AGÊNCIA PARA A REFORMA TECNOLÓGICA DO ESTADO

GUIA DA FAMÍLIA DIGITAL

PARTE 2

SEGURANÇA DIGITAL **PARA TODOS**

PRR Plano de Recuperação e Resiliência · REPÚBLICA PORTUGUESA · Financiado pela União Europeia NextGenerationEU · academia portugal digital

GUIA DA FAMÍLIA DIGITAL

O Futuro é Digital

A Tua Família Também!

Vivemos num mundo cada vez mais digital, onde a *internet* e a tecnologia se tornaram essenciais para o dia a dia. Este guia, que se encontra dividido em seis partes, visa capacitar todas as famílias portuguesas para o mundo digital, de forma simples e segura, permitindo-lhes aceder a serviços *online*, comunicar de forma simples e segura nos meios digitais e protegerem-se de ameaças cibernéticas. No final, poderão ainda encontrar um documento bónus que contém ferramentas úteis para o quotidiano de qualquer Cidadão.

Parabéns, o primeiro passo já foi dado! Continua este percurso e torne-te numa **#FamiliaDigitalPT** de forma segura!

1 O Primeiro Passo para a Digitalização

2 Segurança Digital para Todos

3 A Chave Móvel Digital – A Chave que abre todas as Portas

4 Serviços Públicos ao Alcance de Todos

5 Torna-te um Cidadão Digital Ativo

6 A Família Mestre – A Transformação Digital ao Alcance de Todos!

GUIA DA FAMÍLIA DIGITAL | Ferramentas e Recursos Úteis

PARTE 2

SEGURANÇA DIGITAL **PARA TODOS**

Na parte 1 deste Guia, explorámos conceitos básicos sobre o mundo digital.

Agora, na **Parte 2**, vamos focar-nos na **segurança digital**, abordando estratégias essenciais para proteger a família contra fraudes, ataques informáticos e outros riscos. Mais do que navegar, é essencial fazê-lo com responsabilidade e segurança!

A *internet* está cheia de **vantagens**, mas também **riscos** como fraudes, vírus e ataques informáticos. **Proteger a família *online*** é essencial para navegar sem preocupações.

O QUE VAIS APRENDER NESTA PARTE?

- Criar palavras-passe seguras e usar gestores de *passwords*;
- Como identificar e evitar ataques de *phishing*, fraudes bancárias e esquemas *online*;
- Segurança nas redes sociais: proteger crianças, adolescentes e idosos;
- Atualizações, antivírus e proteção contra redes *Wi-Fi* públicas inseguras.

© ARTE 2025

1. Criar Palavras-Passe Seguras

Os ciberataques são tentativas de **roubo de dados, fraudes ou invasões a contas e dispositivos** que acontecem no mundo digital.

Conforme explorámos na Parte 1 do Guia, as nossas **palavras-passe** devem ser sempre seguras! Vamos relembrar alguns conselhos importantes:

Uma boa palavra-passe é a **primeira linha de defesa** contra *hackers* (piratas informáticos)!

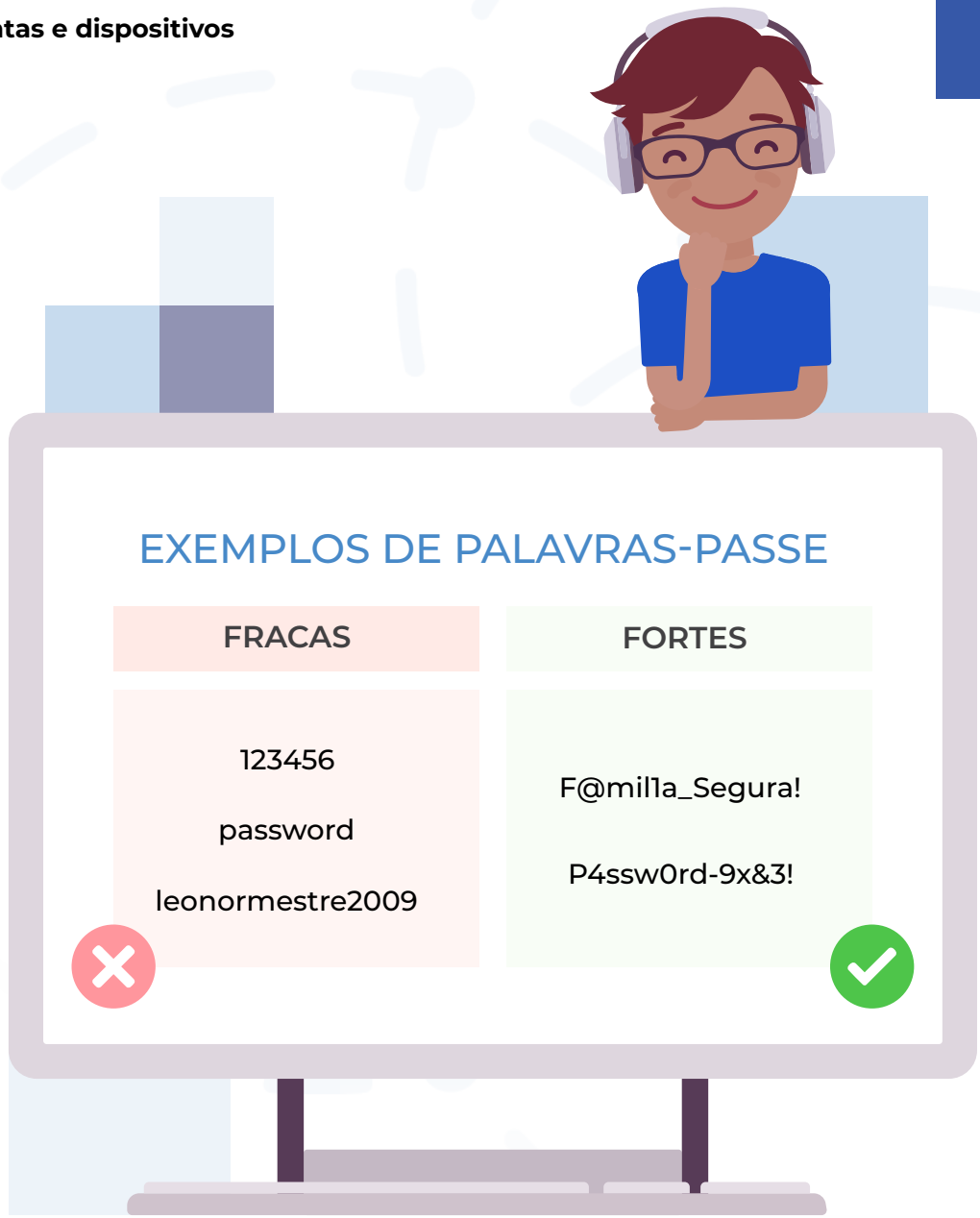
COMO CRIAR UMA PALAVRA-PASSE FORTE?

1. Usa **pelo menos 12 caracteres**;
2. Mistura **letras maiúsculas e minúsculas, números e caracteres especiais**;
3. Não uses **datas de nascimento ou palavras óbvias**.

DICA: Usa um **gestor de palavras-passe** como o ***Google Password Manager, Bitwarden* ou *1Password*** para guardá-las de forma segura!

TESTE PRÁTICO

Cria uma nova palavra-passe para um serviço que usas e vê se o *site* indica que é segura.



@ ARTE 2025

2. Como Evitar Fraudes e Ataques de *Phishing*

Os ciberataques são tentativas de **roubo de dados, fraudes ou invasões a contas e dispositivos.**

TIPOS DE CIBERATAQUES MAIS COMUNS

- ***Phishing*** – *E-mails* falsos que tentam roubar dados pessoais;
- ***Ransomware*** – Bloqueio de ficheiros por *hackers* que pedem resgate para desbloqueio dos mesmos;
- ***Spyware*** – *Software* que espia a tua atividade *online* sem autorização.

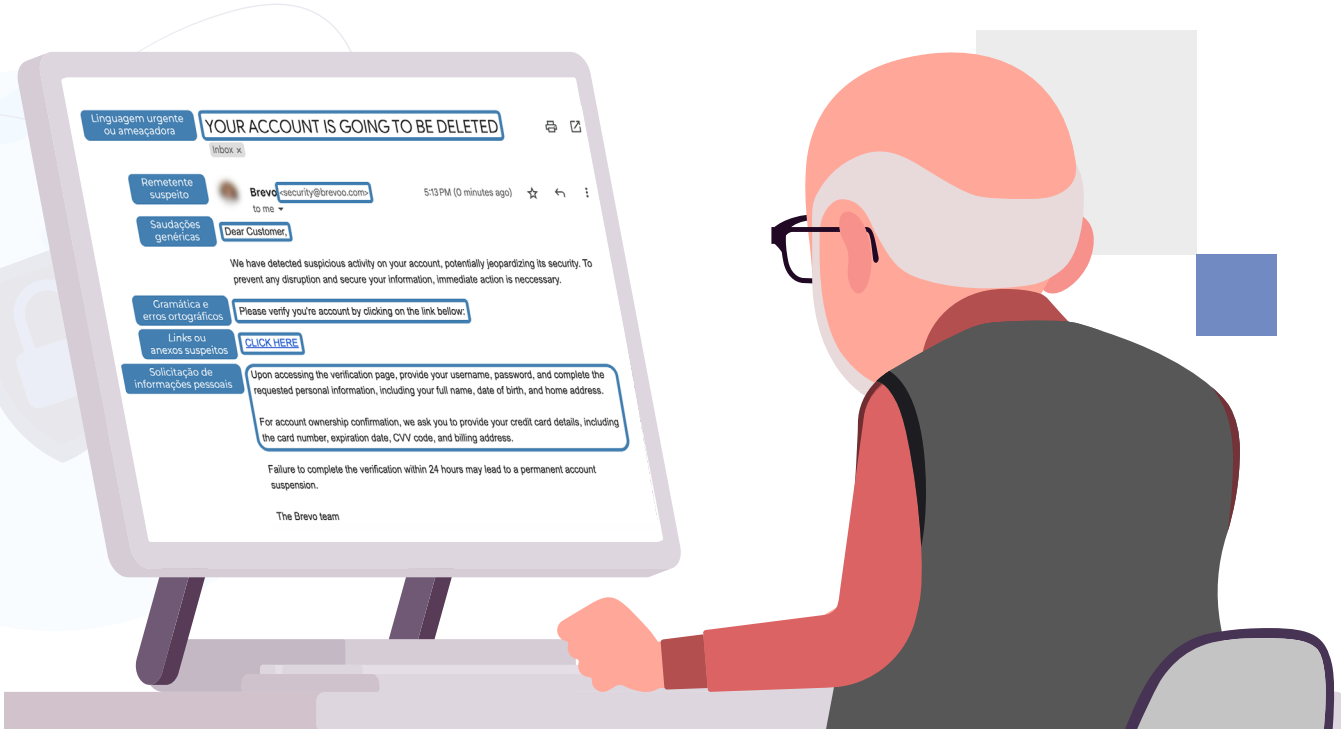
COMO IDENTIFICAR UM *E-MAIL* OU MENSAGEM FALSA?

- **Urgência suspeita:** "A tua conta será bloqueada em 24h!"
- **Erros ortográficos:** "Voçê precissa atualizar seu cartão."
- **Linguagem incomum**: "acessar" ao invés de "aceder"; "deletar" ao invés de "apagar"
- ***Links* estranhos:** Verifica se o *site* **termina em .com, .pt ou .gov.pt.** *Sites* seguros começam com **https://**.
- **Generalização:** A mensagem ou *e-mail* que te pede informações de dados pessoais ou pagamentos, deve ser dirigida a ti de forma específica.

ANTES DE CLICAR NUM *LINK*

- Passa o rato por cima do *link* para ver se é verdadeiro;
- Se tens dúvidas, entra no *site* diretamente sem clicar no *e-mail*.

DICA: Nunca forneças dados bancários por *e-mail* ou SMS. Os bancos nunca pedem essa informação!



© ARTE 2025

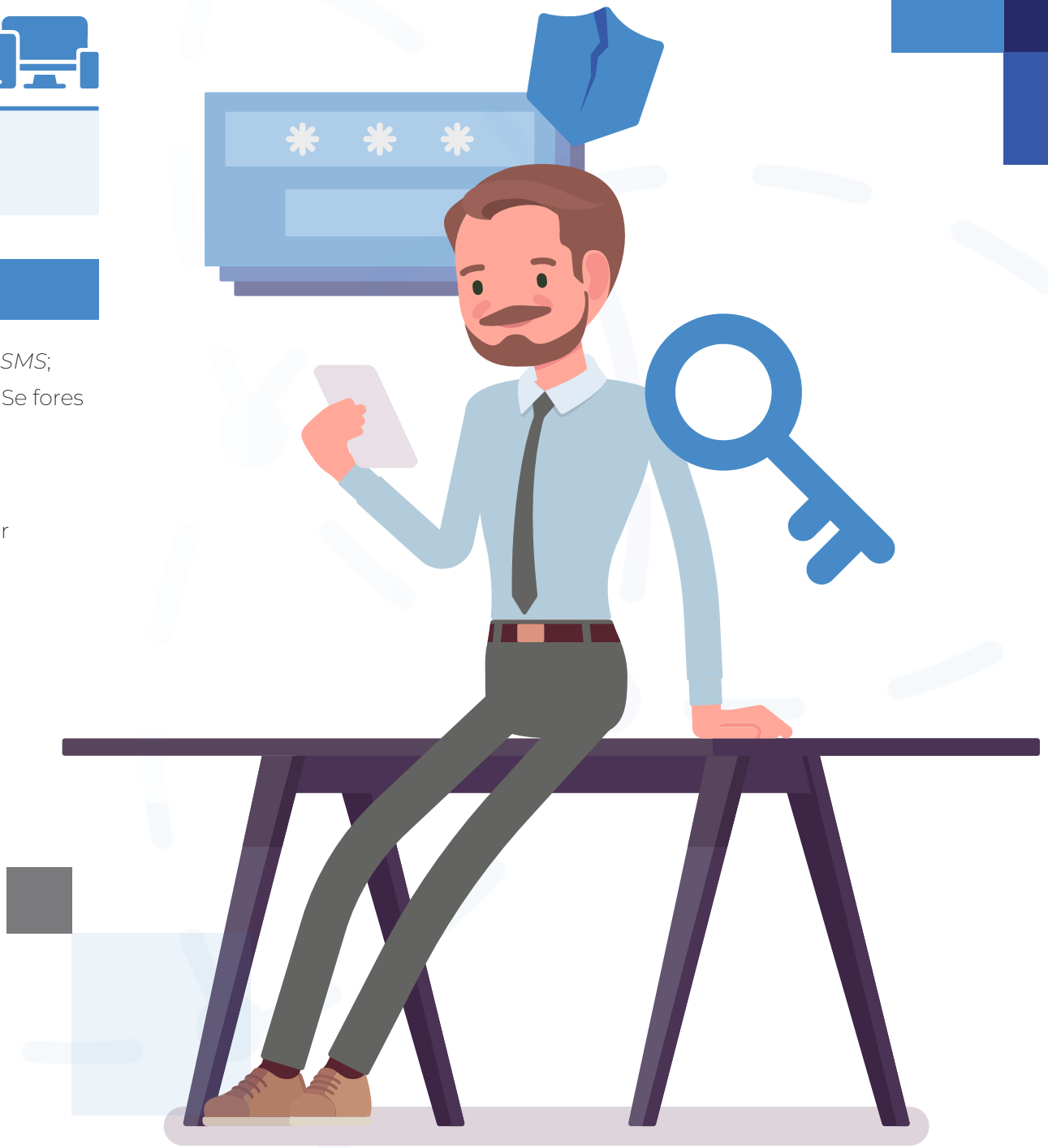
TESTE PRÁTICO

Simula um caso real: Um familiar recebe um *e-mail* suspeito. Como explicarias os sinais de alerta?

COMO EVITAR SER ALVO DE UM ATAQUE?

- **Não cliques em *links* suspeitos** recebidos por *email* ou *SMS*;
- **Evita atender chamadas de números desconhecidos.** Se fores menor, passa o telefone a um adulto;
- **Ativa a autenticação de dois fatores (2FA)** nas contas importantes, sempre que possível;
- **Mantém dispositivos e antivírus atualizados** para evitar vulnerabilidades;
- **Usa uma *VPN*** ao navegar em redes *Wi-Fi* públicas.

O que é uma VPN? : A VPN é uma Rede Privada Virtual, responsável por encriptar os teus dados pessoais, ocultar o teu endereço IP e garantir que a tua navegação em redes pública é segura, privada e protegida.



@ ARTE 2025

3. O que fazer em caso de ataque informático ou perda de dados?

Mesmo com precauções, pode haver **roubo de contas, dados ou ficheiros importantes.**

PASSOS A SEGUIR EM CASO DE CIBERATAQUE

1. **Mudar imediatamente as palavras-passe** das contas afetadas;
2. **Ativar a autenticação de dois fatores (2FA)** para impedir acessos não autorizados, caso ainda não tenhas ativado;
3. **Executar uma verificação de segurança** com um antivírus atualizado;
4. **Se houver roubo financeiro, contactar o banco** e as autoridades (Polícia Judiciária ou Linha *Internet* Segura: 800 219 090).

DICA: Faz **cópias de segurança (*backup*) regulares** dos teus ficheiros para evitar perdas em caso de ataque.

TESTE PRÁTICO

Faz um *backup* dos ficheiros mais importantes no teu computador ou num serviço de armazenamento na nuvem. Este tipo de armazenamento permite que possas aceder aos ficheiros da tua conta sempre que quiseres, através de diferentes dispositivos.

© ARTE 2025

4. Redes Sociais: Proteger os Mais Novos e os Mais Idosos

As redes sociais são divertidas, mas podem ser **perigosas** se não forem usadas com segurança.

Regras essenciais para proteger a privacidade:

1. **Recorrer a autenticação de dois fatores** (2FA) por exemplo no *Facebook, Instagram* e *WhatsApp*.
2. **Evitar partilhar dados pessoais** (morada, telefone, escola).
3. **Desativar a localização automática** nas redes sociais.
4. **Aceitar apenas amigos conhecidos** e denunciar perfis suspeitos.

PARA OS MAIS NOVOS. O QUE PODEMOS FAZER?

- Explicar que **nem todos na *internet* são quem dizem ser.**
- Ensinar a **não falar com desconhecidos** *online*.
- Alertar que devem **avisar um adulto** se virem algo preocupante ou forem vítimas de *bullying* digital.
- **Criar contas com permissões de controlo parental** para maior segurança.

FERRAMENTAS PARA CONTROLAR O TEMPO DE ECRÃ

Equilibrar o uso da tecnologia é essencial para a saúde mental e bem-estar de todos.

- ***Google Family Link***: Para acompanhar a atividade digital, aprovar ou bloquear *apps*, definir limites de tempo de ecrã e localizar o dispositivo em tempo real.
- ***Apple Screen Time***: Para monitorizar a atividade online, definir limites de uso, bloquear *apps* e ver relatórios de tempo de ecrã.
- ***Microsoft Family Safety*:** Para definir limites de tempo de ecrã, filtrar conteúdos online, monitorizar a atividade digital e localizar dispositivos.

@ ARTE 2025

DICA: Define **horários sem ecrã**, como durante as refeições e antes de dormir, para promover um uso equilibrado da tecnologia.

TESTE PRÁTICO

Ativa o ***Google Family Link*** ou o ***Screen Time*** no dispositivo de uma criança e ajusta as restrições de tempo de ecrã.

PARA OS MAIS IDOSOS. O QUE PODEMOS FAZER?

1. Mostrar como detetar perfis falsos.
2. Explicar como evitar partilhar *fake news* (notícias falsas) e *links* suspeitos.

DICA: Faz uma **revisão de privacidade** nas redes sociais da família uma vez por mês!

TESTE PRÁTICO

Vai às tuas redes sociais e ativa a autenticação de dois fatores nas definições de segurança tua conta (se ainda não tiveres).

@ ARTE 2025

5. Manter os dispositivos móveis e o Computador Seguros

Dispositivos desatualizados são alvos fáceis para *hackers* (piratas informáticos)!

COMO MANTER TUDO PROTEGIDO?

1. **Atualiza o sistema operativo regularmente** (*Windows, macOS, Android, iOS*).
2. **Instala um antivírus confiável** *(Bitdefender, Kaspersky, Avast*, etc.).
3. **Evita instalar *apps* desconhecidas** – utiliza apenas as apps disponibilizadas na App Store e Google Play.
4. **Desativa *Bluetooth* e *Wi-Fi* quando não estiverem em uso.**

DICA: Se perderes o telemóvel, podes localizá-lo e bloqueá-lo remotamente com o *Google Find My Device*/Localizar o meu dispositivo (*Android*) ou *Find My iPhone*/Encontrar o meu Iphone (*iOS*), se estiver ativa essa definição.

TESTE PRÁTICO

Confirma se o teu antivírus está atualizado e faz uma verificação no computador!

@ ARTE 2025

6. Comprar *Online* com Segurança

Fazer compras *online* é prático, mas **é preciso ter cuidado** com fraudes!

COMO EVITAR GOLPES EM COMPRAS *ONLINE* ?

1. Usa apenas sites **com HTTPS** no seu *link*/endereço (aparece um cadeado no navegador).
2. Evita lojas sem avaliações ou com preços "milagrosos".
3. Prefere ***MB WAY, PayPal* ou cartões virtuais** para pagamentos seguros.
4. Lê sempre as **políticas de devolução** antes de comprar.

DICA: Se desconfiares de um *site*, pesquisa entre aspas no *Google*: **"Nome da loja + Reclamações".**

TESTE PRÁTICO

Pesquisa um produto que queres comprar e verifica se o *site* é seguro!

Checklist "***Site* Seguro, Vida Segura":**

- ☐ O *site* tem "https" no endereço?
- ☐ O *site* tem avaliações reais, e positivas, de outras pessoas?
- ☐ Os preços são razoáveis e coerentes, em comparação com outras lojas?
- ☐ Diponibiliza pagamentos seguros, como *MB WAY, PayPal* ou um cartão virtual?
- ☐ O *site* possui uma política de devolução fidedigna?
- ☐ Existe um contato real da loja (morada, telefone, *email* válido)?
- ☐ Pesquisa entre aspas no *Google* "Nome da loja + Reclamações"?

@ ARTE 2025

DESAFIO DA
FAMÍLIA DIGITAL

Para cada pessoa na tua família, completa pelo menos **uma destas tarefas:**

- Criar ou atualizar uma **palavra-passe segura;**
- Rever as **configurações de privacidade** nas redes sociais;
- Ativar a **autenticação de dois fatores** numa conta;
- Instalar ou atualizar um **antivírus** no telemóvel/computador;
- Ensinar os fatores a ter em conta para **detetar uma fraude**.

#FamiliaDigitalPT

PARTILHA O TEU PROGRESSO!

Tira uma foto ou faz um vídeo curto e usa a *hashtag* **#FamiliaDigitalPT** nas redes sociais para inspirar outras famílias!

Mais do que um conjunto de regras, a cibersegurança deve ser um hábito diário. Pequenas mudanças, como ativar a autenticação de dois fatores ou rever as configurações de privacidade, podem fazer uma grande diferença na proteção digital da família.

Não nos podemos esquecer que a segurança *online* é uma responsabilidade de todos e que, ao aplicarmos estes conhecimentos, garantimos uma presença *online* mais segura e responsável.

Agora que estás seguro e confiante na utilização da *Internet*, na próxima parte vê como esta ferramenta pode ser útil na realização de Serviços Públicos *online*.

© ARTE 2025