Privacidade de dados e cibersegurança: Reforçar a confiança digital nas empresas

Francisco Peixoto

Centro Nacional de Cibersegurança

Sobre mim

Consultor no Centro Nacional de Cibersegurança, com vasta experiência em resposta a incidentes, análise forense e de implementação de sistemas de gestão de segurança da informação. Ex-CISO da Universidade do Porto, com um forte envolvimento em associações culturais e juvenis.

Certificações: CISSP, CHFI, TRANSITS I, CISO, CC, ISO 27001 Lead Implementer

Índice

"É um pássaro? É um avião? Não, é um incidente!"

O que é um incidente de cibersegurança?

- Muitas vezes é um **cibercrime**, mas pode não o ser…
- Muitas vezes é **intencional**, mas pode não o ser…
- Muitas vezes tem **causa humana**, mas pode não a ter…

Definição de incidente de cibersegurança

"Um evento com um **EFEITO ADVERSO** real na **segurança** das redes e dos sistemas de informação" (Taxonomia RNCSIRTs)

Pode ter diversas **CAUSAS** raiz

Pode ter **IMPACTO relevante/substancial**

a) **Falha** de sistema;
b) Fenómeno **natural**;
c) **Erro** humano;
d) Ataque **malicioso**;
e) Falha no fornecimento de bens ou serviços por **terceiro**.

(Decreto-Lei n.º 65/2021)

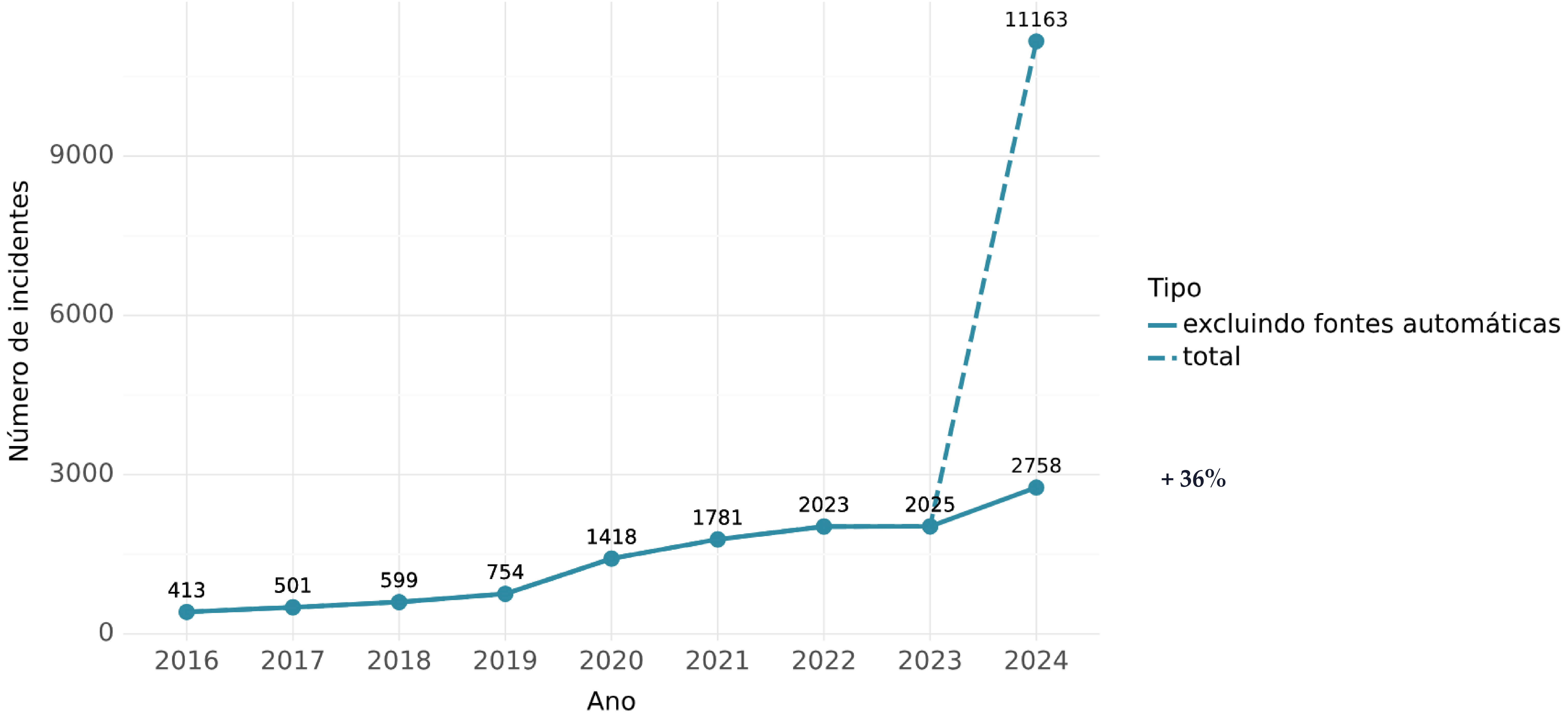
Por isso é que o caso do apagão de dia 28 de abril pode implicar incidentes de cibersegurança, embora sem causa maliciosa…

Mas o ***phishing*** em nome de um Banco ou o ***ransomware*** a uma Câmara Municipal também são incidentes de cibersegurança, claro…

→ Os ataques maliciosos têm origens mais dinâmicas e mais imprevisíveis.

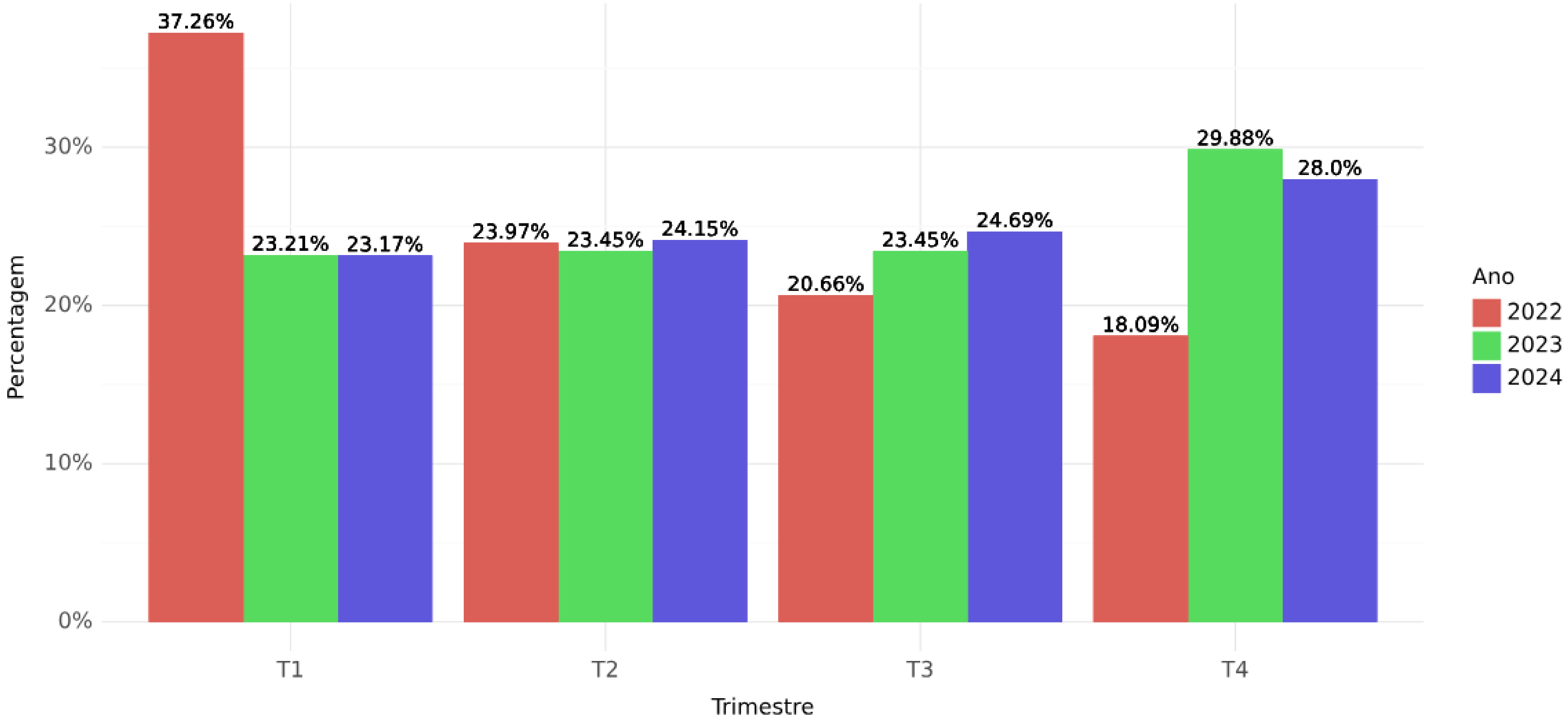
Conhecimento Situacional

Contínuo aumento do n.º de incidentes



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

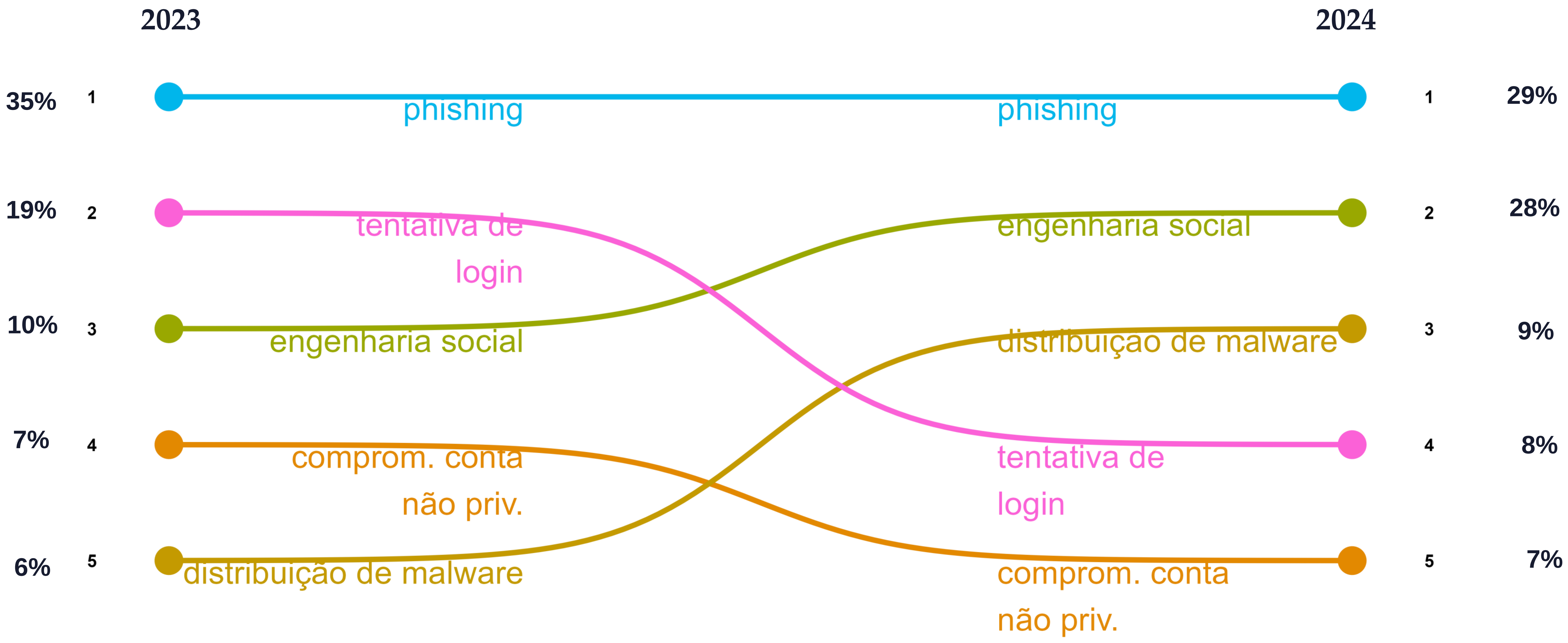
O último trimestre tem maior relevância, mas…



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

CNCS Centro Nacional de Cibersegurança PORTUGAL

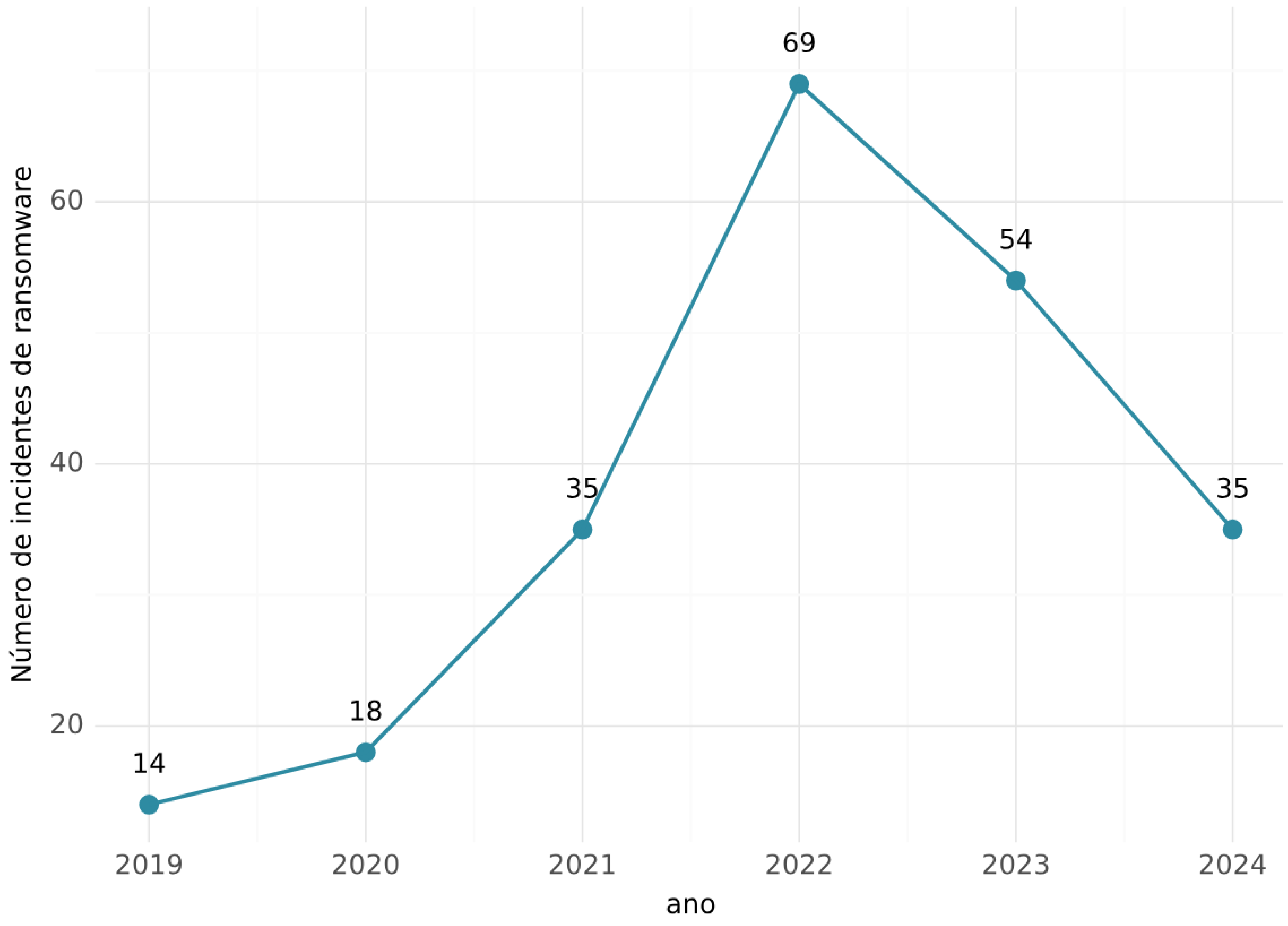
O fator humano é muito importante



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

CNCS Centro Nacional de Cibersegurança PORTUGAL

Quantidade não explica tudo… o impacto…

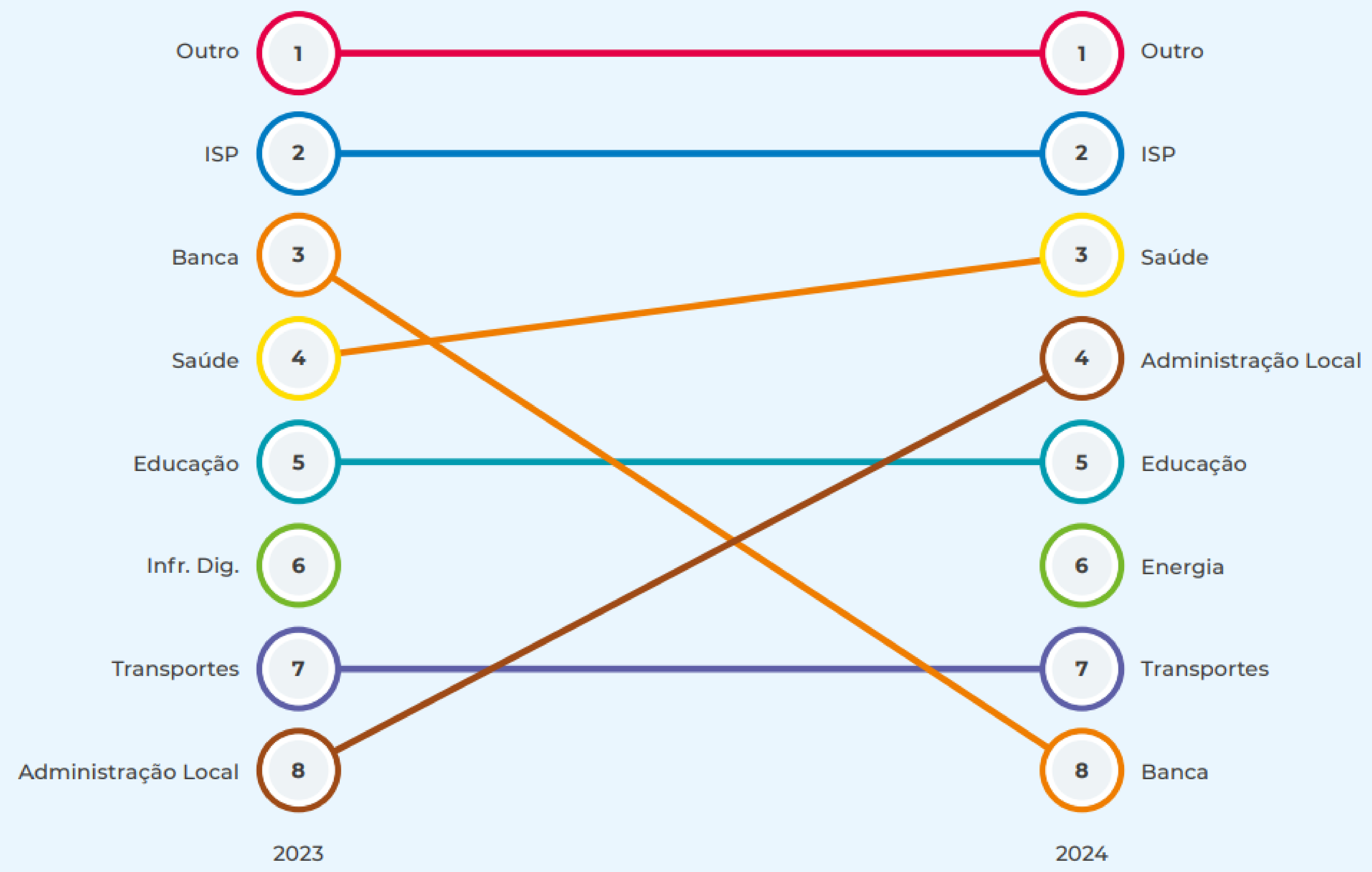


ano do ataque à AMA

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

CNCS Centro Nacional de Cibersegurança PORTUGAL

Setores mais afetados



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

CNCS Centro Nacional de Cibersegurança PORTUGAL

Comprometimento Email Profissional (Engenharia Social) (e.g.)

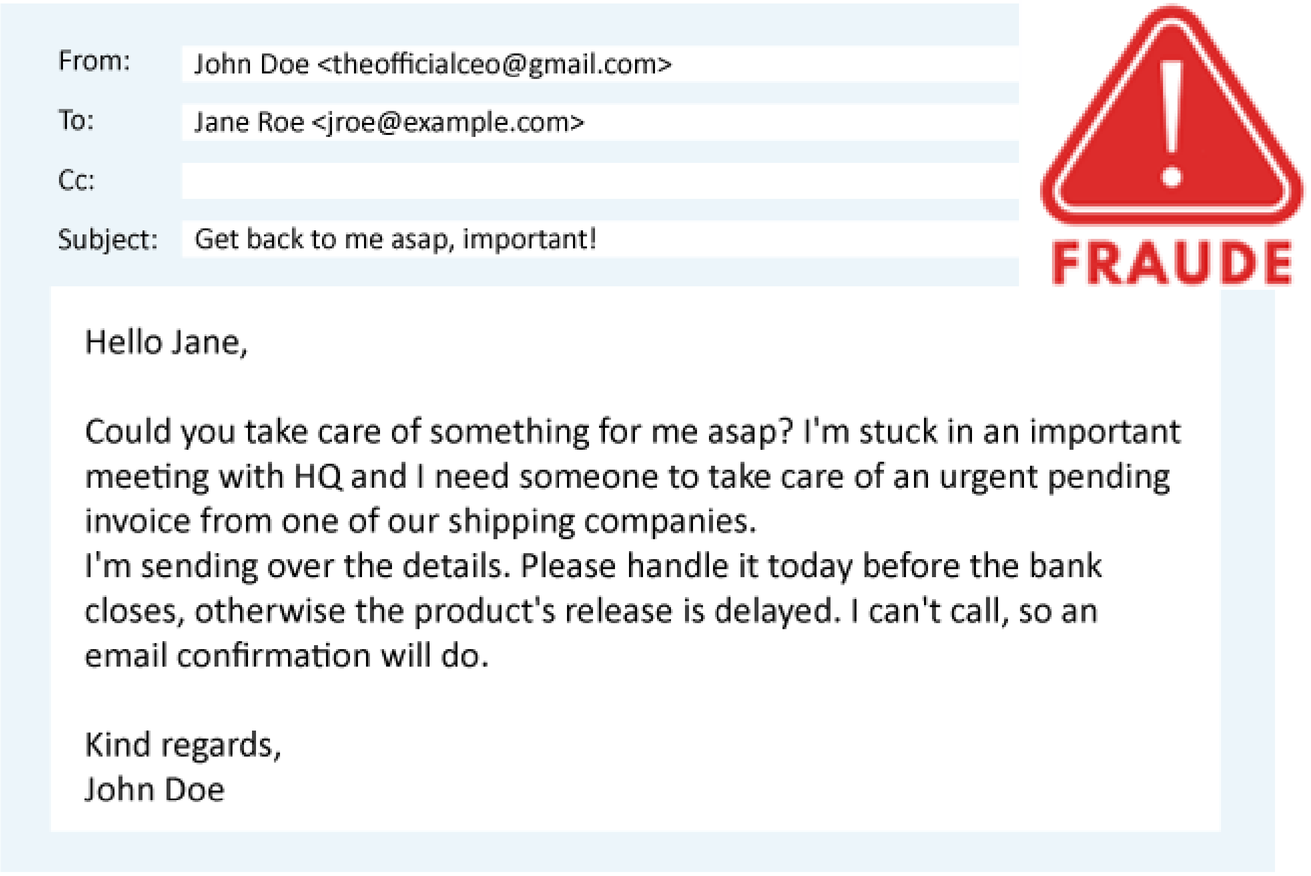
Recolha de credenciais → **Comprometimento** de conta de fornecedor → Aplicação de **pretexto** na troca de *emails* → **Pedido de pagamento** para novo IBAN

Outros *modi operandi*

Personificação de domínio de entidade fornecedora

Personificação de **empregado** para alterar destino do vencimento

Personificação de **superior hierárquico**


From: John Doe <theofficialceo@gmail.com>
To: Jane Roe <jroe@example.com>
Cc:
Subject: Get back to me asap, important!

Hello Jane,

Could you take care of something for me asap? I'm stuck in an important meeting with HQ and I need someone to take care of an urgent pending invoice from one of our shipping companies.
I'm sending over the details. Please handle it today before the bank closes, otherwise the product's release is delayed. I can't call, so an email confirmation will do.

Kind regards,
John Doe

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Imagem: https://vpnoverview.com/pt/seguranca-online/crime-cibernetico/reconhecer-fraude-do-ceo/

Ransomware (e.g.)

Recolha de credenciais → **Comprometimento** de contas → Escalar para privilégios de **administrador** → **Instalação** de *malware*

***Pretexto** aplicado antes*

Outros *modi operandi*

Exploração de **vulnerabilidades**

Comprometimento de **acesso remoto** (RDP)

Emails com anexos e *links* com *malware*

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Imagem: https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259

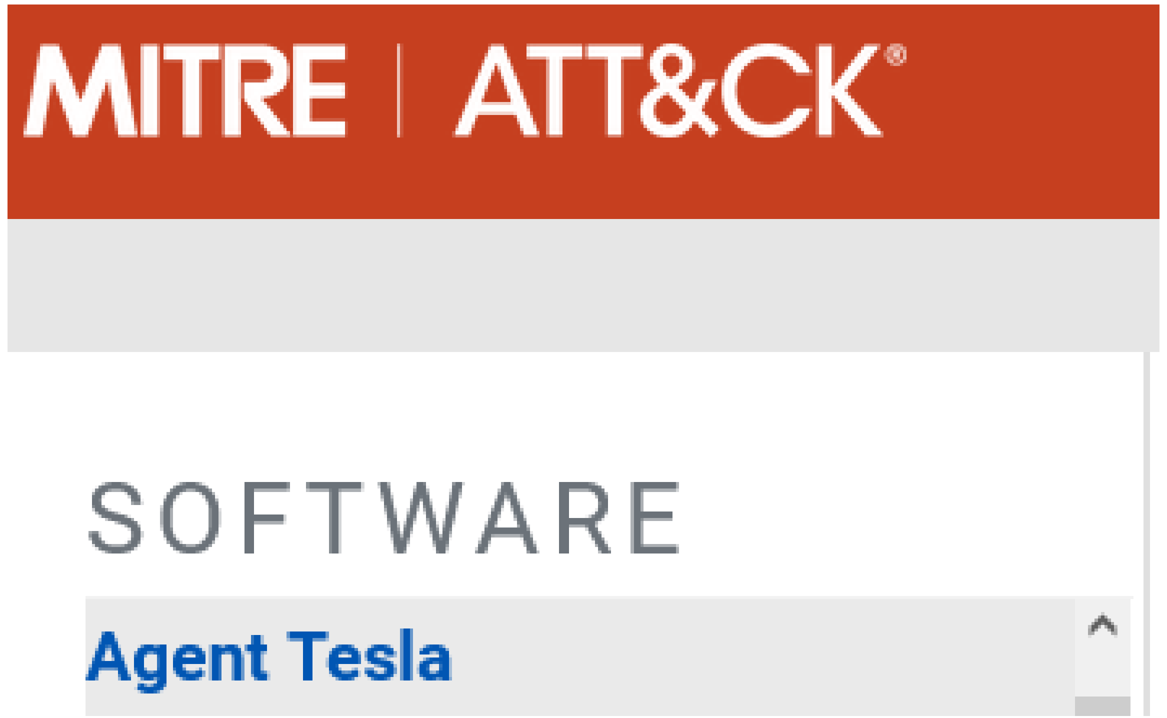
CNCS Centro Nacional de Cibersegurança PORTUGAL

Infostealers (e.g.)

Spearphishing (pretexto sofisticado) → **Clique** em anexo → **Instalação** de *malware* → **Recolha** de informação

Outros *modi operandi*

PENS USB infetadas
Malvertising
Website maliciosos



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Imagem: https://attack.mitre.org/software/S0331/

Perceção de risco elevado

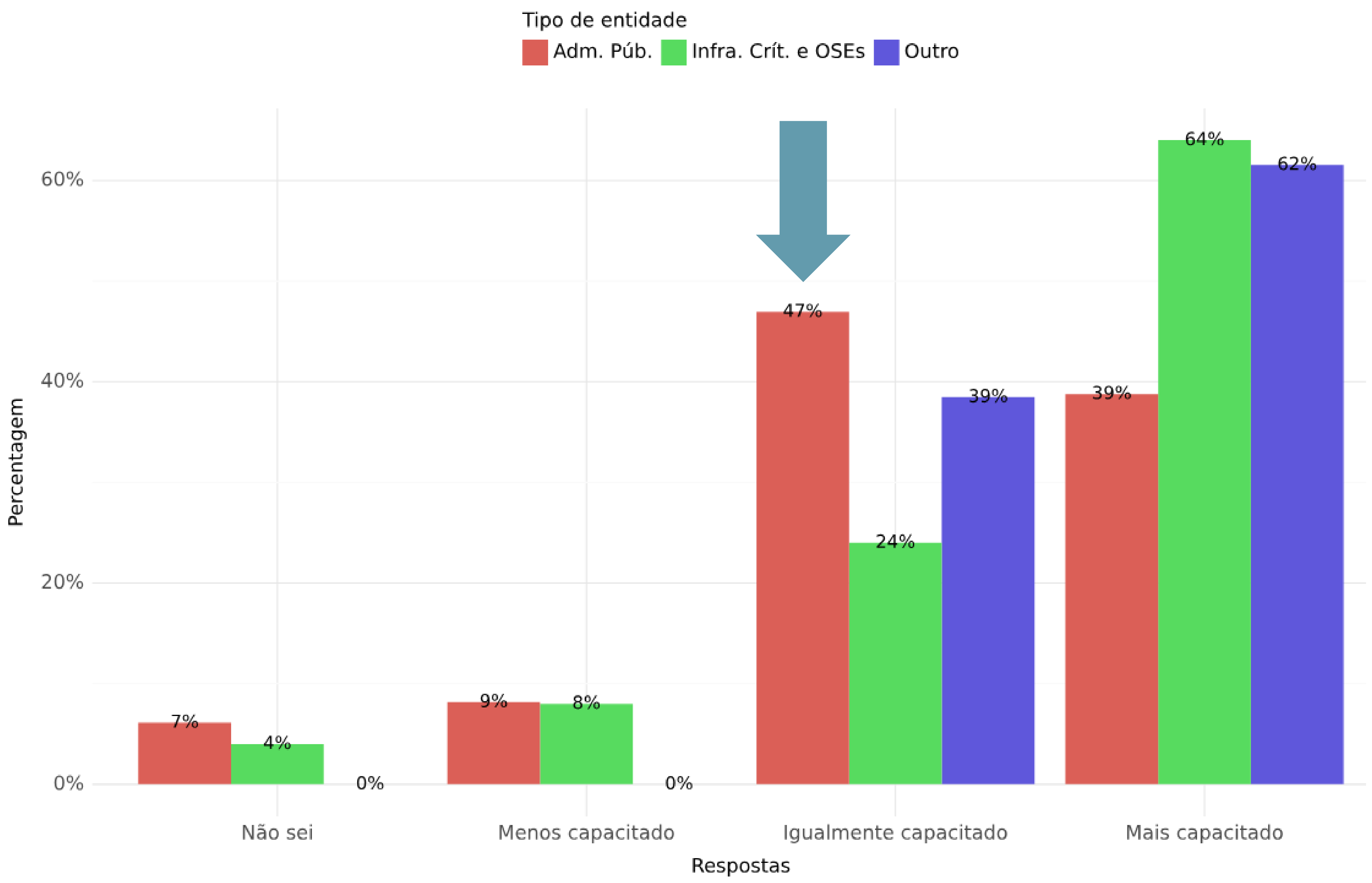
A **perceção de risco** no cibersegurança **continua alta** em 2024 e 2025 e é influenciada pelo contexto geopolítico.

O risco aumentou em **2024** para **92%** dos inquiridos e em **2025** para **90%**

Esta **perceção** é influenciada pelo contexto geopolítico para **95%.**

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Perceção de maior capacitação (menos na AP)



Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Definição de vulnerabilidade

"**Fraqueza** de um ativo ou controlo que **pode ser explorada** por uma ou mais ameaças"

(ISO/IEC 27000)

CAPACIDADES

Condições sociotécnicas vulneráveis (PT)

SUPERFÍCIE DE ATAQUE

- **Elevada Exposição** a plataformas críticas para a cibersegurança:

  email (88%PT e 86%UE);
  chamadas de vídeos *online* (82%PT e 75%UE);
  redes sociais (79%PT e 65%);
  mensagens instantâneas (93%PT e 82%UE).

(Eurostat, 2023)

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Condições sociotécnicas vulneráveis (PT)

RECURSOS HUMANOS

- As Empresas consideram que é **difícil contratar** pessoal de cibersegurança (16%PT e 12%UE).

- **Baixa taxa de profissionais certificados em cibersegurança** (1 em cada 10PT e 2 em cada 10UE).

(Eurobarómtero, 2024)

- Elevada **necessidade de pessoal** de cibersegurança na Administração Pública (75% dos organismos).

(DGEEC, 2024)

Dados CERT.PT/Observatório: https://www.cncs.gov.pt/pt/observatorio/

Condições sociotécnicas vulneráveis (PT)

BOAS PRÁTICAS CRÍTICAS

- **Baixo uso de MFA** na Administração Pública (49% dos organismos).

(DGEEC, 2024)

- **Menor uso de autenticação MFA** nas empresas (28%PT e 31%UE).

(Eurostat, 2023)

Condições sociotécnicas vulneráveis (PT)

SENSIBILIZAÇÃO

- Usam-se **poucos meios de massa** para as ações de sensibilização (1%) e estas **não são suficientemente avaliadas** quanto ao impacto (30%).

  (Inquérito CNCS, 2024)

- **Baixo número de empresas que ofereceram ações de sensibilização ou formação** aos colaboradores no último ano (26%PT e 35%UE).

  (Eurobarometro, 2024)

Notas importantes

- É importante ter uma **visão holística da cibersegurança**, compreender as diversas causas para um incidente e as várias dimensões da capacitação;

- O número de **incidentes** continua a aumentar, bem como a sofisticação das causas e dos *modi operandi* – não olhar só para a quantidade (e.g. BEC, Ransomware, Infostealers)…

- Os **Recursos Humanos** continuam a ser um dos aspetos mais vulneráveis, quer como alvos, quer quanto à quantidade de especialistas disponíveis.

- **Novos requisitos legais** de cibersegurança **abrangem mais organizações do setor privado do que antes.**

Sente-se preparada/o?

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

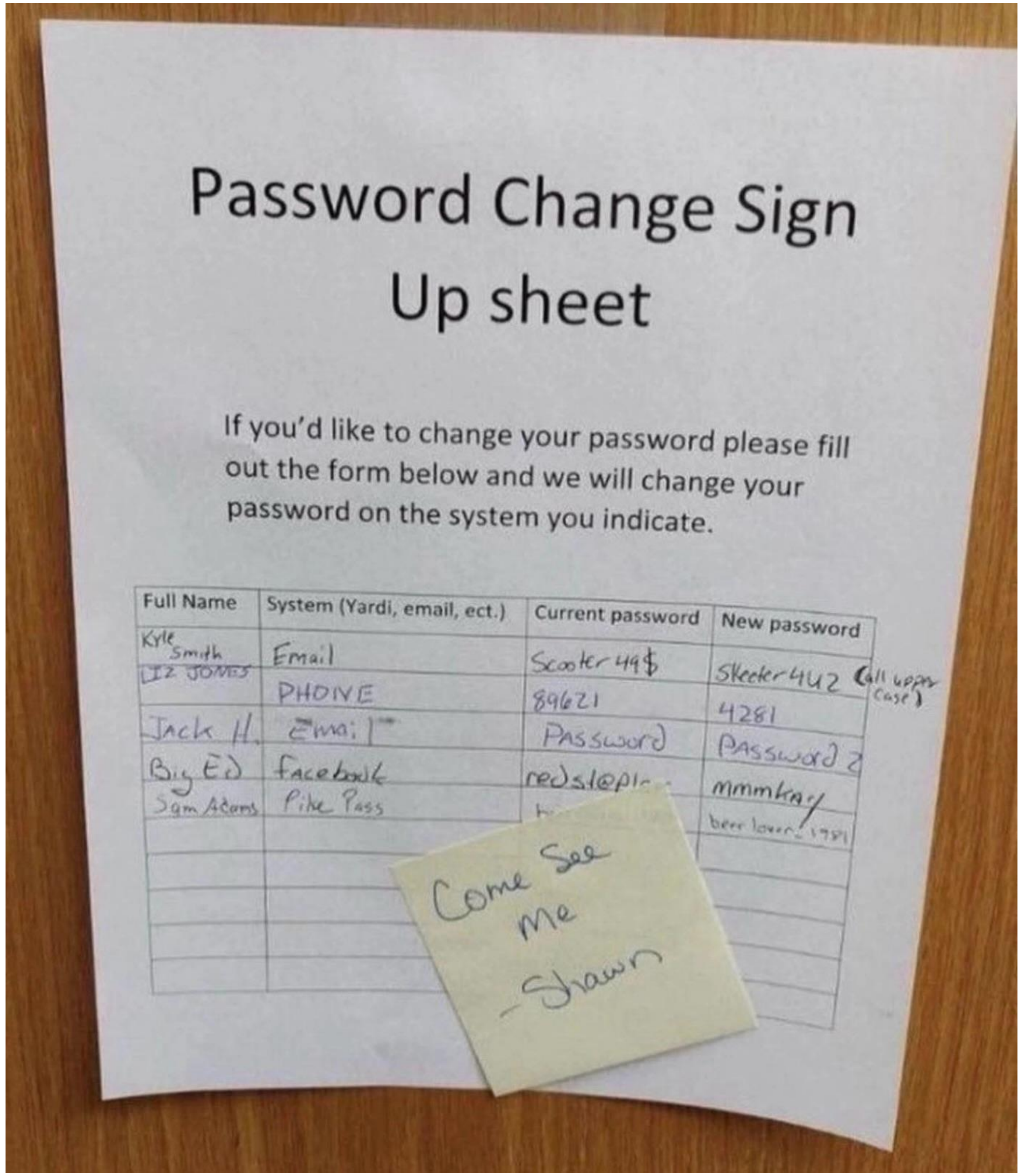
National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Boas práticas: Palavra-Passe

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Boas práticas de Palavras-Passe



CNCS
Centro Nacional de Cibersegurança PORTUGAL

Boas práticas de Palavras-Passe

Uma palavra-passe deve conter…

- Letras minúsculas;
- Letras maiúsculas;
- Números;
- Carateres especiais;
- Tamanho entre 12 e 16 carateres.

E não deve conter…

- Palavras conhecidas ou facilmente adivinháveis.

Boas práticas de Palavras-Passe

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Boas práticas de Palavras-Passe

- Não partilhar palavras-passe
- Usar palavras-passe diferentes para cada serviço
  - utilizar um gestor de palavras-passe
- Criar palavras-passe longas (frases-chave):
  - com pelo menos 12 caracteres
  - não usar termos conhecidos, como nome, cidade onde nasceu
- Alterar as palavras-passe imediatamente caso existam suspeitas de comprometimento
- Evitar guardar as palavras-passe diretamente nos browsers
- Sempre que possível, ativar a autenticação de múltiplo fator

Boas práticas de Palavras-Passe
Autenticação Multifator

Sei

- Password
- PIN
- Padrão
- ...

Tenho

- Chave
- Cartão
- Telemóvel
- …

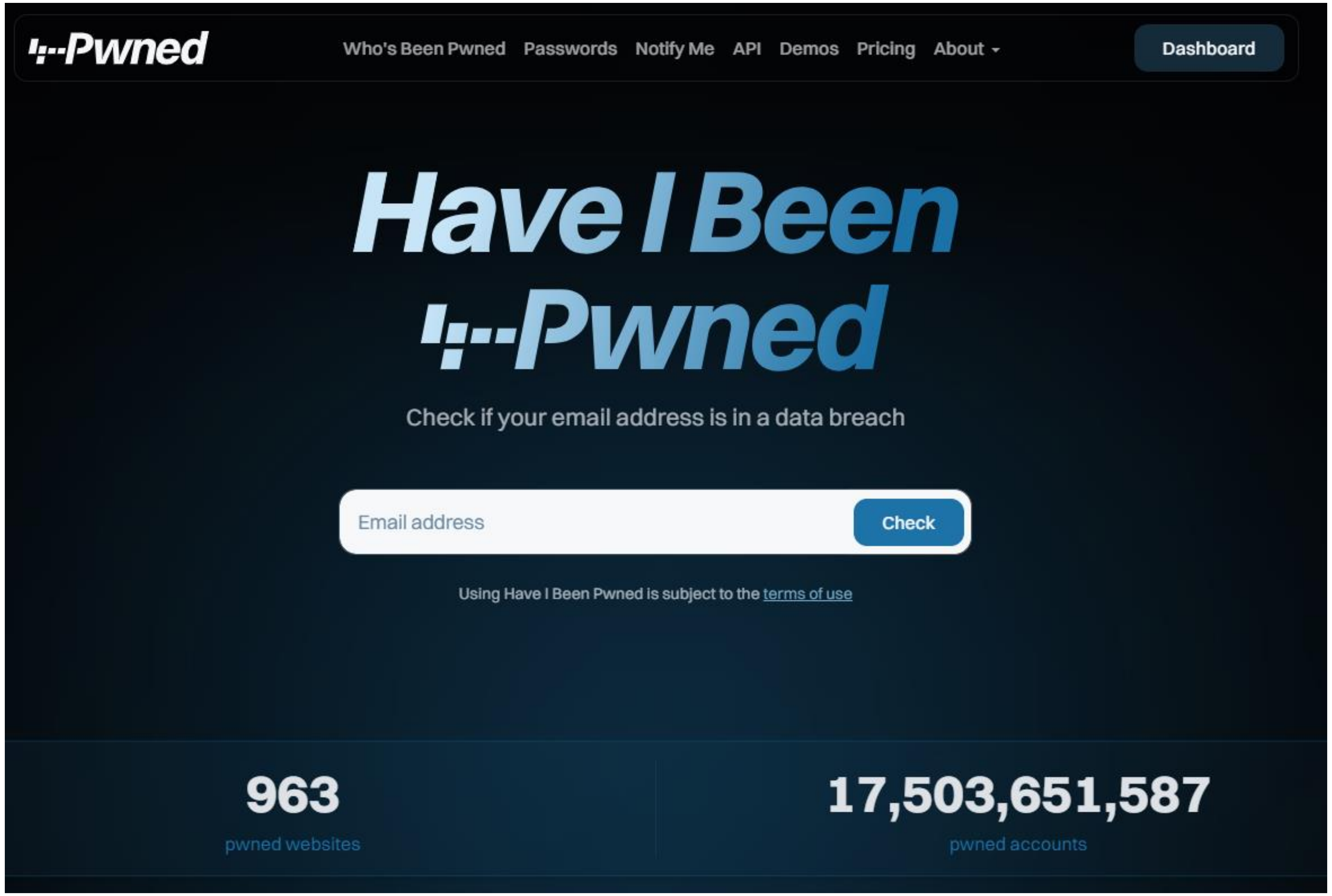
Sou

- Íris
- Impressão Digital
- Voz
- ...

Faço

- Escrita
- Cliques
- Movimentos
- ....

Será que fui comprometido?



https://haveibeenpwned.com/

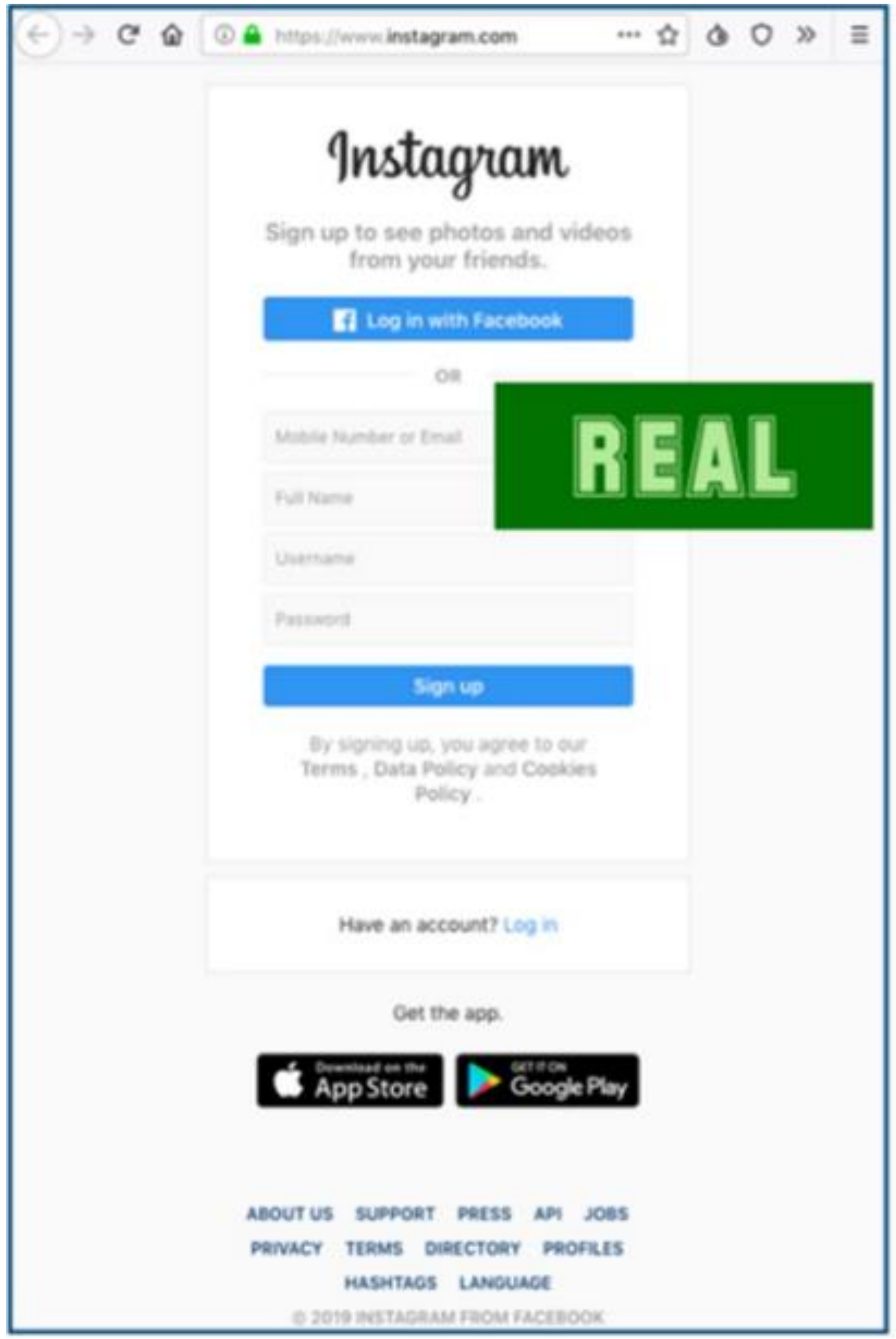
Boas práticas: Navegação Segura

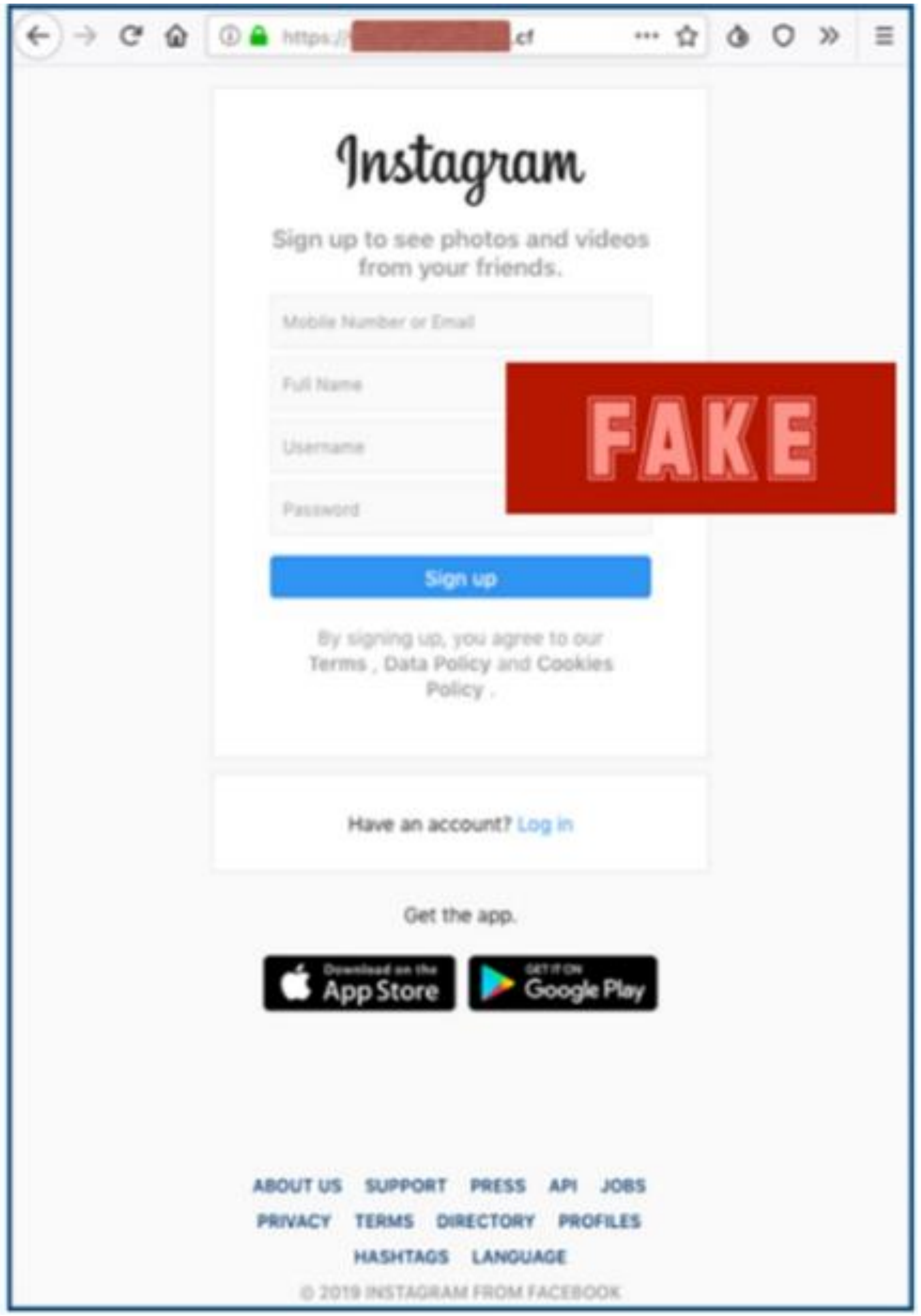
CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

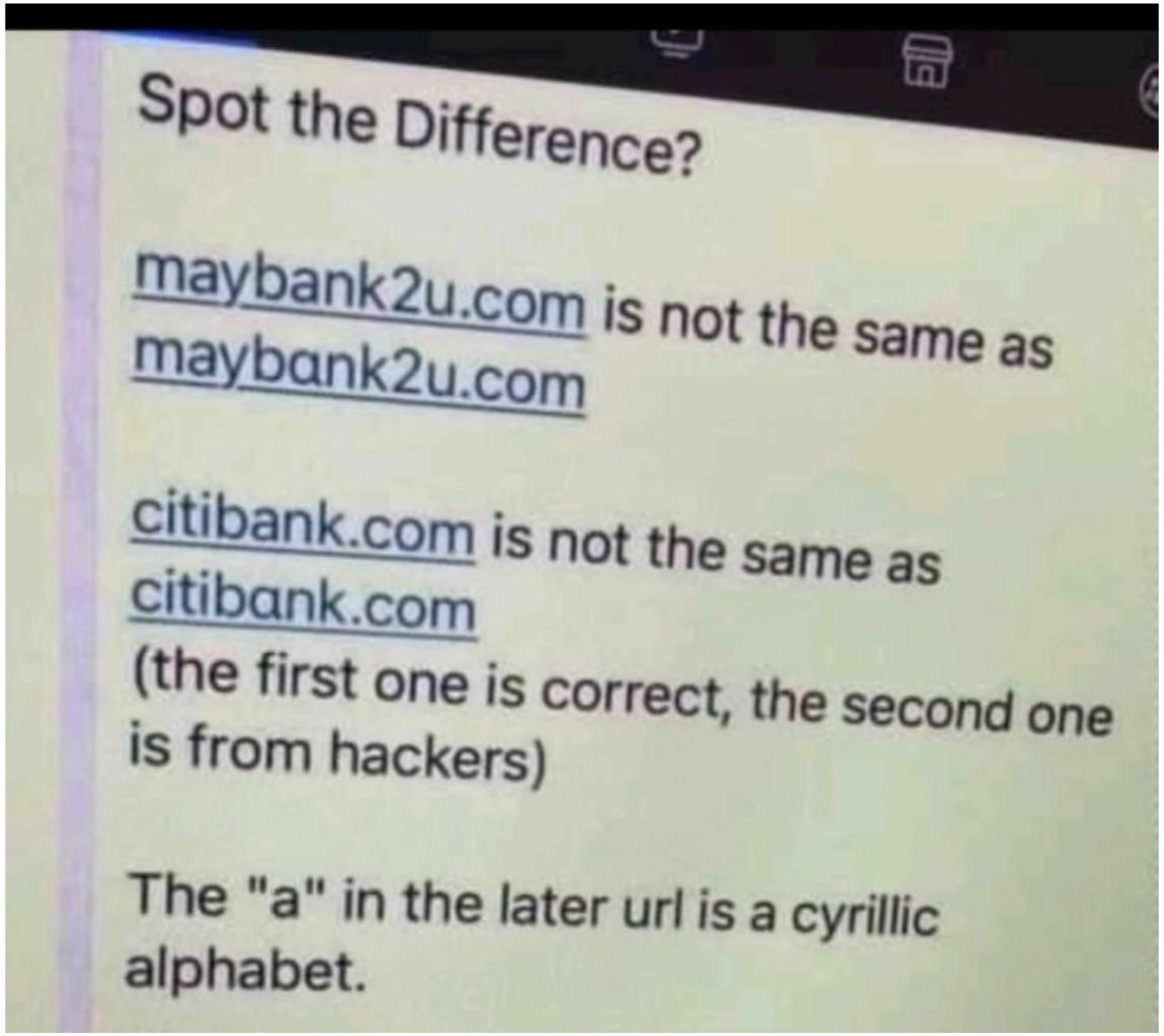
Boas práticas de Navegação Segura

Boas práticas de Navegação Segura





Boas práticas de Navegação Segura



Boas práticas de Navegação Segura

- Verificar se a sua ligação é segura, especialmente quando são enviados dados
- HTTPS não é indicativo de fidedignidade da página
- Ter muita atenção com os URLs

✓ https://fonts.googleapis.com

✗ https://fonts.googlesapis.com

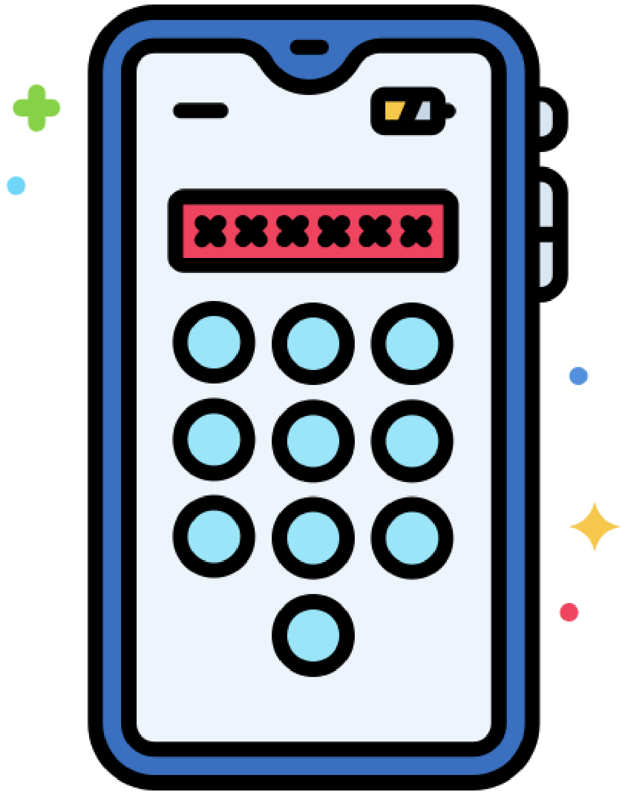
Boas práticas: Dispositivos Móveis

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

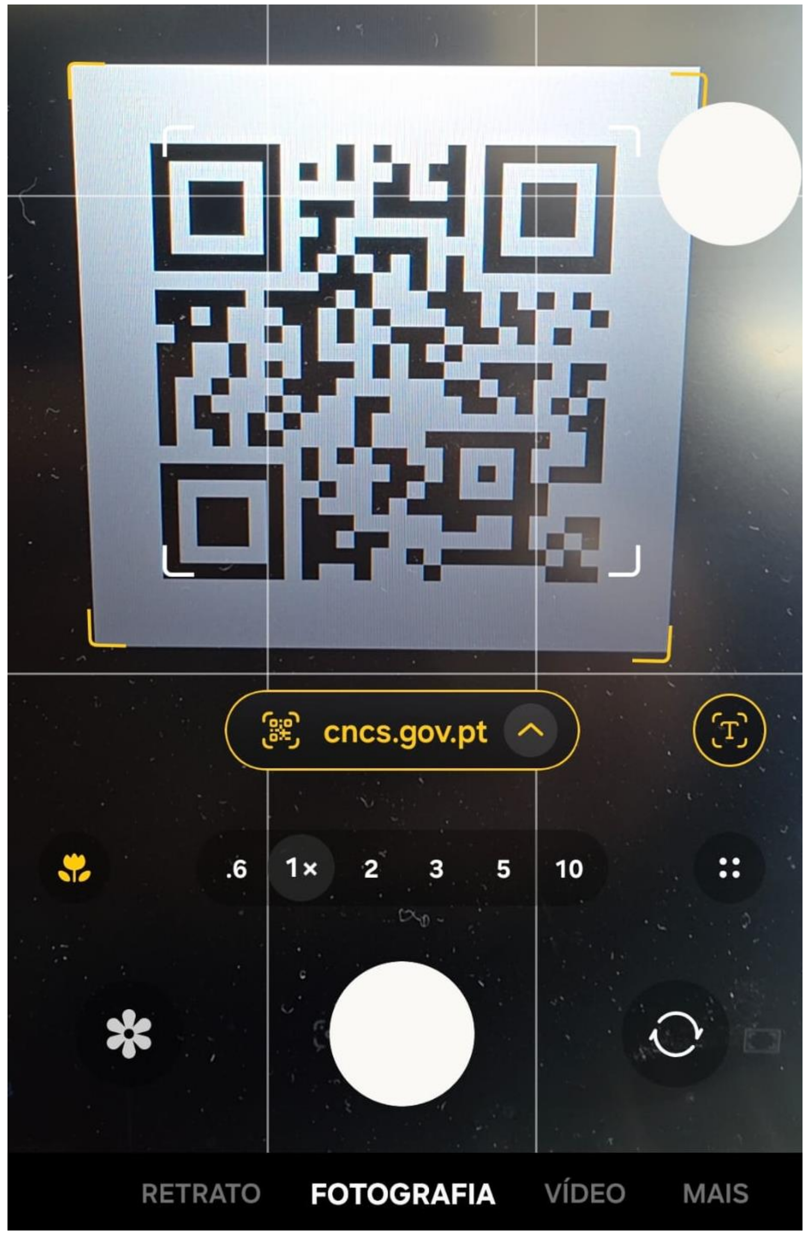
Boas Práticas de Segurança em Dispositivos Móveis

- Utilizar sempre um PIN ou autenticação biométrica
- Não partilhar PIN
- Configurar bloqueio automático e bloquear sempre que não está a usar
- Vigie sempre o seu dispositivo móvel e não o deixe abandonado



Boas Práticas de Segurança em Dispositivos Móveis
Quishing

- Evitar ler códigos QR se não se tiver a certeza da sua legitimidade
- Verificar se não existe um código QR colado por cima do original
- Ao ler códigos QR, verificar o texto antes de aceder a websites ou realizar alguma ação
- Introduzir manualmente o URL em vez de usar o código QR para acesso a algum website
- Alerta GNR: https://www.facebook.com/watch/?v=983127141040346



Boas práticas:
Correio Eletrónico

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Boas Práticas no uso do Correio Eletrónico

#1 Verificar o remetente

- A primeira questão que deve ser colocada é: “Eu conheço esta pessoa?” ou “Estou à espera de um email desta pessoa?”
  - Se a resposta for não a ambas, deve verificar-se o corpo do email com mais cuidado
- Como os cabeçalhos de emails podem ser manipulados, passar o cursor por cima do endereço do remetente de forma a verificar que é legítimo

Boas Práticas no uso do Correio Eletrónico

#2 Verificar os recipientes

- A grande maioria dos e-mails de *phishing* colocam os campos de "Para" e de "CC" em branco, para que os recipientes não vejam a quantidade de pessoas para onde foi enviado

#3 Verificar o Assunto

- É comum os e-mails de *phishing* terem os assuntos todos em maiúsculas ou ter muitos pontos de exclamação

Boas Práticas no uso do Correio Eletrónico

#4 O e-mail contém linguagem urgente ou de ameaça

- É comum os e-mails de *phishing* conterem linguagem urgente ou de ameaça, encorajando ações impulsivas. Não se apresse.

#5 O e-mail contém *links* suspeitos

- Ao passar o rato por cima de um *link*, pode ver-se o endereço do mesmo, podendo assim verificar-se se o mesmo pode ser legítimo ou malicioso.
- Não clicar em *links*, escrever diretamente o endereço na barra de endereços.
- Verificar *links* e anexos em plataformas de segurança.

Boas Práticas no uso do Correio Eletrónico

#6 O e-mail é bom de mais para ser verdade

- Os atacantes usam incentivos monetários para enganar os recipientes a enviarem dados pessoais e/ou dinheiro.

#7 O e-mail contém linguagem "estranha"

- Verificar o e-mail ou as mensagens por erros ortográficos ou usa uma linguagem diferente do habitual.

Boas Práticas no uso do Correio Eletrónico

#8 Pedem dados sensíveis, acessos ou ações

- Evitar partilhar dados, especialmente dados sensíveis (passwords, identificação, ...)
- Estabelecer processos para transferências de fundos, como verificação cara-a-cara

#9 Aparentam saber muita informação

- Não se sentir intimidado, ou fazer alguma ação rápida só porque a pessoa aparenta saber muita informação sobre si
- Usar sistemas que alertem de domínios muitos parecidos com os seus ou dos seus clientes

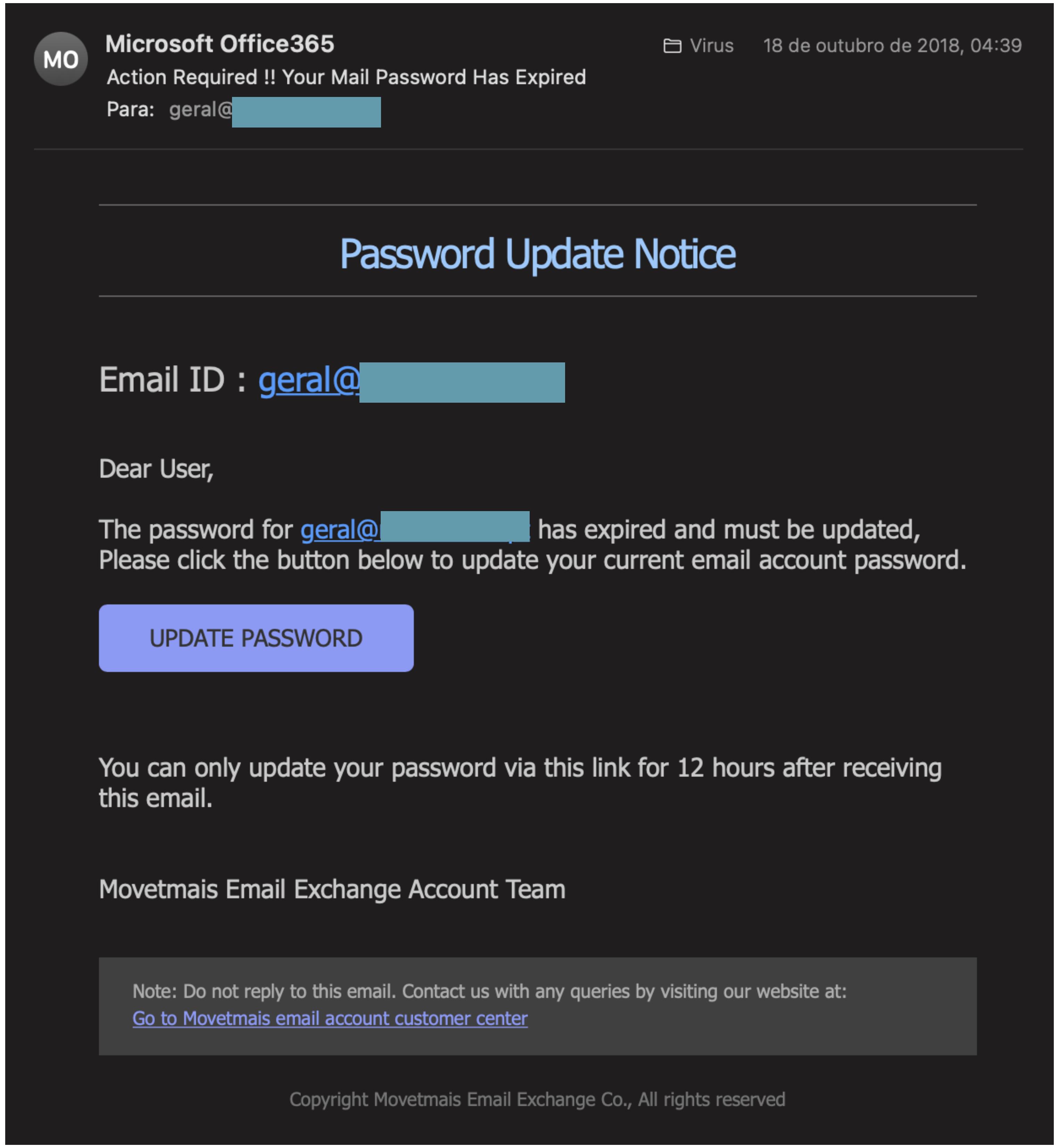
Boas Práticas no uso do Correio Eletrónico

Boas Práticas no uso do Correio Eletrónico

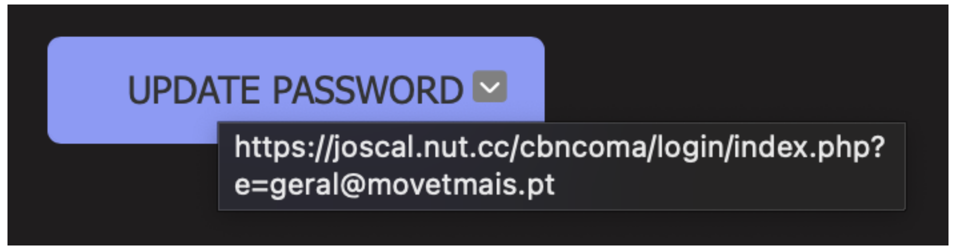
from:	**Jeffrey Brandon <serghayesfr@gmail.com>**
reply-to:	jeffreybrandon009@gmail.com
to:	
bcc:	[redacted]@gmail.com
date:	21 Jul 2022, 07:42
subject:	DEAR RESPECTED ONE
mailed-by:	gmail.com
Signed by:	gmail.com
security:	Standard encryption (TLS) Learn more

- Assunto em maiúsculas
- Nome diferente do e-mail
- Recipientes em “BCC”
- Sem “To”
- “Reply-to” diferente do “From”

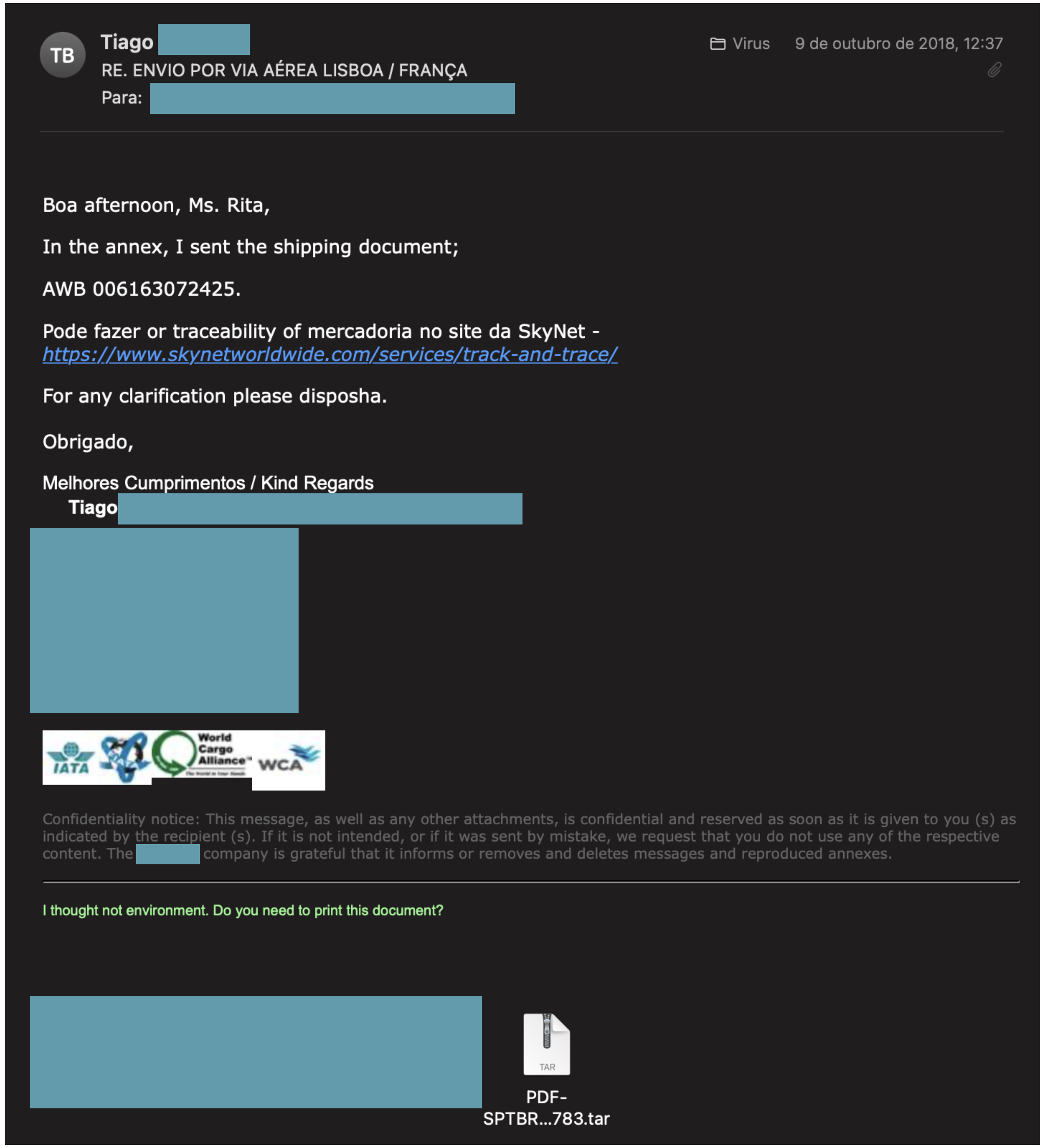
Boas Práticas no uso do Correio Eletrónico



- Pontos de exclamação no Assunto
- Pede uma ação urgente
- O *link* parece não ser um endereço reconhecido
- O email parece ser “genérico” – “Dear User,”



Boas Práticas no uso do Correio Eletrónico


TB Tiago [redacted]
RE. ENVIO POR VIA AÉREA LISBOA / FRANÇA
Para: [redacted]

Virus 9 de outubro de 2018, 12:37

Boa afternoon, Ms. Rita,

In the annex, I sent the shipping document;

AWB 006163072425.

Pode fazer or traceability of mercadoria no site da SkyNet -
https://www.skynetworldwide.com/services/track-and-trace/

For any clarification please disposha.

Obrigado,

Melhores Cumprimentos / Kind Regards
Tiago [redacted]

[redacted]

Confidentiality notice: This message, as well as any other attachments, is confidential and reserved as soon as it is given to you (s) as indicated by the recipient (s). If it is not intended, or if it was sent by mistake, we request that you do not use any of the respective content. The [redacted] company is grateful that it informs or removes and deletes messages and reproduced annexes.

I thought not environment. Do you need to print this document?

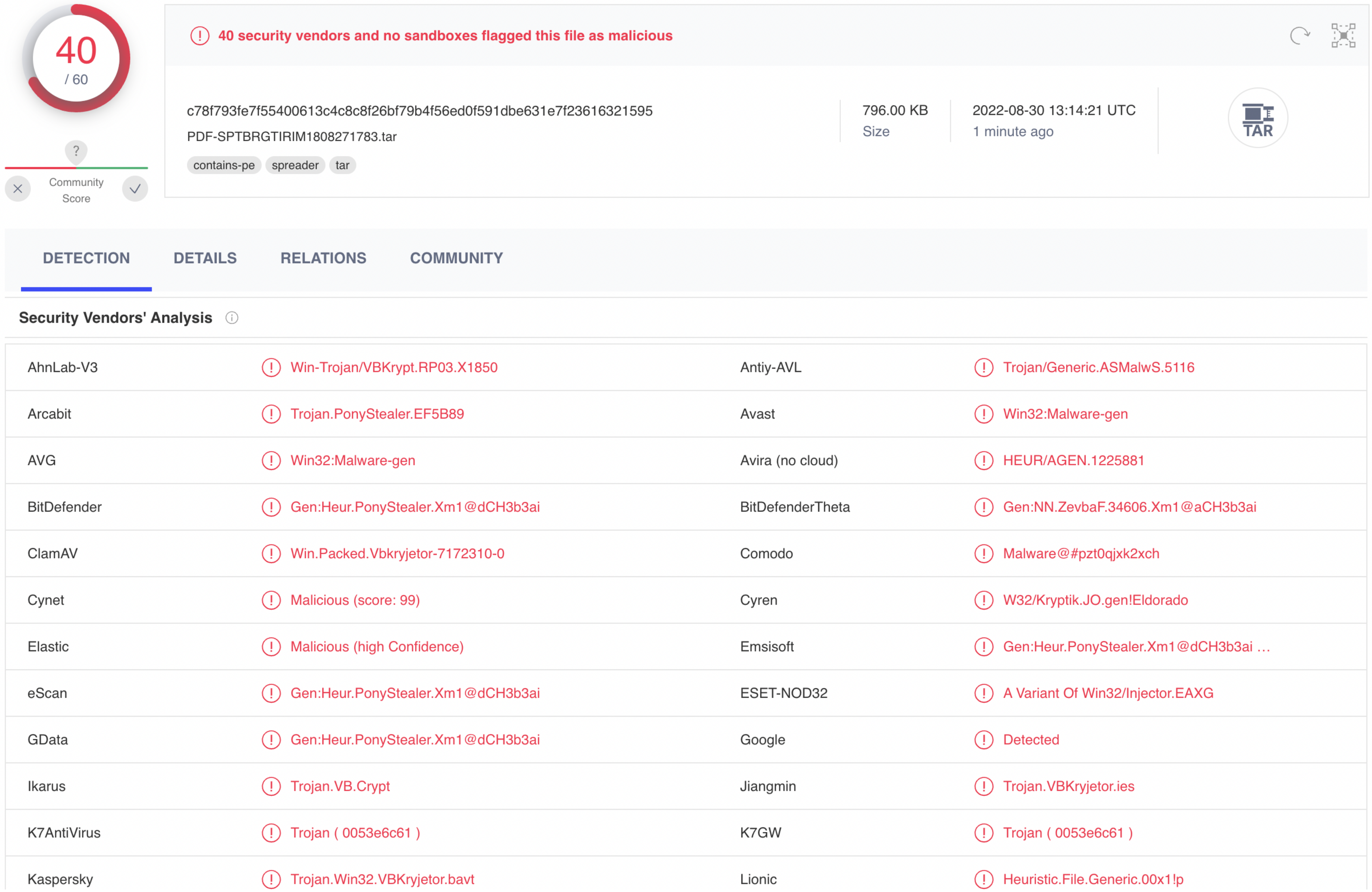
[redacted]

PDF-SPTBR...783.tar

- Assunto em maiúsculas
- O texto tem erros – “Boa afternoon”
- O anexo parece ter uma extensão estranha para o nome e tipo de ficheiro

Boas Práticas no uso do Correio Eletrónico

Boas Práticas no uso do Correio Eletrónico



40 / 60

Community Score

40 security vendors and no sandboxes flagged this file as malicious

c78f793fe7f55400613c4c8c8f26bf79b4f56ed0f591dbe631e7f23616321595
PDF-SPTBRGTIRIM1808271783.tar

contains-pe spreader tar

796.00 KB
Size

2022-08-30 13:14:21 UTC
1 minute ago

TAR

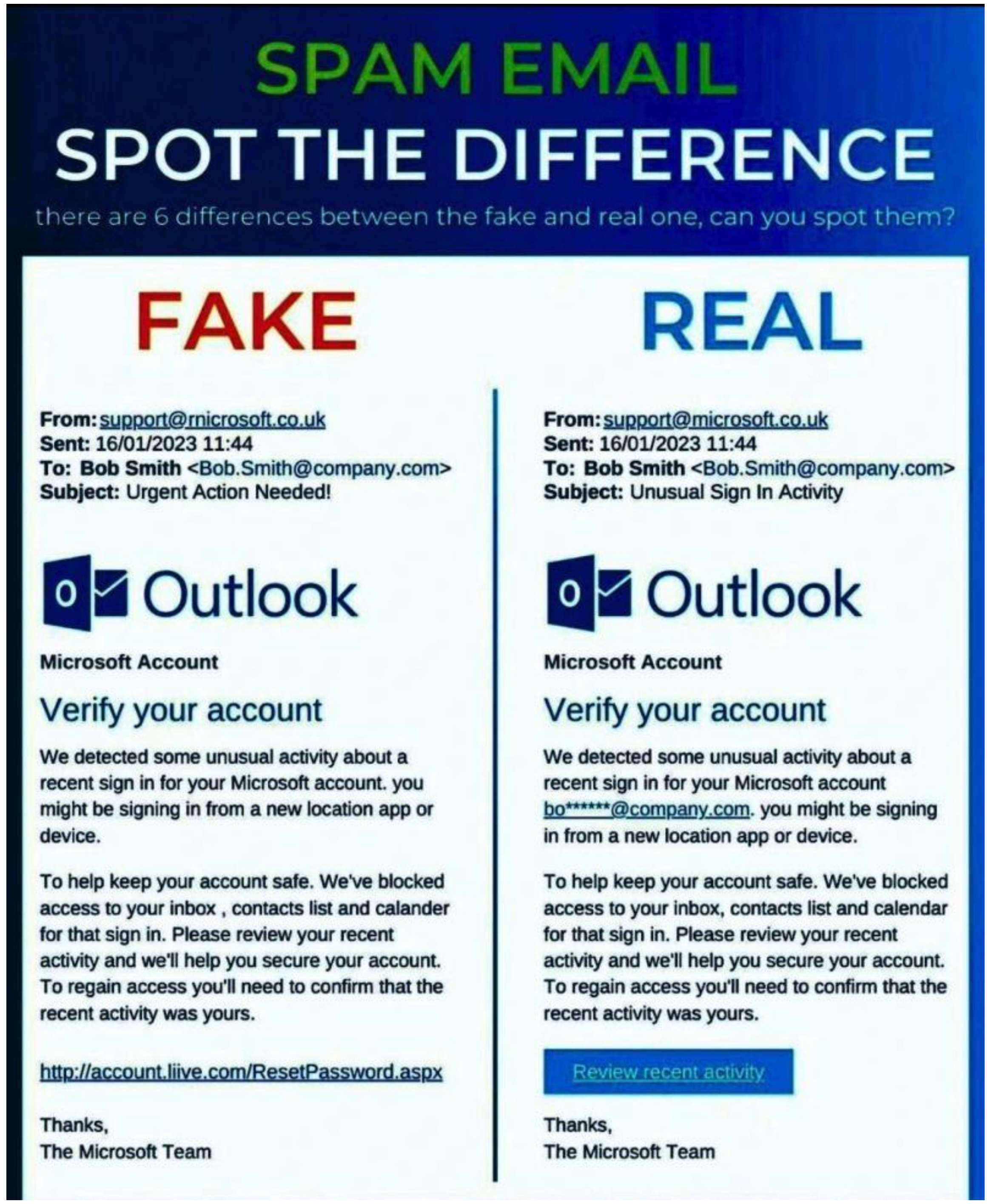
DETECTION DETAILS RELATIONS COMMUNITY

Security Vendors' Analysis

AhnLab-V3	Win-Trojan/VBKrypt.RP03.X1850	Antiy-AVL	Trojan/Generic.ASMalwS.5116
Arcabit	Trojan.PonyStealer.EF5B89	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1225881
BitDefender	Gen:Heur.PonyStealer.Xm1@dCH3b3ai	BitDefenderTheta	Gen:NN.ZevbaF.34606.Xm1@aCH3b3ai
ClamAV	Win.Packed.Vbkryjetor-7172310-0	Comodo	Malware@#pzt0qjxk2xch
Cynet	Malicious (score: 99)	Cyren	W32/Kryptik.JO.gen!Eldorado
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Heur.PonyStealer.Xm1@dCH3b3ai ...
eScan	Gen:Heur.PonyStealer.Xm1@dCH3b3ai	ESET-NOD32	A Variant Of Win32/Injector.EAXG
GData	Gen:Heur.PonyStealer.Xm1@dCH3b3ai	Google	Detected
Ikarus	Trojan.VB.Crypt	Jiangmin	Trojan.VBKryjetor.ies
K7AntiVirus	Trojan (0053e6c61)	K7GW	Trojan (0053e6c61)
Kaspersky	Trojan.Win32.VBKryjetor.bavt	Lionic	Heuristic.File.Generic.00x1!p

- https://virustotal.com/
- Não devem ser enviados ficheiros com informação sensível ou confidencial.

Boas Práticas no uso do Correio Eletrónico



Boas práticas: Conferências Online

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Boas Práticas nas Conferências Online

- Manter o software sempre atualizado
- Pensar antes de publicar informação sensível
- Ser cuidadoso com a webcam e microfone
- Utilizar formas seguras de convidar os participantes
- Controlar a partilha de ecrã
- Criar uma sala de espera
- “Trancar a porta”

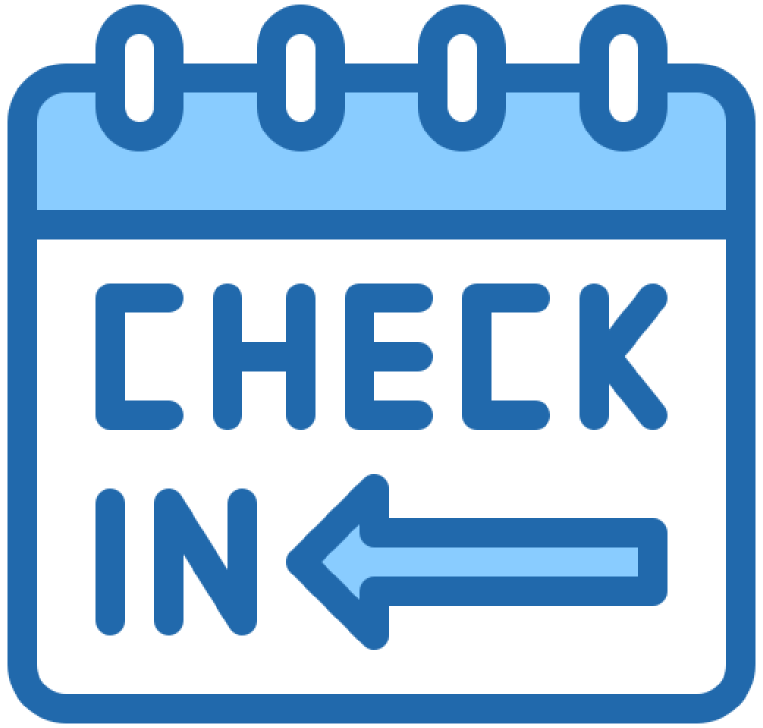
Boas práticas: Viagens

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Boas Práticas em Viagem (Antes da viagem)

- Ler atentamente as normas de segurança estabelecidas pela sua organização
- Estar ciente das leis locais
- Fazer backup dos dados para um local seguro
- Proteger o acesso aos seus dispositivos com passwords fortes
- Evitar viajar com dados sensíveis
- Usar um filtro de privacidade nos seus dispositivos
- Marcar o(s) equipamento(s) com um sinal distintivo



Boas Práticas em Viagem (Durante a viagem)

- Manter os seus equipamentos e arquivos sempre por perto
- Não ligar a redes com fraca segurança e utilizar sempre um serviço de VPN confiável
- Utilizar software de cifra durante a viagem
- Não carregar os seus dispositivos nos terminais elétricos de self-service
- Não conectar periféricos ou outros dispositivos que não sejam confiáveis aos seus dispositivos
- Em caso de inspeção ou apreensão por parte das autoridades, informar imediatamente a entidade proprietária dos equipamentos

Boas Práticas em Viagem (Após a viagem)

- Mudar todas as passwords que usou durante a viagem
- Analisar o(s) seu(s) equipamento(s)

Sente-se preparado/a?

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

Penso que sofri um ataque, o que devo fazer?

- Contactar imediatamente o departamento IT
- Alterar palavras-passe
- Fazer um scan dos dispositivos com um software antivírus
- Contactar o CERT.PT (cert@cert.pt)

E a sua organização, está preparada?

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

National Cybersecurity Center
Rua da Junqueira, 69 | 1300-342 Lisbon
cncs@cncs.gov.pt | (+351) 210 497 400

E a sua organização, está preparada?

C-ACADEMY

FORMAÇÃO AVANÇADA
EM CIBERSEGURANÇA

www.cncs.gov.pt

OS DESAFIOS DA CIBERSEGURANÇA

O CNCS identificou ações gerais para mitigar os desafios à cibersegurança:

Formar mais recursos humanos para capacitar as organizações públicas e privadas.

Criar mecanismos para a retenção dos profissionais ligados à cibersegurança na Administração Pública e nas empresas em Portugal.

Manter os conteúdos de boas práticas, os alertas e as políticas de cibersegurança atualizados com o conhecimento situacional do momento e os tutoriais de mitigação de riscos correspondentes.

OBJETIVOS C-ACADEMY

Abranger pelo menos 9800 formandos até ao primeiro trimestre de 2026

Alcançar uma distribuição geográfica que permita abranger todo o território nacional

INSTITUIÇÕES PARCEIRAS

Protocolos com Instituições de Ensino Superior para o desenvolvimento dos conteúdos e/ou implementação do programa de formação.

21 contratos com as seguintes Instituições de Ensino Superior Público:

Instituto Politécnico da Guarda
Instituto Politécnico de Bragança
Instituto Politécnico de Coimbra
Instituto Politécnico de Lisboa
Instituto Politécnico de Viana do Castelo
Instituto Politécnico de Viseu
Instituto Politécnico do Cávado e Ave
Instituto Politécnico do Porto

ISCTE - Instituto Universitário de Lisboa
Universidade da Beira Interior
Universidade da Madeira
Universidade de Aveiro
Universidade de Coimbra
Universidade de Évora
Universidade de Trás-os-Montes e Alto Douro
Universidade do Algarve
Universidade do Minho
Universidade do Porto
Universidade dos Açores
Universidade Nova de Lisboa
Faculdade de Ciências da Universidade de Lisboa

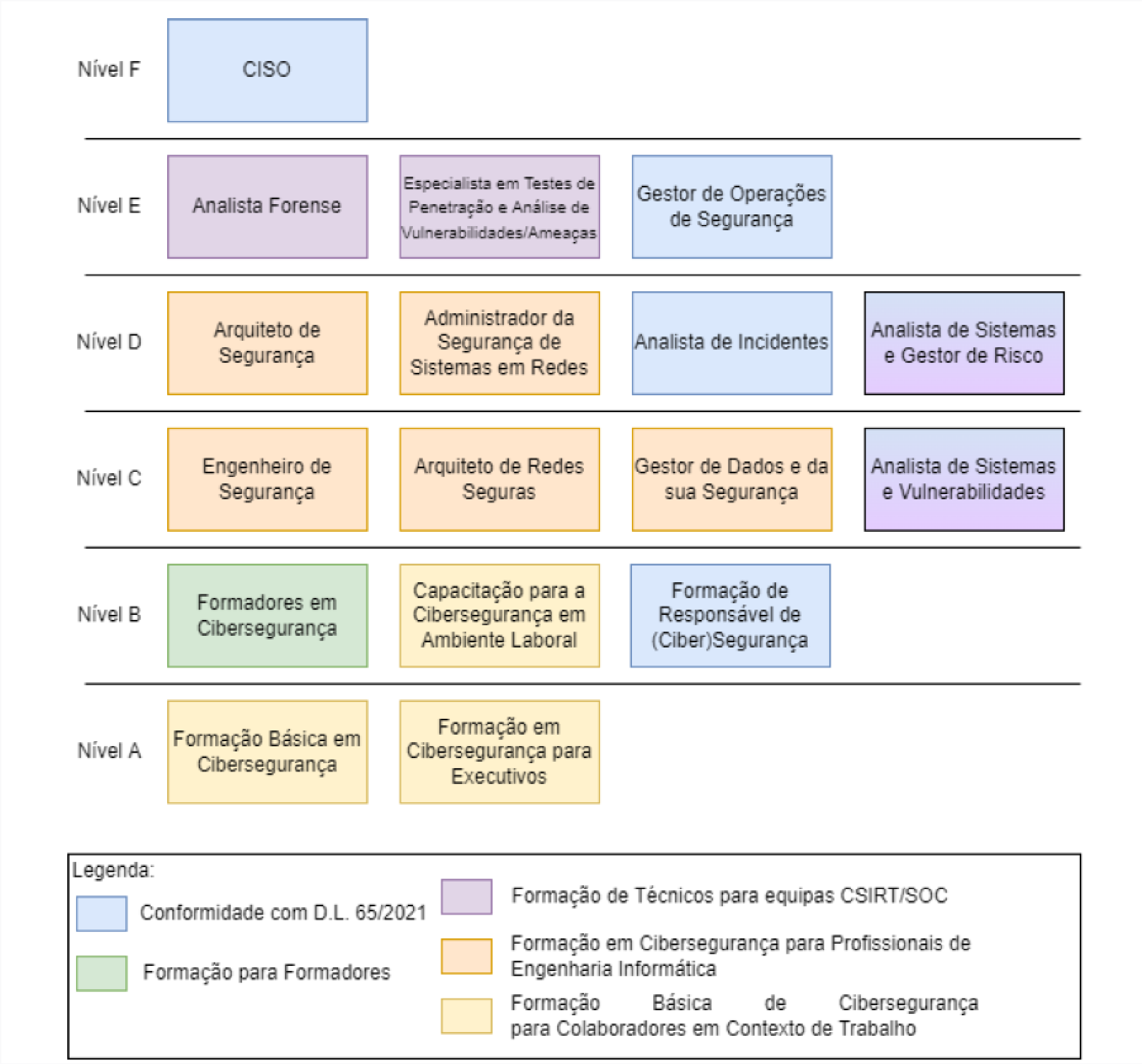
CACADEMY FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA

CNCS

OFERTA FORMATIVA

Este modelo garante uma oferta formativa muito completa:

- 43 Conteúdos
- 17 Percursos Formativos
- 6 Níveis de Dificuldade
- Formação Presencial, à Distância e Mista
- Cargas Letivas 35h | 70h
- Atribuição de ECTS



Analista de Sistemas e Gestor de Risco

Nível C
70 H
Criptologia

Nível D
35 H
Princípios e Metodologias de Gestão de Risco

Nível D
35 H
Gestão de Risco Orientado à Organização

Nível D
35 H
Segurança Aplicada a Sistemas de Informação

PÚBLICO-ALVO

Uma resposta de âmbito nacional e em rede para apoiar as organizações no caminho da maturidade e resiliência em cibersegurança.

Contacto: c-network@cncs.gov.pt

Financiado pela União Europeia
NextGenerationEU

TLP:WHITE

Maio de 2024

A Rede C-Network

- Inovadora e Transformadora
- De Âmbito Nacional
- Para apoiar no desenvolvimento de capacidades em cibersegurança.
- Orientar organizações no caminho da maturidade e resiliência em cibersegurança.

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

Objetivos

- Disponibilizar uma rede composta por 7 centros de competências em cibersegurança dotada de especialistas com competências diversas.
- Apoiar em regime de proximidade 2000 entidades;
  - Entidades Abrangidas pelo RJSC
  - Administração Pública
  - PMEs

Objetivos

- Apoiar a transformação digital das organizações, sob o ponto de vista de cibersegurança, ao nível da capacitação, dos processos, na obtenção de financiamento e na operação diária, sem se substituir à indústria;
- Fomentar a colaboração e cooperação entre as várias entidades, ao nível regional e nacional;
- Promover o empreendedorismo e a criação de ecossistemas regionais de cibersegurança.

PRR Plano de Recuperação e Resiliência | REPÚBLICA PORTUGUESA | Financiado pela União Europeia NextGenerationEU

Centros de Competência em Cibersegurança

Missão: identificar e analisar as necessidades das organizações presentes nas sua regiões e, seguidamente, orientá-las no sentido aumentar sua maturidade e resiliência.

Primeiro Contacto com Entidades Regionais

Análise das necessidades

Apoio efetivo com o objetivo de aumentar a resiliência e a maturidade em cibersegurança

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

O Centro de Competências em Cibersegurança

:cccnorte

:ccccentro

:ccclisboa e vale do tejo

:cccalentejo

:cccalgarve

:cccmadeira

:cccaçores

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

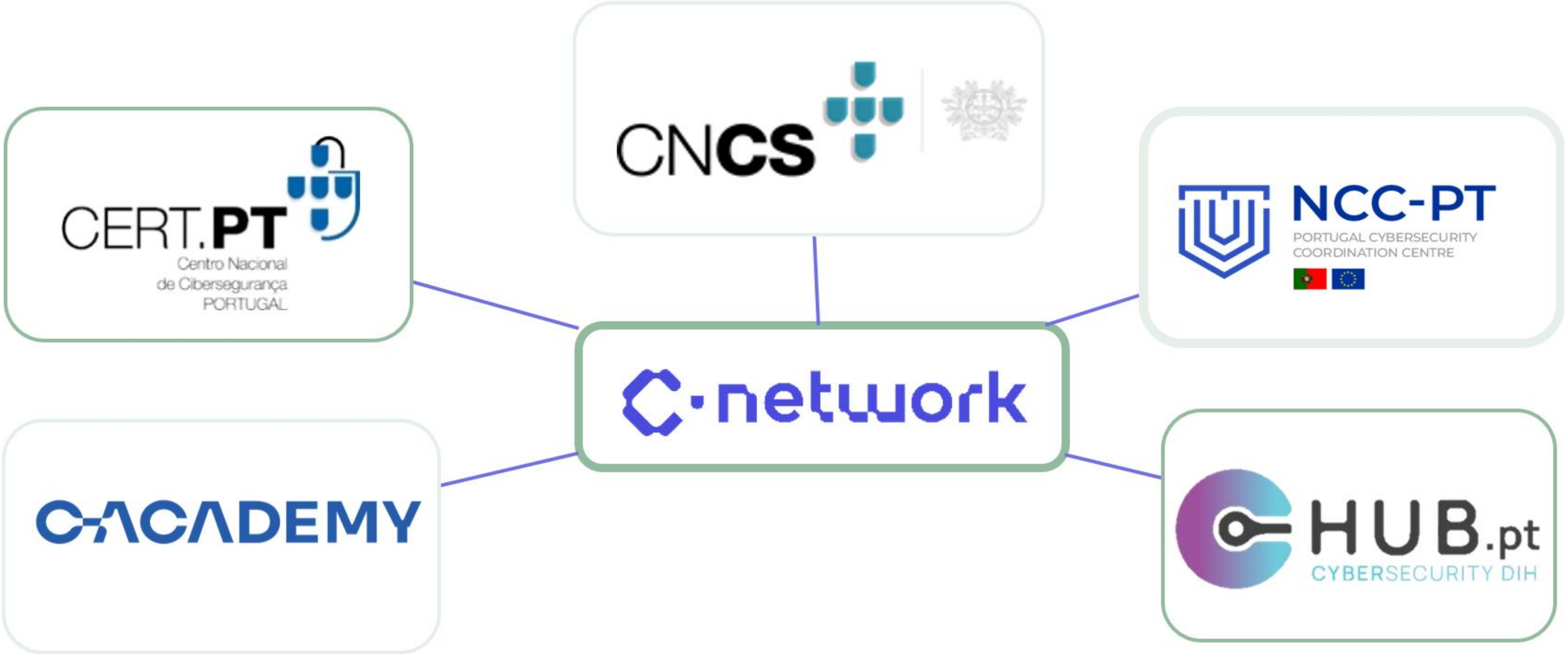
Atividades a Desenvolver

As atividades a desenvolver pelos Centros de Competências em Cibersegurança, com as organizações inserem-se nos seguintes grupos:

- Cooperação e Partilha
- Capacitação Organizacional
- Inovação
- Capacitação Humana
- Coordenação de Incidentes

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

Sinergias e Parcerias



PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia
NextGenerationEU

Centro Nacional de Cibersegurança PORTUGAL

Centro Nacional de Coordenação NCC-PT

O NCC-PT

Centro de Nacional de Coordenação em Cibersegurança

Centro de Nacional de Coordenação em Cibersegurança

NCC-PT
PORTUGAL CYBERSECURITY COORDINATION CENTRE

O Regulamento (EU) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021.

Procede à criação do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (**ECCC**)
e
Rede de Centros Nacionais de Coordenação (**NCCs**)

Coordenar as medidas de apoio financeiro relativo a iniciativas da União Europeia em matéria de investigação e desenvolvimento, da inovação, da tecnologia e do desenvolvimento industrial no domínio da cibersegurança, nomeadamente ao abrigo do **Horizonte Europa** — Programa-Quadro de Investigação e Inovação, criado pelo Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho de 28 de abril de 2021, e do **Programa Europa Digital**, criado pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho.

Designação e Competências:

- Em 2022, através de **Despacho 11491/2022** o CNCS foi designado como **Centro Nacional de Coordenação de Cibersegurança.**

- O CNCS para cumprir e prosseguir as atribuições referidas no artigo 7º do Regulamento (EU) 2021/887 atua em articulação e cooperação com a **Agência Nacional para a Inovação (ANI) e a Fundação para a Ciência e a Tecnologia (FCT).**

NCC-PT
PORTUGAL CYBERSECURITY COORDINATION CENTRE

O NCC-PT

O Consórcio

National Coordination Centre

Consortium Coordination

Management and coordination
Single Point of Contact
Legal and ethical supervision
International cooperation
Community engagement
Community validation
Technical assistance to stakeholders
Dissemination activities

Member (ANI – Agência Nacional de Inovação)

Community engagement
Capacity building
Innovation and Knowledge transfer
National Industry Cooperation
FSTP to industry management
Technical assistance to stakeholders
Dissemination activities

Member (FCT – Fundação para a Ciência e a Tecnologia)

Community engagement
Capacity building
Innovation and Knowledge transfer
National Higher education Cooperation
FSTP to Higher Education management
Technical assistance to stakeholders
Dissemination activities

Guias e Referenciais

Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400

Guias e Referenciais

- https://www.cncs.gov.pt/pt/guias-referenciais/
  - Guia de Gestão de Riscos
    - https://www.cncs.gov.pt/pt/gestao-de-risco/
  - Guia para a Seleção de Soluções de Autenticação Multifator
    - https://www.cncs.gov.pt/pt/guia-mfa/
  - Guia de Transição Digital
    - https://www.cncs.gov.pt/pt/guia-de-transicao-digital
  - Referencial de Competências em Cibersegurança
    - https://www.cncs.gov.pt/pt/referencial-de-competencias/
  - Referencial de Comunicação de Crise
    - https://www.cncs.gov.pt/pt/referencial-de-comunicacao/

Projetos

- C-Network
  - https://www.cncs.gov.pt/pt/c-network/
- C-Academy
  - https://www.cncs.gov.pt/pt/c-academy/
  - https://www.c-academy.pt/CNCS/web/home/
- NCC-PT
  - https://www.cncs.gov.pt/pt/ncc-pt/

Ferramentas

- https://www.cncs.gov.pt/pt/ferramentas/
- Webcheck.pt
  - https://www.cncs.gov.pt/pt/webcheck/
- CyberCheckUp
  - https://www.cncs.gov.pt/pt/quadro-nacional/#cibercheckup

Cursos e Redes

- CNCS na NAU
  - https://www.nau.edu.pt/pt/parceiros/centro-nacional-de-ciberseguranca/
- CNCS no Youtube
  - https://www.youtube.com/@CentroNacionaldeCibersegurança
- CNCS no LinkedIn
  - https://www.linkedin.com/company/centro-nacional-de-ciberseguran%C3%A7a---portuguese-national-cybersecurity-centre

Obrigado!

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Francisco Peixoto
francisco.peixoto@cncs.gov.pt