DIGITAL 04

Segurança móvel pessoal

Este módulo descreve alguns cuidados a ter ao usar tecnologia móvel.

Iniciar >

Cofinanciado pelo Programa Erasmus+ da União Europeia

O apoio da Comissão Europeia à produção desta publicação não constitui um endosso do conteúdo, que reflete apenas a opinião dos autores, e a Comissão não pode ser responsabilizada por qualquer uso que possa ser feito da informação nela contida.

DIGITAL MÓDULO 4

Segurança móvel pessoal

Nas últimas décadas, os dispositivos móveis passaram por uma grande evolução, deixaram de apenas fazer chamadas para ganhar muitas mais utilidades. Por exemplo acesso a serviços bancários, aplicações diversas e à Internet. Com estes novos recursos, surge a preocupação com a segurança dos dados. Neste módulo, vai aprender sobre proteção de dados, como criar e alterar palavras-passe, navegação Wi-Fi segura e como proteger do ciberbullying e *trolls* da internet.

Público-alvo

Este módulo é destinado a todos que desejam aprender sobre navegação segura online, proteção de dados, *cookies* e como a lei protege as suas informações pessoais (RGPD).

Este material pode ser um desafio para alguns utilizadores. Nesse caso, seria útil trabalhar o conteúdo com um companheiro ou amigo.

Os facilitadores podem usar este material para informar e fornecer conselhos sobre os aspetos de segurança das tecnologias digitais.

O que irá aprender

1. Proteção de dados da UE RGPD e consentimento de *cookies.*
2. Como criar e modificar palavras-passe.
3. O que é *hacking* e como se pode proteger?
4. Como proteger do ciberbullying.

Capítulos neste módulo

DIGITAL | MÓDULO 4 | CAPÍTULO 1

Introdução à segurança móvel e propriedade de dados

“Informação é poder!” As informações pessoais são um dos nossos bens mais valiosos. Atualmente, este importante recurso é desvalorizado pelos consumidores, mas não pelas empresas! Algumas das maiores empresas do mundo foram bem sucedidas pelo uso inteligente dos dados. Este capítulo explica a propriedade de dados na era da computação móvel e “a nuvem”.

O que irá aprender

1. O que é o Regulamento Geral de Proteção de Dados.
2. Proteção de dados pessoais sob RGPD.
3. Como gerir as *cookies.*
4. Tipos de dados pessoais.
5. Onde os dados são guardados.
6. Como fazer uma cópia de segurança do seu dispositivo móvel.

Análise de dados – uma das novas indústrias que mais cresceu

A recolha e análise de dados é importante para as empresas entenderem as necessidades dos clientes. A análise de dados, ajuda as empresas a melhorar os serviços para os clientes.

A análise de dados torna os sites e as aplicações mais úteis e permite, por exemplo, que um utilizador consiga ver o número de passos dados num dia. A análise de dados é frequentemente aplicada aos dados pessoais.

Dados pessoais, dispositivos móveis e tecnologia vestível

Dados pessoais são informações relacionadas a um indivíduo verificado.

As empresas devem proteger as informações pessoais dos cidadãos de acordo com a lei do **Regulamento Geral de Proteção de Dados (RGPD)** codificando **informações** confidenciais armazenadas ou enviadas por redes públicas.

O RGPD será referido posteriormente neste capítulo.

Proteger os dados recolhidos por dispositivos móveis

Quando uma pessoa ou organização obtém acesso sem consentimento ou permissão às informações pessoais – morada, idade, género, problemas de saúde, situação financeira, interesses, etc… – isto pode causar problemas para a pessoa cujos dados são recolhidos.

Dados pessoais são dados que se referem a uma pessoa identificável. Essas informações ajudam a personalizar um serviço para si. As empresas devem proteger as suas informações pessoais de acordo com a lei **RGPD** encriptando as informações confidenciais enviadas a terceiros por redes públicas.

Mais informações em https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx.

O que é RGPD?

Para evitar que as empresas obtenham dados pessoais sem consentimento, a Comissão Europeia introduziu o **Regulamento Geral de Proteção de Dados (RGPD)**.
O RGPD protege os dados pessoais dos cidadãos que vivem e trabalham na União Europeia. As organizações que operam na UE devem ter consentimento para processar os dados pessoais.

RGPD – que direitos oferece na UE?

O RGPD oferece os seguintes direitos para os indivíduos:

- Direito de ser informado
- Direito de acesso
- Direito de retificação e exclusão de informação
- Direito de restringir o processamento
- Direito à portabilidade dos dados
- Direito de se opor
- Direitos sobre perfis automatizados

Que tipos de dados podem ser classificados como dados pessoais?

Para entender a importância dos direitos de privacidade dos dados na UE, precisamos conhecer os tipos de dados pessoais que podem ser afetados pelo RGPD.

Vejamos alguns exemplos comuns de tipos de dados que podem ser considerados dados pessoais e, portanto, vale a pena proteger.

Exemplos de dados pessoais

1

2

3

Informações demográficas são dados pessoais

Quando uma pessoa preenche um formulário para, por exemplo, solicitar um subsídio, está a confiar na organização que fez o formulário para tratar as informações confidenciais em sigilo. Este é um exemplo de dados pessoais.

Exemplos de dados pessoais

1

2

3

Os registos de saúde contêm dados pessoais

Uma visita a um médico é considerada uma visita confidencial. Os dados registados sobre um paciente também são altamente confidenciais e, portanto, podem ser considerados dados pessoais.

Exemplos de dados pessoais

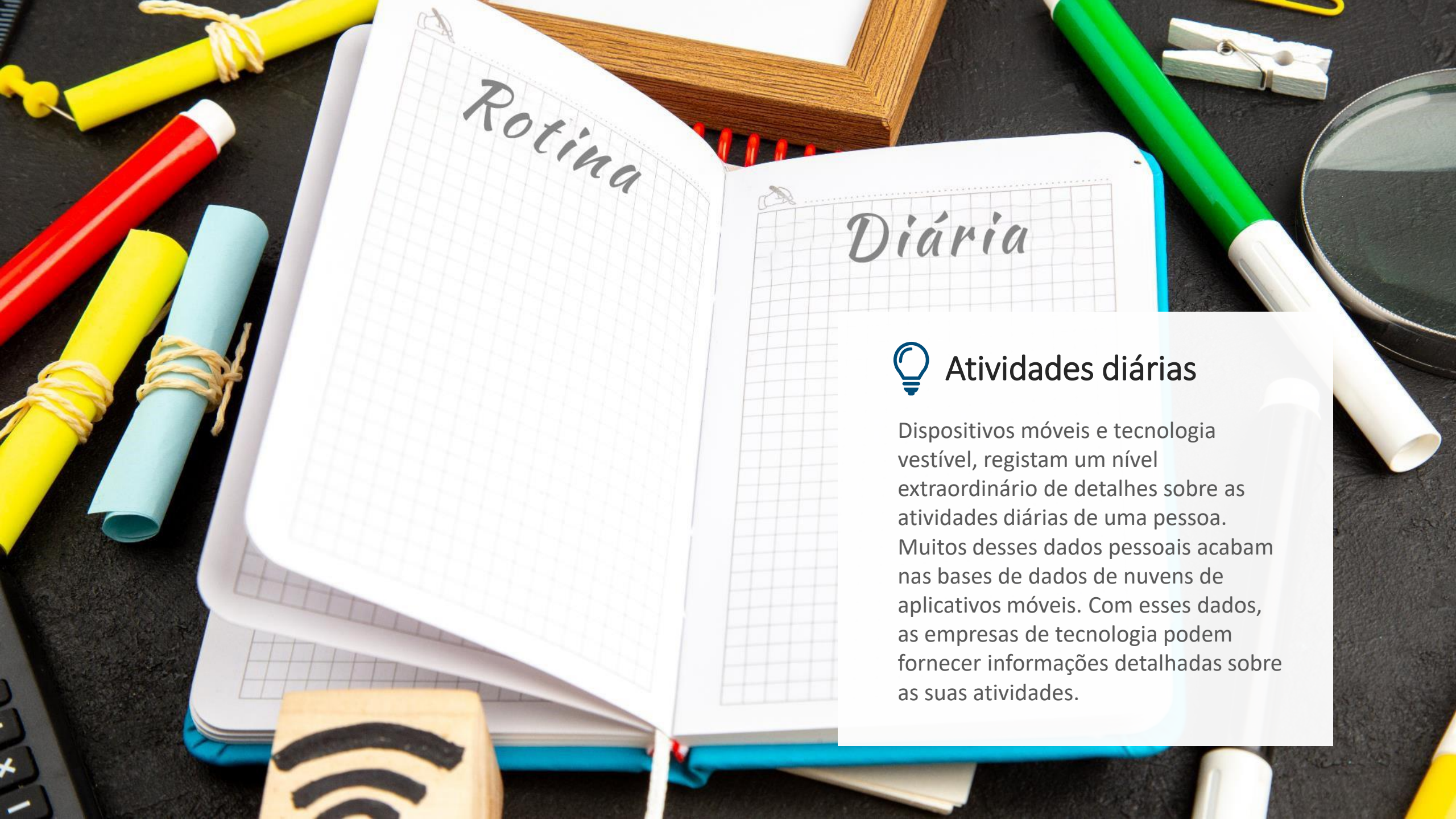
1

2

3

Registos de atividades diárias são dados pessoais

Um registo de compras feitas, locais visitados e viagens feitas por uma pessoa também são dados pessoais.



Atividades diárias

Dispositivos móveis e tecnologia vestível, registam um nível extraordinário de detalhes sobre as atividades diárias de uma pessoa. Muitos desses dados pessoais acabam nas bases de dados de nuvens de aplicativos móveis. Com esses dados, as empresas de tecnologia podem fornecer informações detalhadas sobre as suas atividades.

Tipos de dados pessoais

4

5

Informações financeiras são dados pessoais

Informações financeiras, classificações de créditos e saldos bancários são outra categoria de dados pessoais. Estes podem ser usados para categorizar a pessoa como uma grande consumidora ou uma consumidora cautelosa.

Tipos de dados pessoais

4

5

Imagens ou gravações também são dados pessoais

Os proprietários de câmaras de videovigilância devem ter cuidado ao armazenar imagens de vídeo, pois podem conter dados pessoais. O mesmo se aplica às gravações de áudio. Ambos só devem ser mantidos com o consentimento de quem está registado.

Cookies: acordos para fornecer dados pessoais a uma empresa

Cookies são pequenos arquivos que os sites enviam para o dispositivo para recordar certas informações. Por exemplo, preferências desportivas ou detalhes de início de sessão.

De acordo com os regulamentos do RGPD, um site deve obter o consentimento do utilizador para instalar *cookies* no seu dispositivo.

Se estiver preocupado com a análise dos seus dados, poderá selecionar as opções “Rejeitar todos” ou “Concordar com os selecionados” (conforme representado na imagem). Desativar os *cookies* significa que o site não se adapta aos seus interesses e não consegue recuperar detalhes como palavras-passe ou compras.

Mensagens falsas – um aviso!

Às vezes, mensagens apelativas aparecem no seu dispositivo móvel. Quando recebe uma mensagem de um prémio ou de uma oportunidade que parece boa demais para ser verdade, geralmente, é uma maneira para tentar extorquir dinheiro.

Quando uma mensagem como esta é recebida, é importante **não** preencher um formulário, **não** clicar nas hiperligações ou **não** partilhar informações pessoais, como números de telefone, *e-mail* ou morada, a menos que saiba que a mensagem veio de uma fonte fidedigna. Da mesma forma, as notícias que lê no telefone podem ser “notícias falsas”.

O que é a nuvem?

A chamada nuvem é uma rede mundial de computadores e um *software* que é executado nesses mesmos computadores. Os dados pessoais podem ser recolhidos e armazenados num computador na nuvem em qualquer lugar do mundo. Os dados criados por si também podem ser armazenados na nuvem e pode aceder aos mesmos a partir de múltiplos dispositivos.

Dados na nuvem são processados e armazenados num centro de dados e não no dispositivo do utilizador.

A nuvem é muito útil para dispositivos móveis

Problema: Limite no armazenamento

A maioria dos dispositivos móveis têm armazenamento limitado. A determinada altura, o espaço do armazenamento acaba e o processamento fica lento.

Solução: Armazene e analise os dados na nuvem

Arquivos, fotos, vídeos podem ser copiados para a nuvem. É bom manter várias cópias, os computadores na nuvem são bastante desenvolvidos. No entanto, é importante lembrar que a segurança na nuvem pode ser comprometida.

Segurança na nuvem

Quão seguro são os dados quando eles saem do dispositivo móvel e são armazenados num computador na nuvem?

Além das empresas usarem os dados do utilizador para vender mais produtos, os dados pessoais na nuvem podem ser comprometidos e usados para fins criminosos. A segurança na nuvem é importante para os dados pessoais e dispositivos móveis.
Certifique-se que o seu fornecedor de serviços e dados tenham base na União Europeia.

Dados na nuvem: onde manter os arquivos? Local ou na nuvem?

Vantagens

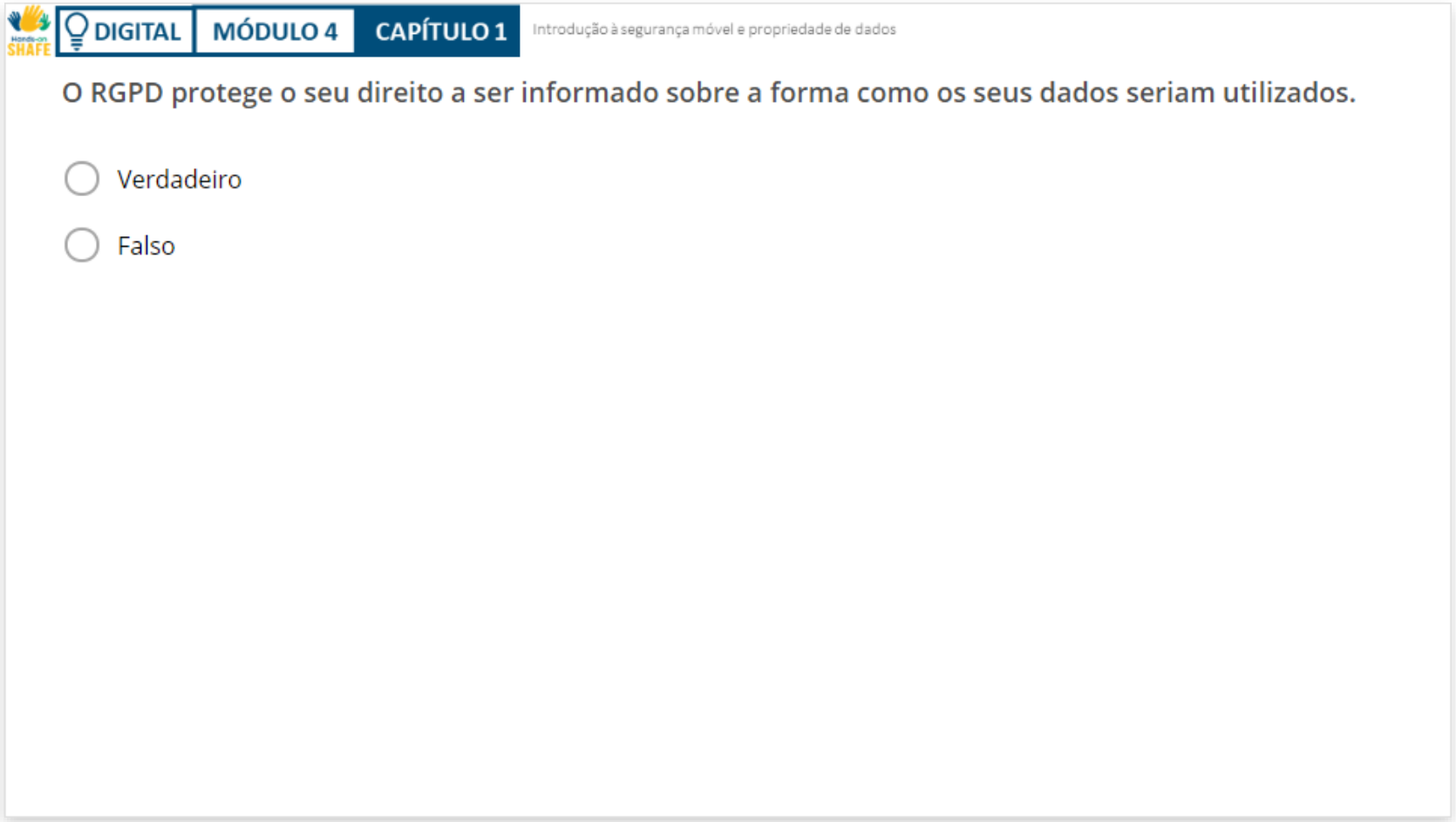
- Personalização e melhor serviço
- Mais espaço de armazenamento, já que um dispositivo móvel tem armazenamento limitado
- Mais dados significa decisões “mais inteligentes”
- Todos os dados parecem estar “num só lugar”

Desvantagens

- O utilizador está a aceitar a perda de privacidade dos dados para o fornecedor da nuvem
- Possibilidade de roubo e fraude
- Uma vez que os dados estão na nuvem, é extremamente difícil excluí-los

Quiz

Click the **Quiz** button to edit this object

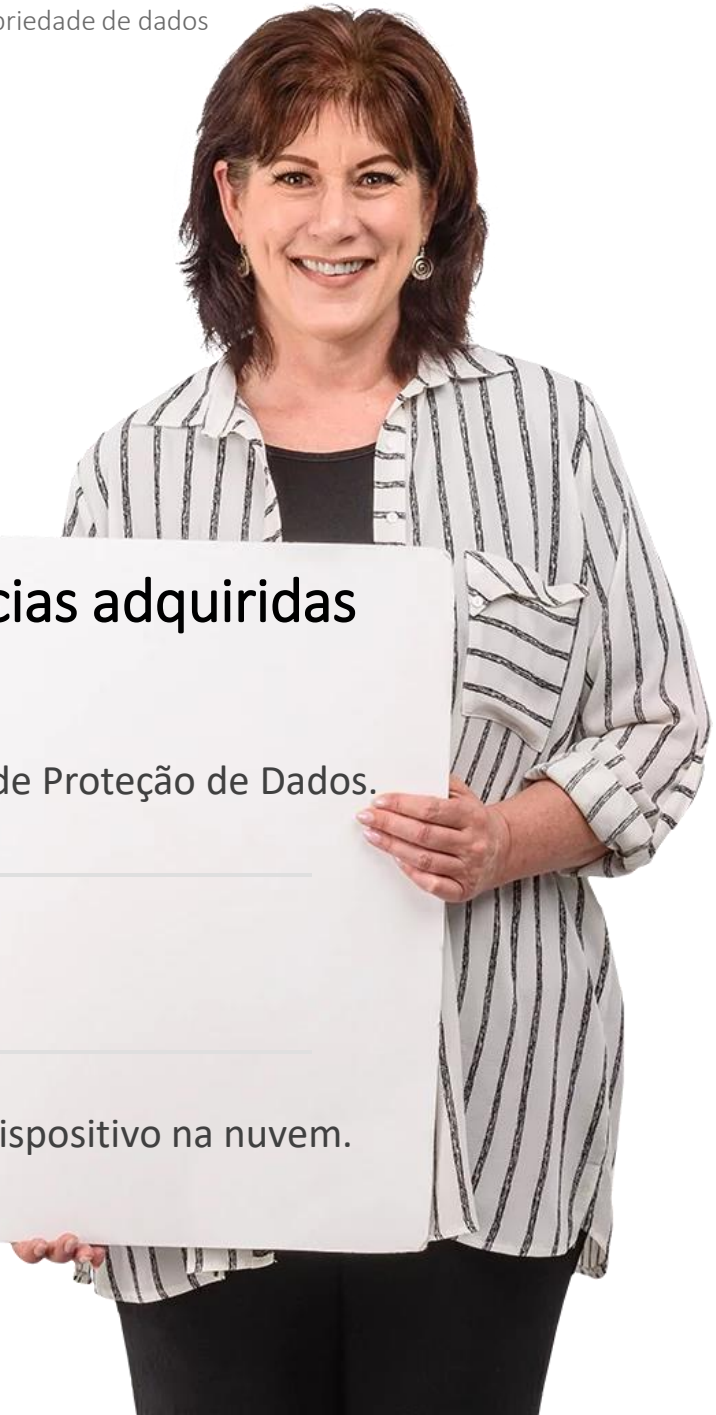


Resumo do capítulo

1. Privacidade de dados.
2. Como o Regulamento Geral de Proteção de Dados protege os dados.
3. Como gerir as *cookies.*
4. Perceber a forma de trabalhar a nuvem.
5. Entender como os dados são armazenados na nuvem.
6. A partir deste capítulo, adquiriu um conhecimento prático da privacidade dos dados móveis.

Capítulo concluído!

Parabéns! Concluiu este capítulo com sucesso!



Resumo das competências adquiridas

1. O Regulamento Geral de Proteção de Dados.
2. Como gerir as *cookies*.
3. Armazenar dados do dispositivo na nuvem.

O que vem a seguir?

Agora pode repetir este capítulo ou seguir a nossa recomendação para continuar a aprendizagem, clicando num dos botões abaixo:

Reiniciar

Seguinte

DIGITAL | MÓDULO 4 | CAPÍTULO 2

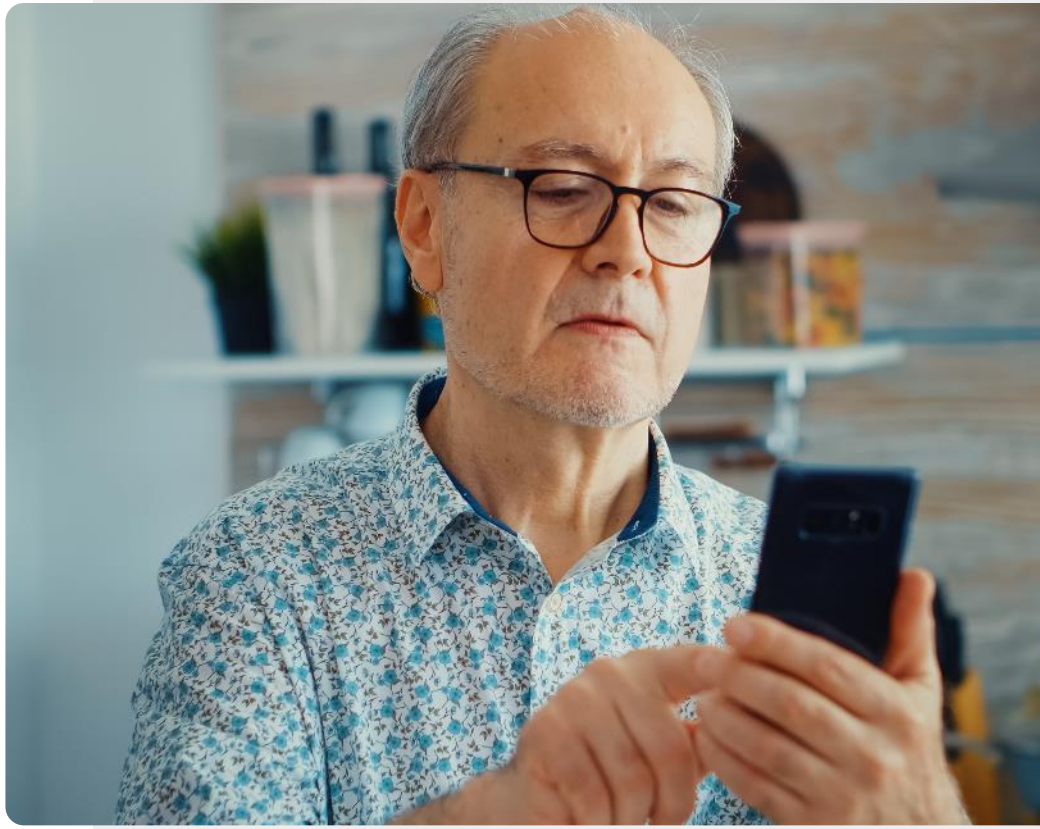
Autenticação

Neste capítulo irá aprender sobre autenticação, que é um processo de reconhecimento da identidade de um utilizador para permitir acesso aos serviços. A tecnologia de autenticação oferece suporte à segurança e proteção de informações pessoais. Aqui irá aprender tipos de autenticaçãoabordagens biométricas e como criar palavras-passe fortes.

Autenticação – como os dispositivos sabem quem é o utilizador atual

Autenticação é um processo usado para reconhecer a identidade de um utilizador. Geralmente, acontece quando uma aplicação é aberta e valida a entrada ao utilizador, para garantir que nenhum outro utilizador tenha acesso aos dados.

Sistemas diferentes requerem informações diferentes, chamadas **credenciais,** para confirmar uma identidade. Essa credencial geralmente é uma palavras-passe, mas também pode envolver outras formas de autenticação.



O que irá aprender

1. O que é autenticação e porque é importante.
2. Tipos de autenticação.
3. Como criar uma palavra-passe forte.
4. Diferentes tipos de autenticação biométrica.

Tipos de autenticação

O número de maneiras de autenticar um utilizador de dispositivo móvel, teve uma considerável evolução nas últimas décadas.

Vamos rever alguns dos principais tipos de autenticação que podem estar disponíveis num dispositivo móvel.

Alguns tipos de autenticação

1

2

3

Autenticação com base na palavra-passe

As palavras-passe são provavelmente a forma mais comum de autenticação. As palavras-passe que são seguras geralmente contêm letras, números e outros caracteres. Este tópico será abordado posteriormente neste capítulo.

Alguns tipos de autenticação

1

2

3

Autenticação com base em certificados

Um certificado digital é um documento eletrónico, com base em algo fidedigno, como uma carta de condução ou um passaporte. Um exemplo é o certificado digital que mostra os detalhes completos da vacinação para COVID-19.

Alguns tipos de autenticação

1

2

3

Autenticação biométrica

A autenticação biométrica é um processo de segurança com base nas características únicas do utilizador do dispositivo, como a cara, a voz ou as impressões digitais. Veremos que os dispositivos móveis suportam diferentes tipos de autenticação biométrica.

Alguns tipos de autenticação

4

5

Autenticação com base em *token*

Essa abordagem permite que o usuário insira credenciais apenas uma vez e crie uma chave digital secreta – o ***token***. O utilizador pode usar o *token* com o intuito de aceder aos sistemas em vez de inserir as credenciais novamente.

Alguns tipos de autenticação

4

5

Autenticação por multi-fator (MFA)

Assim que o utilizador for identificado, um código é enviado para o dispositivo móvel para que o utilizador insira o código recebido na aplicação ou no site. Esta é a **autenticação por dois fatores**.

Autenticação por palavra-passe

Vamos selecionar alguns destes tipos de autenticação e analisar mais detalhadamente.

Provavelmente, o tipo de autenticação mais popular e usado em dispositivos móveis há muitos anos é a palavra-passe.

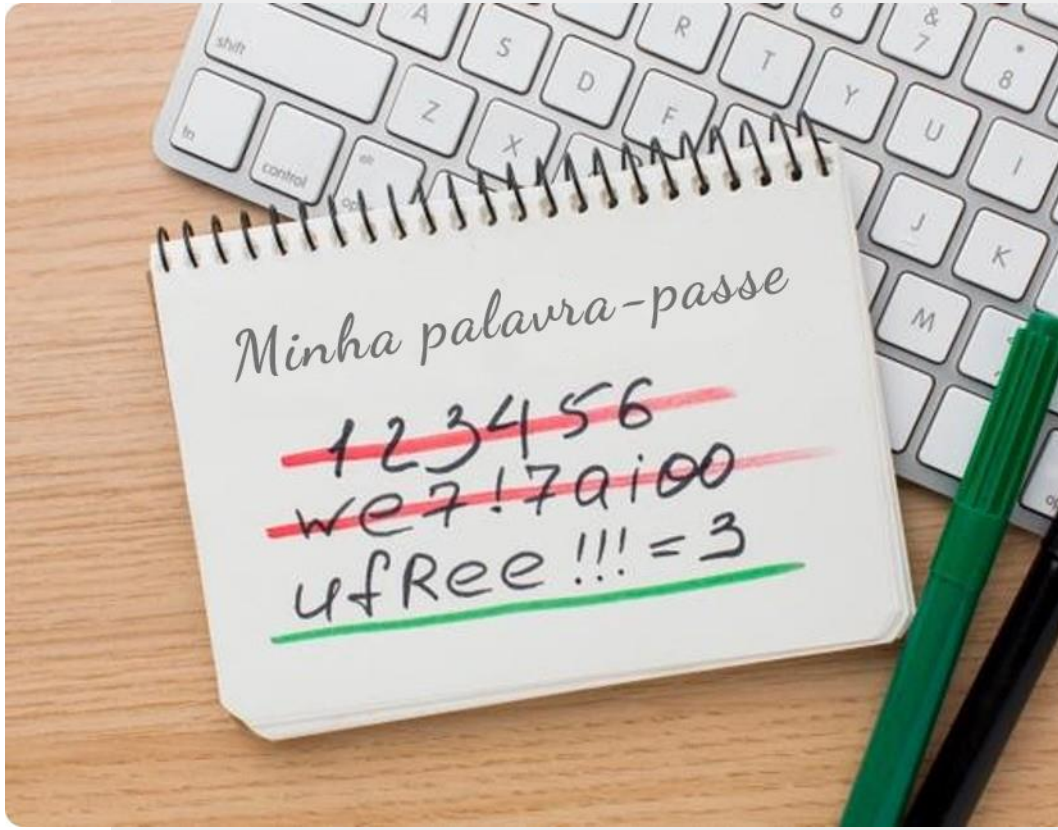
A palavra-passe na imagem é fácil de adivinhar, por isso não é muito segura. Podemos melhorá-la?

Autenticação de uma Palavra-passe mais forte

Muitos *sites* exigem que selecione uma palavra-passe que tenha algumas das seguintes propriedades:

- Pelo menos 8 caracteres
- Conter letras maiúsculas e minúsculas
- Conter um número
- Conter um caractere de pontuação

Vejamos agora como uma palavra-passe fácil de lembrar, pode ser feita com esses elementos.



Criar uma palavra-passe forte

1

2

3

Escolha uma palavra que seja fácil de lembrar

Pegue uma caneta e um pedaço de papel. Escreva uma palavra longa ou palavras com um significado forte, mas que não sejam óbvio para mais ninguém. Por exemplo: “paciência” ou “Byzantium” ou “antílope”.

Criar uma palavra-passe forte

1

2

3

Substitua alguns caracteres na palavra ou frase

Use substitutos de caracteres, por exemplo:

1 = ! e = 3 a = @ 8 = % E =£ I =| S = $ S = 5

C =(T = + G = 6 O = 0 I = 1 Z = 2 B = 8

Por exemplo, Carolina pode ficar (@rol1nA

Criar uma palavra-passe forte

1

2

3

Use a palavra-passe para um dispositivo ou site

Agora, destrua cuidadosamente o papel da palavra-passe ou coloque num local seguro, como um cofre.

Agora pode inserir a nova palavra-passe no dispositivo ou *site*.

Proteja a palavra-passe

Depois de criar a palavra-passe, precisa de protegê-la.

O melhor é lembrar da palavra-passe, mas se decidir anotar, a palavra-passe deve ser armazenada num local realmente seguro.

Nunca deve armazenar uma palavra-passe, em qualquer lugar, como no telefone ou perto dele.

Ajude o António!

O António quer fazer uma palavra-passe segura. Como deve fazer isso?

- Conheça e saiba mais sobre o António Encontre informações sobre o António aqui.
- O António escolheu a frase **semlimites** como palavra base, para a palavra-passe.
- Use as etapas descritas para ajudar o António a tornar a palavra-passe **semlimites** mais forte, ao usar as etapas descritas nos slides anteriores.

Palavras-passe de telefone e códigos SIM

Os dispositivos móveis podem ser configurados com palavras-passe para proteger arquivos. Os **cartões SIM** num dispositivo, ligam-no a uma rede telefónica e vêm com um **código PIN** que se introduz para aceder à rede. Através disso, têm permissão de acesso aos números telefónicos do SIM e, se o telefone for roubado, o SIM pode ser movido para outro telefone.

Se o código PIN for inserido incorretamente 3 vezes, será necessário um segundo código chamado código PUK. Por esse motivo, é importante manter o **código PIN** e o **código PUK** num local seguro.

Autenticação biométrica

Um sistema de autenticação biométrica reconhece características únicas do utilizador do dispositivo para permitir que ele se conecte ao dispositivo ou sistema.

Vamos ver algumas dessas abordagens agora.

Autenticação biométrica para tecnologia móvel

1

2

3

Leitores de impressão digital

As impressões digitais são únicas e podem ser usadas para identificar um utilizador. Muitos dispositivos móveis modernos têm leitores de impressão digital embutidos e o telefone pode ser desbloqueado pelo utilizador ao colocar o dedo sobre esse leitor.

Autenticação biométrica para tecnologia móvel

1

2

3

Reconhecimento da retina

Tal como as impressões digitais, os padrões nos olhos são únicos para cada pessoa. A câmara de alguns dispositivos móveis pode reconhecer o padrão da retina do proprietário e usá-lo para desbloquear o dispositivo.

Autenticação biométrica para tecnologia móvel

1

2

3

Reconhecimento facial

Outra abordagem de autenticação do utilizador semelhante é o reconhecimento facial. Do mesmo modo, uma câmara é usada para reconhecer as características faciais únicas do proprietário para desbloquear o dispositivo.

Ajude o José!

O José deseja usar autenticação em seu telefone. Você pode ajudá-lo a escolher?

- Conheça e saiba mais sobre o José. Você pode encontrar informações sobre o José aqui.
- O José costumava trabalhar para uma empresa de Tecnologias de Informação, então ele é um utilizador confiante da tecnologia, mas não está familiarizado com as abordagens modernas de autenticação. Ele gostaria de proteger o telemóvel para que outras pessoas não possam aceder às suas informações.
- A partir das informações que aprendeu nos slides anteriores, ajude o José sobre a qual abordagem de autenticação ele pode utilizar.

Autorização

Depois do dispositivo autenticar o utilizador, tem **autorização** (permissão) para aceder ao dispositivo ou sistema.

Um utilizador pode ter autorização para usar todos os recursos do dispositivo ou apenas alguns deles.

É fácil confundir a **autenticação**, que identifica o utilizador e a **autorização**, que acontece depois.

Quiz

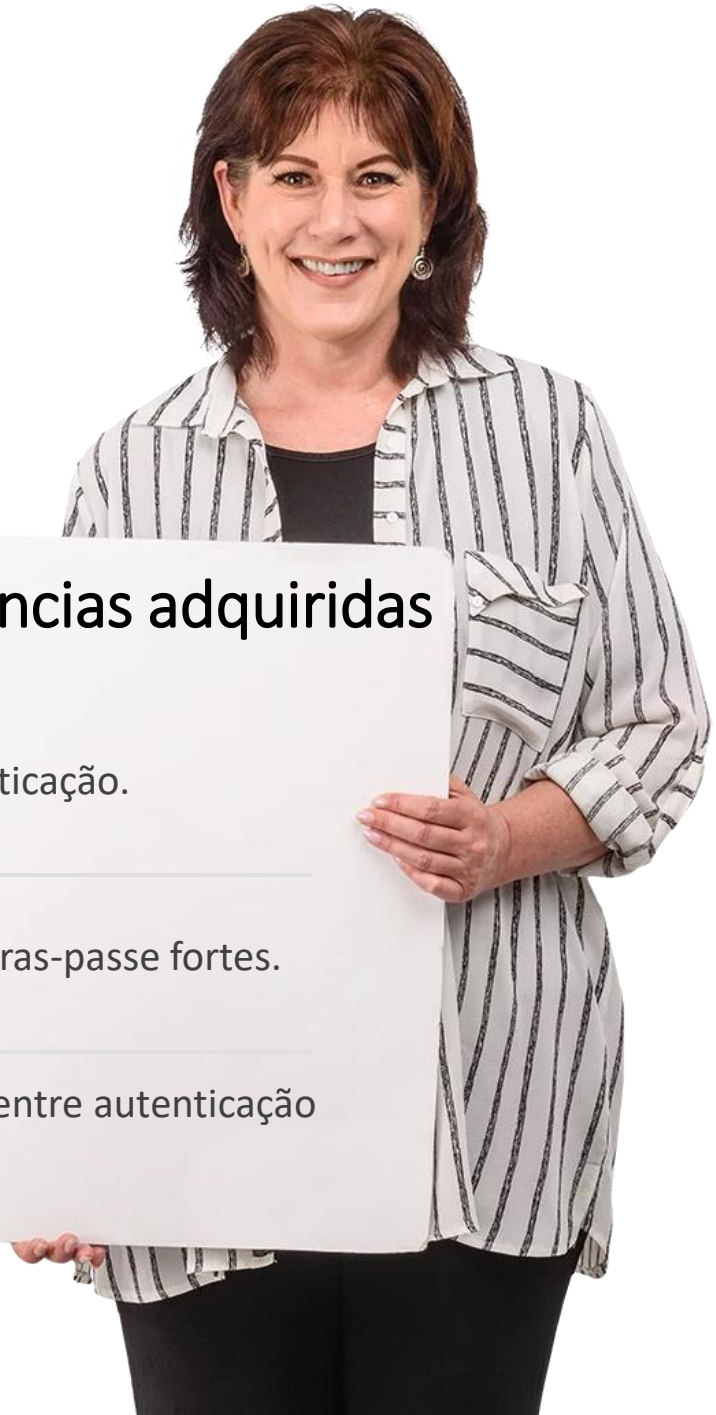
Click the **Quiz** button to edit this object

Resumo do capítulo

1. Aprendeu sobre autenticação e como é usada para proteger o acesso às informações.
2. Conheceu vários tipos de autenticação.
3. Aprendeu como criar formas de guardar suas palavras-passe em segurança.
4. Por favor, experimente os recursos de segurança do dispositivo móvel. Eles vão protegê-lo.
5. Esperamos que pratique a técnica de criação de palavras-passe para criar palavras-passe seguras.

Capítulo concluído!

Parabéns! Concluiu este capítulo com sucesso!



Resumo das competências adquiridas

1. Aprendeu sobre autenticação.
2. Aprendeu a criar palavras-passe fortes.
3. Aprendeu a diferença entre autenticação e autorização.

O que vem a seguir?

Agora pode repetir este capítulo ou seguir a nossa recomendação para continuar a aprendizagem, clicando num dos botões abaixo:

Reiniciar

Seguinte

DIGITAL | MÓDULO 4 | CAPÍTULO 3

Proteger um dispositivo móvel

No mundo físico, o dispositivo móvel pode ser roubado. No mundo digital, o seu dispositivo também é vulnerável a ataques e vírus. Este capítulo é sobre como proteger o dispositivo móvel, a privacidade e informações contra ataques cibernéticos, como vírus.

O que irá aprender

1. Como proteger os dispositivos contra acessos não autorizados.
2. Como proteger os dispositivos contra vírus.
3. O que é *ransomware*, *malware* e DDoS.
4. Como usar um *hotspot* com segurança.

Como proteger um dispositivo móvel contra acessos não autorizados

1

2

3

Bloqueie o dispositivo móvel

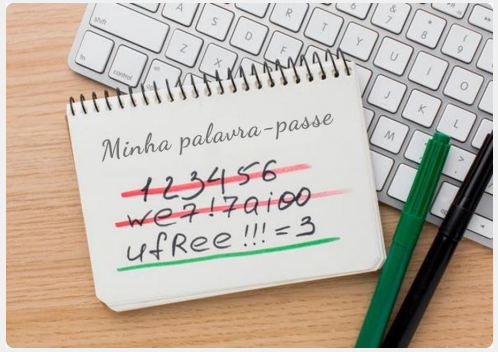
Bloqueie o dispositivo móvel com palavras-passe ou, melhor ainda, com a autenticação biométrica ativada. Bloqueie o cartão SIM com um código PIN e mantenha os códigos PIN e PUK num local fácil de lembrar, mas seguro.

Como proteger um dispositivo móvel contra acessos não autorizados

1

2

3



Use palavras-passe fortes

No último capítulo, aprendeu a criar e usar palavras-passe fortes, com letras maiúsculas e minúsculas, números e caracteres especiais. Vale a pena usar caneta e papel para o fazer.

Como proteger um dispositivo móvel contra acessos não autorizados

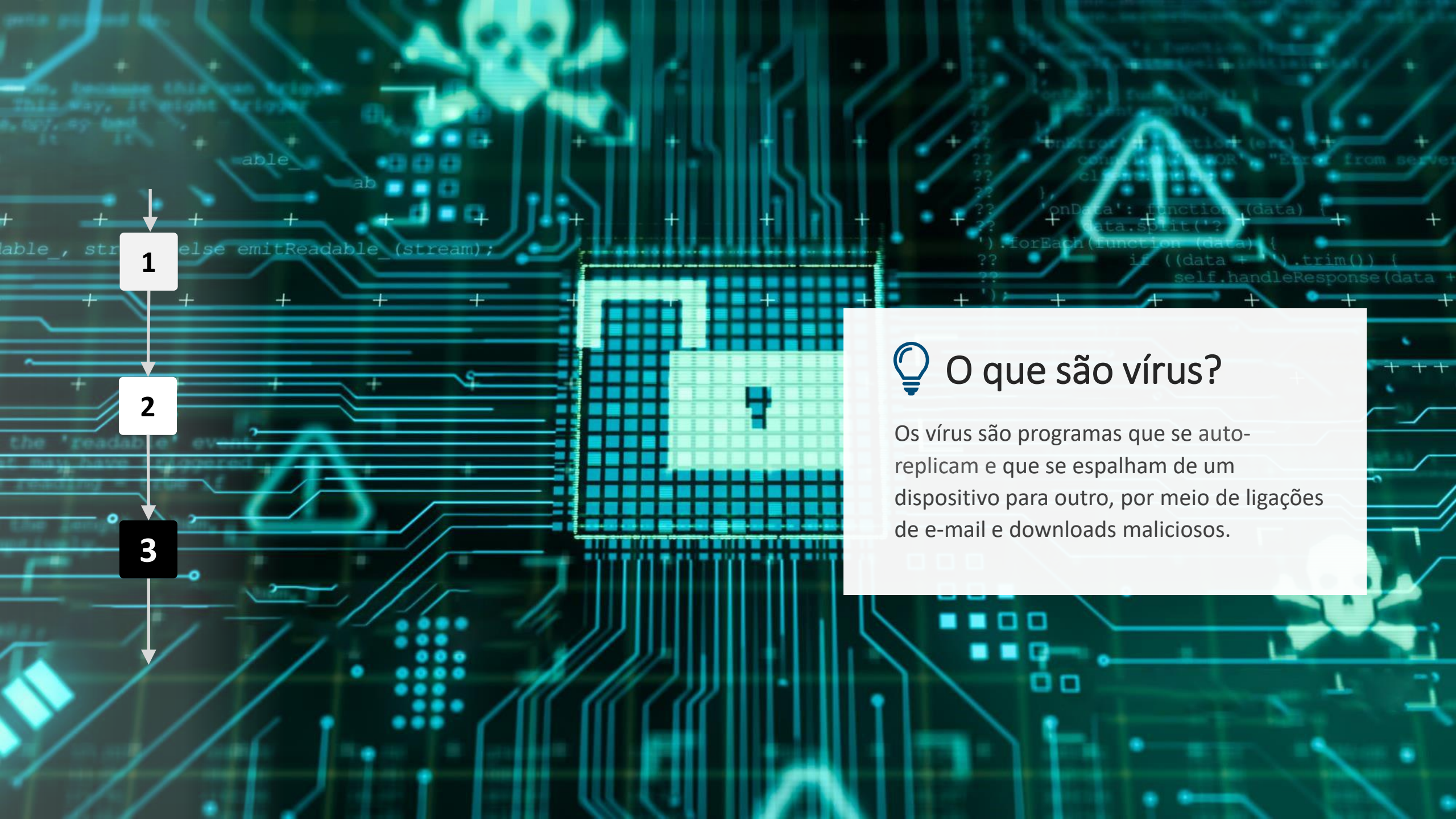
1

2

3

Atenta nas transferências

Faça transferências apenas de ficheiros como documentos, vídeos, músicas ou imagens, de *sites* em que confia, como fabricantes de dispositivos, grandes empresas de *software* ou empresas dos *media*. Alguns arquivos descarregados de *sites* não confiáveis podem conter vírus e danificar o seu *hardware*. Sites com endereços que começam com **"https"** são protegidos contra isso.



O que são vírus?

Os vírus são programas que se auto-replicam e que se espalham de um dispositivo para outro, por meio de ligações de e-mail e downloads maliciosos.

Como proteger um dispositivo móvel contra acessos não autorizados

4

5

6

Mantenha o dispositivo atualizado

O fabricante do dispositivo móvel envia notificações sobre novas atualizações de *software*. As atualizações ajudam a proteger o dispositivo contra falhas de segurança que podem permitir que alguém obtenha dados do dispositivo. Descarregue essas atualizações de *software* no dispositivo e atualize.

Como proteger um dispositivo móvel contra acessos não autorizados

4

5

6

Encripte os dados no dispositivo móvel

A maioria dos dispositivos móveis tem a opção de encriptar os dados. Se um telefone for roubado, a criptografia tornará mais difícil para alguém sem autorização ver os dados armazenados no dispositivo. Um utilizador autorizado poderá usar o dispositivo normalmente.

O que é a criptografia?

A criptografia é um método pelo qual as informações são convertidas em códigos ilegíveis que ocultam o verdadeiro significado da informação, exceto para o utilizador que possui a chave.

A aplicação da rede social do Facebook e WhatsApp possui criptografia de ponta a ponta, para que a comunicação entre dois utilizadores não possa ser vista por terceiros.

Como proteger um dispositivo móvel contra acessos não autorizados

4

5

6

Tenha cuidado com o Wi-Fi público

Utilizar Wi-Fi em espaços públicos como aeroportos e cafés pode ser arriscado. Às vezes, o que pensa ser o Wi-Fi do café é, na verdade, o computador de um *hacker* que pode usar a conexão com o telefone para fins impróprios. Na dúvida, não conecte!

Wi-Fi e crime

Os cibercriminosos às vezes espiam as redes Wi-Fi públicas e recolhem dados que são transferidos por Wi-Fi.

Desta forma, o criminoso pode obter dados bancários, palavras-passe e outras informações confidenciais.

Vantagens e Desvantagens: De usar Wi-Fi público?

Vantagens

- Grátis
- Os dados móveis não são gastos
- Fácil de conectar
- Disponível

Desvantagens

- Não é seguro
- Wi-Fi do “hotspot” de uma organização pode ser falsificada
- Normalmente, menos velocidade do que a própria cobertura móvel

O que é ataque de *hack*?

O objetivo de um ataque de *hack* é obter acesso por danos, roubo de dados ou intenção de destruir os dados de uma organização.

Malware, *Ransomware*, DDoS

Malware é um *software* projetado intencionalmente para causar danos num computador, servidor, utilizador ou rede de computadores. O *software* que causa danos não intencionais devido a alguma deficiência é normalmente descrito como um *bug* (um erro) de *software*. Existe uma variedade de tipos de *malware*, incluindo vírus de computador, *worms*, cavalos de Tróia, *ransomware*, *spyware*, *adware*, entre outros.

Ransomware é um *malware* que impede a vítima de aceder ficheiros no seu computador. Geralmente é descarregado através de uma ligação num *e-mail*, *site* ou rede social. Uma vez descarregado, ele encripta todos os ficheiros de dados no computador e um ecrã de bloqueio aparece, exigindo um pagamento de resgate para permitir que os ficheiros sejam concedidos. **NÃO clique** em ligações, textos ou *e-mails* suspeitos!

A mitigação de **DDoS** refere-se ao processo de proteção bem-sucedida de um servidor ou rede direcionado de um ataque distribuído de negação de serviço (DDoS). Ao utilizar equipamentos de rede especialmente projetados ou um serviço de proteção com base em nuvem, uma vítima visada é capaz de mitigar a ameaça recebida.

Ajude o José!

O José adicionou autenticação ao telefone. Será que pode sugerir outras maneiras de proteger as informações?

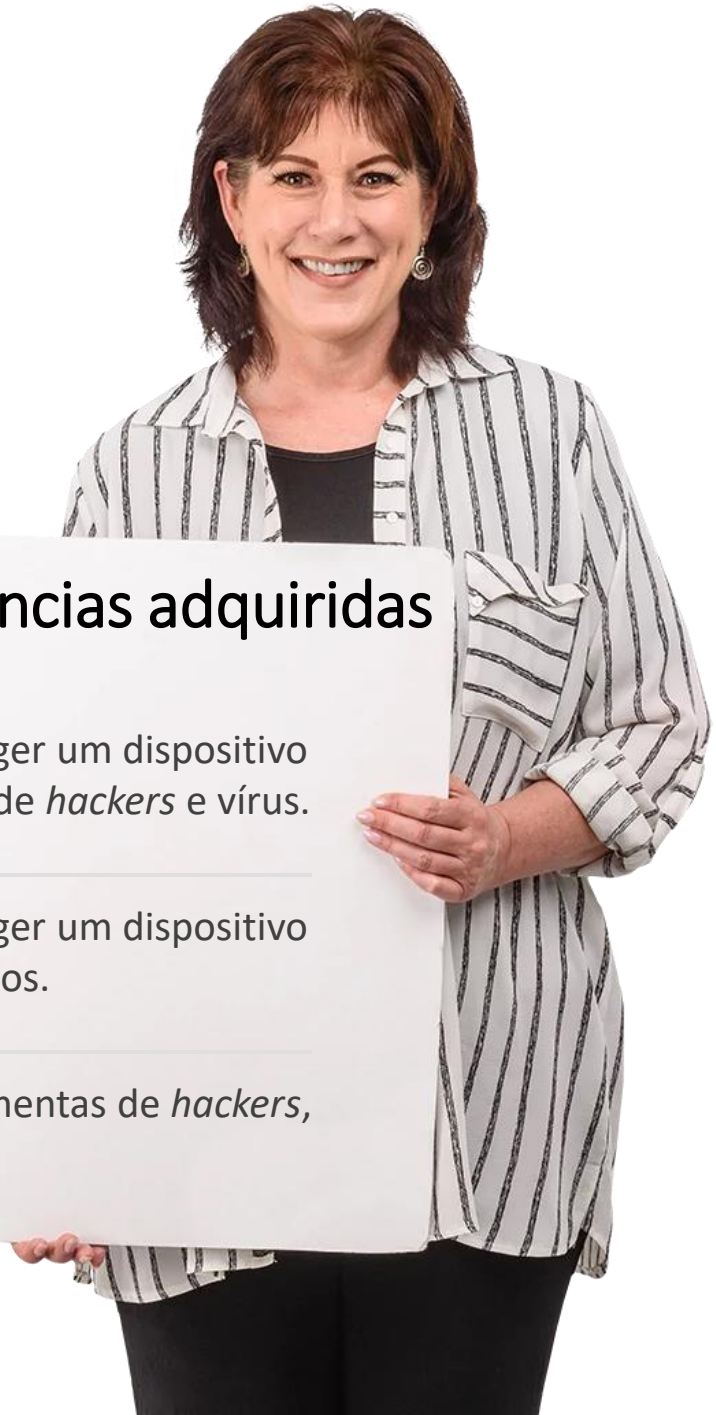
- Conheça e saiba mais sobre o José. Você pode encontrar informações sobre Tom aqui.
- O José costumava trabalhar para uma empresa de Tecnologias de Informação, então ele é um utilizador confiante de tecnologia. Ele agora está a usar autenticação, mas deseja usar seu telemóvel de maneira segura para que outras pessoas não possam aceder às suas informações.
- A partir das informações que aprendeu nos slides anteriores, sugira outras ações que o José pode tomar em consideração para proteger suas informações.

Resumo do capítulo

1. Aprendeu como proteger um dispositivo móvel.
2. Aprendeu a diferença entre vírus e ataques de *hackers.*
3. Aprendeu sobre *ransomware*, *malware* e *DDoS.*
4. Agora está ciente dos perigos de usar Wi-Fi público.

Capítulo concluído!

Parabéns! Concluiu este capítulo com sucesso!



Resumo das competências adquiridas

1. Aprendeu como proteger um dispositivo móvel contra ataques de *hackers* e vírus.
2. Aprendeu como proteger um dispositivo móvel em locais públicos.
3. Aprendeu sobre ferramentas de *hackers*, como *malware.*

O que vem a seguir?

Agora pode repetir este capítulo ou seguir a nossa recomendação para continuar a aprendizagem, clicando num dos botões abaixo:

Reiniciar

Seguinte

DIGITAL | MÓDULO 4 | CAPÍTULO 4

Ciberbullying e como lidar com conteúdo impróprio

O que deve fazer, caso se torne alvo de ciberbullying? Se as pessoas não veem a pessoa, é mais fácil não se aperceberem do mal que é feito pelo ciberbullying. Neste capítulo, reformulamos os aspetos humanos da comunicação digital e o que é apropriado ou não partilhar *online*.

O que irá aprender

1. Estar ciente do ciberbullying.
2. Como lidar com conteúdo impróprio.
3. O que partilhar ou não *online.*
4. Amigos *online*: quão seguro é?

O que é ciberbullying?

O ciberbullying é definido como ***um ato agressivo e intencional realizado por um grupo ou um indivíduo, através de formas virtuais, repetidamente e ao longo do tempo contra uma vítima que não tem forma de se defender facilmente. - Smith 2018***

Diz-se geralmente que o ciberbullying envolve três elementos:

- intenção de prejudicar
- desequilíbrio de poder
- repetição do ato

Tipos de ciberbullying

O ciberbullying pode acontecer por meio de mensagens de texto, chamadas, *e-mails*, mensagens instantâneas, redes sociais ou em salas de conversa.

Pode assumir a forma de palavras ofensivas, comentários depreciativos, publicação de informações falsas em fóruns públicos ou blogs, *hackear* contas para ameaças pessoais de natureza violenta ou sexual.

Como lidar com o ciberbullying

De acordo com especialistas, existem várias maneiras de lidar com um agressor cibernético.

Ignorar: Sempre que possível, ignore o agressor.

Registe: Anote a data, a hora e o conteúdo de todo o *bullying*, para que possa denunciar, se for necessário.

Apoio de amigos: Partilhe a experiência com amigos e parentes, para não se sentir isolado.

Denuncie: Entre em contato com o moderador do *site* ou fórum.

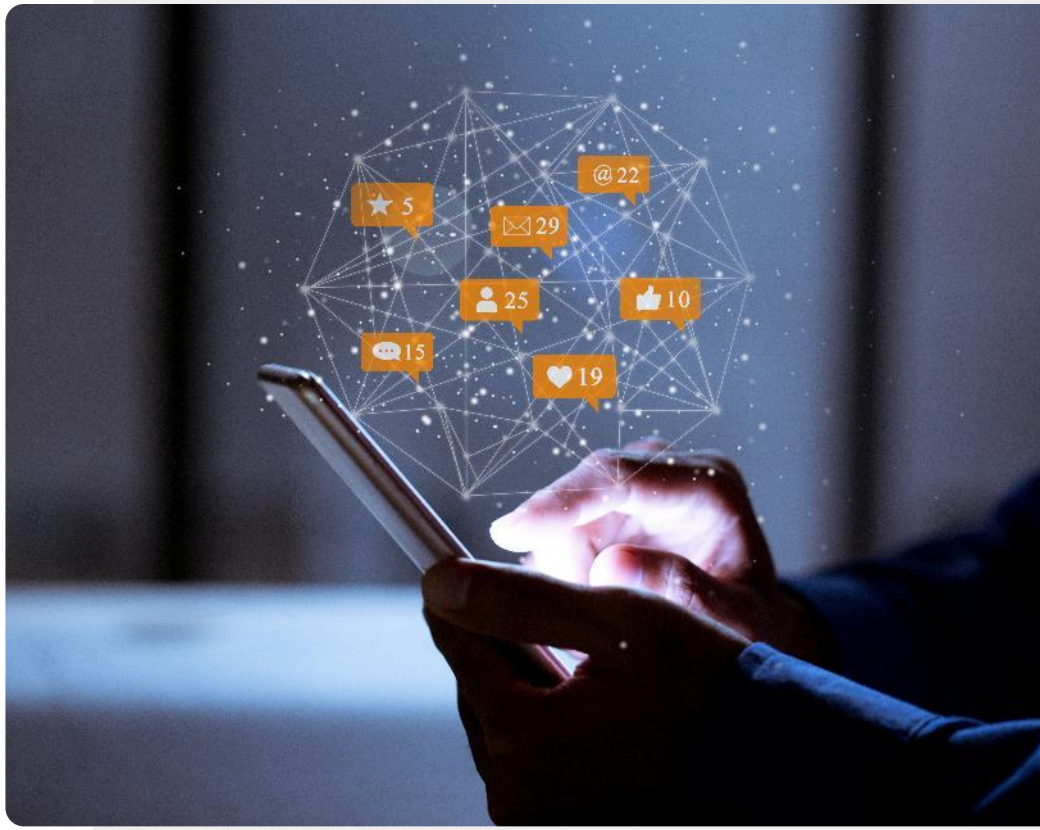
Partilhar informações nas redes sociais

Quando partilha informação nas redes sociais, deve presumir que fica por muito tempo. Pense que a sua publicação pode causar problemas.

"Embora possa parecer que a informação está a ser partilhada apenas com os seus amigos e familiares, também pode ser partilhada com hackers e oportunistas que examinam através das redes sociais".

"Uma vez que a informação seja revelada, pode ser usada por qualquer número de personagens sem escrúpulos."

Joseph Turow - Penn State



Onde denunciar casos de ciberbullying

O fornecedor de serviços ou a rede social pode ajudá-lo a bloquear mensagens e chamadas indesejadas.

Se a situação for mais grave, a polícia local pode investigar comunicações ameaçadoras.

Remover identidades *online*

Geralmente é possível alterar o perfil nas redes sociais para que não fique visível para o público em geral.

Nem sempre é possível excluir as publicações nas redes sociais ou fóruns na Internet, mas pode excluir a sua identidade, para que essas publicações se tornem anónimas.

Em alguns casos, pode enviar uma solicitação para um motor de pesquisa, como o Google, para que os dados não apareçam nas pesquisas.

Foi *pwned*?

Pwned é um estrangeirismo frequentemente usado como sinónimo para comprometimento de dados. Ao aceder o *e-mail* ou conta na rede social de outro utilizador, uma pessoa pode enviar *e-mails* e mensagens mal intencionadas.

Isto acontece quando há uma falha de dados de um serviço *online* que inclui a sua palavra-passe. Se usar a mesma palavra-passe em várias contas diferentes, como *e-mail* e redes sociais, a conta poderá ser invadida.

https://haveibeenpwned.com/

Escolha os seus amigos online com cuidado

Escolher amigos online: avalie com cuidado as informações que recebe de “novos” amigos.

Não partilhe as informações pessoais e tenha conversas neutras.

Não empreste dinheiro para nenhum “novo” amigo.

Um verdadeiro amigo estará interessado em conhecer os seus interesses e não em utilizá-lo para resolver os seus problemas.

Fazer novos amigos online

Vantagens

- Pode conectar-se com pessoas de todo o mundo.
- Pode descobrir muitos mais amigos que partilham os mesmos interesses online do que numa comunidade local.
- Salas de conversa *online* podem ser mais fáceis do que pessoalmente.
- É possível desativar a conta se algo der errado.

Desvantagens

- Se preferir comunicar pessoalmente, a distância pode ser um problema.
- Deve ter cuidado para não divulgar informações pessoais a um estranho. A identificação pode ser falsa.
- É mais fácil para as pessoas ofenderem *online*, já que não veem a outra pessoa.

O que é conteúdo impróprio?

Conteúdo impróprio inclui imagens de *"ataques terroristas, decapitações e bombardeamentos; crueldade com humanos e animais; locais de automutilação; conteúdo pró-anorexia; transtorno alimentar; conteúdo pró-suicídio; abuso sexual e violação; violência e conteúdo angustiante; sites de ódio; pornografia online".*

Na gíria da Internet, uma pessoa que publica conteúdo impróprio com a intenção de provocar ou insultar outros utilizadores é chamada de *troll*.

Como lidar com conteúdo impróprio

A maioria dos fornecedores de pesquisa tem recursos para oferecer suporte para lidar com conteúdo impróprio. Por exemplo, a “Pesquisa Segura” *(SafeSearch)* da Google está localizado em https://www.google.com/preferences.

É a primeira opção na página, e clique no ícone quadrado localizado ao lado de "Ativar a Pesquisa Segura".

Também pode optar por bloquear a Pesquisa Segura e o Google irá bloquear textos em *sites* adultos e imagens associadas a esses sites.

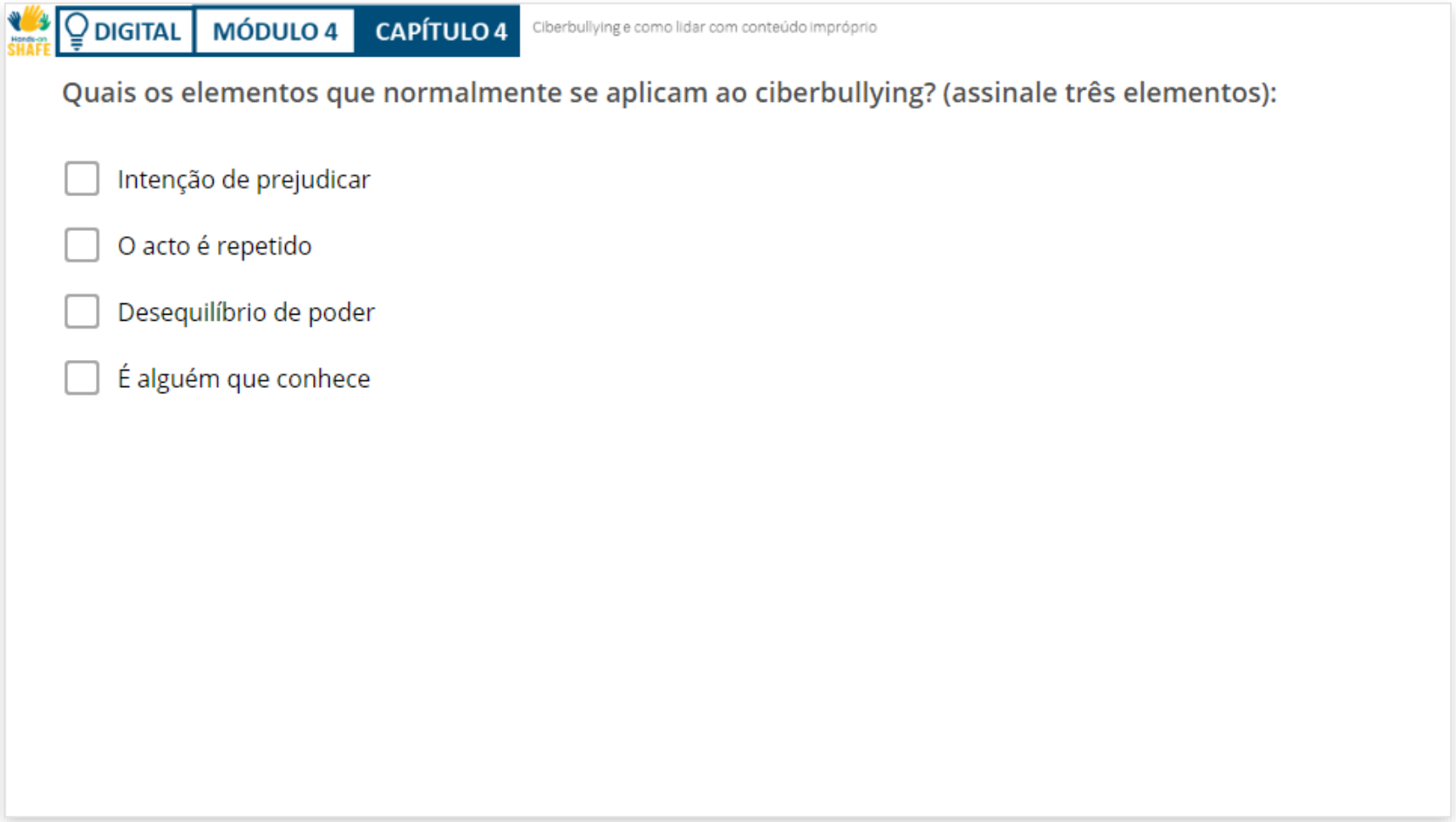
Ajude a Teresa

A Teresa está chateada com um incidente de ciberbullying. Pode ajudá-la?

- Conheça e saiba mais sobre a Teresa. Você pode encontrar informações sobre Teresa aqui.
- A Teresa usa a tecnologia para manter contato com os amigos, mas recentemente foi afetada pelo ciberbullying. Até agora, não é um caso grave, mas ainda assim, ela gostaria de saber como lidar com isso – principalmente se continuar.
- A partir das informações que aprendeu nos slides anteriores, dê conselhos à Teresa sobre como lidar com o ciberbullying.
- Se o ciberbullying ficar mais sério, a quem a Teresa deve contatar?

Quiz

Click the **Quiz** button to edit this object

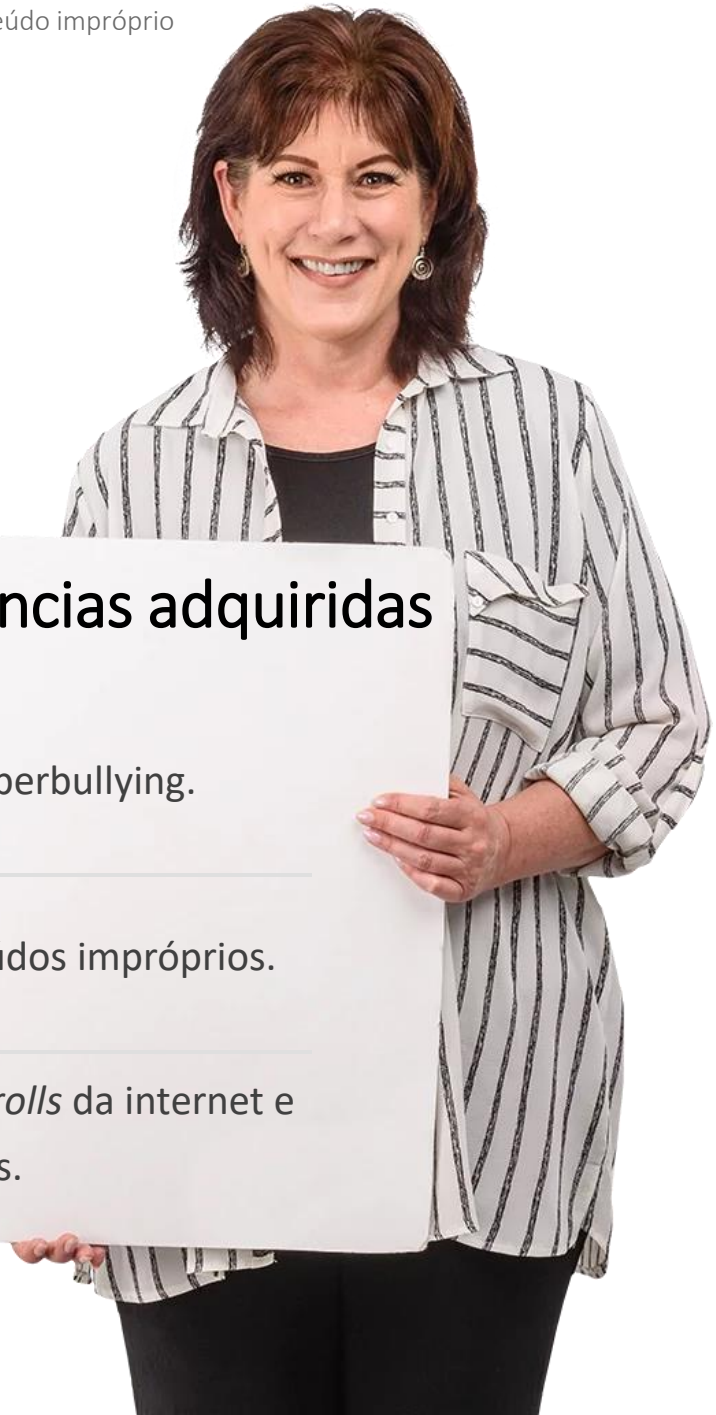


Resumo do capítulo

1. Aprendeu sobre ciberbullying, como reconhecê-lo e denunciá-lo.
2. Aprendeu sobre conteúdo impróprio e como bloquear.
3. Aprendeu a estar seguro enquanto conhece novos amigos *online.*
4. Aprendeu a ter cuidado ao partilhar dados *online* uma vez publicados, é difícil remover.
5. Se não gostar de algo: pode bloquear, denunciar ou desativar a sua conta.

Capítulo concluído!

Parabéns! Concluiu este capítulo com sucesso!



Resumo das competências adquiridas

1. Como reconhecer o Ciberbullying.
2. Como bloquear conteúdos impróprios.
3. Como reconhecer os *trolls* da internet e não cair em armadilhas.

O que vem a seguir?

Agora pode repetir este capítulo ou seguir a nossa recomendação para continuar a aprendizagem, clicando num dos botões abaixo:

Reiniciar

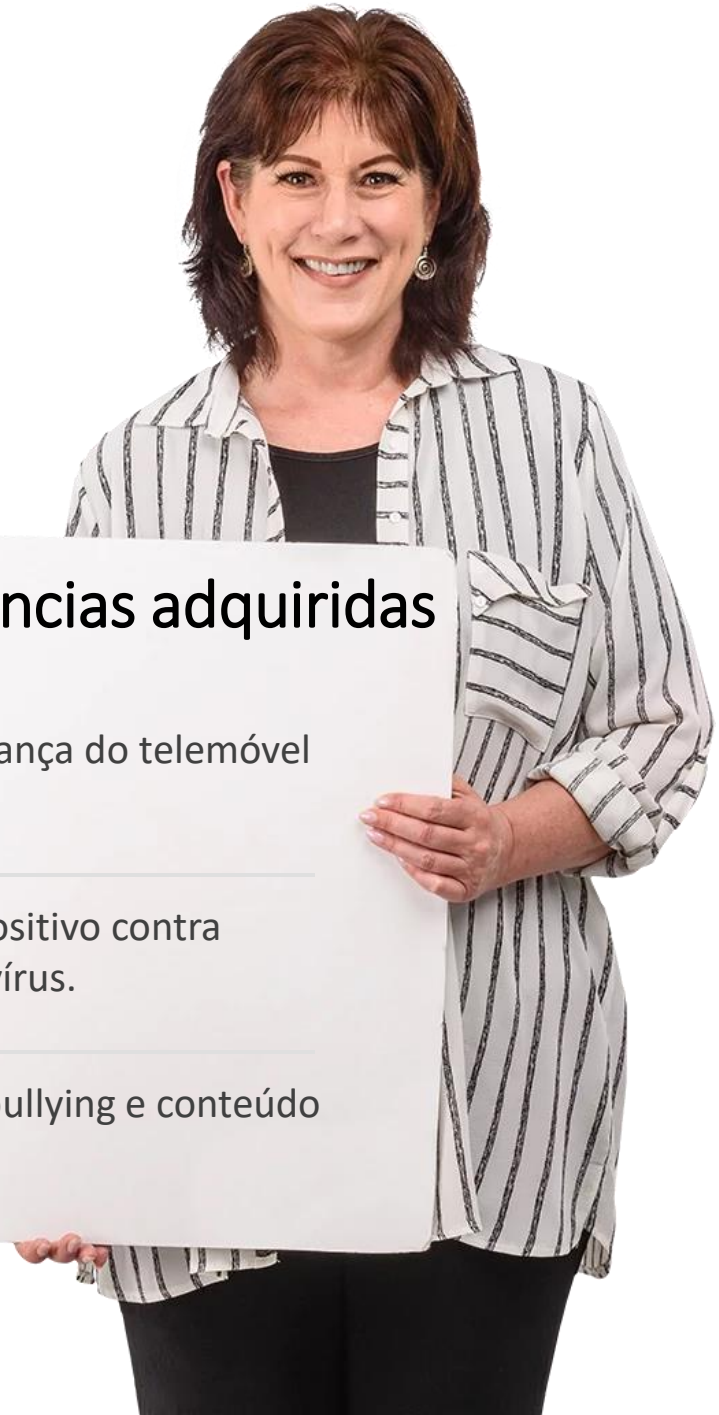
Seguinte

Resumo do módulo

1. Aprendeu sobre a segurança do telemóvel.
2. Aprendeu sobre o Regulamento Geral de Proteção de Dados, RGPD.
3. Aprendeu sobre os tipos de autenticação.
4. Aprendeu como criar palavras-passe fortes.
5. Aprendeu sobre as ferramentas de ataques de *hackers*: *Malware, Ransomware,* DDoS.
6. Aprendeu sobre ciberbullying e como não se tornar uma vítima.
7. Aprendeu a ajustar as configurações da Pesquisa Segura do Google para evitar conteúdo impróprio.

Módulo completo!

Parabéns! Concluiu este módulo com sucesso!



Resumo das competências adquiridas

1. Aprendeu sobre segurança do telemóvel pessoal e RGPD.
2. Como proteger o dispositivo contra ataques de *hackers* e vírus.
3. Como lidar com ciberbullying e conteúdo impróprio.

O que vem a seguir?

Agora pode repetir este módulo ou seguir a nossa recomendação para continuar a aprendizagem, clicando num dos botões abaixo:

Reiniciar

Seguinte