



Cibersegurança: tendências e desafios atuais (PME)

Pedro Xavier Mendonça
(CNCS)

OBJETIVO DA APRESENTAÇÃO

Mostrar a **importância da cibersegurança** para as PME e o **contexto de ameaças** que as pode afetar.

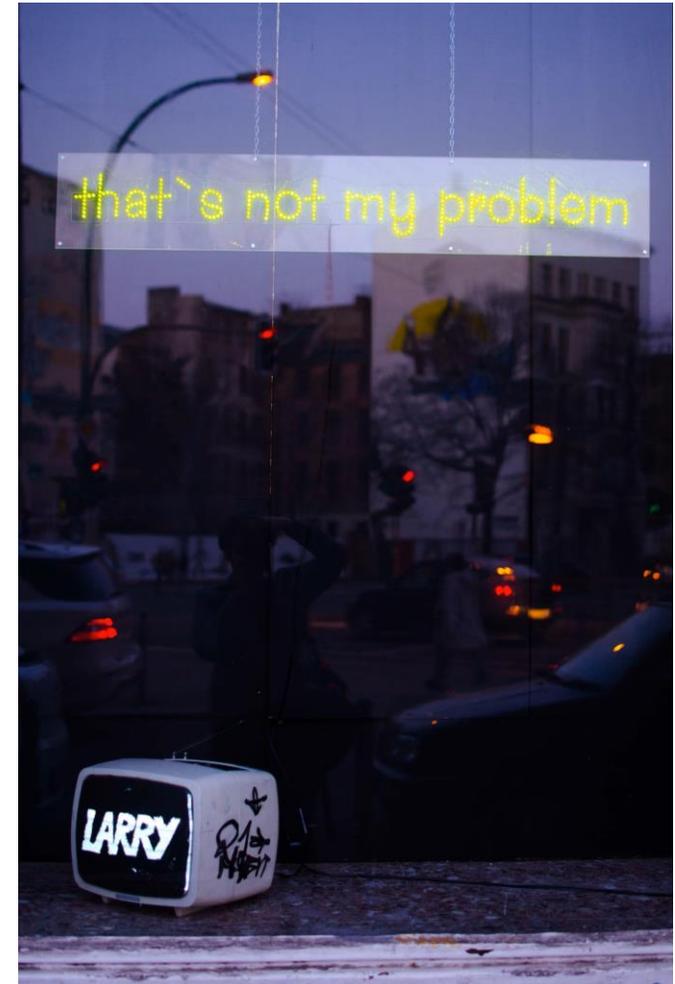
CIBERSEGURANÇA NAS PME

“Ninguém se interessa por mim!”

“Não tenho nada de valor!”

“Quem não deve não teme!”

“Vão furtrar o quê?!”



Aneta Pawlik

DESIGUALDADE NA CIBERSEGURANÇA

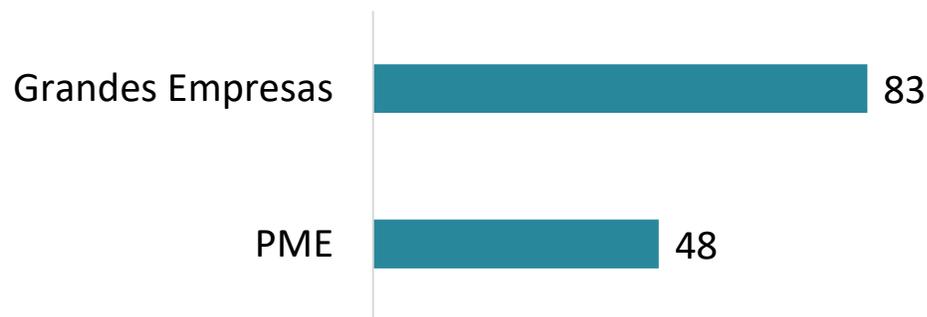


Há uma crescente **desigualdade entre empresas** na capacitação para a cibersegurança, nomeadamente entre PME e grandes empresas:

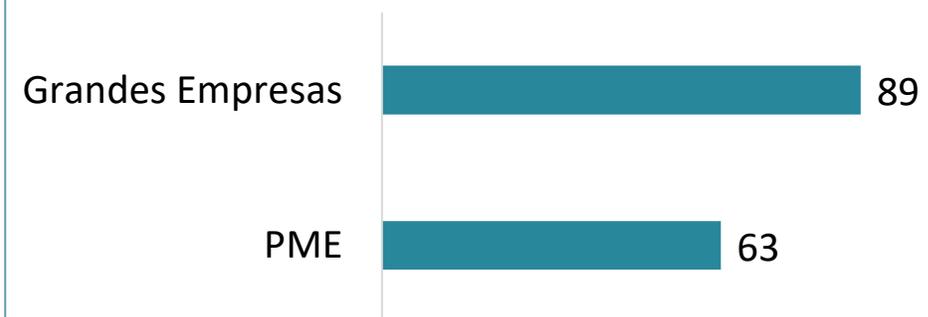
– **90% dos executivos** inquiridos pelo WEF consideram que este é um **problema urgente**.

(WEF, 2024)

Empresas com **política de segurança para as TIC** definida ou revista nos últimos dois anos, Portugal, 2022 (%)



Empresas que **sensibilizaram os seus empregados** para as obrigações de segurança nas TIC, Portugal, 2022 (%)



(Eurostat, 2022)

ECONOMIA DA CIBERSEGURANÇA EM PORTUGAL



Aspetos positivos (2021)

- **Existem pelo menos 144 empresas** que oferecem serviços de cibersegurança;
- Os profissionais de cibersegurança são **relativamente novos e com formação elevada**;
- Verifica-se um **aumento da cooperação** entre empresas com a criação de mais Comunidades de Cibersegurança.



Problemas que persistem (2021 e 2022)

- Pouco mais de um terço das PME tem um **orçamento abaixo dos 3000 euros** em cibersegurança;
- Pelo menos **uma em cada seis PME tem dificuldades em contratar** profissionais de cibersegurança;
- As razões principais são a **escassez de profissionais** (para 78%) e **o seu elevado custo** (para 57%).

(CNCS, 2022)

TOTAL DE INCIDENTES REGISTRADOS PELO CERT.PT 2015 -2023

NÚMERO DE INCIDENTES REGISTRADOS PELO CERT.PT POR ANO*



* Quebra de série em 2020: devido a alterações na taxonomia utilizada pelo CERT.PT em 2020 (RNCSIRT, 2023), a partir desse ano passaram a ser contabilizadas as vulnerabilidades como incidentes. Os dados anteriores a 2020 não incluem as vulnerabilidades. Todavia, o seu efeito no total não é significativo.

Fonte: CERT.PT

(CNCS, 2024)

CRIME E CIBERCRIME PARTICIPADO EM PORTUGAL 2009-2023

PERCENTAGEM DE CRIMES RELACIONADOS COM A INFORMÁTICA EM RELAÇÃO AO TOTAL DE CRIMES REGISTRADOS PELAS AUTORIDADES POLICIAIS*



*Os crimes relacionados com a informática incluem os crimes informáticos juntamente com a burla informática/comunicações e a devassa por meio de informática. Verifica-se uma quebra de série em 2022: crimes antes registados como “burla informática/comunicações” passaram a ser registados como “abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento” (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

(CNCS, 2023)

Fonte: DGPJ

O FATOR HUMANO NA CIBERSEGURANÇA

extorsões e fraudes



Em 2023, pelo menos **45%** dos incidentes registados pelo CERT.PT envolvem diretamente o **fator humano**.



As **PME continuam a ser um dos principais alvos** de cibercriminosos que têm como objetivo obter ganhos económicos através de **extorsões e fraudes**.



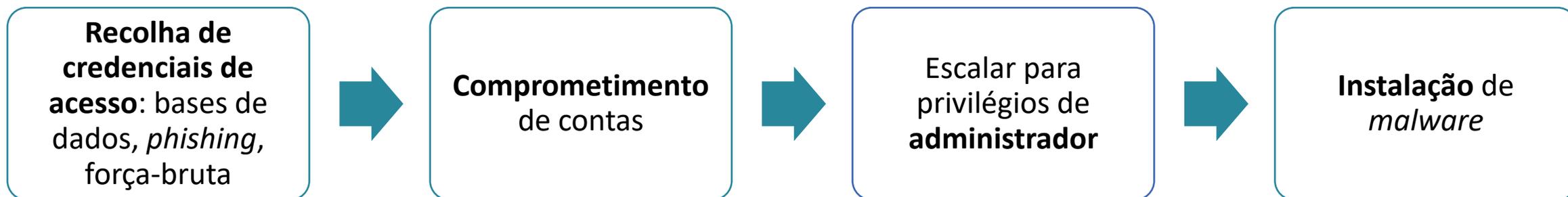
O **ransomware** é também uma preocupação, nomeadamente pelo impacto.



São preocupantes os casos de **comprometimento de email empresarial**, com *phishing*, CEO Fraud, entre outros.

RANSOMWARE

modi operandi mais frequentes



Outros *modi operandi*

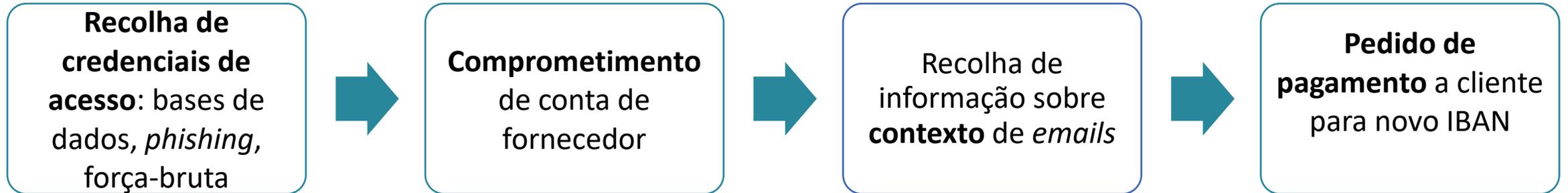
Exploração de vulnerabilidades

Comprometimento de acesso remoto (RDP)

Emails com anexos e *links* com *malware*

CEO FRAUD (BEC)

modi operandi mais frequentes



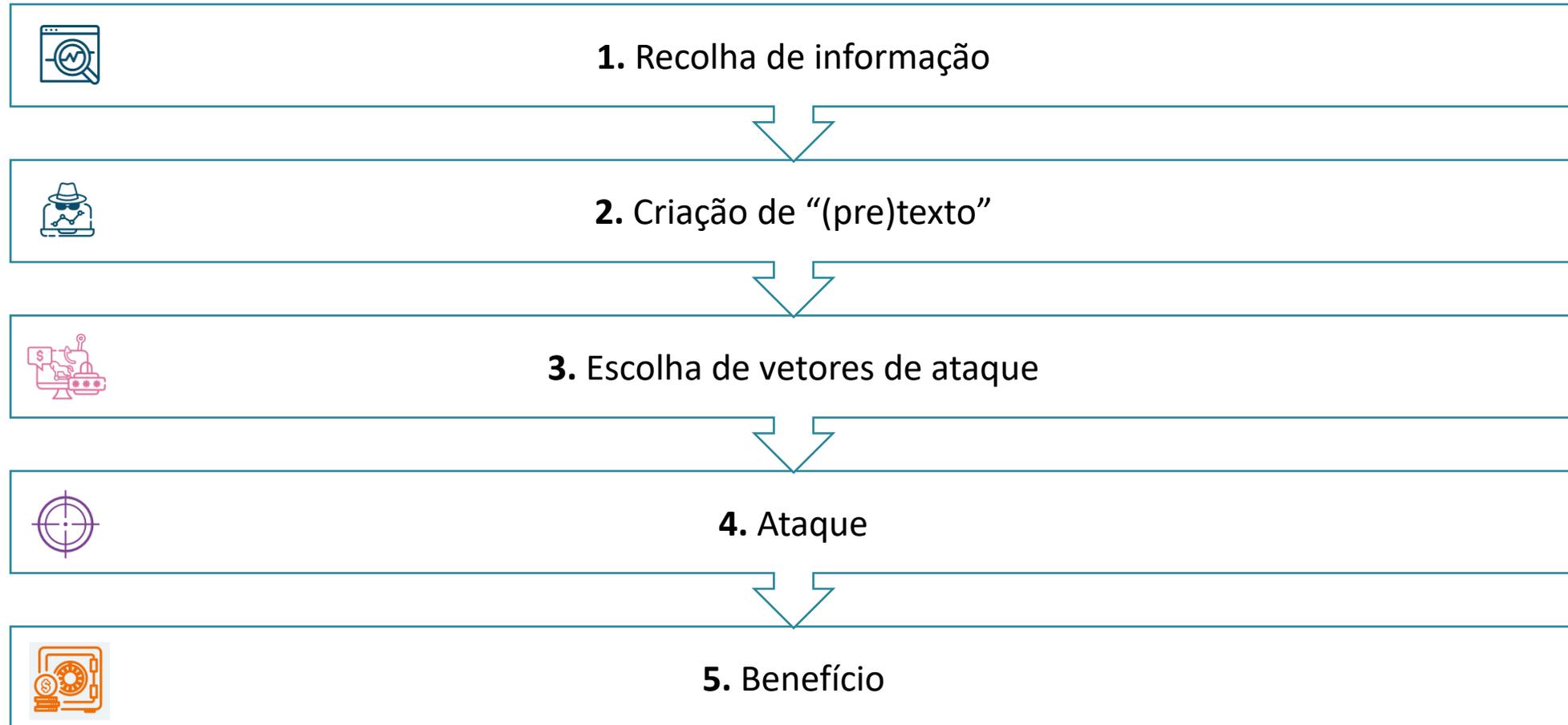
Outros *modi operandi*

Personificação de entidade fornecedora e clientes – *typosquatting*

Personificação de empregado para alterar destino do vencimento

Personificação de superior hierárquico a requisitar cartões de oferta

CADEIA DE ATAQUE DA ENGENHARIA SOCIAL



(Adaptado de Hadnagy, 2018)

O QUE FAZER?



Identificar – inventariar quais os ativos críticos para a organização



Guardar – fazer *backups* regulares



Multiplicar – aplicar o múltiplo fator de autenticação

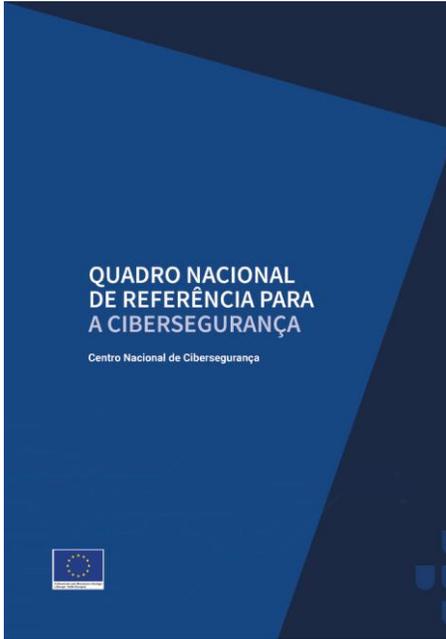


Atualizar – manter os sistemas atualizados



Formar – disponibilizar sensibilização e treino aos empregados

INSTRUMENTOS CNCS



Guia para Gestão dos Riscos de Segurança da Informação e Cibersegurança



v1.1 dezembro 2022
Centro Nacional de Cibersegurança

GOVEIN 19 Financiamento pelo Mecanismo Interligar a Europa - União Europeia



Referencial de Comunicação de Risco e de Crise em Cibersegurança



v1.0
Abril de 2024
Centro Nacional de Cibersegurança



Cidadão Ciberseguro

O Cidadão Ciberseguro é um curso de e-learning curto, simples e acessível ao cidadão/colaborador em geral, com o intuito de o dotar de conhecimentos que permitam proteger-se e adotar boas práticas de [ciber-higiene](#) em diferentes contextos diários, incluindo no local de trabalho.



Cidadão Ciberinformado

O curso de e-learning Cidadão Ciberinformado destina-se a qualquer cidadão que procure aprender a identificar notícias falsas e a verificar a veracidade da informação consultada online, evitando a partilha de [desinformação](#) e contribuindo para um ciberespaço verdadeiramente democrático.



Consumidor Ciberseguro

Através do curso de e-learning Consumidor Ciberseguro os formandos poderão obter conhecimentos que lhes permitam proteger-se e adotar boas práticas quando realizam compras online, evitando de modo mais eficaz a burla e o roubo de credenciais de cartões de crédito, por exemplo. Com este curso cada um poderá fazer compras online com mais segurança.



Cidadão Cbersocial

O curso de e-learning Cidadão Cbersocial é uma iniciativa do Centro Internet Segura, coordenado pelo Centro Nacional de Cibersegurança. Trata-se de um curso interativo, que procura ser apelativo para todas as pessoas que queiram saber como utilizar as [redes sociais](#) de um modo mais seguro e protegendo a sua privacidade.



Webcheck

Verifique a segurança do seu domínio

Verifique se o seu domínio cumpre com as boas práticas e standards que contribuem para uma navegação na internet e envio de correio eletrónico mais seguros e confiáveis.

INÍCIO > SENSIBILIZAÇÃO E FORMAÇÃO >

Recursos para Sensibilização

OBRIGADO



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