Fraudes: como detetar e evitar

Pedro Xavier Mendonça
Centro Nacional de Cibersegurança

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Índice

1. **A componente social** da cibersegurança;
2. **Análise de incidentes e do cibercrime** – a importância da engenharia social;
3. **Conhecer a engenharia social** para melhor nos defendermos.

Alguma vez foi contactado por um príncipe da Nigéria?

HELLO Inbox x

Masinga Mbeki <masinga.mbeki@laposte.net> Unsubscribe

to me

Dear Sir,
I am prince Masinga Mbeki from Nigeria. Your help would be very appreciated.
I want to transfer all of my fortune outside if Nigeria due to a frozen account.
If you could be so kind and transfer a small sum of 3 500 USD to my account,
I would be able to unfreeze my account and transfer my money outside of
Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

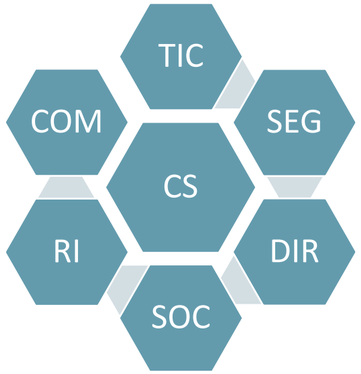
Please contact me to proceed

Prince Masinge Mbeki

1. A componente social da cibersegurança

Visão holística da Cibersegurança

A cibersegurança relaciona-se com **vários setores** e **disciplinas**



A. Tem implicações no **TODO SOCIAL**:

serviços essenciais, administração pública, empresas, indivíduos.

B. Convoca **VÁRIAS ÁREAS DISCIPLINARES**:

tecnologias de informação e comunicação, segurança, direito, economia, sociologia, psicologia, comunicação, relações internacionais …

CNCS

Domínios de desenvolvimento em Cibersegurança (Cyberwatching)

Áreas de desenvolvimento na cibersegurança horizontais e verticais – Cyberwatching (Fovino *et al*., 2019)

Engenharia social: componente social da cibersegurança enquanto ato de manipulação

O que é a engenharia social?

“O ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança.”

NIST Digital Identity Guidelines. 2017

2. Análise de incidentes e do cibercrime – a importância da engenharia social

Incidentes e cibercrime
principais números

2019/2020	**aumento** de 79% no nº de incidentes registados pelo CERT.PT (S/V) (CNCS, 2021a)
	aumento de 27% no nº de crimes informáticos participados (RASI, 2021)
	aumento de 183% no nº de denúncias ao Gabinete de Cibercrime do MP (PGR, 2021)
	+ 101% no nº de **incidentes** registados pelo CERT.PT no **primeiro semestre** de 2020 face ao mesmo período de 2019 (CNCS, 2020)
2020/2021	**+ 23%** no nº de **incidentes** registados pelo CERT.PT no **primeiro semestre** de 2021 face ao mesmo período de 2020 (CNCS, 2021b)
2009/2020	**+ percentagem**, de **0,6% em 2009 para 7,4% em 2020**, de crimes informáticos e relacionados a informática, entre todos os crimes participados no país (CNCS, 2021a)

Tipos de incidentes registados **pelo CERT.PT** *2019-2020* (TOP 10)

Relevância clara do ***phishing/smishing***

2019				2020*					Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	% *C/V*	% *S/V*	Tendência absoluta %	Lugar RK
1º	*Phishing/smishing*	236	31	1º	*Phishing/smishing*	613	43	46	+ 160	=
2º	Infeção (*malware*)	123**	16	2º	Sistema infetado (*malware*)	169	12	13	+ 37	=
3º	Compromisso de Conta	95	13	3º	Distribuição de *malware*	119	8	9	+ 116	+
4º	Exp. de vuln. (intrusão)	58	8	4º	Compromisso de conta não privilegiada	111	8	8	N/A	N/A
5º	Distribuição (*malware*)	55	7	5º	Acesso não autorizado	58	4	4	+ 867	+
6º	Tentativa de *login*	30	4	6º	Compromisso de aplicação	55	4	4	N/A	N/A
7º	*Scan*	28	4	7º	Sistema vulnerável (vulnerabilidade)	41	3	N/A	N/A	N/A
8º	DoS/DDoS	27	4	8º	Utilização Ilegítima de nome de terceiros	32	2	2	+ 68	+
9º	Utilização ilegítima de nome de terceiros	19	3	9º	Indeterminado (outro)	28	2	2	+ 65	+
10º	Exp. de vuln. (tentativa de intrusão)	18	2	10º	Tentativa de *login*	26	2	2	- 13	-

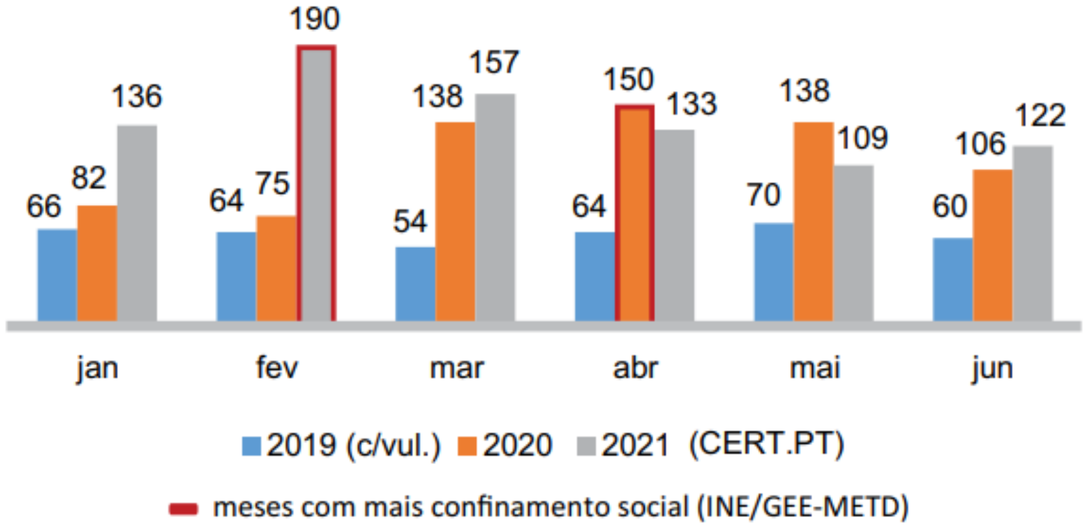
* Devido às alterações efetuadas na taxonomia adotada pelo CERT.PT (RNCSIRT, 2020), optou-se por não comparar tipos de incidentes que antes cobriam apenas um (compromissos de conta e de aplicação) ou as vulnerabilidades.
** Dos quais, 24 são de *ransomware*. Com as alterações à taxonomia, o *ransomware* passou a ser identificado com o tipo "Modificação não autorizada", perfazendo 18 casos em 2020, menos 6 do que no ano anterior. Contudo, muitos dos casos de *ransomware*, devido ao seu caráter criminal mais evidente, não são reportados diretamente ao CERT.PT, mas sim às autoridades.

Tabela 2 | CERT.PT

(CNCS, 2021a)

Nº de incidentes registados pelo **CERT.PT**
1º semestre de 2019, 2020 e 2021, e picos de confinamento social

"Os períodos de estado de emergência (de março a maio de 2020 e de novembro de 2020 a abril de 2021) e em particular os de recolhimento geral coincidem com as curvas ascendentes em termos de registos de incidentes por parte do CERT.PT, tendência já identificada em 2020 e que permanece em 2021"
(Boletim 4/2021, CNCS)



(CNCS, 2021b)

O caso do *phishing/smishing*, em Portugal
ações solicitadas pelos atacantes

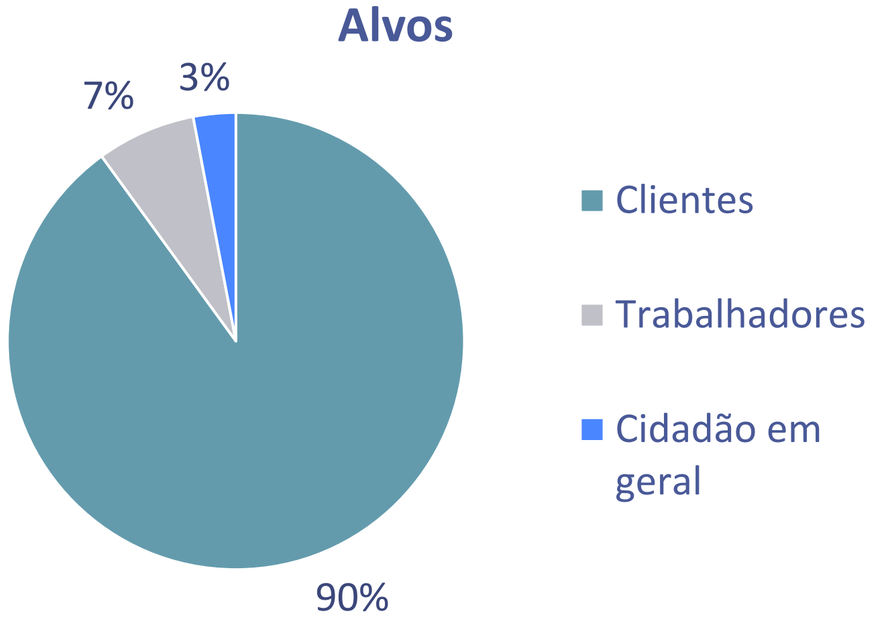
Análise de *conteúdo* ao *phishing/smishing* registado pelo CERT.PT durante o 2º trimestre de 2020 (160 incidentes)

99% dos casos **não referem a temática da pandemia** diretamente.

Os casos de *phishing/smishing* analisados solicitam ações específicas:

- 79% incentivam o ***login* numa conta;**
- 12% **pedem dados** relacionados a um produto/serviço;
- 7% prometem um **ganho financeiro;**
- 3% referem-se ao **preenchimento de um documento.**

Outros aspetos: 3% são *spear phishing* e 94% pedem para clicar num URL.



(CNCS, 2020)

O caso do *phishing/smishing*, em Portugal
técnicas de persuasão

Considerando os **6 princípios de persuasão** de Cialdini (2006) (autoridade, escassez, reciprocidade, consistência, afinidade e prova social)**:**

1º Autoridade (90%), comum no *phishing/smishing* bancário;

2º A **escassez** de uma oferta como uma oportunidade (8%), frequente na venda de produtos e serviços;

3º Casos em que se apela a uma **reciprocidade**, à retribuição por um favor/benefício prestado (1%), situações em que se promove a interação social.

Não se verifica a presença dos outros 3 princípios em qualquer dos incidentes de *phishing/smishing*.

Autoridade, Santander

Escassez, CTT

(CNCS, 2020)

Outros casos de engenharia social

Os casos categorizados como engenharia social **(13% do total)** pelo CERT.PT no 1º semestre de 2021 e respetiva vulnerabilidade humana explorada:

1. Sextortion (49%):	o medo da exposição excessiva da intimidade;
2. CEO Fraud (12%):	a crença na autoridade do pedido de um chefe sem que a vítima se “atreva” a verificar esse pedido;
3. Burla de caso fictício de herança (11%);	a disponibilidade para o outro quando este traz uma notícia positiva, como dinheiro;
4. Burla com MBWay (7%);	a falta de literacia digital quanto ao funcionamento de uma plataforma tecnológica.
5. Outros (21%)	

(CNCS, 2021b)

3. Conhecer a engenharia social para melhor nos defendermos

Cadeia de ataque de engenharia social 1/2

Ataque dirigido (centrado na pessoa)

Recolha de informação	Criação de "(pre)texto"	Planeamento de vetores de ataque	Ataque	Benefício
Redes socias, Motores de busca, Documentos disponíveis, Sites de vendas, OSINT	Enquadramento que simula uma realidade: o CEO a solicitar transferência; *stakeholder* a pedir dados sensíveis	*Spear phishing, vishing, smishing, malware,* técnicas de persuasão	Realização da ação de manipulação	Transferência bancária; dados pessoais; segredos industriais; informação sensível

(Adaptado de Hadnagy, 2018)

O caso da simulação de voz através de IA

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

Em 2019, o CEO de uma empresa de energia no UK recebeu uma **chamada**, supostamente, do seu chefe, o diretor executivo da empresa-mãe, na Alemanha, que lhe **pediu para transferir os fundos** respeitantes a um fornecedor húngaro, cerca de 220 mil euros. O autor da chamada disse que o pedido era **urgente** e que a transferência deveria ser feita numa hora.

Foi utilizada **IA para simular a voz original (*deepfake*)** do diretor executivo, com sotaque incluído. A voz original pode, muitas vezes, ser encontrada *online* em vídeos publicados – **PESCA À LINHA**.

Recolha de informação: vídeos *online;* redes sociais; *website* (possivelmente).

(Pre) texto: superior hierárquico a pedir transferência urgente.

Vetor de ataque: *vishing* e argumentos da escassez e autoridade.

CNCS

Fonte: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Cadeia de ataque de engenharia social 2/2

Ataque massificado (centrado na marca simulada)

Recolha de informação	Criação de "(pre)texto"	Planeamento de vetores de ataque	Ataque	Benefício
Website da organização a simular; meios e conteúdos de comunicação usados por esta disponíveis *online*	Enquadramento que simula uma realidade: bloqueio de credenciais de banco; ativação de conta de *streaming*; prémio a reclamar; imagens íntimas (*sextortion*)	*Phishing, vishing, smishing, malware,* técnicas de persuasão	Realização da ação de manipulação	Transferência bancária; dados pessoais; credenciais

(Adaptado de Hadnagy, 2018)

O caso do *smishing* bancário

SMS enviados massivamente, de modo indiscriminado, numa lógica de **PESCA À REDE**, em 2021, em nome do Novo Banco, solicitando clique e/ou dados.

Recolha de informação: imagem do Novo Banco *online.*

(Pre)texto: bloqueio de dados de acesso.

Vetor de ataque: *smishing* e argumentos da escassez e autoridade.

Fonte: https://www.novobanco.pt/seguranca/alertas-fraude

Caso MISTO da fraude com MBway

1º Um burlão contacta um vendedor OLX e confirma que quer comprar um artigo.

2º E pergunta ao vendedor se pode fazer o pagamento através da funcionalidade MBway - "Enviar dinheiro".

3º O burlão usa a funcionalidade "Pedir dinheiro" em vez de "Enviar dinheiro".

4º O vendedor recebe uma notificação MBway que lhe pede para "Enviar Dinheiro" e carrega em "Enviar dinheiro" por erro. Assim, paga em vez de receber.

Noutros casos, o vendedor é conduzido a associar o nº de telemóvel do burlão à plataforma MBway do vendedor, permitindo que o burlão controle a mesma.

Recolha de informação: *website* do OLX.

(Pre)texto: compra de produto *online*.

Vetor de ataque: *vishing* e argumento da autoridade (com base na falta de literacia digital).

Adaptado de https://help.olx.pt/hc/pt/articles/360006716518-Como-evitar-fraudes-com-o-MB-Way

O que fazer

Aprender a identificar a engenharia social

- Desconfiança metodológica, triangulação da informação, oportunidade da mensagem, correção formal.

Desenvolver **políticas de segurança**

- Identificar as ameaças, as respetivas boas práticas e integrá-las na política de segurança da informação.

Verificar

- Lançar simulações de *phishing* e fazer *pentest* de engenharia social.

Lançar **programas** de sensibilização

- Educar através de estratégias de sensibilização atualizadas.

CNCS

(Adaptado de Hadnagy, 2018)

Notas conclusivas

- **A componente social da cibersegurança é central** quando definimos as boas práticas e procuramos a melhor proteção possível contra as ameaças do ciberespaço;

- Os dados do Observatório de Cibersegurança mostram que as técnicas de **engenharia social** são chave no sucesso de uma parte substancial dos incidentes de cibersegurança e no cibercrime;

- É importante **conhecer as técnicas** de engenharia social de modo a nos protegermos e desconfiarmos q.b. das abordagens que nos fazem *online* ou por telemóvel.

Contactos em caso de ser vítima:

CNCS: cert@cert.pt

PGR: cibercrime@pgr.pt

PJ: unc3t@pj.pt

Referências

Cialdini, R. (2006) *Influence: The Psychology of Persuasion*. HarperCollins.
CNCS (2020) *Boletim 03/2020*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.
CNCS (2021a) *Relatório Cibersegurança em Portugal – Riscos e Conflitos 2021*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.
CNCS (2021b) *Boletim 04/2021*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.
Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., (2019) *A Proposal for a European Cybersecurity Taxonomy*, Publications Office of the European Union, Luxembourg, doi:10.2760/106002 (online), JRC118089.
NIST (2017) *Digital Identity Guidelines*. NIST.
Hadnagy, C. (2018) *Social Engineering: The Science of Human Hacking*. Wiley
PGR (2021) *Nota Informativa Cibercrime: Denúncias Recebidas 2020*, Procuradoria-Geral da República, Gabinete Cibercrime.
RASI (2021) *Relatório Anual de Segurança Interna 2020*. Sistema de Segurança Interna.

Observatório de Cibersegurança: https://www.cncs.gov.pt/pt/observatorio/

OBRIGADO

Contacto: pedro.mendonca@cncs.gov.pt

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL