*** - É um *software* que usa criptografia para impossibilitar o acesso do indivíduo-alvo aos seus dados, como fotografias ou documentos, até que um resgate seja pago. Este *malware* é ativado quando o utilizador clica num *link* colocado numa rede social ou numa imagem que redireciona o utilizador para um *website* externo, o qual, por sua vez espalha o código malicioso.

Exemplo de um *ransomware*
As aplicações de *chat* como o Whatsapp e o Facebook Messenger são frequentemente usados para ataques de *ransomware*. Neste exemplo, os cibercriminosos enviam, pelo Facebook Messenger, mensagens enganosas que contêm anexos de imagens SVG. Os utilizadores que clicam na imagem são transportados para um *pop-up* que convida à instalação de uma extensão no *browser* ou um *add-on* para ver um vídeo. Mais tarde, após o código malicioso infetar o sistema dos utilizadores, aparece um outro *pop-up*, exigindo um pagamento para desbloquear os ficheiros do utilizador.



2. **Cavalo de Tróia (*Trojan horse*) -** É um tipo de código ou *software* malicioso que parece legítimo mas que pode assumir o controlo do computador. Um cavalo de tróia é concebido para roubar dados (*logins*, dados financeiros e até dinheiro eletrónico), instalar mais *malware*, modificar ficheiros, monitorizar a atividade do utilizador (observação de ecrã, *keylogging*, etc.), utilizar o computador em *botnets* e tornar anónima a atividade na Internet por parte do atacante. Um *Trojan* atua como uma aplicação ou ficheiro legítimo para enganar os indivíduos e leva-los a descarregar e instalar *malware*. Uma vez instalado, um *Trojan* pode executar a ação para a qual foi concebido.

Normalmente, um cavalo de Tróia encontra-se escondido em publicidade falsa ou é enviado aos utilizadores através de mensagens instantâneas.

3. Vírus - Uma forma de *malware* que é capaz de se reproduzir e de se espalhar para outros computadores. Os vírus propagam-se frequentemente para outros computadores, anexando-se a vários programas e executando código quando um utilizador executa um desses programas infetados. Os vírus podem também propagar-se através de ficheiros de *script*, documentos e vulnerabilidades de *cross-site scripting* em aplicações *web*. Os vírus podem ser utilizados para roubar informação, prejudicar computadores e redes anfitriões, criar botnets, roubar dinheiro, fazer publicidade e muito mais.

4. *Greyware* - Uma forma de *malware* que, no fundo, não faz qualquer dano físico aos dados, ao contrário de outros *malwares*, mas apresenta-se de modos mais incómodos, como *adware* e *spyware*. Tem uma alta prevalência nas redes sociais, geralmente sob a forma de "*click bait*" ('isco de cliques'), quando um artigo cativante leva os utilizadores a um *website* que lhes pede para fazer uma ação, como instalar um falso *plugin* de redes sociais ou preencher um inquérito rápido antes de aceder à notícia em si. A informação desejada é então extraída e vendida a outros cibercriminosos e pode, inclusive, ser utilizada em tentativas de invadir contas pessoais.

Exemplo de *Greyware*
Um exemplo infame ocorreu após a morte do ator Robin Williams, em 2014. Apenas 48 horas depois da sua morte, um suposto vídeo de despedida de Williams começou a circular no Facebook. Os utilizadores que clicaram no *link* para o dito vídeo foram conduzidos a um *site* falso da BBC News. Depois, foram instruídos a partilhar o vídeo no Facebook antes de o poderem ver. Depois de partilharem o conteúdo conforme solicitado, uma segunda página falsa apareceu e solicitou o preenchimento de um inquérito *online*. Foram recolhidas informações pessoais e depois vendidas a comerciantes inescrupulosos na Internet.

5. *Worms* - Os *worms* estão entre os tipos mais comuns de *malware*. Os *worms* conseguem modificar e apagar ficheiros, roubar dados, instalar uma "porta dos fundos" e permitir que um *hacker* ganhe controlo sobre um computador e as configurações do seu sistema. Podem até injetar *software* malicioso adicional num computador. Os *worms* podem ser transmitidos através de vulnerabilidades de *software* ou podem penetrar o computador através de anexos em *emails* de *spam* ou mensagens instantâneas. Uma vez abertos, estes ficheiros podem fornecer um *link* para um *website* malicioso ou descarregar automaticamente os *worms*. Uma

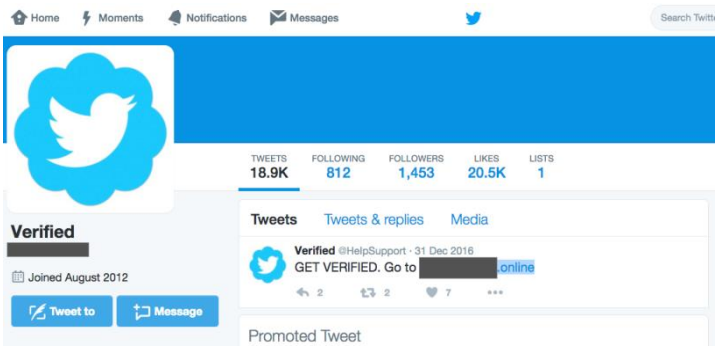
vez instalado, o *worm* infeta o dispositivo silenciosamente, sem o conhecimento do utilizador. Os *worms* propagam-se frequentemente enviando mensagens instantâneas em massa, com anexos infetados, aos contactos dos utilizadores.

Como se pode observar, todo este *malware* utiliza a mesma estratégia para atrair o utilizador, nomeadamente, esquemas ou ataques de *phishing*. Os **ataques de *phishing*** utilizam fontes maliciosas para recolher informações pessoais e financeiras ou infetar o dispositivo do utilizador com *malware*.
O primeiro passo de um anexo de *phishing* é sempre o mesmo: aparece um *link*, foto, vídeo, um artigo, ou um anúncio no seu *feed* de redes sociais ou na sua aplicação de mensagens instantâneas. Pode parecer ter vindo de qualquer pessoa - uma fonte de notícias, uma celebridade, um negócio, a própria rede social ou mesmo um contacto de confiança. Na maioria das vezes, essas fontes são imitações de contas reais ou utilizadores cuja conta na rede social tenha sido comprometida ou cuja identidade tenha sido roubada.

Exemplo de uma conta impostora

O Twitter tem uma ferramenta que verifica a legitimidade das contas a fim de reduzir a atividade fraudulenta, denominada "Twitter *Verified*". Esta é a verdadeira conta:

Não demorou muito tempo até aparecer uma conta clone, alegando ser a verdadeira conta de verificação e direcionando os utilizadores para todo o tipo de *payloads* maliciosas.



O *phishing* nas redes sociais joga com as emoções e necessidades humanas básicas, como a confiança, segurança, luto, medo de perder dinheiro, desejo de receber algo em troca de nada, vontade de encontrar uma pechincha ou desejo de encontrar amor ou popularidade/estatuto. Geralmente também declaram ou insinuam a necessidade de agir urgentemente para evitar um problema ou tirar partido de uma oferta.

Exemplos de *scams* de *Phishing*
• OMG! Já viste esta fotografia tua? • Detalhes secretos sobre a morte de Michael Jackson! • Apenas 1% das pessoas consegue resolver este desafio! Completa o quizz agora! • A Adidas está a oferecer 3.000 pares de sapatos grátis para celebrar o seu 93º aniversário. Consiga já os seus sapatos grátis! Estes são esquemas de *phishing* muito comuns que envolvem uma pergunta, uma celebridade, uma marca ou um facto que desperte o interesse do utilizador e depois direcionam-nos para um *login* falso por forma a obter informações de *login* ou instalam automaticamente *malware* num computador.

O segundo passo de um ataque de *phishing* é redirecionar o utilizador para um *website* que solicita detalhes confidenciais ou faz com que o computador ou dispositivo móvel seja infetado por *malware*. Este *malware* pode ser instalado automaticamente ou após solicitação de *download* de um programa, extensão de um *browser* ou aplicação.

Em alternativa, o *post*, *tweet* ou mensagem pode instruir o utilizador a fazer uma chamada telefónica para um número específico. Isto pode resultar no pedido de detalhes confidenciais ou na adição de uma taxa exorbitante à conta telefónica.

2. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de dados pessoais nas redes sociais_02_01

Situação: Qual dos seguintes factos é falso?
Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é falsa.
As redes sociais são um instrumento de marketing eficaz para as empresas

- O Facebook é a rede social mais utilizada
- A maioria dos utilizadores das redes sociais acede às plataformas através de dispositivos móveis
- Hoje em dia, as pequenas e médias empresas utilizam as redes sociais para impulsionar o crescimento dos seus negócios
- Os utilizadores tendem a escolher uma só rede social, utilizando-a todos os dias

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Proteção de dados pessoais nas redes sociais _02_02

Situação: Estás a navegar no Facebook e vês a seguinte publicação:

O que deves fazer?

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

- Meu deus, hoje é o meu dia de sorte! Clico em "CONTINUAR" e dou-lhes todos os dados necessários para ganhar o cartão oferta. Depois disso, partilho esta oportunidade com todos os meus amigos do Facebook!
- Só tenho 4 minutos para reclamar o meu preço! Clico em "CONTINUAR" e dou-lhes todos os dados necessários para ganhar o prémio. Mas depois de ver que tenho de dar detalhes bancários, desisto pois dá demasiado trabalho.
- Fico curioso e clico em "CONTINUAR". Depois de ver que é necessário dar-lhes dados pessoais, fecho o separador. Acho que é um golpe.
- Não clico na publicação. Não posso ganhar uma lotaria em que nunca participei! Assinalo a publicação como fraudulenta, alertando o Facebook que é um *scam*.

3.Desenvolver conhecimento - algumas dicas de segurança para o uso de redes sociais

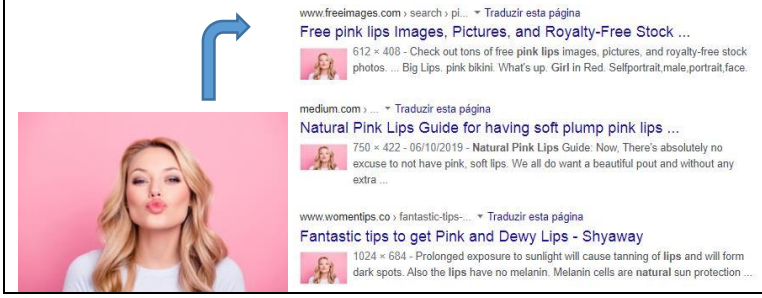
Agora que já conhecemos a enorme variedade de riscos de utilização das redes sociais, não vale a pena sentirmos que a única solução para garantir a segurança e privacidade é eliminar as todas as contas das redes sociais! O segredo é utilizar as redes sociais ao mesmo tempo com uma maior compreensão dos riscos e sabendo como agir adequadamente.
Existem alguns comportamentos comuns de burlões e *hackers* que nos podem alertar para a possibilidade de um esquema de *phishing*. Enquanto navegamos na rede social de eleição devemos estar sempre atentos a estes sinais de alerta que indicam que um *post* é uma tentativa de *phishing*:

Sinal de alerta #1: Pedidos de amizade de estranhos

Recebeste um pedido de amizade de um desconhecido? Alguém que não reconheces enviou-te uma mensagem privada? Uma empresa ou uma figura pública pediu para te começar a seguir?
Plataformas como o Facebook, Instagram e Twitter estão cheias de perfis falsos com a intenção de aplicar um golpe de *phishing*. Não aceites quaisquer pedidos de amizade sem verificação. Se alguém te estiver a incomodar, é boa ideia denunciar e bloquear tais perfis.

Dica rápida
Fazer uma pesquisa inversa da foto do perfil. Na maioria das vezes, os *hackers* usam fotografias já

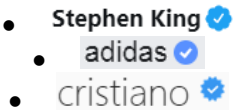
disponíveis *online*. Se surgirem resultados de diferentes *websites* que utilizam essa fotografia para diferentes fins a conta é falsa.



Dica rápida

Já reparaste na marca de verificação azul ao lado dos nomes de celebridades ou de empresas em plataformas sociais? É este o aspeto dela:

- Twitter:
- Facebook:
- Instagram:



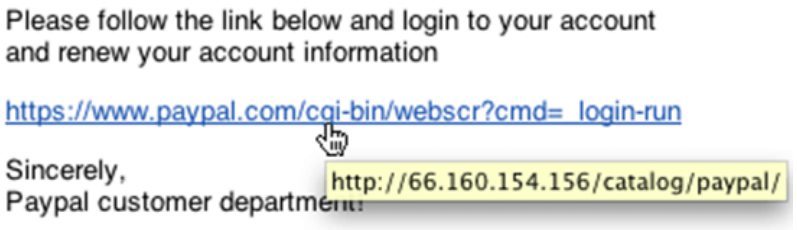
Esta marca de verificação está implementada em quase todas as redes sociais e significa que **a conta é verificada** como autêntica e pertence a uma celebridade ou a uma marca líder da indústria.
Por exemplo, se receberes uma mensagem direta da conta "Twitter *Verified*" sem a marca de verificação, cuidado - é provável que seja falso!

Sinal de alerta #2: Clique neste *link*!

O objetivo de um ataque de *phishing* é geralmente o de levar as pessoas a descarregar um anexo (por exemplo, uma foto enviada numa mensagem direta) ou a clicar num *link*. Por vezes, os criminosos imitam fontes de confiança para incentivar as pessoas a clicar num *link* (ou a descarregar uma aplicação) que contém *malware*. O que parece ser um *link* legítimo pode ser um *link* disfarçado que remeta para um *website* criminoso.
Portanto, não é recomendado clicar em qualquer *link* que redirecione para outro *site*. Em vez disso, é mais seguro ir diretamente para a fonte - *website* da marca, página do banco, etc - e confirmar se se vê nas redes sociais o verdadeiro anúncio ou publicidade.

Dica rápida

Uma forma rápida de atestar se a hiperligação redireciona para uma fonte de confiança é passar o rato por cima do texto da hiperligação. Se se conseguir ver o URL completo, isso pode ajudar a perceber se conduz a um *website* legítimo.



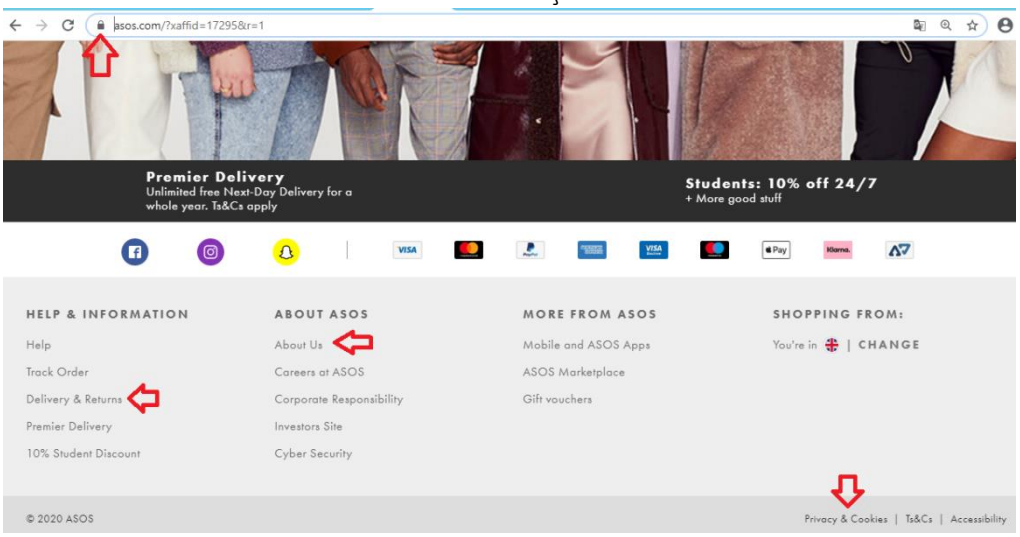
Qual é a principal pista que devemos procurar no URL?
Devemos prestar atenção ao início do URL: os URLs seguros começam com "https" em vez de apenas "http" de maneira a indicar que estão encriptados. O "s" em "https" significa "seguro".
Portanto, este *hiperlink* é um esquema de *phishing*!

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

Dica rápida

E se clicares num *link*? O que deves fazer?
Se esse link redirecionar para um *website*, há alguns sinais que podem indicar se uma empresa é real ou não.
Portanto, antes de fazer qualquer coisa, como introduzir as suas credenciais de *login* ou clicar no botão de *download*, convém reparar nos seguintes pontos:

- Na barra de pesquisa aparece "https" ou um símbolo de um cadeado - isso significa que **o *website* está protegido**.
- **Reparar no domínio -** os cibercriminosos são muito matreiros. Na maioria das vezes, os domínios são muito semelhantes ao verdadeiro, por exemplo "as0s.com" ou "asos.net".
- **Há um endereço físico e um número de telefone -** as empresas respeitáveis listam as suas informações para que possam ser contactados se houver um problema.
- **Política de devolução -** as empresas de renome tendem a listar a sua política de devolução, bem como a sua política de expedição.
- **Declaração de privacidade -** os *sites* respeitáveis devem dizer como protegem a informação dos utilizadores e se fornecem as suas informações a terceiros.



Sinal de Alerta #3: Promoções e concursos demasiado bons para serem verdadeiros!

Este é um esquema de *phishing* muito comum. Ao apresentarem preços muito baixos, oferecerem prémios irresistíveis ou darem descontos, os golpistas conseguem enganar os utilizadores para lhes cederem informações privadas.

Dica rápida

Quais são os sinais mais comuns de que um concurso é um esquema?

- A página social tem poucos seguidores;
- A gramática e ortografia são más;
- O requisito de informações muito pessoais, como o nome da mãe, primeiro animal de estimação, se tem filhos, etc. Tudo para tentar obter pistas para decifrar as senhas pessoais!
- Uma enorme persistência e sensação de "urgência" no diálogo!

Como se pode concluir, existem formas de detetar golpes de *phishing* nas redes sociais, de modo a evitar um ataque cibernético que comprometa quaisquer dados pessoais. Mas ter um olhar atento não é suficiente. Em relação aos ciberataques, o melhor remédio é a prevenção. Então, o que podemos fazer para estar sempre um passo à frente dos cibercriminosos nas redes sociais?

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

Verificar as definições de privacidade

As redes sociais fiáveis permitem a personalização das definições de privacidade para um nível que confortável para cada um. Que tipo de informação desejamos tornar pública? As fotografias? Os passatempos? E com quem queremos partilhar essa informação? Com amigos das redes sociais ou com toda a gente?

Alterar as definições de privacidade pode permitir o bloqueio de estranhos e pessoas que não são seus amigos de ver o perfil pessoal e as informações partilhadas.

Para o fazer, deve-se verificar as "definições" da conta nas redes sociais.

Manter o *software* de segurança actualizado

Ter o mais recente *software* de segurança, *browser* e sistema operativo é a melhor defesa contra vírus, *malware* e outras ameaças *online*.

Também é possível instalar no navegador uma extensão que bloqueie anúncios indesejados.

Escolher senhas fortes

A criação de uma palavra-passe forte impedirá os *hackers* de obterem acesso à conta e de a utilizarem para *spam* ou ataques maliciosos. Uma~senha forte não tem menos de 8 caracteres e consiste tanto em letras como em números. Também deve ser alterada a cada 3 meses e deve ser única para cada conta.

***Dica**: utilize uma frase-senha em vez de uma palavra-passe, por exemplo "IAte27P0tat0s".*

Guardar bem segredos pessoais

É crucial evitar a partilha de informações pessoais *online* porque essas informações, incluindo endereços electrónicos, números de telefone e números de segurança social, valem muito dinheiro para *hackers* e empresas de mineração de dados. Esses dados podem ser utilizados para resgate, roubo de identidade ou para adivinhar palavras-passe.

É pertinente dar uma vista de olhos aos próprios perfis nas redes sociais e tentar mantê-los estéreis - as pessoas que precisam de saber a nossa data de nascimento, endereço de correio electrónico e número de telefone já os sabem.

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

Utilizar uma VPN

Para manter conversas, mensagens e chamadas seguras, podemos utilizar uma Rede Privada Virtual (VPN - *Virtual Private Network,* em inglês). Uma VPN é um túnel encriptado entre dois dispositivos que permite aceder de forma privada e segura a todos os *websites* e serviços *online*.

Como os dados são encriptados, os *hackers*, os governos e mesmo os fornecedores de serviços de Internet não podem ver ou controlar quaisquer informações enquanto ligado a um servidor VPN.

Há muitos fornecedores de VPN *online* e estes variam em termos de preços e personalização.

Nunca esquecer de fazer o *logout*

É importante nunca esquecer esta regra de ouro: sair sempre de todas as plataformas de redes sociais quando se acaba de as utilizar. Se não fizermos logout, estamos a permitir que qualquer pessoa com acesso ao computador, legalmente ou não, abra o navegador ou aplicação e tenha acesso instantâneo às contas nesses *sites*, sem introduzir quaisquer palavras-passe ou nomes de utilizador.

3. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de dados pessoais nas redes sociais_03_01
OE_Proteção de dados pessoais nas redes sociais_03_02

Situação: Quais são os sinais de um possível esquema de *phishing* que devemos ter em mente enquanto navegamos nas redes sociais?
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.

- Gramática e ortografia da publicação.
- A presença de hiperligações: apenas uma fonte credível pode publicar uma hiperligação para o seu *website*.
- O *hiperlink* não coincide com o URL.
- Se um amigo enviar uma fotografia para descarregar, não há perigo de o fazer.
- A conta de uma marca famosa deve ser verificada pela própria plataforma para ser de confiança.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de dados pessoais nas redes sociais_03_01 and OE_Proteção de dados pessoais nas redes sociais_03_02

Situação: O que devemos fazer para garantir um uso mais seguro das redes sociais?
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.

- É mais seguro utilizar a mesma palavra-passe para todas as contas. Dessa forma, não se corre o risco de a esquecer.
- Antes de aceitar um novo pedido de amizade deve-se sempre verificar a autenticidade do perfil e conta em questão.
- Nunca se deve revelar os detalhes de onde estamos de férias, a fazer compras ou a viajar, bem como quando partiremos ou regressaremos a casa.
- Não há problema em operar um computador com acesso à Internet sem instalar qualquer *software* anti-*malware* e antivírus.
- A fim de acompanhar toda a atividade social dos ciberamigos, temos de estar sempre ligados às nossas conta.

Fontes

Akilawala, T. (16 Agosto, 2014) *Fake Robin Williams goodbye video on Facebook is a scam.* Retirado de https://www.bgr.in/news/fake-robin-williams-goodbye-video-on-facebook-is-a-scam-321750/

Crowdstrike (15 Outubro, 2019) *The 11 most common types of malware*. Retirado de https://www.crowdstrike.com/epp-101/types-of-malware/

Constanza, T. (19 Agosto, 2019) *Scam on Facebook exploits Robin Williams' suicide.* Retirado de https://www.siliconrepublic.com/enterprise/scam-on-facebook-exploits-robin-williams-suicide

DuPaul, N. (12 Outubro, 2012) *Common Malware Types: Cybersecurity 101.* Retirado de https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Foreman, C. (20 Junho, 2017) *10 Types of Social Media and How Each Can Benefit Your Business*. Retrieved from https://blog.hootsuite.com/types-of-social-media/

Get Safe Online (n. d.) *Social Media Phishing. https://www.getsafeonline.org/social-networking/social-media-phishing/*

GMA News Online (15 Agosto, 2014) *Beware of Robin Williams goodbye video scam.* Retirado de https://www.gmanetwork.com/news/hashtag/content/375009/beware-of-robin-williams-goodbye-video-scam/story/

Kietzmann, J. H. and Hermkens, K. (2011) *Social media? Get serious! Understanding the functional building blocks of social media*. Business Horizons (Submitted manuscript). 54 (3): 241–251. doi:10.1016/j.bushor.2011.01.005.

Mohsin, M. (7 Fevereiro, 2020) *10 Social Media Statistics You Need to Know in 2020 [Infografico].* Retirado de https://www.oberlo.com/blog/social-media-marketing-statistics

NortonLifeLock (n. d.) *What is a Trojan? Is it a virus or is it malware?* Retirado de https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

NortonLifeLock (n. d.) *What is a computer worm, and how does it work?* Retirado de https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Obar, J. A. and Wildman, S. (2015) *Social media definition and the governance challenge: An introduction to the special issue.* Telecommunications Policy. 39 (9): 745–750. doi:10.1016/j.telpol.2015.07.014. SSRN 2647377

SNL. 2010. Saturday Night Live. Temporada 36, Episódio 10. Estreado a 18 Dezembro. NBC. Retirado de https://www.youtube.com/watch?v=md3of7O02e4&list=PLS_gQd8UBhLghdS1aaLqVJ74rWi4ffT8&index=14

Woodfield, M. (26 Novembro, 2014) *Should I Buy from This Site? How to Know if a Website is Secure.* Retirado de https://www.digicert.com/blog/how-to-know-if-a-website-is-secure/

ZeroOEX Alpha Team (15 Fevereiro, 2017) *Social Media Impersonators Go Phishing: 3 Emerging Tactics*. https://www.zerofox.com/blog/social-media-impersonators-phishing/

Para relembrar

Vivemos num mundo cada vez mais global onde a Internet nos permite comunicar com qualquer pessoa em qualquer parte do mundo. As redes sociais tornaram-se uma **parte integrante das nossas vidas** e são uma ótima forma de nos mantermos ligados aos outros.
As redes sociais como o Facebook, Instagram ou YouTube são populares entre todas as faixas etárias e estão constantemente à procura de cativar atuais e futuros utilizadores.

No entanto, apesar de todas as vantagens que estas plataformas oferecem aos utilizadores, existem muitos **riscos de segurança e privacidade** relacionados com o seu uso constante e descuidado. De facto, os autores de fraudes aproveitam os hábitos dos utilizadores das redes sociais para os atrair para **esquemas de *phishing* e ataques** que comprometem os seus dispositivos e dados. Por conseguinte, todos devem assumir a sua responsabilidade na manutenção de um **ambiente seguro *online***, ao mesmo tempo que compreendem os riscos de ter uma presença *online*. Ser **cauteloso, escolher uma senha forte ou instalar software antivírus** são algumas das muitas medidas que um utilizador deve adotar para obter o controlo da sua segurança enquanto utiliza as redes sociais.

À medida que o mundo evolui para um mercado digital único, é fundamental que todos estejam cientes das leis aplicadas à proteção de dados pessoais, como o RGPD e como isso se aplica a diferentes cenários digitais.
Por fim, **o governo, a sociedade e os utilizadores finais devem trabalhar em conjunto para proteger a privacidade e a segurança dos dados pessoais nas redes sociais**.

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

As respostas corretas estão assinaladas a negrito

Situação: O que são as 'redes sociais'?
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.

- ***Websites* e aplicações que permitem às pessoas enviar mensagens e fotografias.**
- **As redes sociais são uma forma de comunicação eletrónica (como *websites* para relacionamentos sociais).**
- ***Websites* e programas de computador que permitem às pessoas comunicar e partilhar informações na Internet utilizando um computador ou telemóvel.**
- **As redes sociais referem-se a *websites* e aplicações que são concebidos para partilhar conteúdos rapidamente.**

Situação: Quais são os direitos de proteção de dados pessoais que se aplicam no Whatsapp?
Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: apenas uma resposta está errada.

- **O direito de encriptação das mensagens, o que significa que o WhatsApp não pode ler as mensagens enviadas a outras pessoas.**
- **O direito de eliminar a própria conta do Whatsapp, sem que haja a eliminação das mensagens entregues a outras pessoas.**
- **Se se apagar simplesmente a aplicação Whatsapp no próprio dispositivo, sem apagar a conta, a informação pessoal será mantida.**
- O WhatsApp guarda e armazena informações sobre cada um de nós, e nós não podemos voltar a utilizar essas informações em mais nenhum lado do mundo.

Situação: Qual dos seguintes factos é falso?
Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é falsa.
As redes sociais são um instrumento de marketing eficaz para as empresas

- O Facebook é a rede social mais utilizada
- A maioria dos utilizadores das redes sociais acede às plataformas através de dispositivos móveis
- Hoje em dia, as pequenas e médias empresas utilizam as redes sociais para impulsionar o crescimento dos seus negócios
- **Os utilizadores tendem a escolher uma só rede social, utilizando-a todos os dias**

Situação: Estás a navegar no Facebook e vês a seguinte publicação:

O que deves fazer?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Meu deus, hoje é o meu dia de sorte! Clico em "CONTINUAR" e dou-lhes todos os dados necessários para ganhar o cartão oferta. Depois disso, partilho esta oportunidade com todos os meus amigos do Facebook!

- Só tenho 4 minutos para reclamar o meu preço! Clico em "CONTINUAR" e dou-lhes todos os dados necessários para ganhar o prémio. Mas depois de ver que tenho de dar detalhes bancários, desisto pois dá demasiado trabalho.
- Fico curioso e clico em "CONTINUAR". Depois de ver que é necessário dar-lhes dados pessoais, fecho o separador. Acho que é um golpe.
- **Não clico na publicação. Não posso ganhar uma lotaria em que nunca participei! Assinalo a publicação como fraudulenta, alertando o Facebook que é um *scam*.**

Situação: Quais são os sinais de um possível esquema de *phishing* que devemos ter em mente enquanto navegamos nas redes sociais?
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.

- **Gramática e ortografia da publicação.**
- A presença de hiperligações: apenas uma fonte credível pode publicar uma hiperligação para o seu *website*.
- **O *hiperlink* não coincide com o URL.**
- Se um amigo enviar uma fotografia para descarregar, não há perigo de o fazer.
- **A conta de uma marca famosa deve ser verificada pela própria plataforma para ser de confiança.**

Situação: O que devemos fazer para garantir um uso mais seguro das redes sociais?
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.

- É mais seguro utilizar a mesma palavra-passe para todas as contas. Dessa forma, não se corre o risco de a esquecer.
- **Antes de aceitar um novo pedido de amizade deve-se sempre verificar a autenticidade do perfil e conta em questão.**
- **Nunca se deve revelar os detalhes de onde estamos de férias, a fazer compras ou a viajar, bem como quando partiremos ou regressaremos a casa.**
- Não há problema em operar um computador com acesso à Internet sem instalar qualquer *software* anti-*malware* e antivírus.
- A fim de acompanhar toda a atividade social dos ciberamigos, temos de estar sempre ligados às nossas conta.