Módulo 2

Ciber-higiene e boas práticas de cibersegurança

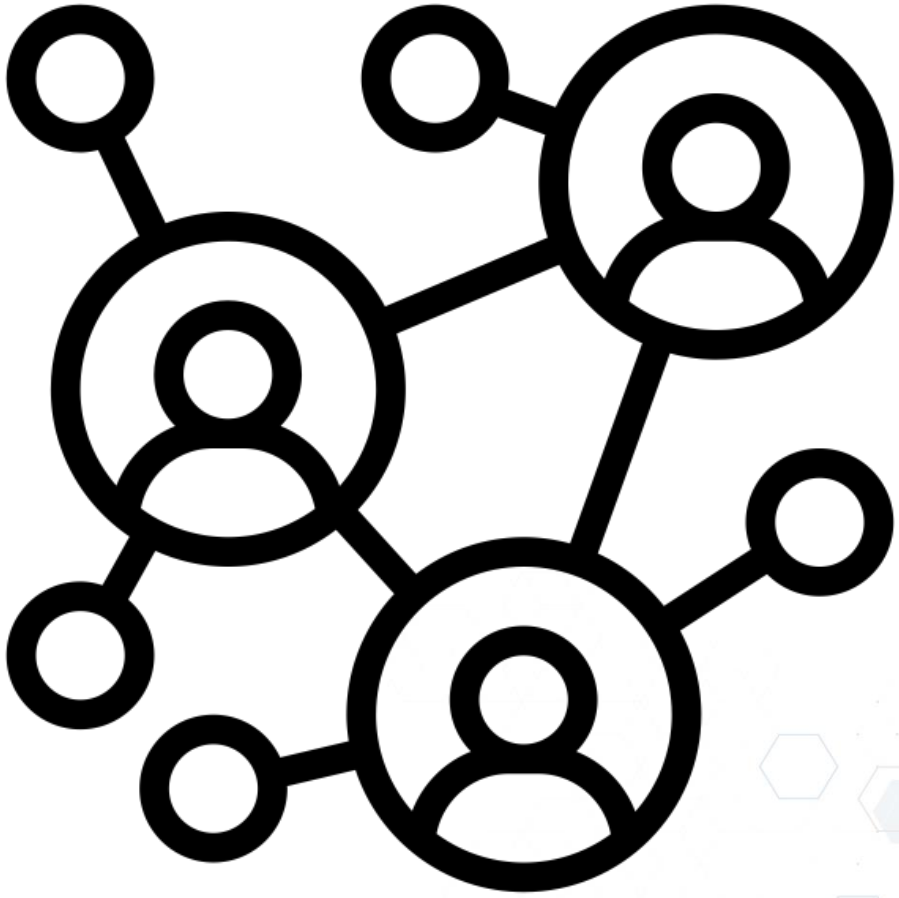
Conteúdo de sensibilização em ciber-higiene
Centro Nacional de Cibersegurança

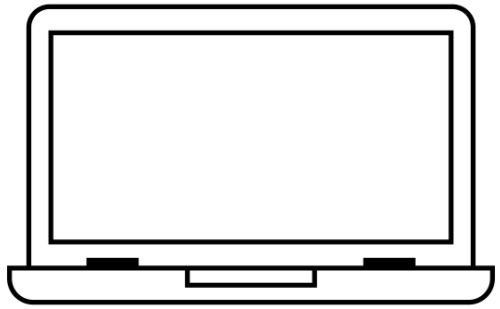
CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Índice

1. **Viver** em **rede**;
2. **Cuidados** de **ciber-higiene**;
3. **Pontos críticos**;
4. **Boas práticas:** *password*, *email*, redes sociais, *hardware* e navegação;
5. **Desafio** para **manual** de boas práticas.

Vivemos em rede

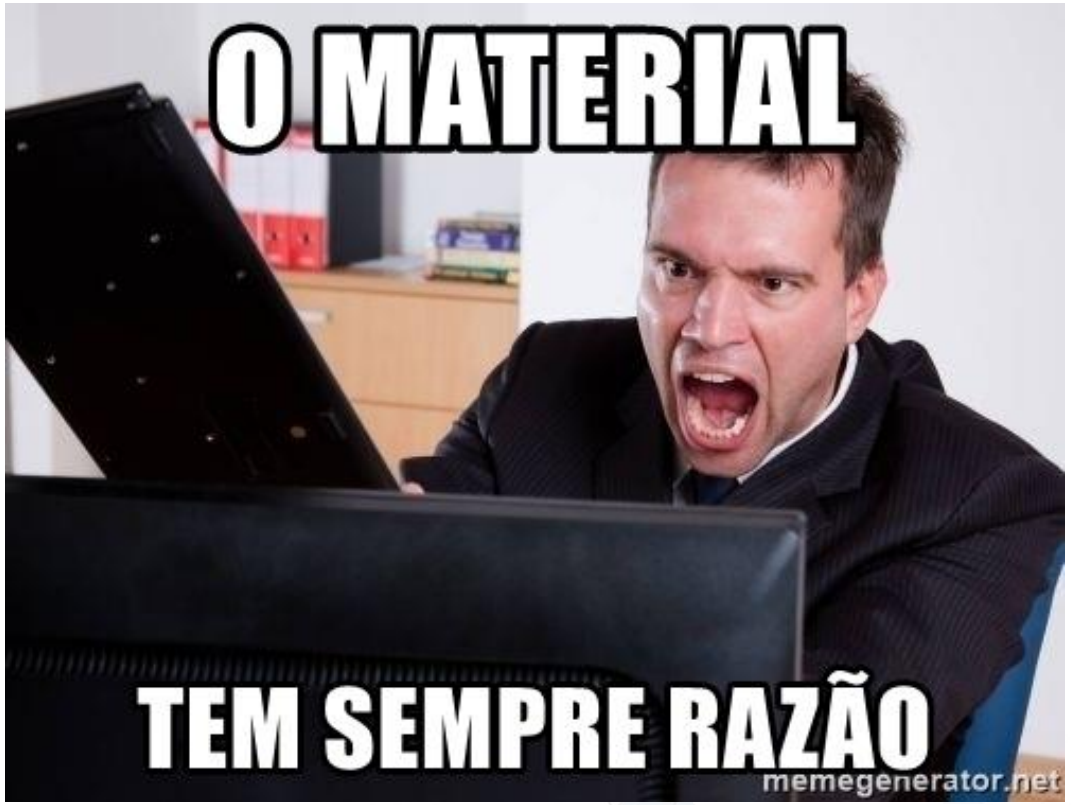




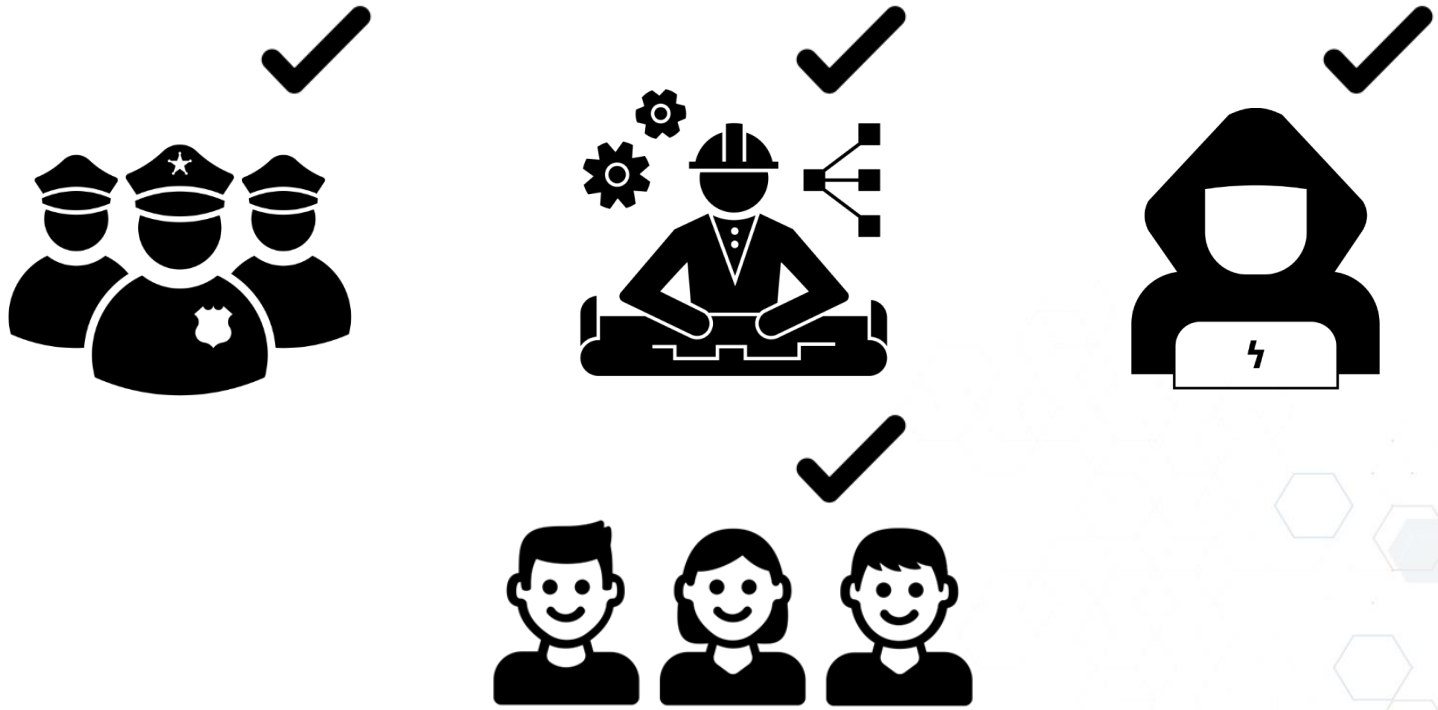
Esta rede é feita de tecnologia…

…e pessoas

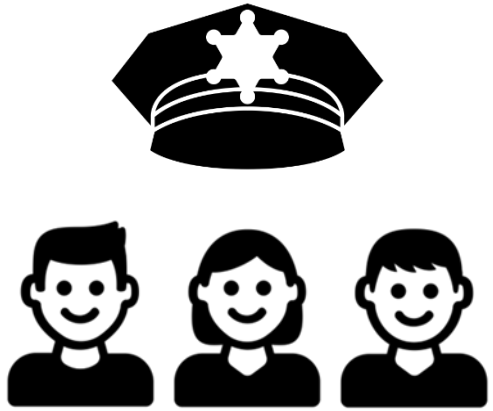
A RESPONSABILIDADE pela cibersegurança é das pessoas, não da tecnologia



…uma responsabilidade não apenas de forças de segurança, informáticos ou *hackers*, mas de todos…



Somos todos agentes de cibersegurança



Lava as mãos todos os dias?

Porquê?

Porque sabe que existem micro-organismos maliciosos.

Na **cibersegurança** também é preciso higiene,

Ciber-higiene.

Porquê?

Porque existem ciberameaças, também invisíveis.

Conhecemos as ameaças

É preciso saber o que fazer

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

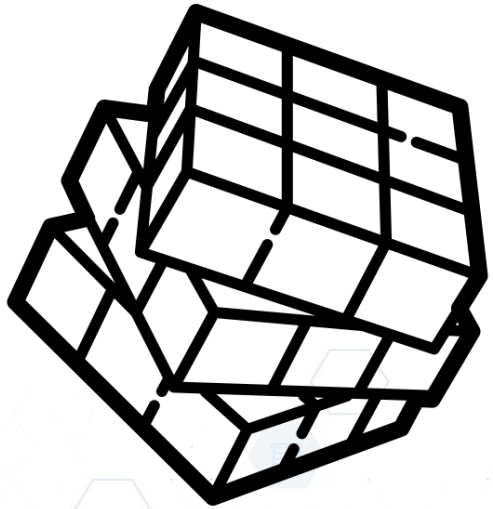
É preciso
AÇÃO

Como agir em casa, no trabalho ou em viagem nestes pontos críticos?

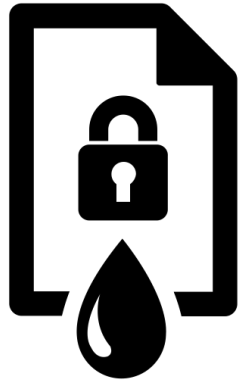
Password	*Email*	Redes sociais
Hardware	Navegação	

Password

Comportamento a estimular: **complicar**



A ***password*** é fundamental para **proteger** **informação pessoal e corporativa**.



O **comprometimento** da ***password*** pode estar envolvido no **roubo de identidade** e no ***data breach***.

Altera sempre a ***password*** por **defeito**?

Ver vídeo: https://www.youtube.com/watch?v=ijArYCsBnQ4

REGRA DAS 8 COMPLICAÇÕES

A ***password***	**deve** ser **secreta** e **sem termos óbvios**
	deve ser **complexa** e **memorizável – pode ser uma frase**
	deve ser **alterada** caso desconfie de comprometimento
	deve ser usada **numa só plataforma**
	deve, se possível, utilizar **autenticação de duplo fator**
	deve ser alterada sempre por **defeito**
	deve ser guardada em **gestor c/ base de dados cifrada**
	não deve ser guardada em ***browsers***

CNCS Centro Nacional de Cibersegurança PORTUGAL

Evitar uso de

Bernard Hermant

- **poucos** caracteres;
- **nome** do utilizador;
- **nomes próximos** do utilizador, como de localidade ou familiar;
- **termos fáceis** de digitar (ex.: qwerty, 123456, abcdefg);

Quanto mais fácil for uma *password*, **mais fácil será descobri-la**

manualmente ou com **força bruta** (*software* de tentativa-erro).

Como fazer uma ***password*** forte. **Utilizar**:

12+caracteres

letras **Ma**iúsculas

letras **mi**núsculas

4Lgarismos

C@racteres especiais

Não necessariamente por esta ordem.

Qual destas *passwords* **é a mais forte**?

E a mais **forte e fácil de memorizar**?

1. Go$1od#vi@j@r
2. abecedario
3. bobysantarem14
4. Ante$1u0ueEu
5. joao1979
6. 9A7ga%Mcu%li
7. D3;g&%$9sdf

Email

Comportamento a estimular: **desconfiar**

O ***email*** é a **porta aberta** que muitos **ataques** usam para **entrar** nos sistemas privados e/ou das empresas.

Filip Kominik

O que fazer, para **prevenir** e **reagir** a um ***ransomware***?

Ver vídeo: https://www.youtube.com/watch?v=ivqBfHe1ZwM

https://www.nomoreransom.org/

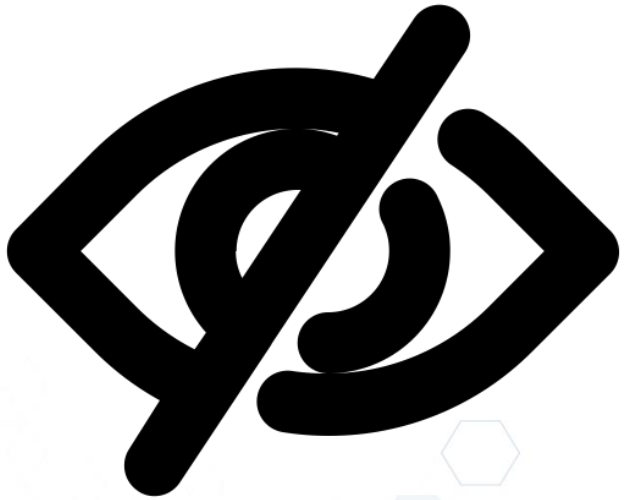
REGRA DAS 6 DESCONFIANÇAS

- Abrir apenas *emails* de origem conhecida;
- Caso abra, não clicar em nenhum *link* ou anexo;
- Verificar o endereço e a veracidade dos *emails* conhecidos;
- Não enviar informação sensível por *email* ;
- Identificar o *spam* para que o sistema faça uma seleção prévia;
- Terminar sempre a sessão quando finaliza a utilização do *email.*

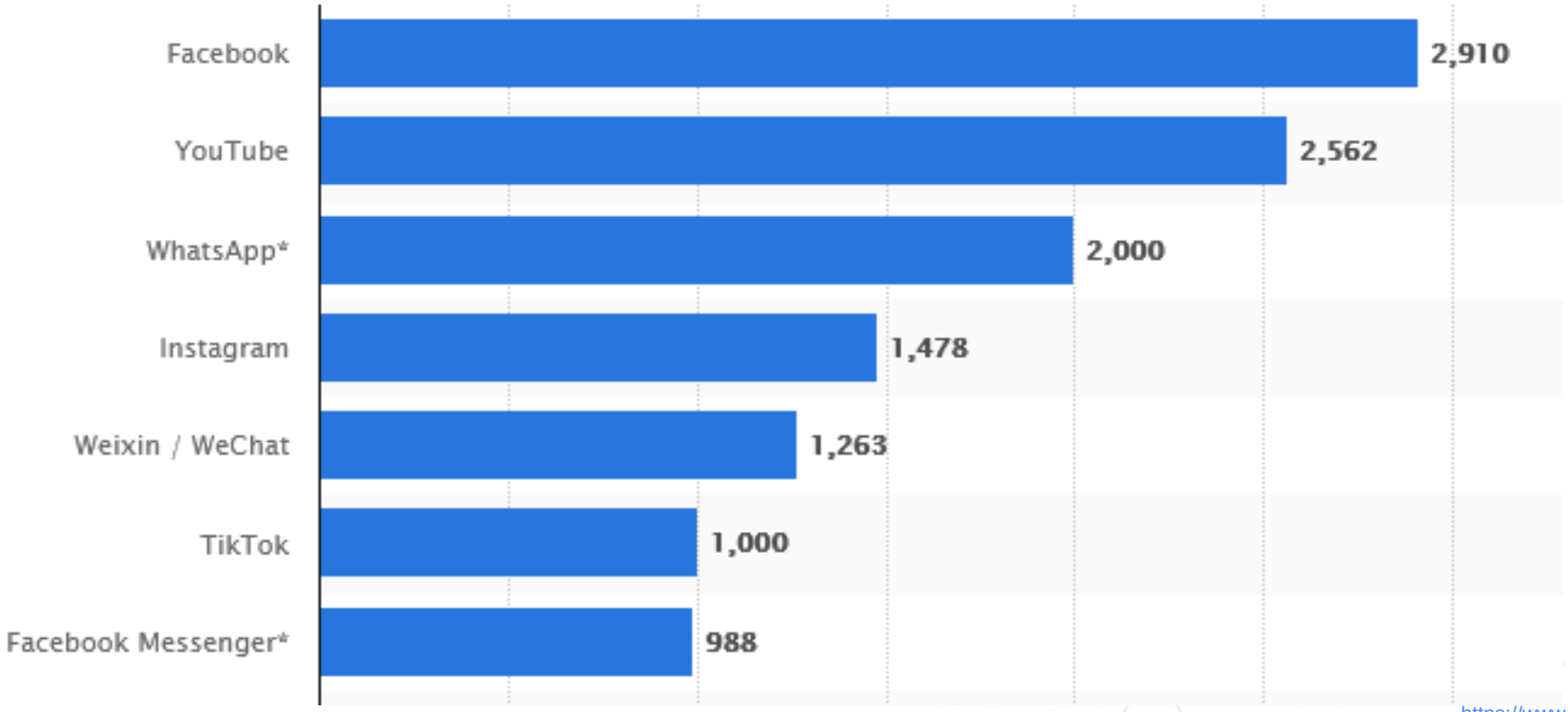
CNCS Centro Nacional de Cibersegurança PORTUGAL

Redes sociais

Comportamento a estimular: **preservar**



As **redes sociais** são onde as pessoas se expõem mais ao **furto de identidade** e à **engenharia social**.



https://www.statista.com

Nº de utilizadores por rede social no mundo, em janeiro de 2022 (milhões)

*pertencem ao Facebook

5 “A NÃO FAZERES” NAS REDES

Não aceitar conexões com **desconhecidos;**

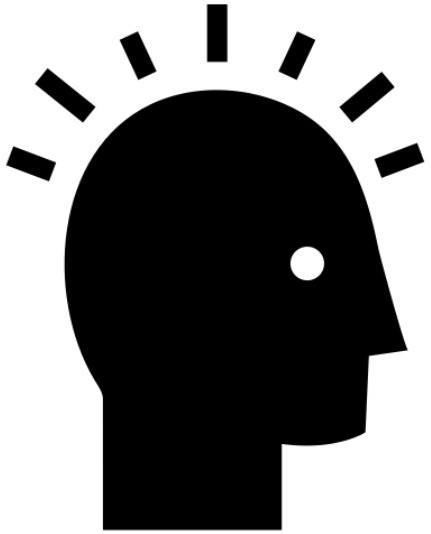
Não indicar telefone ou moradas no **perfil;**

Não **partilhar** locais, imagens de crianças ou dados sensíveis;

Não partilhar notícias **falsas** – verifique sempre a fonte;

Não clique em *posts* suspeitos – pode ser ***phishing.***

SE FIZER, TER CONSCIÊNCIA DE QUE…



Aquilo que **publica** **pode ser usado por terceiros;**

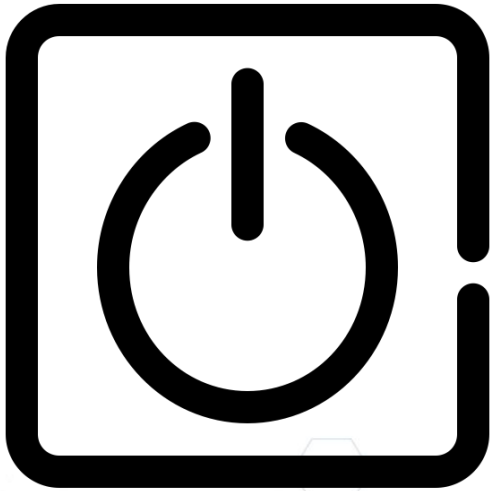
Por cada **gosto**, cria um **perfil utilizável na publicidade;**

Quando acede a plataformas usando **contas de redes sociais**, **partilha** os seus dados;

Ao colocar uma **imagem** nas redes sociais, **abdica dos direitos** sobre a mesma.

Hardware

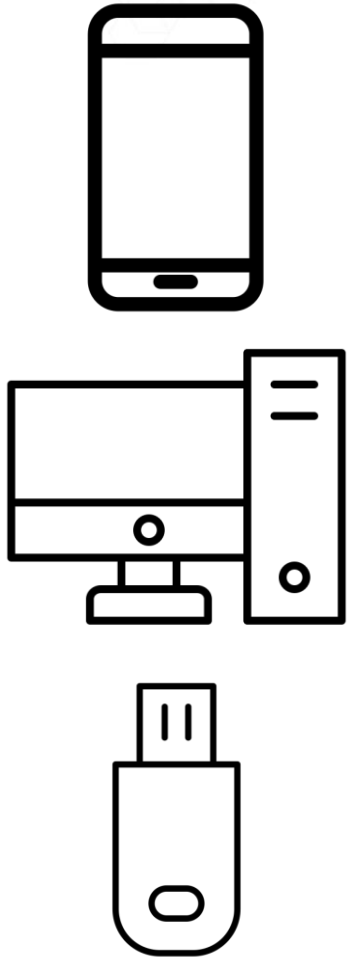
Comportamento a estimular: **bloquear**



O que faria se encontrasse uma *pen* **USB** na rua?

Ver vídeo: https://www.youtube.com/watch?v=ytEga1_14d0

HARDWARE CHECKLIST



Cobrir câmaras e desativar microfone ✓

Ativar **bloqueio** e não deixar dispositivos **desbloqueados** ✓

Usar ***passwords*** *e* limite de tentativas ✓

Evitar olhares indiscretos ✓

Em viagem, **identificar e vigiar** dispositivos ✓

Em **organizações**, **cifrar** informação e **proteger** perímetro ✓

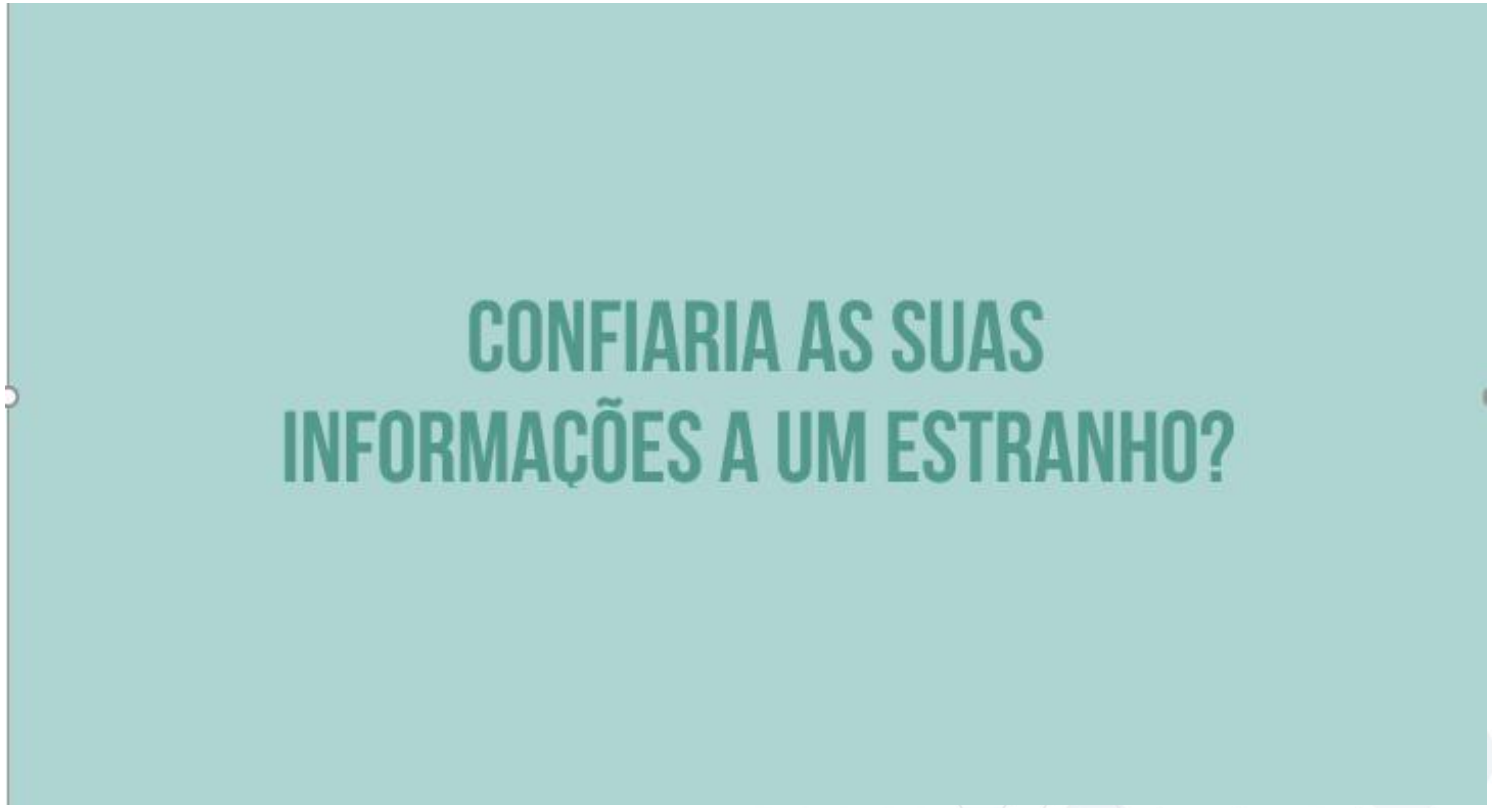
Proteger as portas USB ✓

Não usar *pen* USB desconhecida ✓

Navegar

Comportamento a estimular: **prevenir**

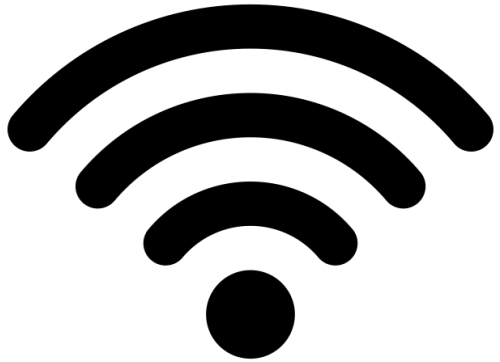
Usa **redes** ***Wi-fi*** **públicas**?



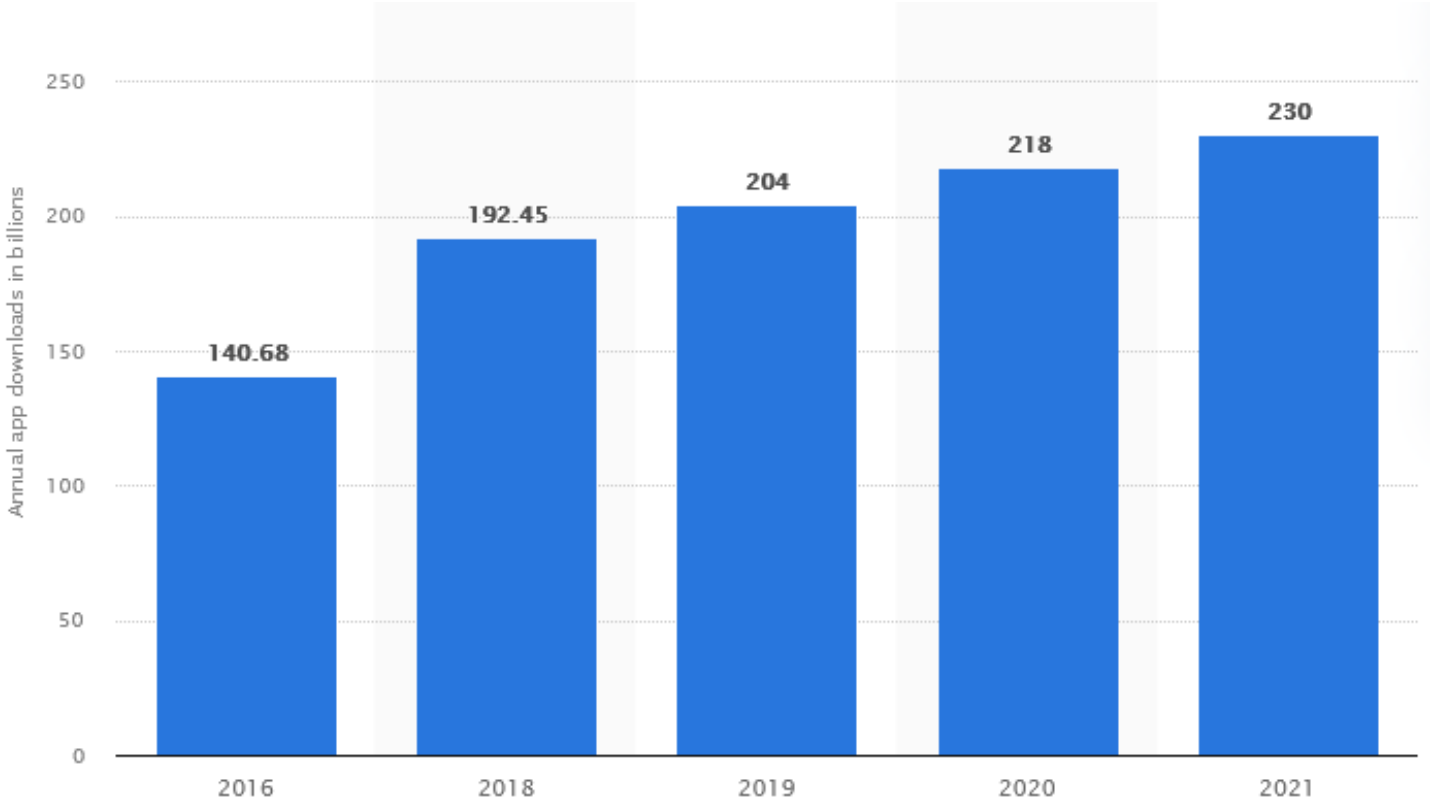
Ver vídeo: https://www.youtube.com/watch?v=SjecXAHjgKo

IMPORTANTE:

Através do ***Wi-Fi*** público é possível **aceder aos dados** dos dispositivos ligados.



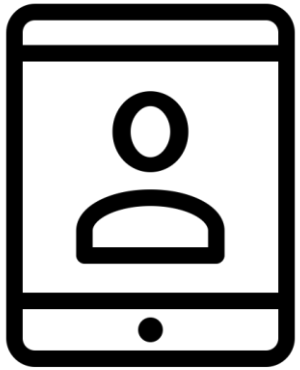
O mundo das **Ap**licações tem crescido, mas muitas são **maliciosas**.



https://www.statista.com

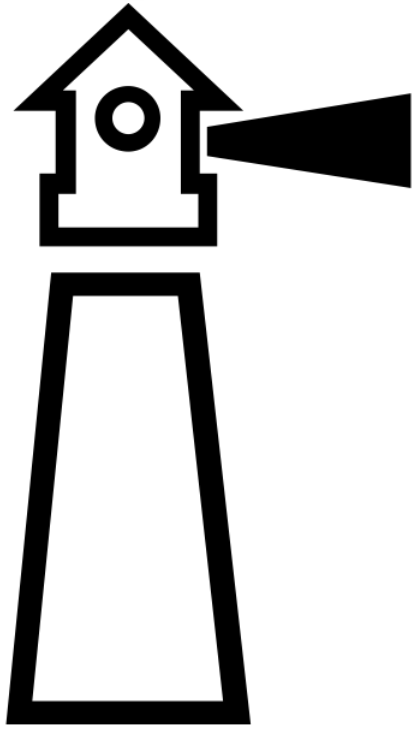
Quantidade de *downloads* de aplicações (em mil milhões)

As *APP*titudes certas



- Usar plataformas conhecidas para *download*
- Verificar as *reviews*, pontuação e escolhas do editor
- Não instalar *Apps* duvidosas
- Denunciar *Apps* fraudulentas
- Não autorizar o acesso a funcionalidades desnecessárias
- “Não há almoços grátis”

Avisos à navegação



Usar ***firewall;***

Considere que **endereços** com “**https**” são **mais seguros**;

E-Banking: confirmar **autorização** do BP ao Banco;

Compras *online*: desconfiar de **ofertas** demasiado boas, recolher **informação** sobre o vendedor, usar formas de **pagamento** seguras, guardar o **registo** das transações;

Acompanhar a navegação das **crianças.**

Em teletrabalho, tele…cuidado

Utilize apenas **dispositivos** **autorizados** pela usa organização;

Não os **partilhe** com ninguém – mesmo familiares ou amigos;

Faça ***backups*** regulares para um dispositivo externo;

Não partilhe informação **profissional** **nas redes sociais**.

E em videoconferências… cuidados redobrados

Restrinja o evento a **utilizadores autenticados**;

Crie uma ***password*** **de acesso único** a cada reunião;

Não autorize a gravação automática da reunião;

Não partilhe informação sensível;

Tenha um plano de **fundo neutro**;

Desligue a *webcam* e o microfone no final da reunião;

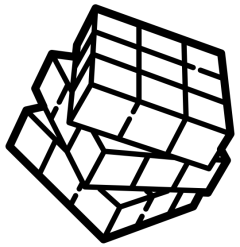
Opte pela utilização de **salas de espera**;

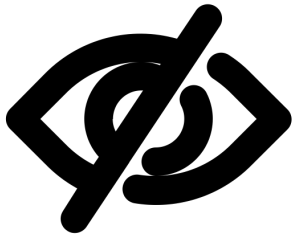
Na partilha do ***desktop***, **evite ficheiros expostos**.

Aviso extra:
mantenha o sistema e o antivírus atualizados

Revisão de comportamentos
ciberseguros

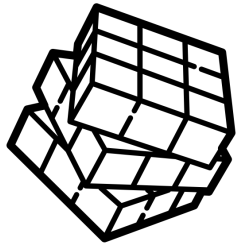
Password	*Email*	Redes sociais	*Hardware*	Navegar
Complicar	**Desconfiar**	**Preservar**	**Bloquear**	**Prevenir**

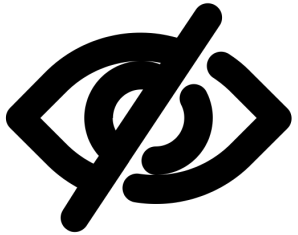




DESAFIO

Password	*Email*	Redes sociais	*Hardware*	Navegar
Complicar	**Desconfiar**	**Preservar**	**Bloquear**	**Prevenir**

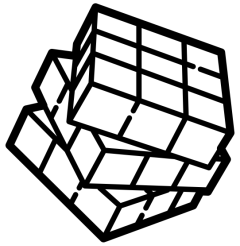
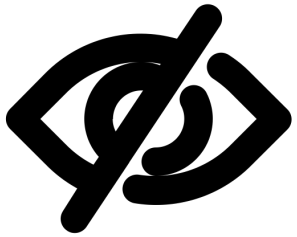




Indique DUAS BOAS PRÁTICAS para **CADA UM** destes domínios que pudesse fazer parte do MANUAL DE BOAS PRÁTICAS de cibersegurança da sua organização.

DESAFIO

2 cada

Password	*Email*	Redes sociais	*Hardware*	Navegar
Complicar	**Desconfiar**	**Preservar**	**Bloquear**	**Prevenir**
				

Ideias a reter

- A **cibersegurança** depende muito do **comportamento** humano;
- Ter **hábitos** diários de **ciber-higiene** é fundamental para a segurança;
- Existem alguns **pontos críticos**: a ***password***, o ***email***, as **redes sociais**, o ***hardware*** e a **navegação**;
- É importante ter **o comportamento certo** e as **práticas certas** em relação a cada um destes aspetos;
- As organizações ganham em ter **manuais** simples de **boas práticas** de cibersegurança.

Referências bibliográficas:

CNCS (2022) *Relatório Cibersegurança em Portugal – Riscos e Conflitos* 2022. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.
ENISA (2021) *ENISA Threat Landscape Report 2021*. ENISA.

Ícones Flaticon:
“Proibido” por Roundicons
“Aviso” por Freepik

Webgrafia:
https://dyn.cncs.gov.pt/pt/boaspraticas/
https://www.enisa.europa.eu
https://www.youtube.com/channel/UCxWGbCv8YC8a0ImlYebUblg
https://www.statista.com
https://www.todoscontam.pt/pt-PT/Principal/Paginas/Homepage.aspx

Ícones Noun Project (thenounproject.com):
“Rede” por Becris
“Laptop” por Adrian Syauqi Khairullah
“People” por Adrien Coquet
“Polícia” por Adric Rodríguez
“Engenheiro” por Laymic
“Hacker” por Zahroe
“Chapéu de polícia” por Iconika
“Lavar as Mãos” por Vicons
“Ação” por ahmad
“Trabalho” por Bakunetsu Kaito
“Casa” por Royal@design
“Viagem” por Iconstock
“Puzzle” por Maxim Kulikov
“Unlock” por Jems Mayor
“Data Leak” por Opher Aloni
“Estalar de dedos” por Artem Kovyazin
“Suspeito” por AlfredoCreates@flaticondesign.com
“Privacidade” por notplayink
“Consciência” por Yu luck
“Desconecta” por vigorn
“Smartphone” por Laura H
“Computador” por amy morgan
“Pen drive” por krishna
“Cinto de segurança” por Orin zuu
“Wifi” por i cons
“App” por Three Six Five
“Tablet user” por throwaway
“Farol” por yanti anis
“Mar” por Marko Fuček
“Teletrabalho” por Andrew McKinley
“Apresentação” por Gerald Wildmoser
“Degrau” por Adrien Coquet

Obrigado(a)

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL