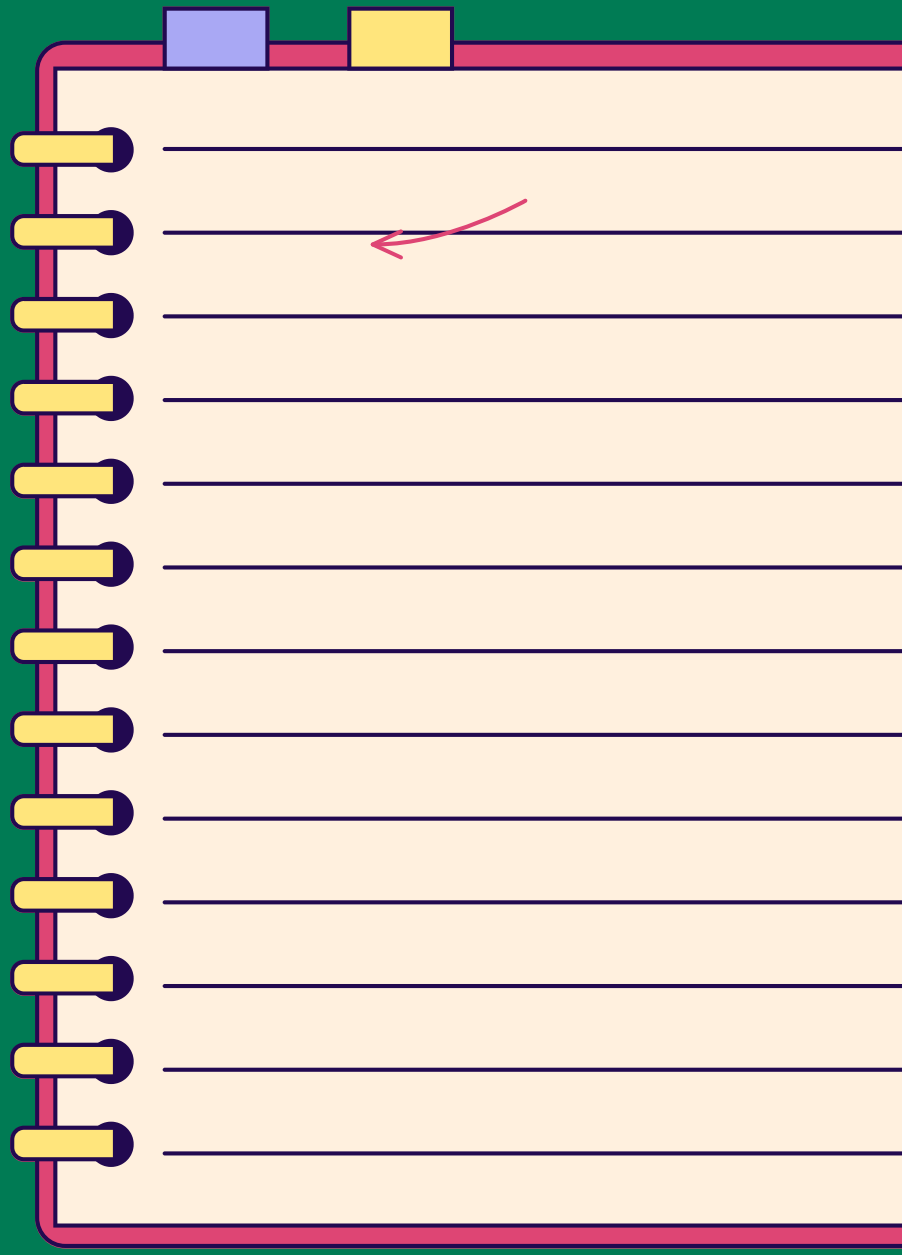
MÓDULO 1 - ESCOLHER O SEU DISPOSITIVO
E PROTEGÊ-LO

CAPÍTULO 3

PROTEÇÕES DIGITAIS PARA DISPOSITIVOS ELETRÓNICOS



Skills to Connect

INTRODUÇÃO

Proteger seus dispositivos digitalmente significa guardar os seus dados e evitar qualquer roubo ou “hackeamento” de suas informações. Desde a evolução da tecnologia e dos dispositivos digitais, os hackers estão constantemente a desenvolver novas estratégias para obter os nossos dados, ou mesmo “sequestrá-los” com um resgate.

Portanto, é essencial proteger os seus dispositivos para evitar inconvenientes posteriores.

Neste capítulo abordaremos diversos temas: antivírus, senhas e outros sistemas para proteger as suas informações e impedir que alguém tenha acesso a elas, a importância das atualizações e de verificar se confia nos sites com os quais partilha as suas informações.

Aqui vamos nós!

1 ANTIVÍRUS

TUDO O QUE PRECISA SABER SOBRE ANTIVÍRUS!

O QUE É UM ANTIVÍRUS?

- Um antivírus é um programa concebido para detectar, neutralizar ou erradicar softwares maliciosos (vírus, cavalos de Tróia, “ransomware”, “spyware”, etc.) de dispositivos eletrónicos.
- Também desempenha um papel preventivo contra as infecções e permitindo verificações frequentes do seu computador para detectar ficheiros suspeitos. Um dispositivo sem antivírus é como uma casa com a porta aberta: atrai intrusos indesejados.
- O antivírus atua como um guarda de segurança, protegendo seu sistema contra ataques.

PORQUE É NECESSÁRIO UM ANTIVÍRUS?

- Em 2019, um dos fornecedores de antivírus relatou ter detectado 2,6 milhões de ameaças, isso é enorme! Proteger o seu dispositivo é essencial. Qualquer dispositivo conectado à Internet está potencialmente à mercê de ataques e cibercriminalidade. Mas não pára por aí. Um dispositivo também pode ser infectado através de uma chave USB ou de um disco rígido externo, que são infectados através de outro dispositivo. Nesse caso, você pode infectar outras pessoas ou ser infectado por outras pessoas.
- Os possíveis impactos incluem:
  - Interrupção e lentidão do computador.
  - Bloqueio, eliminação ou encriptação de ficheiros em troca de pagamento (“ransomware”).
  - Roubo de dados pessoais (dados bancários, trabalhos realizados).
  - Controlo remoto do computador.
  - Phishing para capturar senhas ou pagamentos.
  - Uso do poder computacional do computador para fins maliciosos.

1 ANTIVÍRUS

TUDO O QUE PRECISA SABER SOBRE ANTIVÍRUS!

COMO FUNCIONA UM ANTIVÍRUS?

- Os antivírus usam três métodos principais de detecção:
  - Detecção específica: compara ficheiros no computador com bancos de dados de programas maliciosos conhecidos para detectá-los.
  - Detecção genérica: procura variantes de vírus conhecidos.
  - Detecção heurística: identifica vírus desconhecidos analisando o comportamento do programa.

COMO ESCOLHER O ANTIVÍRUS CERTO?

Recursos importantes:

- **Proteção geral:** avalie primeiro a proteção geral, antes de examinar os recursos adicionais.
- **Resultados do teste:** verifique ações específicas, especialmente para phishing.
- **Recursos adicionais:** alguns antivírus incluem ferramentas como gestor de senhas ou VPNs.
- **Apenas um antivírus:** Instalar vários antivírus é contraprodutivo porque correm o risco de bloquear-se um ao outro.

1 ANTIVÍRUS

TUDO O QUE PRECISA SABER SOBRE ANTIVÍRUS!

COMO COMPARAR DIFERENTES ANTIVÍRUS?

- Use um comparador de antivírus (como *Test Achat* na Bélgica, por exemplo)
- O sistema operacional também desempenha um papel. Os resultados dos testes de antivírus nem sempre são exatamente os mesmos para uma versão do Windows ou uma versão do macOS (Apple);
- Para produtos pagos, procure as promoções em vigor, dependendo da quantidade de dispositivos que deseja proteger;
- Os produtos gratuitos incluem publicidades, o que é mais ou menos incómodo.

Requisitos do sistema

- Verifique os requisitos mínimos do sistema para evitar abrandar o funcionamento do seu dispositivo.

Marcas populares

- Avast, AVG, Avira, Bitdefender, ESET, F-Secure, G Data, Kaspersky, McAfee, Microsoft, Norton, Panda Security, Sophos, Trend Micro.
- Alguns oferecem versões gratuitas com publicidades; as versões pagas oferecem suporte ao cliente e menos publicidades.

Dicas de compras

- Procure promoções de produtos pagos.
- Desmarque a renovação automática se não quiser.
- Teste uma versão gratuita antes de assumir um compromisso financeiro, para ver se é fácil começar e se acha fácil de usar. Isso permite fazer uma primeira verificação e análise do seu computador.

1 ANTIVÍRUS

TUDO O QUE PRECISA SABER SOBRE ANTIVÍRUS!

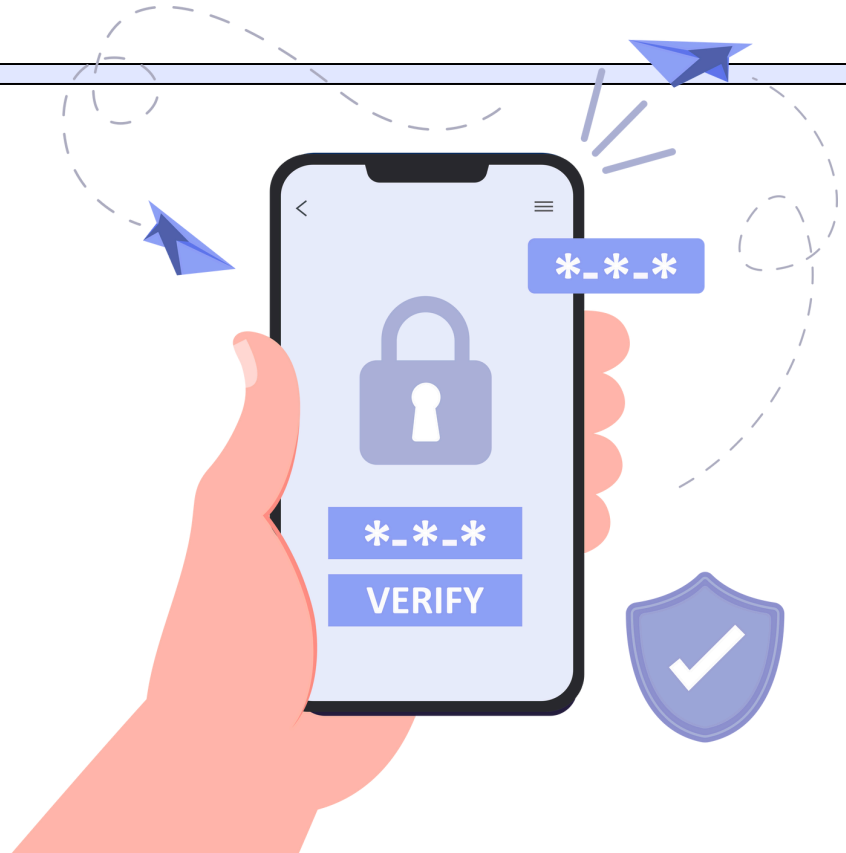
BOAS PRÁTICAS PARA USAR UM ANTIVÍRUS

- **Analisar suportes amovíveis :** verifique pens e discos rígidos externos para evitar qualquer contaminação.
- **Colocar arquivos suspeitos em quarentena:** evite apagá-los imediatamente, ao colocá-los em quarentena pode verificar sua origem antes de tomar uma decisão.
- **Fazer atualizações frequentes:** certifique-se de que o antivírus esteja atualizado antes de cada verificação. Ative atualizações automáticas, se for possível.
- **Fazer verificações frequentes:** programe verificações frequentes do seu sistema para detectar ameaças a tempo.
- **Cortar a ligação com a Internet em caso de infecção:** isso evita que o programa malicioso comunique dados remotamente.
- **Usar senhas seguras:** altere suas senhas regularmente e use senhas complexas.
- **Evitar links suspeitos:** não clique em links questionáveis em e-mails ou sites não seguros.

2 APLICAÇÕES SEGURAS

PORQUE É QUE A SEGURANÇA DAS APLICAÇÕES É IMPORTANTE?

Ao descarregar aplicações, pode expor inadvertidamente os seus dados pessoais. Algumas aplicações podem até conter programas maliciosos que roubam esses dados ou danificam o seu dispositivo.
Eis algumas dicas simples para se proteger.



2 APLICAÇÕES SEGURAS

DICAS DE SEGURANÇA PARA DESCARREGAR APLICAÇÕES

1. DESCARREGAR APENAS DE FONTES OFICIAIS

- Usar lojas de aplicações oficiais como Google Play Store para Android ou App Store para iPhone.
- Evitar sites desconhecidos e lojas de aplicações que possam oferecer aplicações não verificados.
- Não baixar aplicações clicando em links recebidospor e-mails ou mensagens não solicitadas.
- Evitar sites duvidosos que oferecem aplicações gratuitas ou pirateadas.
- Exemplo: se receber um link via mensagem para descarregar uma nova aplicação de saúde, verifique primeiro a sua legitimidade.

2. FICAR ATENTO ÀS PERMISSÕES SOLICITADAS

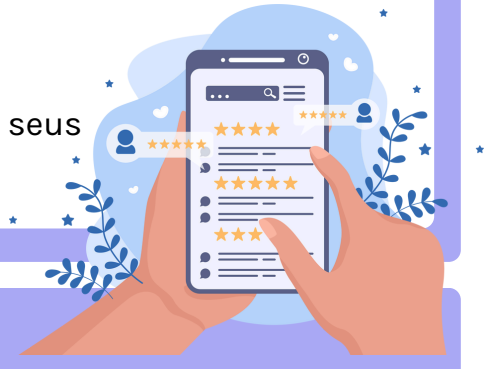
- Quando instala uma aplicação, ela solicita permissões para acessar determinados recursos do seu telemóvel.
- Se uma aplicação solicitar permissões que pareçam excessivas, tome cuidado!
- Exemplo: uma aplicação de gestão de tarefas não deve precisar de acesso às suas fotos.

2 APLICAÇÕES SEGURAS

DICAS DE SEGURANÇA PARA DESCARREGAR APLICAÇÕES

3. LER COMENTÁRIOS E CLASSIFICAÇÕES

- Antes de descarregar uma aplicação, veja o que outros usuários dizem sobre ela.
- Desconfie de aplicações com poucas ou muitas avaliações negativas.
- Exemplo: se está à procura de uma aplicação para registar as suas viagens entre os seus diferentes beneficiários, escolha um que tennha muitas avaliações positivas.



4. ATUALISAR AS APLICAÇÕES REGULARMENTE

- As atualizações costumam corrigir problemas de segurança.
- Ative as atualizações automáticas para não precisar se preocupar com elas.

5. CUIDADO COM APLICAÇÕES GRATUITAS

- Algumas aplicações gratuitas podem financiar os seus serviços apresantando anúncios ou contendo spyware. Prefira aplicações de editores conhecidos e bem avaliados. Por exemplo, uma apliação gratuita para tomar notas pode coletar os seus dados para vendê-las aos anunciantes.

2 APLICAÇÕES SEGURAS

DICAS DE SEGURANÇA PARA DESCARREGAR APLICAÇÕES

6. MONITORIZAR O DESEMPENHO DO SEU TELEMÓVEL

- Se o seu telemóvel ficar lento de repente ou agir de forma estranha após a instalação de uma aplicação, desinstale-a.
- Nas configurações do seu telemóvel, é possível verificar quanta bateria e dados as aplicações estão a consumir. Se parecer muito, saia da página e/ou desinstale a aplicação.

7. CUIDADO COM APLICAÇÕES FREEMIUM!

- Algumas aplicações são gratuitas no início, mas são pagos após um período de teste ou exigem pagamentos para desbloquear funcionalidades adicionais. Por exemplo, uma aplicação é pago após um mês de uso gratuito, mas solicitará diretamente que você insira os seus dados bancários e posteriormente debitar-lhe-á dinheiro.
- Leia os termos de serviço com atenção e verifique se existem custos ocultos antes de instalar uma aplicação.

3 CÓDIGOS E OUTROS BLOQUEIOS

PORQUE É QUE A SEGURANÇA DOS DISPOSITIVOS É IMPORTANTE?

Dispositivos móveis, como telemóveis e tablets, geralmente contêm informações pessoais importantes. Proteger os dispositivos é essencial para evitar que essas informações caiam em mãos erradas.
Entre as proteções disponíveis, códigos, impressões digitais, etc. são métodos de bloqueio: seu dispositivo não pode ser visto sem ser desbloqueado.

Isto impede qualquer pessoa de ter acesso ao seu dispositivo.

EIS UMAS DICAS SIMPLES PARA PROTEGER OS SEUS DISPOSITIVOS USANDO ESTES MÉTODOS DE BLOQUEIO:

3 CÓDIGOS E OUTROS BLOQUEIOS

PORQUE É QUE A SEGURANÇA DOS DISPOSITIVOS É IMPORTANTE?

O QUE É UMA SENHA OU PIN?

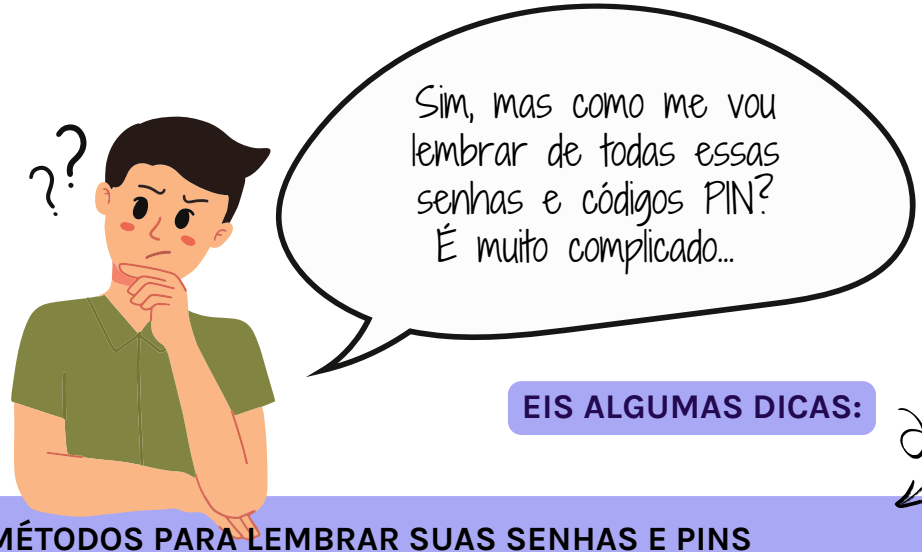
- Uma senha é uma série de letras, números e, às vezes, símbolos que escolhe e cria para proteger o seu dispositivo.
- Um PIN é um código numérico (geralmente de 4 ou 6 dígitos) que insere para desbloquear o seu dispositivo.
- Evitam que pessoas não autorizadas acessem as suas informações pessoais se lhe tirarem o telemóvel.

COMO CRIAR UMA SENHA?

- Criar uma senha complexa ou código PIN é a melhor maneira de garantir a segurança do seu dispositivo. Quanto mais complexo for, mais difícil será descobrir. Um código PIN “1234” é muito simples. Da mesma forma, é aconselhável não utilizar uma senha muito óbvia, por exemplo o nome dos seus filhos, pois é muito fácil para os hackers encontrarem essas informações e desbloquearem os seus dispositivos.
- **Critérios para uma boa senha ou PIN:**
  - Usar uma combinação de letras (maiúsculas e minúsculas), números e símbolos. Por exemplo, "A!d3_@D0m1c1l3".
  - Comprimento: Quanto maior for a senha, melhor. Tente usar pelo menos 12 caracteres.
  - Complexidade: Misture diferentes tipos de caracteres (letras, números, símbolos).
  - Diversidade: Evite usar a mesma senha para várias contas.
  - PIN: Use um código de 6 dígitos em vez de um código de 4 dígitos para maior segurança. Por exemplo, “482193” é muito mais seguro que “1111”.

4 BLOQUEAR OS SEUS DISPOSITIVOS

USE UMA SENHA OU PIN



EIS ALGUMAS DICAS:

MÉTODOS PARA LEMBRAR SUAS SENHAS E PINS

- **Memorização:** Crie frases fáceis de lembrar e use as primeiras letras de cada palavra. Por exemplo: “O meu cão Bruno adora brincar no parque!” torna-se "0MCB@BN_P!".
- **Gestor de senhas:** Use um gestor de senhas para armazenar e gerar senhas complexas e seguras. Só precisa memorizar uma senha principal.
- **Anotações seguras:** Se for absolutamente necessário anotar as suas senhas, não as escreva tal e qual, use indicações ou códigos que só você pode entender e guarde-as algo seguro (ex: atividade favorita do Bruno: brincar no parque)

4 BLOQUEAR OS SEUS DISPOSITIVOS

USAR IMPRESSÃO DIGITAL

IMPRESSÃO DIGITAL

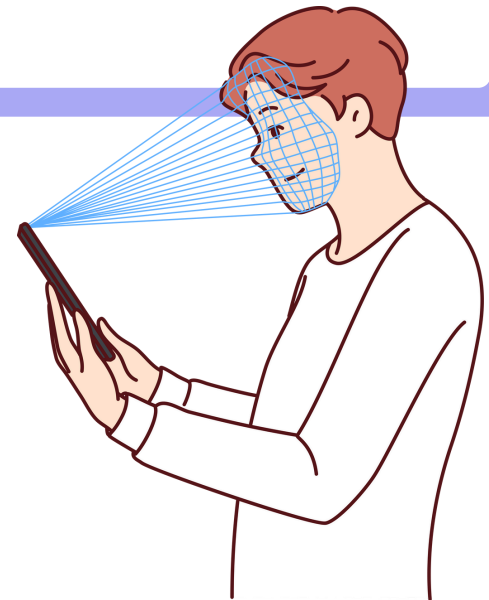
- **O que é a impressão digital?**
  - É um método de segurança que usa a sua impressão digital para desbloquear o seu dispositivo.
- **Porquê usá-la?**
  - É rápido e conveniente. Basta colocar o dedo no sensor para desbloquear o dispositivo.
  - É mais seguro do que simples senhas ou PINs porque cada impressão digital é única.
- **Como ativá-la?**
  - Nas configurações do seu telemóvel,
  - Procure opções de segurança ou biometria,
  - Siga as instruções para registrar a sua impressão digital.

4 BLOQUEAR OS SEUS DISPOSITIVOS

USE IDENTIFICAÇÃO FACIAL

IDENTIFICAÇÃO FACIAL

- **O que é a identificação facial?**
  - É um método de segurança que utiliza uma câmera para reconhecer a sua cara e desbloquear o seu dispositivo.
- **Porquê usá-la?**
  - Tal como a impressão digital, é rápido e conveniente.
  - É seguro porque é difícil alguém fingir a sua cara.
- **Como ativá-la?**
  - Nas configurações do seu telemóvel,
  - Procure opções de segurança ou biometria,
  - Siga as instruções para registrar o seu rosto.



4 BLOQUEAR OS SEUS DISPOSITIVOS

DICAS GERAIS DE SEGURANÇA DE DISPOSITIVOS

1

Não compartilhe as suas senhas ou códigos PIN!

Guarde essas informações para proteger os seus dados.

2

Mude as suas senhas regularmente!

Atualize as suas senhas com frequência para aumentar a segurança.

3

Use proteção adicional para aplicações sensíveis!

Se tiver aplicações que contenham informações confidenciais (como aplicativos bancários), adicione uma camada extra de segurança (como uma senha ou impressão digital para acessar essas aplicações).

4

Tenha cuidado em ambientes inseguros!

Evite desbloquear o seu telemóvel ou introduzir as suas senhas em público, onde alguém possa ver.

5 AUTENTICAÇÃO COM DOIS FATORES

O QUE É A AUTENTICAÇÃO COM DOIS FATORES?

- A autenticação com dois fatores (ou 2FA, "Two-Factor Authentication") ou “validação em duas etapas” é um método de segurança que adiciona uma camada extra de proteção ao iniciar sessão nas suas contas online.
- Requer não apenas uma senha, mas também um segundo elemento de verificação, muitas vezes chamado de "fator", que é algo que tem (como o seu telemóvel) ou algo que é (como uma impressão digital) e que permitirá provar que é realmente você .

RESUMINDO: IDENTIFICA-SE DUAS VEZES EM VEZ DE UMA!

5 AUTENTICAÇÃO COM DOIS FATORES

PORQUÊ IMPLEMENTAR A AUTENTICAÇÃO COM DOIS FATORES?

REFORÇAR A SEGURANÇA

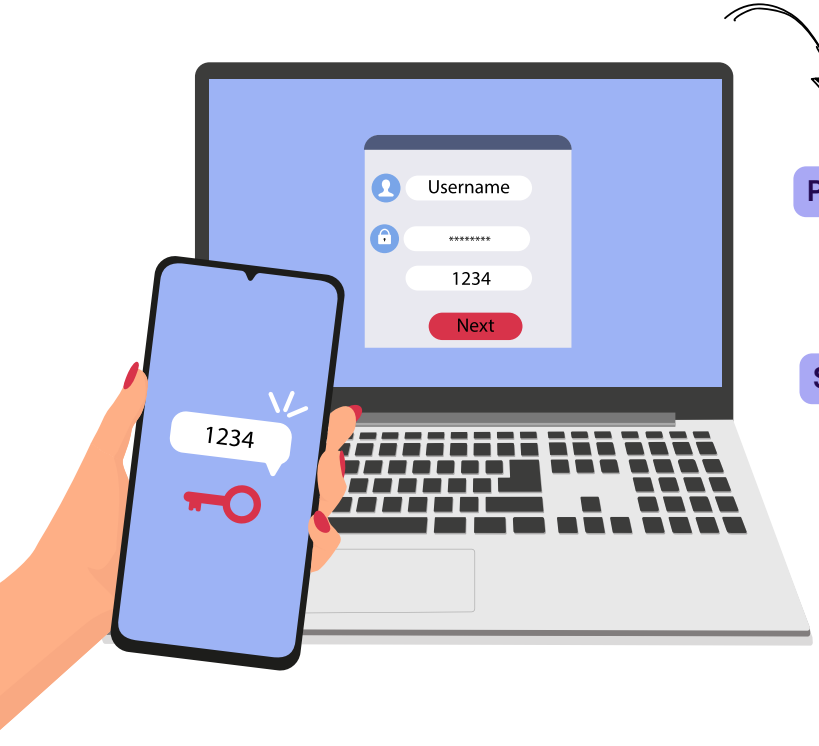
- Mesmo que alguém descubra a sua senha, será difícil ter acesse à sua conta sem o segundo fator. Portanto isto reduz significativamente o risco de pirataria informática, pois um atacante precisaria tanto da sua senha como do segundo fator.
- As senhas podem ser roubadas ou adivinhadas, mas o segundo fator, geralmente as elementos físicos que possui, é muito mais difícil de ser comprometido. Pode ficar descansado sabendo que suas contas estão mais protegidas.

PROTEGER DADOS CONFIDENCIAIS

- Os seus dados ficam muito mais seguros com a dupla autenticação do que com uma única senha. Pense em particular nas suas contas bancárias, e-mails, etc.
- Enquanto ajudante doméstico, poderá ter (acesso a) informações pessoais e sensíveis no seu telemóvel ou computador (como consultas, anotações sobre o beneficiário, etc.). Portanto é importante fazer tudo para garantir a proteção destes dados!

5 AUTENTICAÇÃO COM DOIS FATORES

PORQUÊ IMPLEMENTAR A AUTENTICAÇÃO COM DOIS FATORES?



PRIMEIRA ETAPA:

- Introduza o seu nome de utilizador e senha normalmente.

SEGUNDA ETAPA:

- Ser-lhe-á pedido fornecer um segundo elemento de verificação.
- Este pode ser:
  - **Código enviado por mensagem:** recebe um código no seu telemóvel que tem de introduzir.
  - **Aplicação de autenticação:** uma aplicação como Google Authenticator ou Microsoft Authenticator gera um código único e limitado no tempo.
  - **Chave de segurança física:** um pequeno dispositivo que insere na entrada USB.
  - **Reconhecimento biométrico:** usando a sua impressão digital ou reconhecimento facial.

5 AUTENTICAÇÃO COM DOIS FATORES

COMO ATIVAR A AUTENTICAÇÃO COM DOIS FATORES?

NUMA CONTA GOOGLE

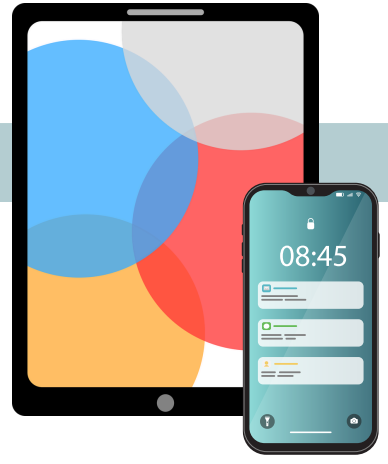
- Nas configurações da conta Google,
- Selecione “Segurança” e depois “Verificação em duas etapas”.
- Siga as instruções para adicionar o seu número de telefone ou uma aplicação de autenticação.

Para Android
(smartphone e tablet)

NUMA CONTA ICLOUD

- Nas configurações, clique no seu nome na parte superior,
- Selecione “Senha e segurança” e depois “Ativar autenticação com dois fatores”.
- Siga as etapas para configurar.

Para Apple
(smartphone e tablet)



NUM COMPUTADOR WINDOWS

- No site da sua conta da Microsoft,
- Em “Segurança”, selecione “Mais opções de segurança” e depois “Configurar autenticação com dois fatores”.
- Escolha o seu método preferido e siga as instruções.

6 ATUALIZAÇÕES

O QUE SÃO ATUALIZAÇÕES?

- As atualizações de telemóvel, computador ou tablet são como consultas regulares com um médico. São cruciais para manter a segurança e o desempenho do dispositivo. Corrigem vulnerabilidades de segurança, adicionam novos recursos e melhoram a estabilidade das aplicações.
- Por exemplo, se utiliza uma aplicação para as viagens entre os seus beneficiários, uma atualização poderia corrigir um erro que estava desperdiçando o seu tempo surgerindo caminhos mal otimizados ou sem ter em conta determinadas alterações.
- Lembre-se de ativar as atualizações automáticas para garantir a segurança do seu dispositivo sem que tenha de se preocupar com isso.

6 ATUALIZAÇÕES

COMO IMPLEMENTAR ATUALIZAÇÕES?

PARA DISPOSITIVOS ANDROID

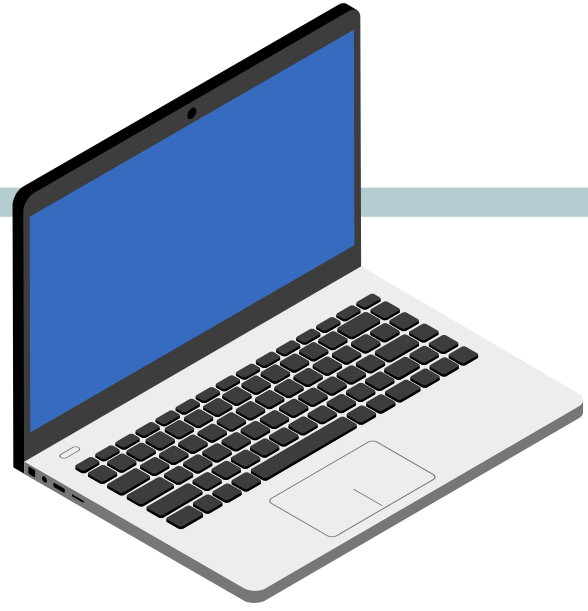
- Clique em “Configurações” no seu telemóvel.
- Deslize para baixo e clique em “Sistema”.
- Clique em “Avançado” e depois em “Atualizações do sistema”.
- Clique em “Verificar atualizações”. Se uma atualização estiver disponível, siga as instruções para a instalar.
- Certifique-se de que a opção de atualizações automáticas esteja ativada.

6 ATUALIZAÇÕES

COMO HABILITAR ATUALIZAÇÕES

PARA COMPUTADORES WINDOWS:

- Clique no menu “Iniciar” e selecione o ícone “Configurações” (roda dentada).
- Clique em “Atualização e segurança”.
- Clique em “Windows Update” no menu esquerdo.
- Clique em “Verificar atualizações”. Se houver atualizações disponíveis, serão instaladas automaticamente.
- Certifique-se de que as atualizações automáticas estejam ativadas. Windows costuma instalar atualizações automaticamente por defeito.



6 ATUALIZAÇÕES

COMO HABILITAR ATUALIZAÇÕES

PARA DISPOSITIVOS IOS (APPLE):

- Clique em “Configurações”.
- Deslize para baixo e clique em “Geral”.
- Clique em “Atualização de software”.
- Clique em “Atualizações automáticas” e ative “Descarregar atualizações iOS” e “Instalar atualizações iOS”.

7 A FUNÇÃO “LOCALIZAR”

O QUE É?

- A função “Localizar” é essencial para ajudar a encontrar o seu telemóvel. É ainda mais importante quando tem um trabalho móvel. Imagine que perde o seu telemóvel no caminho entre duas casas. Com este recurso, pode localizá-lo num mapa, ligar para localizá-lo ou até bloquear o acesso remotamente para proteger os seus dados confidenciais e os dos seus beneficiários.
- Ative esse recurso nas configurações do telemóvel para ter mais serenidade e segurança em relação às suas informações de trabalho.

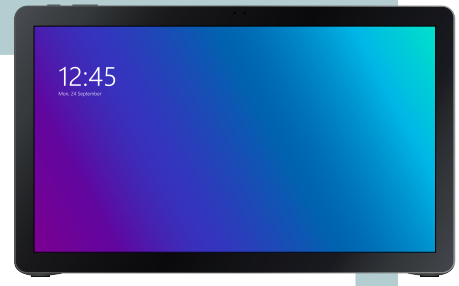
7 A FUNÇÃO “LOCALIZAR”

COMO ATIVAR ATUALIZAÇÕES?

PARA SMARTPHONES ANDROID:

- Clique em “Configurações”.
- Clique no seu nome na parte superior do ecrã.
- Clique em “Encontrar” e depois em “Encontrar o meu iPhone”
- Ative “Encontrar o meu iPhone” e “Enviar a última localização”.

PARA TABLETS ANDROID:



- Clique em “Configurações”.
- Deslize para baixo e clique em “Segurança”.
- Clique em “Encontrar o meu dispositivo”.
- Certifique-se de que a função esteja ativada.

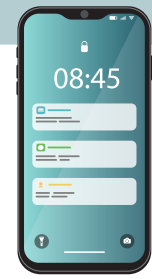
PARA COMPUTADORES WINDOWS

- Clique no menu “Iniciar” e selecione o ícone “Configurações”.
- Clique em “Atualização e segurança”.
- Clique em “Encontrar meu dispositivo” no menu esquerdo.
- Selecione “Editar” em “Localizar o meu dispositivo desativado” e ative a função.

7 A FUNÇÃO “LOCALIZAR”

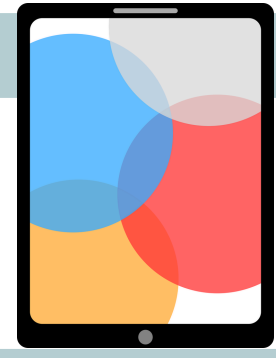
COMO ATIVAR ATUALIZAÇÕES?

PARA SMARTPHONES IOS (APPLE):



- Clique em “Configurações”.
- Clique no seu nome na parte superior do ecrã.
- Selecione “Encontrar” e depois “Encontrar o meu iPhone”
- Ative “Encontrar o meu iPhone” e “Enviar a última localização”.

PARA TABLETS IOS (APPLE):



- Clique em “Configurações”.
- Clique no seu nome na parte superior do ecrã.
- Selecione “Encontrar” e depois em “Encontrar o meu iPad”.
- Ative “Encontrar o meu iPad” e “Enviar a última localização”.

PARA COMPUTADORES MACOS (APPLE)

- Clique no menu “Apple” no canto superior esquerdo do ecrã e selecione “Preferências do Sistema”.
- Clique em “ID Apple” e depois em “iCloud”.
- Assinale a caixa “Encontrar o meu Mac”. Pode ser necessário iniciar sessão com o seu ID Apple.

AO SEGUIR ESTES PASSOS, PODE GARANTIR QUE OS SEUS DISPOSITIVOS ESTEJAM ATUALIZADOS E POSSAM SER ENCONTRADOS EM CASO DE PERDA OU ROUBO. ISSO GARANTE A SEGURANÇA DE SUAS INFORMAÇÕES PESSOAIS E PROFISSIONAIS, ESSENCIAIS PARA OS AJUDANTES DOMÉSTICOS.

Eis alguns recursos recomendados para verificar e aprender mais sobre esses procedimentos:

1. **Sites oficiais da Microsoft:**
   - Suporte Microsoft para Windows Update
   - Suporte Microsoft para Encontrar o Meu Dispositivo
2. **Sites oficiais da Apple:**
   - Suporte da Apple para atualizações no macOS:
   - Suporte da Apple para atualizações no iOS
   - Suporte da Apple para “Encontrar o meu Mac”
   - Suporte da Apple para “Encontrar o meu iPad”
3. **Sites oficiais do Android e do Google:**
   - Suporte do Google para atualizações do Android

Estes recursos são atualizados regularmente e oferecem instruções passo a passo e capturas de ecrã para ajudá-lo a implementar as medidas de segurança em vários dispositivos.