Módulo 1

Ciber(in)segurança

Conteúdo de sensibilização em ciber-higiene
Centro Nacional de Cibersegurança

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Índice

1. **As nossas ilusões** e o receio necessário;
2. **Cibersegurança** e **cibercrime;**
3. **Principais ameaças** e casos;
4. **Exercício.**

Seremos ciberingénuos?

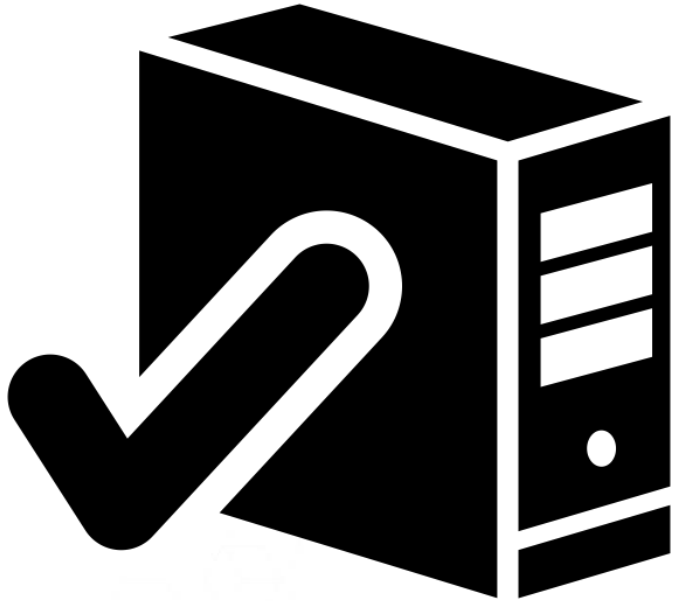
-4 ← -3 ← -2 ← -1 ← 0 → 1 → 2 → 3 → 4

Responda às perguntas ao longo da apresentação. Cada resposta certa soma 1 valor. Cada resposta errada subtrai 1 valor. O objetivo é ter pelo menos 4 valores.

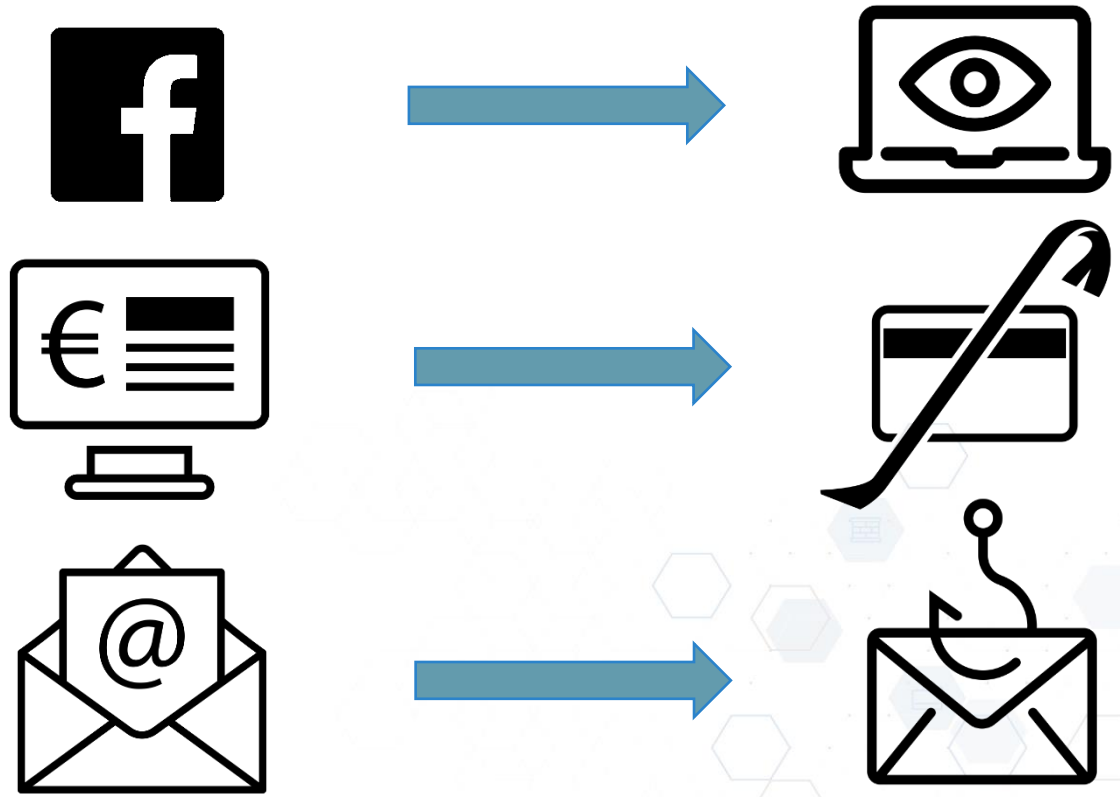
Objetivo: 4 valores

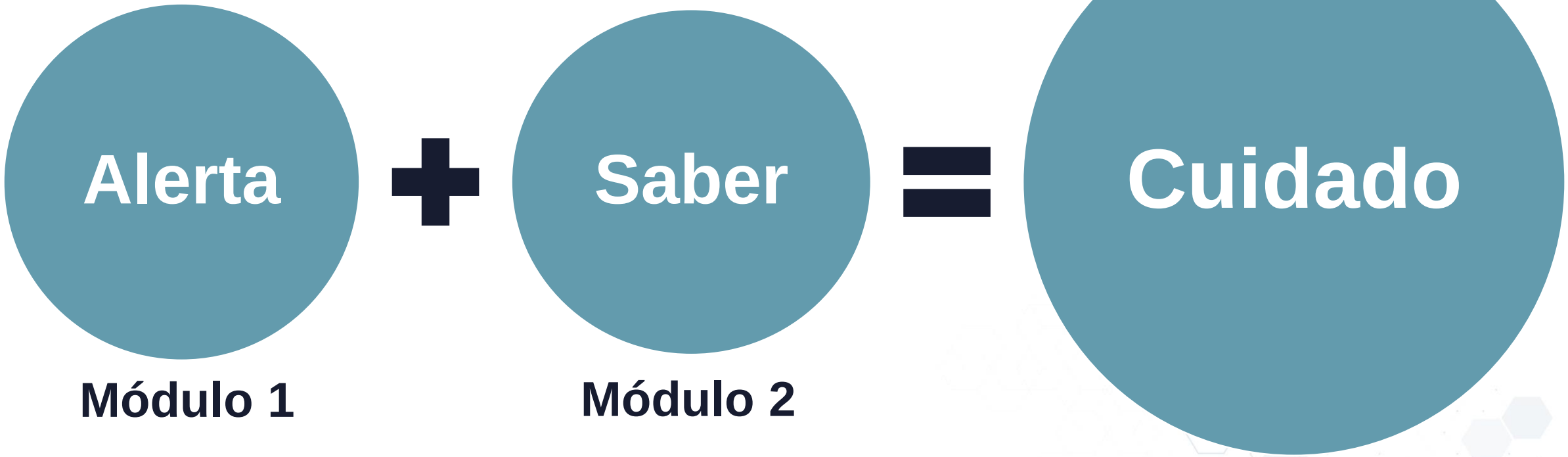
A nossa ilusão

Tecnologia **útil** igual a tecnologia **boa**



As **tecnologias digitais** implicam **novas ameaças**





Afirmação 1 – *verdadeira ou falsa?*

A cibersegurança diz respeito sobretudo aos cuidados de segurança que os responsáveis de informática devem ter.

Resposta certa 1 – *falsa*

A cibersegurança diz respeito **também aos utilizadores**. Uma parte importante dos incidentes resulta de falhas comportamentais.

Cibersegurança: práticas que visam manter o ciberespaço **seguro**

Números das ciberameaças em Portugal
em 2021 (1/2)

Número de incidentes registados pelo CERT.PT, entre 2015 e 2021*

* C/V: contabilizando as vulnerabilidades como incidentes (a partir de 2020).

Figura 2 | CERT.PT

+ 26% em 2021 relativamente a 2020.

O *phishing*/*smishing* (40% dos incidentes), a engenharia social (14%) e a distribuição de *malware* (13%) foram os tipos de incidentes mais registado pelo CERT.PT em 2021 (CERT.PT – Equipa de Resposta a Incidentes de Segurança Informática Nacional).

Consultar *Relatório Cibersegurança em Portugal, Riscos e Conflitos 2022* (CNCS, 2022) para esclarecimento de conceitos: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

(CNCS, 2022)

Números das ciberameaças em Portugal
em 2021 (2/2)

Percentagem de crimes relacionados com a informática em relação ao total de crimes registados pelas autoridades policiais, entre 2009 e 2021

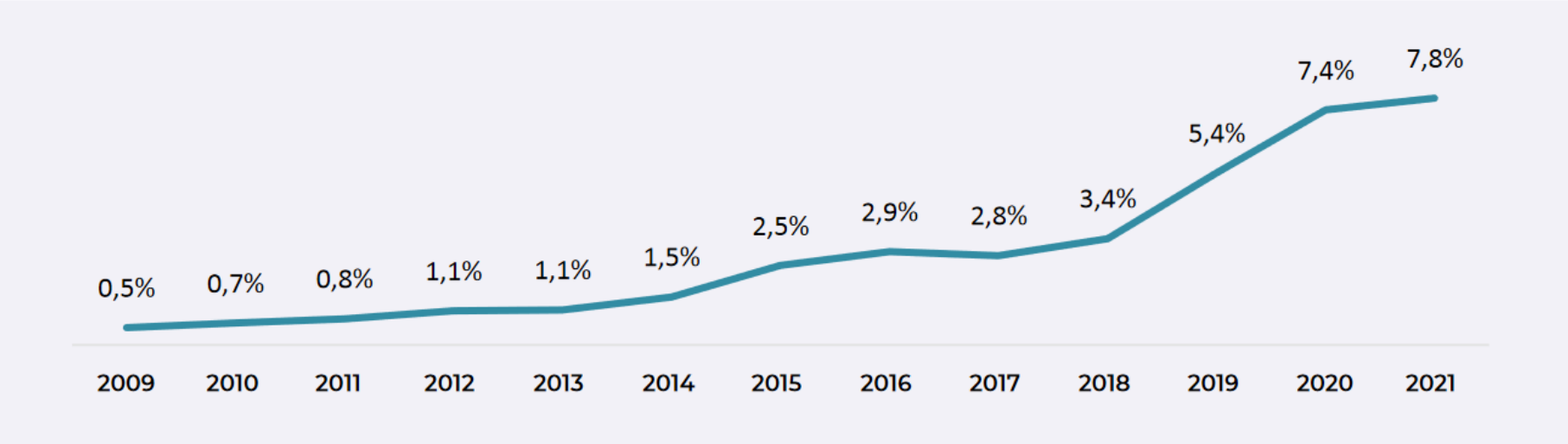


Figura 19 | DGPJ

A burla informática/comunicações é o crime relacionado com a informática com mais participações às autoridades em 2021 (91% do total), seguida do acesso/interceção ilegítimos (com 3%) (DGPJ).

Registos de crimes participados às autoridades.

Consultar *Relatório Cibersegurança em Portugal, Riscos e Conflitos 2022* (CNCS, 2022) para esclarecimento de conceitos: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

(CNCS, 2022)

Afirmação 2 – *verdadeira ou falsa?*

Para garantir a cibersegurança de uma organização, o mais importante não é a capacidade de resposta.

Resposta certa 2 – *verdadeira*

O momento em que o atacante recolhe e explora a informação disponível é o de maior vulnerabilidade do alvo. **A prevenção** é a melhor defesa.

Kill Chain

Preparação de ataque
De 1 a 3

1. **Reconhecimento**
2. ***Weaponisation***
3. **Distribuição/ Entrega**

Ataque
De 4 a 7

4. **Exploração**
5. **Instalação**
6. **Comando e controlo**
7. **Ação**

(ENISA, 2019)

Casos

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Afirmação 3 – *verdadeira ou falsa?*

O phishing é um tipo de SPAM que procura vender produtos em massa.

Resposta certa 3 – *falsa*

O phishing é uma técnica em que se manipula um utilizador com o fim de lhe captar dados e conduzi-lo a realizar ações contra os seus interesses.

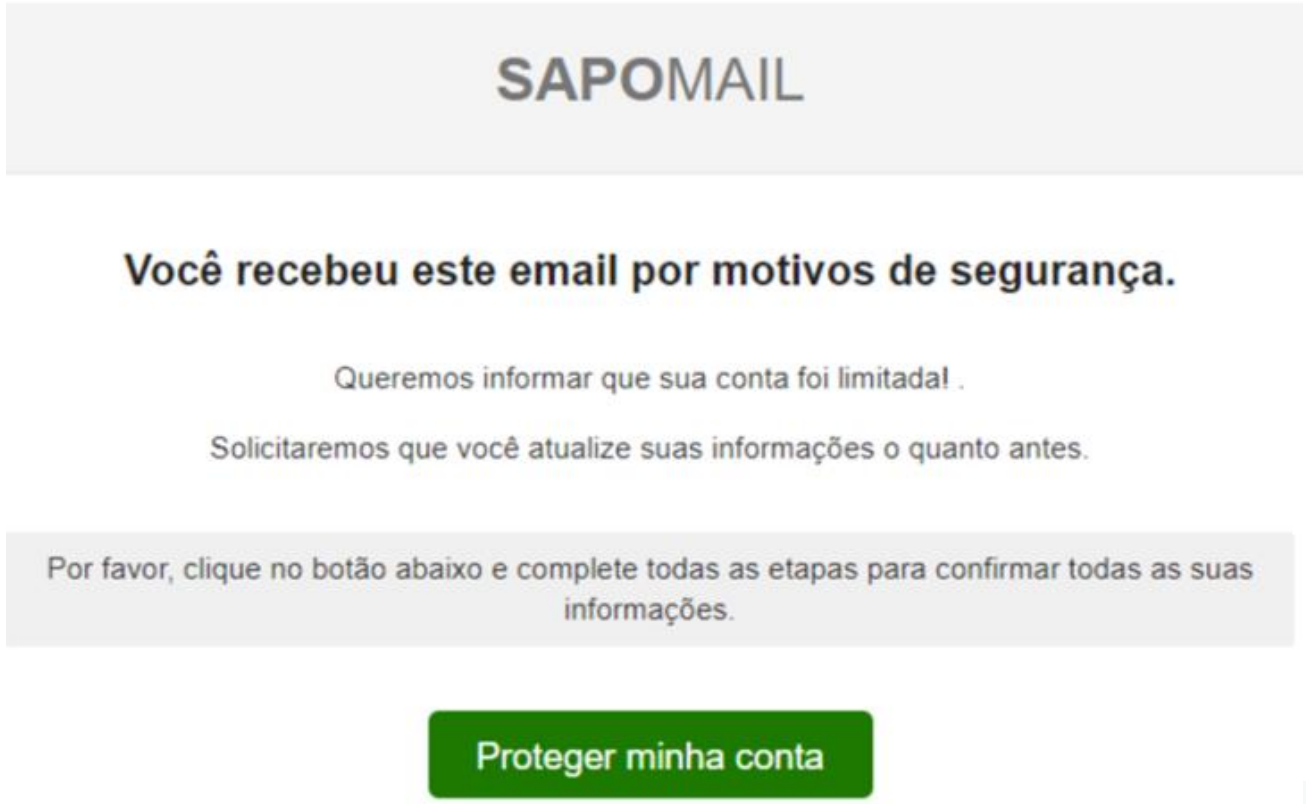
Phishing

Uso de **engenharia social** para que destinatários **"mordam um isco"**, abrindo um **anexo** malicioso, clicando num **URL** inseguro ou introduzindo ***passwords*** em páginas de aparência legítima.

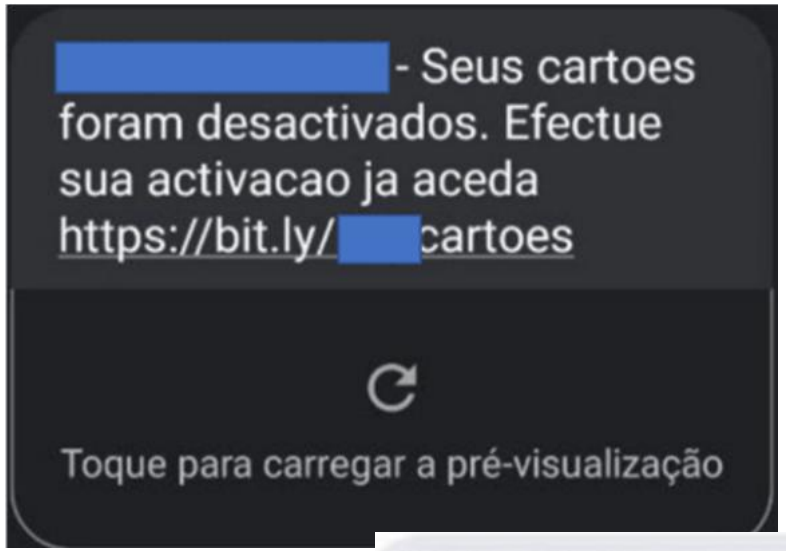
Kill chain – 1, 2 e 3

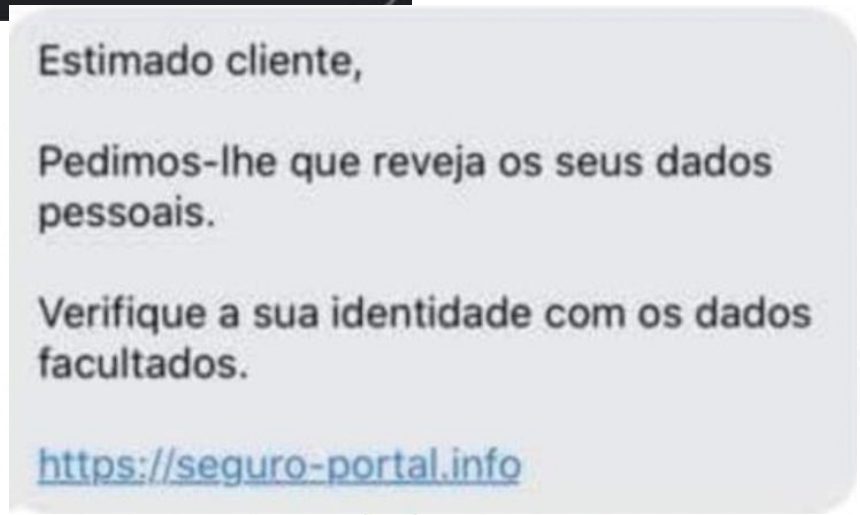
rawpixel

Em **2020**, *emails* em nome da **SAPO** simulavam que a conta tinha sido “limitada” e pediam que os utilizadores **atualizassem os seus dados**, clicando num *link* malicioso…

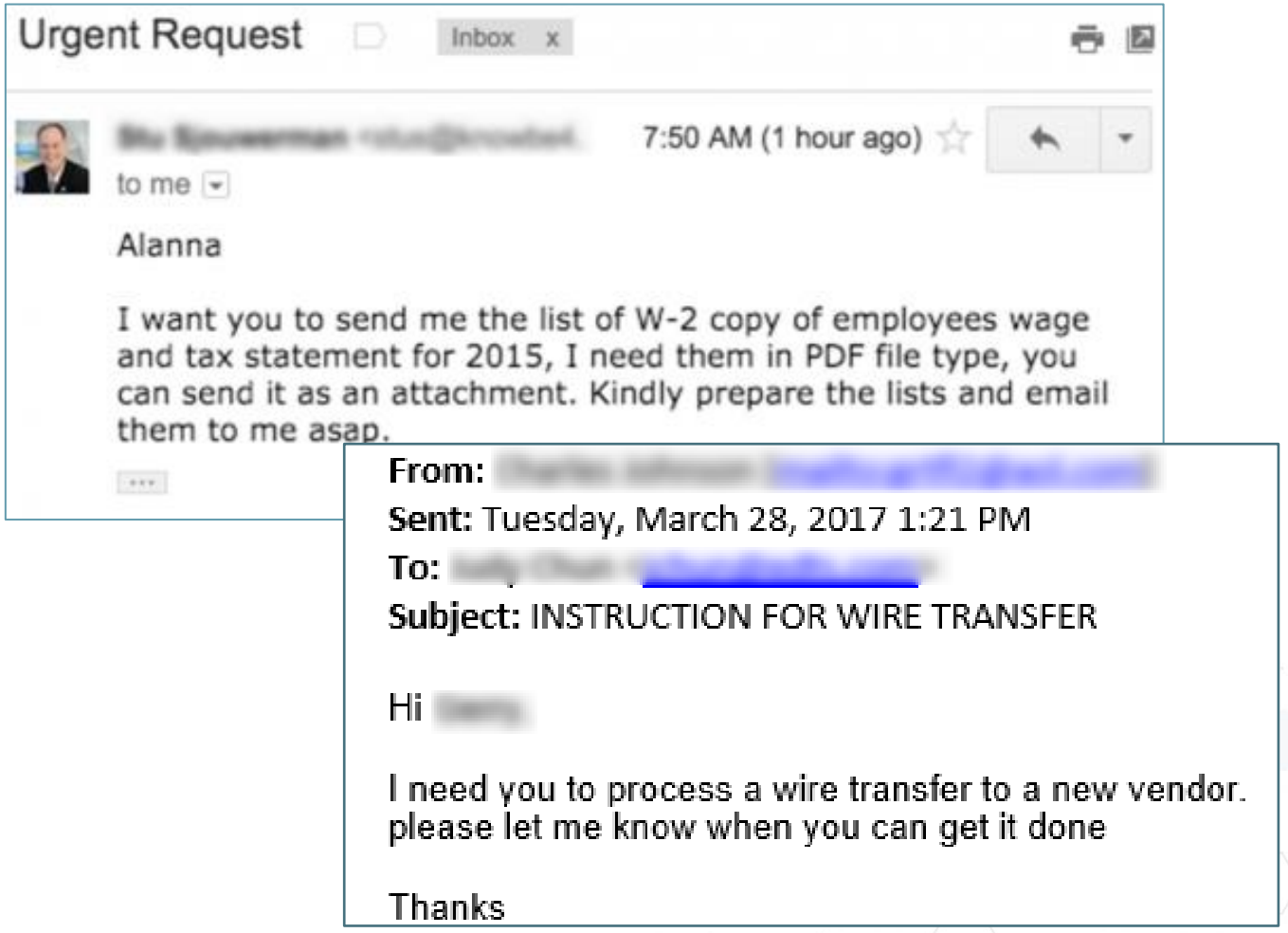


Cada vez mais são utilizadas **SMS** para este tipo de ataque, a que se chama ***smishing***. Este tipo de ação afeta frequentemente o setor da banca.





Por vezes, os atacantes **recolhem informação** sobre o alvo e usam isso para tornar a mensagem **mais credível** e o ataque mais **preciso** (*spear-phishing*).



Fonte das imagens: https://www.edts.com/edts-blog/15-examples-of-phishing-emails-from-2016-2017

Uma das **técnicas** mais usadas no ***Phishing*** é o ***typosquatting***: pequeno **erro tipográfico** que conduz a *website* malicioso.

Fonte de imagem:
https://www.sosdailynews.com/news.jspx?articleid=%20DF3E8D50A5F4A6E748E1DCE1C2F3EB81

MICORSOFT.COM

flytap.com

HOTMAIL.CM

Onde estão os **erros**?

Afirmação 4 – *verdadeira ou falsa?*

Ter unicamente pessoas conhecidas nas redes sociais é a melhor maneira de garantir que a minha informação privada se mantém privada.

Resposta certa 4 – *falsa*

É **sempre possível alguém aceder** a informação que colocamos *online*, quer através de perfis de terceiros, quer de fugas de dados.

Furto de identidade

Recolha de dados sobre indivíduos e uso dos mesmos para **simular a identidade** dessa pessoa. A técnica de **engenharia social** também é usada neste tipo de ataque.

Kill chain – 1, 2 e 3

CeruleanSon

O CEO de uma empresa de segurança na Suécia foi **declarado falido** porque um pirata informático pediu um **empréstimo** em seu nome com **dados roubados.**

Swedish CEO is declared bankrupt after identity theft

Alf Goransson

Independent.ie (12/02/2019)

Fonte de imagem: https://www.independent.ie/business/swedish-ceo-is-declared-bankrupt-after-identity-theft-35924277.html

As **redes sociais** são um **meio comum** para roubo de identidade.

Roubo de identidade aumenta de expressão nas redes sociais

Invadir um perfil de facebook para, em nome de outra pessoa, extorquir dinheiro, é um dos meios que preocupa a Judiciária

Iva Domingues vítima de usurpação de identidade nas redes sociais

CATARINA FURTADO VÍTIMA DE PIRATARIA NA INTERNET: "NÃO SOU EU!"

A apresentadora lançou o alerta nas redes sociais.

tvmais

01 DE AGOSTO DE 2018

Conceição Lino mostra LADO NEGRO do Facebook: é impressionante»

A Rede, reportagem que a SIC exibe esta terça-feira, revela casos reais de portugueses que foram enganados e manipulados através das redes sociais. Conceição Lino revela pormenores.

Fontes das imagens, por ordem:

https://www.dn.pt/sociedade/interior/roubo-de-identidade-aumenta-de-expressao-nas-redes-sociais-5007344.html

http://tvmais.sapo.pt/celebridades/2018-08-01-Catarina-Furtado-vitima-de-pirataria-na-internet-Nao-sou-eu

https://www.jn.pt/pessoas/in/interior/iva-domingues-vitima-de-usurpacao-de-identidade-nas-redes-sociais-8777659.html

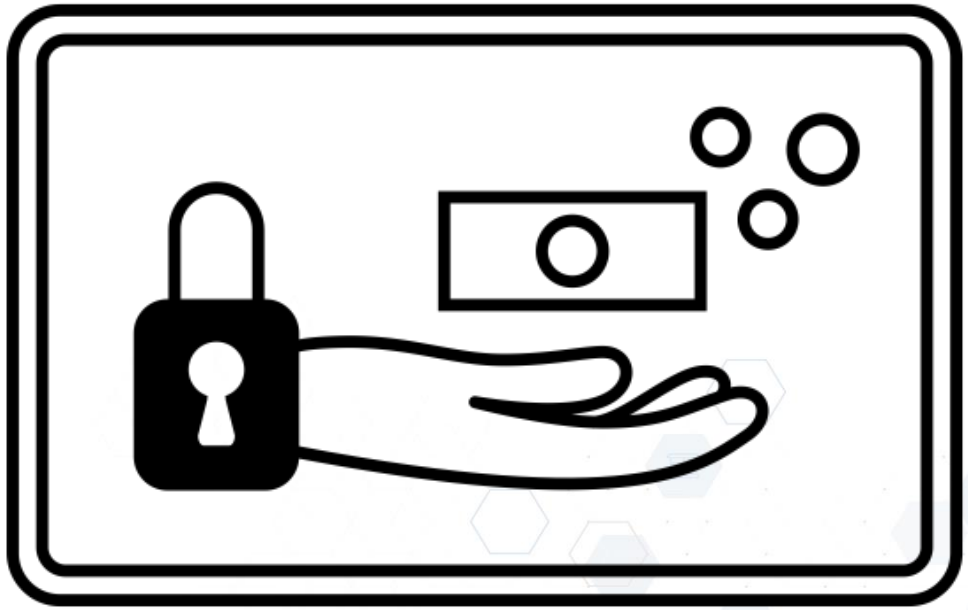
https://www.tv7dias.pt/conceicao-lino-mostra-lado-negro-do-facebook

CNCS Centro Nacional de Cibersegurança PORTUGAL

Ransomware

Os atacantes acedem a arquivos e/ou vários dispositivos e **bloqueiam o acesso** aos mesmos. Para devolver esse acesso, o atacante **exige um resgate** em criptomoedas.

Kill chain – 5, 6 e 7



O **Wannacry** foi um *ransomware* que, em 2017, aproveitou uma falha no Windows para se espalhar por cerca de **230 mil** computadores (Bitsight).

Fonte da imagem:
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

Diário de Notícias

12 AGO 2018

O vírus informático que paralisou os hospitais CUF

O grupo foi atacado a 3 de agosto e os computadores de serviço ficaram bloqueados. Empresa responsável garante que não houve dados comprometidos

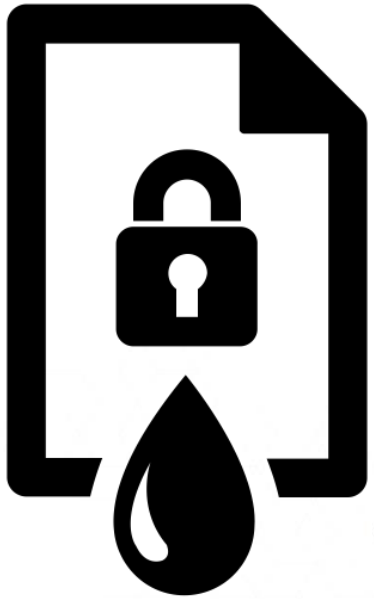
Em 2018, um ***ransomware*** (**SamSam**) afetou os **hospitais CUF**. Neste caso não foi necessário pagar resgate. Mas os atacantes entraram no sistema meses antes do ataque. (DN)

Fonte da imagem: https://www.dn.pt/edicao-do-dia/12-ago-2018/o-virus-informatico-que-paralisou-os-hospitais-cuf-9709054.html

Data breach

Kill chain – de 1 a 7

Exfiltração de **dados** considerados sensíveis ou privados de uma organização e/ou indivíduos.



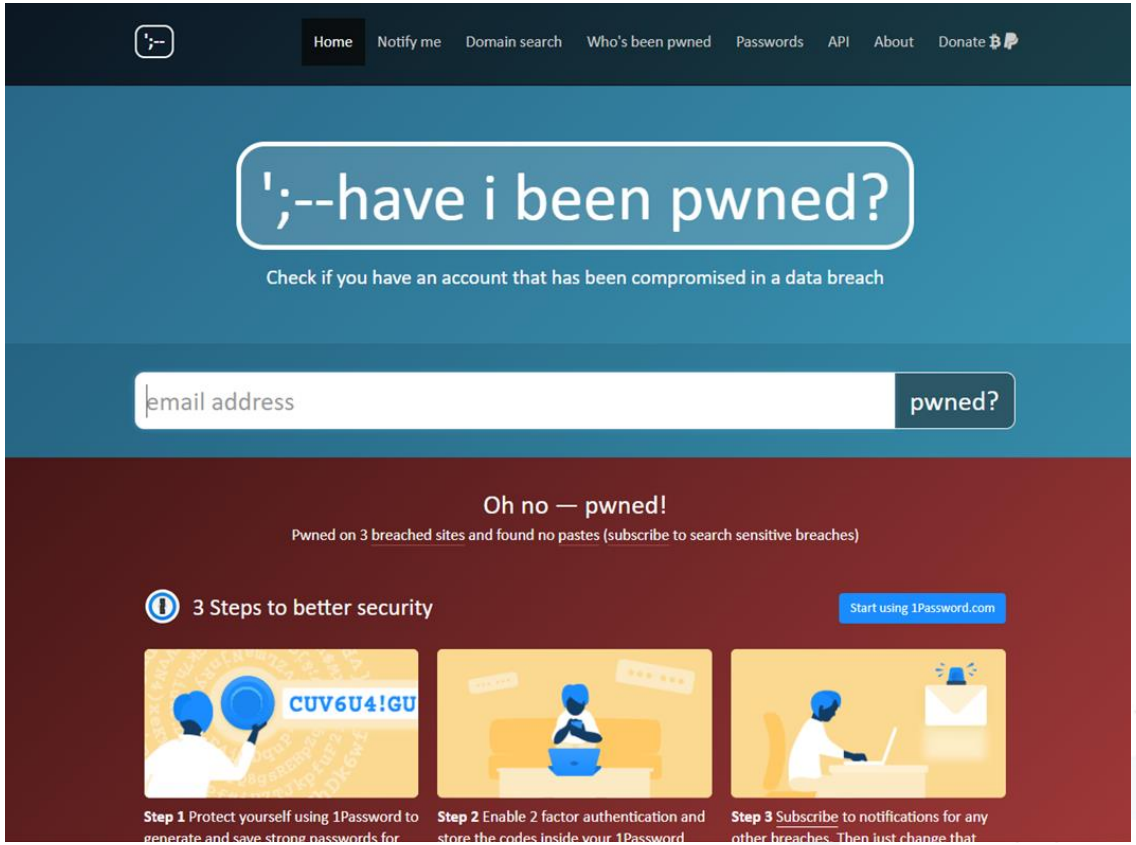
Afirmação 5 – *verdadeira ou falsa?*

As minhas *passwords* com certeza nunca foram comprometidas.

Resposta certa 5 – *?*

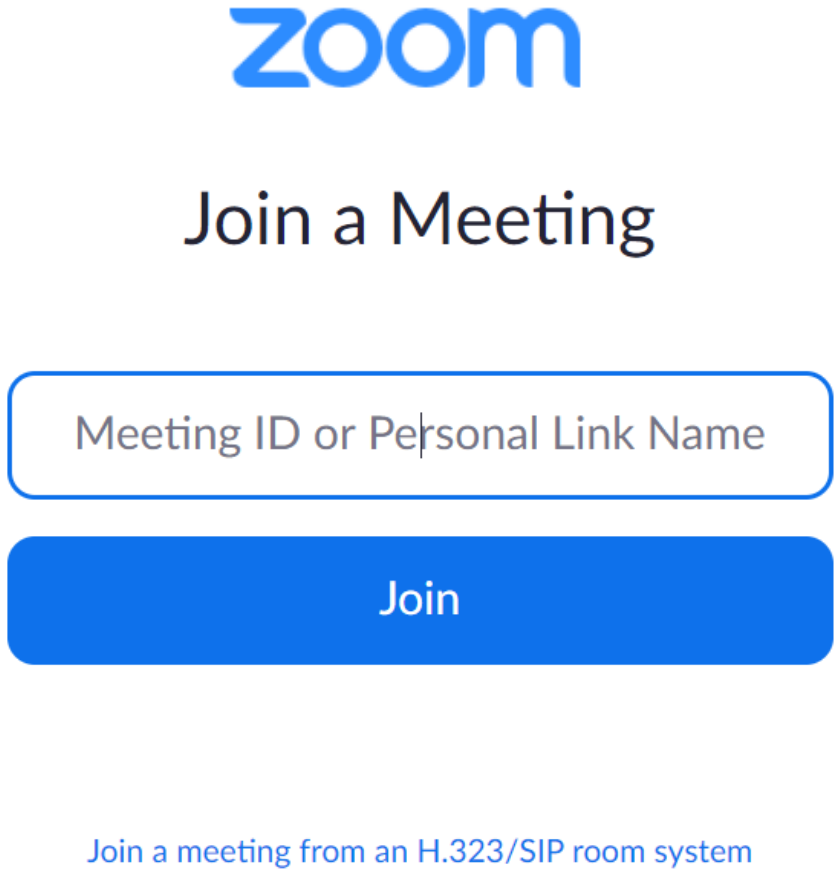
Verifiquem no próximo *slide*.

Troy Hunt, um informático, construiu um *website* onde é possível **verificar** se em algum momento uma conta com o nosso *email* **foi comprometida**.



https://haveibeenpwned.com

Em 2020, durante o período de confinamento devido à pandemia de Covid-19, milhares de ***passwords*** **de contas e reuniões de Zoom foram colocadas à venda** na Dark Web – e em alguns casos foram oferecidas.



Fonte da imagem: https://zoom.us/join

Afirmação 6 – *verdadeira ou falsa?*

Qualquer um pode fazer um ciberataque.

Resposta certa 6 – *verdadeira*

Existem aplicações gratuitas ou baratas que permitem a qualquer um descobrir *passwords* ou outra informação sensível.

Principais agentes das ciberameaças

- Cibercrimimosos
- Atores Estatais
- Hacktivistas
- Ameaça Interna
- *Cyber-offender*

Consultar *Relatório Cibersegurança em Portugal, Riscos e Conflitos 2022* (CNCS, 2022) para esclarecimento de conceitos: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

(CNCS, 2022)

Quantos pontos de Ciberingenuidade?

- 4: não percebo nada disto
  0: estou nos mínimos
+4: sou o maior

Objetivo: 4 valores

Ideias **a reter**

- O ciberespaço apresenta **muitas** **ameaças**;
- A **cibersegurança** procura **proteger-nos** dessas ameaças;
- O cibercrime tem muitos **custos** para as **organizações**;
- Os ciberatacantes **reconhecem** e depois **exploram** o alvo;
- Os ataques mais comuns **aproveitam-se** da **informação** que disponibilizamos ou de ligações maliciosas a que acedemos.

No próximo módulo…

Saberemos o que fazer perante estas ameaças e quais as **boas práticas** a adotar.

Referências bibliográficas:

CNCS (2022) *Relatório Cibersegurança em Portugal – Riscos e Conflitos 2022*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.
ENISA (2019) *ENISA Threat Landscape Report 2018 15 Top Cyber-Threats and Trends*. ENISA.

Ícones Noun Project (thenounproject.com):
“Computador” por Yazmin Alanis
“Privacidade” por Gregos Cresnar
“Banco” por Alfredo Creates
“Email” por Rivercon
“Phishing” por Tomas Knopp
“Cibersegurança1” por Krisada
“Cibersegurança2” por Made
“Ransomware” por Emilegraphics
“Data Leak” por Opher Aloni

Obrigado(a)

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL