Nome: _____ **Data:** _____ **Pontuação:** _____

Burlas online e engenharia social Guia de proteção

Phishing por e-mail, domínios falsificados, vishing, burlas de apoio técnico, verificação fora de banda, BEC

VISÃO GERAL DA APRENDIZAGEM SOBRE BURLAS ONLINE

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pela defesa contra burlas online. Vais explorar sites de phishing falsos, táticas de engenharia social, burlas de suporte técnico, vetores de fraude por transferência bancária e métodos de verificação de pagamentos.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/golpes-online/

O teu roteiro de aprendizagem sobre proteção contra burlas online

- Identifica indicadores comuns de burlas de suporte técnico e de domínios com erros de digitação (typosquatting).
- Implementa protocolos de verificação de email (SPF, DKIM, DMARC) contra a falsificação.
- Estabelece a verificação de transações fora de banda para evitar a fraude em transferências bancárias empresariais.

INSTRUÇÕES DO GUIA SOBRE BURLAS ONLINE

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à proteção contra burlas em linha. Termina com a atividade bónus Pensa rápido.

PROTEÇÃO CONTRA BURLAS ONLINE E ENGENHARIA SOCIAL (INTRODUÇÃO)

As burlas online exploram o comportamento humano através de phishing, pop-ups de suporte, vishing e fraude por transferência bancária. Aplicar a verificação de transações fora de banda e as regras de domínio SPF/DKIM/DMARC ajuda a bloquear os vetores de engenharia social à entrada.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é o principal indicador de uma burla de suporte técnico?

- A. Uma janela pop-up que afirma que o teu sistema está infetado e exige que ligues para um número de telefone
- B. Uma atualização de segurança automática transferida de um registo oficial
- C. Um gestor de palavras-passe que se recusa a preencher credenciais num domínio corporativo
- D. Uma cópia de segurança de ficheiros em segundo plano numa configuração de unidade externa

2. Que técnica usa domínios de remetente falsificados para roubar dados bancários?

- A. Phishing por e-mail
- B. Análise de portas
- C. Injeção de memória
- D. Destruição criptográfica

3. O que representa a fraude por transferência bancária?

- A. Enganar as vítimas, através de engenharia social, para enviarem dinheiro para contas empresariais falsas
- B. Encriptar bases de dados do sistema usando payloads de ransomware
- C. Consultar bases de dados através de comandos de injeção de SQL
- D. Fazer cópias de segurança de ficheiros do sistema para discos de armazenamento offline

4. Porque é que os burlões criam lojas online falsas?

- A. Roubar dados de cartões de crédito e credenciais de pagamento dos compradores
- B. Alojar tabelas de bases de dados de análise de software malicioso em sandbox
- C. Para acelerar a entrega de encomendas online
- D. Para testar gratuitamente novos designs de sites

5. O que significa vishing?

- A. Burlas de phishing por voz através de redes telefónicas para roubar credenciais
- B. Analisar redes locais à procura de dispositivos de sistema não protegidos
- C. Restaurar bases de dados do sistema após uma violação não autorizada
- D. Executar código não confiável dentro de contentores virtuais seguros

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. As burlas de phishing visam apenas utilizadores finais, nunca alvos executivos de whaling.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Os domínios falsificados usam muitas vezes pequenos erros de digitação (como amaz0n.com) para imitar marcas de confiança.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. As burlas de suporte técnico podem ser resolvidas concedendo acesso remoto a quem telefona.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. A engenharia social explora a psicologia humana, como o medo e a urgência, para contornar regras de segurança.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Os pedidos de transferência bancária devem ser sempre verificados através de canais de comunicação fora de banda.

○ Verdadeiro ○ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Os e-mails fraudulentos que enganam os utilizadores chamam-se _____ .

2. Os endereços web que imitam marcas de confiança são _____ .

3. As burlas por voz que visam dados bancários chamam-se _____ .

4. Uma janela pop-up que exige dinheiro para remover vírus é uma _____ de suporte técnico.

5. Confirmar um pedido de pagamento exige _____ por um canal externo.

6. O redirecionamento de transações comerciais para contas de ladrões é fraude por _____ bancária.

BANCO DE PALAVRAS DE VOCABULÁRIO

BURLA FALSIFICADOS PHISHING SMISHING TRANSFERÊNCIA VERIFICAÇÃO VISHING WHALING

Escreve aqui as tuas respostas:

1.
2.
3.
4.
5.
6.

Ponto de controlo 4: Associação de conceitos de segurança

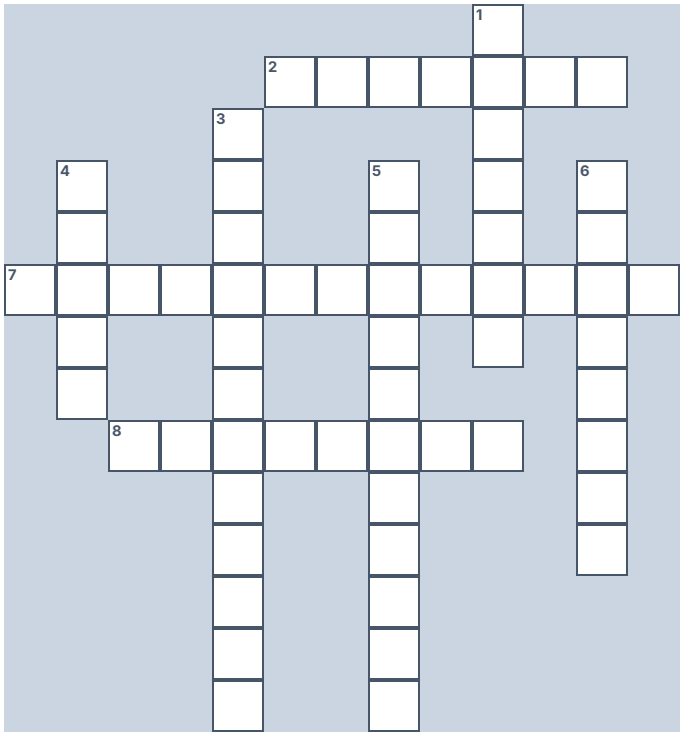
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. PHISHING	A	Redirecionamento fraudulento de transações bancárias para contas de criminosos.
☐	2. FALSIFICADO	B	Esquema fraudulento concebido para roubar dinheiro ou credenciais de acesso às vítimas.
☐	3. VISHING	C	Enviar mensagens de texto fraudulentas para roubar credenciais de contas móveis.
☐	4. FRAUDE	D	Chamadas de voz fraudulentas concebidas para roubar credenciais e dados de contas.
☐	5. VERIFICAÇÃO	E	Ataques de phishing direcionados com o objetivo de roubar credenciais a executivos de topo (C-level).
☐	6. WIRE	F	Remetente de email ou endereço de site imitado, concebido para parecer legítimo.
☐	7. WHALING	G	Campanhas de email fraudulentas concebidas para roubar credenciais de início de sessão e palavras-passe.
☐	8. SMISHING	H	Confirmar os dados de pagamento através de um método de contacto secundário de confiança.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

2. Ataques de phishing direcionados que visam roubar credenciais a executivos de topo. (7)

7. Redirecionamento fraudulento de transações bancárias para contas criminosas. (13)

8. Envio de mensagens de texto fraudulentas para roubar credenciais de contas móveis. (8)

VERTICAIS

1. Chamadas de voz fraudulentas concebidas para roubar credenciais e dados de contas. (7)

3. Endereço de remetente de e-mail ou de site imitado para parecer legítimo. (12)

4. Esquema fraudulento concebido para roubar dinheiro ou credenciais de acesso às vítimas. (5)

5. Confirmar os dados de pagamento através de um método de contacto secundário de confiança. (11)

6. Campanhas fraudulentas de e-mail concebidas para roubar credenciais de início de sessão e palavras-passe. (8)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

2 horizontal: Ataques de phishing direcionados que visam roubar credenciais a executivos de topo. (7 letras):

7 horizontal: Redirecionamento fraudulento de transações bancárias para contas criminosas. (13 letras):

8 horizontal: Envio de mensagens de texto fraudulentas para roubar credenciais de contas móveis. (8 letras):

VERTICAIS

1 vertical: Chamadas de voz fraudulentas concebidas para roubar credenciais e dados de contas. (7 letras):

3 vertical: Endereço de remetente de e-mail ou de site imitado para parecer legítimo. (12 letras):

4 vertical: Esquema fraudulento concebido para roubar dinheiro ou credenciais de acesso às vítimas. (5 letras):

5 vertical: Confirmar os dados de pagamento através de um método de contacto secundário de confiança. (11 letras):

6 vertical: Campanhas fraudulentas de e-mail concebidas para roubar credenciais de início de sessão e palavras-passe. (8 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

S C G M Z Y G Y O W U K V P B
O N N V G N I H S I H P T M W
D G I V D Y U K R B X Z Y H M
A R H Q X I P D A D J Q A V W
C W S L J H T H G B E L I K T
I S I V R Z E H E S I C A L Q
F C M Z M K V R U N A S W J M
I M S H H N H R G A L R U B F
S K T L R W H B U F Y O Y W S
L H T X A P U N V I S H I N G
A T R A N S F E R E N C I A N
F Z O I Q T I P V U O U U K A
E P V E R I F I C A C A O M K
A N V G G P Q X Y J K V J Y W
Y P J I Z I J N A E I A S A J

LISTA DE PALAVRAS DE VOCABULÁRIO

PHISHING FALSIFICADOS VISHING BURLA VERIFICACAO TRANSFERENCIA WHALING SMISHING

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO
A. PHISHING
B. FALSIFICADOS
C. VISHING
D. BURLA
E. VERIFICACAO
F. TRANSFERENCIA
G. WHALING
H. SMISHING

	DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO
	1. Endereço de remetente de e-mail ou de site imitado para parecer legítimo.
	2. Confirmar os dados de pagamento através de um método de contacto secundário de confiança.
	3. Redirecionamento fraudulento de transações bancárias para contas criminosas.
	4. Envio de mensagens de texto fraudulentas para roubar credenciais de contas móveis.
	5. Ataques de phishing direcionados que visam roubar credenciais a executivos de topo.
	6. Chamadas de voz fraudulentas concebidas para roubar credenciais e dados de contas.
	7. Campanhas fraudulentas de e-mail concebidas para roubar credenciais de início de sessão e palavras-passe.
	8. Esquema fraudulento concebido para roubar dinheiro ou credenciais de acesso às vítimas.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. NSHPIHGI
2. VSGNIHI
3. VCIAREAOFCI
4. GHILNWA
5. ADCISLIAFFOS
6. LBRAU
7. NCRFTRESAIAEN
8. SMHGSNII

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Dispositivos que podem ser hackeados			
2	Frases que os burlões costumam usar			
3	Métodos de pagamento que os burlões pedem			
4	Tipos de burlas online			
5	Ofertas boas demais para serem verdade			
6	Locais onde denunciar uma burla			
7	Palavras relacionadas com cibersegurança			
8	Pessoas que podes avisar sobre burlas			
9	Coisas de que fazes cópia de segurança			
10	Sinais de alerta num email			
11	Sinais de que um computador está infetado			
12	Formas de verificar uma loja online			
13	Formas de proteger as tuas contas			
14	Coisas a fazer se fores burlado			
15	Coisas a fazer depois de uma fuga de dados			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: PREVENÇÃO DE BURLAS DE TRANSFERÊNCIAS BANCÁRIAS EMPRESARIAIS

👷

Cenário: O departamento financeiro recebe um email urgente de um endereço de fornecedor falsificado, a pedir que as futuras transferências de faturas sejam dirigidas para um novo número de encaminhamento.

Questão para debate: Descreve a política de verificação contra fraude por transferência bancária e indica os mecanismos de autenticação de email.

ESTUDO DE CASO 2: INCIDENTE DE PHISHING DE WHALING CONTRA EXECUTIVOS

👷

Cenário: Um executivo clicou numa ligação de phishing que afirmava conter um documento seguro de uma reunião do conselho de administração e introduziu as suas credenciais empresariais principais num portal falsificado.

Questão para debate: Detalha os passos de resposta ao incidente e explica como auditar os inícios de sessão dos executivos.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

4	5	20	5	20	1		15		16	8	9	19	8	9	14	7		3	15	13
			22	5	18	9	6	9	3	1	3	1	15		4	5				
						13	5	14	19	1	7	5	14	19						

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é uma burla online?

Um esquema fraudulento que usa canais digitais para levar as vítimas a enviar dinheiro ou a revelar credenciais pessoais.

Q2: Qual é o principal indicador de phishing por e-mail?

Uma mensagem que alega urgência (como a suspensão da conta) e te encaminha para uma ligação que não corresponde ao domínio oficial.

Q3: O que é o typosquatting?

Registar domínios com erros ortográficos comuns de marcas populares (como amaz0n.com) para alojar sites de phishing falsos.

Q4: O que é uma burla de falso apoio técnico?

Uma janela pop-up que afirma que o teu PC está infetado, levando-te a ligar para um número e a pagar por software de limpeza falso ou serviços de acesso remoto. [1]

Q5: O que é o vishing?

Ataques de phishing que usam chamadas telefónicas de voz para enganar as vítimas e levá-las a fornecer dados bancários ou de início de sessão.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: O que significa fraude eletrónica (wire fraud)?

Redirecionamento de transações de pagamento para contas fraudulentas através da usurpação da identidade de fornecedores ou executivos.

Q7: O que é o whaling?

Uma forma altamente direcionada de spear phishing que visa diretamente alvos de elevado valor, como quadros executivos de topo de empresas.

Q8: O que é o smishing?

Mensagens de texto fraudulentas enviadas para dispositivos móveis, com ligações que levam a portais falsos ou a falsas atualizações de rastreio.

Q9: Porque é crítica a verificação fora de banda?

Confirma os detalhes da transação através de um canal de comunicação separado (como uma chamada telefónica), evitando cadeias de email comprometidas.

Q10: Como funciona uma burla de escrow falso?

Os burlões criam um site de conta de garantia (escrow) falsificado, afirmam que os fundos estão retidos em segurança e depois roubam o depósito por transferência do comprador.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como usam os burlões o BEC (Business Email Compromise) para executar fraude por transferência bancária?

Sequestram a conta de e-mail de um funcionário legítimo, monitorizam as conversas de faturas e enviam dados de faturação atualizados com contas bancárias fraudulentas.

Q2: Qual é o risco dos ataques homógrafos IDN em burlas online?

Usar carateres não ASCII que parecem idênticos a letras normais (por exemplo, o 'a' cirílico) para registar domínios falsificados que imitam marcas reais.

Q3: Porque é que a inspeção dos cabeçalhos de correio eletrónico é importante na deteção de burlas?

Revela o IP real do servidor de origem e o estado da validação SPF/DKIM, mostrando se o domínio do remetente é falsificado.

Q4: Como exploram os burlões de falso apoio técnico o software de ambiente de trabalho remoto?

Usam utilitários como o AnyDesk ou o TeamViewer para se ligarem ao dispositivo da vítima, instalar malware e roubar palavras-passe guardadas.

Q5: Qual é o objetivo das burlas de pagamento antecipado?

Enganar as vítimas para que paguem taxas de processamento antecipadamente em troca de uma grande recompensa financeira que não existe.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: Como usam os burlões a definição de perfis em redes sociais para phishing direcionado?

Compilam estruturas organizacionais de empresas e nomes de funcionários para redigir e-mails de spear phishing convincentes.

Q7: Porque oferecem as lojas Web falsas descontos muito elevados?

Para atrair compradores a introduzir os dados do cartão de crédito, capturando credenciais para reutilização ou revenda em fóruns de carding.

Q8: Como bloqueiam os registos DMARC as burlas de phishing?

O DMARC permite que os proprietários de domínios peçam aos recetores que ponham em quarentena ou rejeitem o correio que falhe as verificações alinhadas de SPF e DKIM, bloqueando a falsificação direta. [5]

Q9: Qual é a ameaça dos portais de recolha de credenciais?

Páginas de destino falsificadas, concebidas para parecerem exatamente espaços de trabalho do Microsoft 365 ou da Google, que roubam as credenciais de início de sessão à medida que são introduzidas.

Q10: Como é que as equipas de segurança comunicam e desativam domínios de burla?

Submetendo provas de fraude ao email de abusos do registador, ao fornecedor de alojamento e ao registo Google Safe Browsing.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

O phishing e a falsificação (spoofing) foram o tipo de crime mais comunicado ao IC3 do FBI em 2025, com 191,561 queixas. [2]

2. PERSPETIVA SOBRE SEGURANÇA

O comprometimento de email empresarial (BEC) causou mais de $3 mil milhões em perdas comunicadas ao IC3 do FBI em 2025. [2]

3. PERSPETIVA SOBRE SEGURANÇA

Os domínios typosquatting diferem dos nomes reais das marcas num ou dois carateres, pelo que um olhar rápido pode não os detetar.

4. PERSPETIVA SOBRE SEGURANÇA

As burlas de suporte técnico causaram mais de 2,1 mil milhões de dólares em perdas comunicadas ao IC3 do FBI em 2025. [2]

5. PERSPETIVA SOBRE SEGURANÇA

Os ataques homógrafos parecem idênticos nas barras de endereço dos navegadores, a menos que o navegador apresente as configurações em punycode.

6. PERSPETIVA SOBRE SEGURANÇA

As burlas por mensagem SMS (smishing) usam mensagens curtas e urgentes com ligações, deixando às vítimas pouco contexto para detetar a fraude.

7. PERSPETIVA SOBRE SEGURANÇA

Os ataques de whaling visam os e-mails de executivos porque estes controlam o acesso a grandes transferências bancárias.

8. PERSPETIVA SOBRE SEGURANÇA

Verificar as alterações de pagamento ligando para um número de telefone conhecido e guardado é uma defesa essencial contra a fraude de transferências BEC.

9. PERSPETIVA SOBRE SEGURANÇA

Os sites falsos de contas de garantia (escrow) são uma burla comum nos mercados online: parecem um serviço de pagamento seguro, mas roubam a transferência bancária do comprador.

10. PERSPETIVA SOBRE SEGURANÇA

O Google Safe Browsing avisa os utilizadores antes de abrirem sites que sinalizou por phishing ou software malicioso.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Qual é o principal indicador de uma burla de suporte técnico? → Uma janela pop-up que afirma que o teu sistema está infetado e exige que ligues para um número de telefone

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

Que técnica usa domínios de remetente falsificados para roubar dados bancários? → Phishing por e-mail

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

O que representa a fraude por transferência bancária? → Enganar as vítimas, através de engenharia social, para enviarem dinheiro para contas empresariais falsas

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Porque é que os burlões criam lojas online falsas? → Roubar dados de cartões de crédito e credenciais de pagamento dos compradores

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que significa vishing? → Burlas de phishing por voz através de redes telefónicas para roubar credenciais

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Falso: o phishing também visa executivos; o whaling é phishing dirigido a dirigentes de topo.

7 **Pergunta 7** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os domínios falsificados usam muitas vezes pequenos erros de digitação (como amaz0n.com) para imitar marcas de confiança.

8 **Pergunta 8** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Falso: dar acesso remoto a um burlão de falso apoio técnico permite-lhe instalar malware e roubar dados.

9 **Pergunta 9** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A engenharia social explora a psicologia humana, como o medo e a urgência, para contornar regras de segurança.

10 **Pergunta 10** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os pedidos de transferência bancária devem ser sempre verificados através de canais de comunicação fora de banda.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

G 1. PHISHING	F 2. FALSIFICADO	D 3. VISHING	B 4. FRAUDE
H 5. VERIFICAÇÃO	A 6. WIRE	E 7. WHALING	C 8. SMISHING

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 PHISHING	2 FALSIFICADOS	3 VISHING	4 BURLA
5 VERIFICAÇÃO	6 TRANSFERÊNCIA		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 B – FALSIFICADOS	2 E – VERIFICACAO	3 F – TRANSFERENCIA	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – BURLA

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar PHISHING, FALSIFICADO e VISHING por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

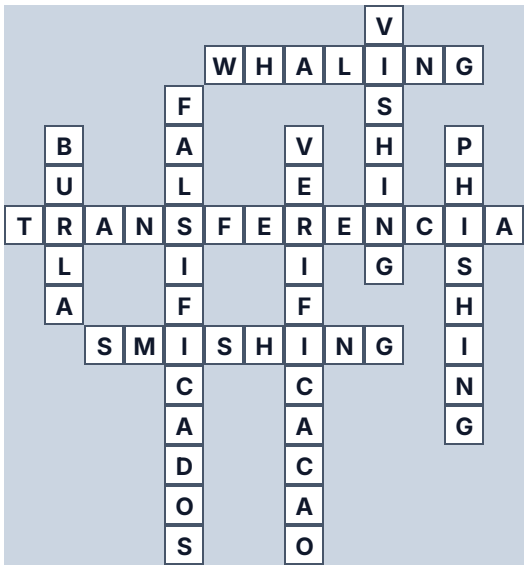
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

S	C	G	M	Z	Y	G	Y	O	W	U	K	V	P	B
O	N	N	V	G	N	I	H	S	I	H	P	T	M	W
D	G	I	V	D	Y	U	K	R	B	X	Z	Y	H	M
A	R	H	Q	X	I	P	D	A	D	J	Q	A	V	W
C	W	S	L	J	H	T	H	G	B	E	L	I	K	T
I	S	I	V	R	Z	E	H	E	S	I	C	A	L	Q
F	C	M	Z	M	K	V	R	U	N	A	S	W	J	M
I	M	S	H	H	N	H	R	G	A	L	R	U	B	F
S	K	T	L	R	W	H	B	U	F	Y	O	Y	W	S
L	H	T	X	A	P	U	N	V	I	S	H	I	N	G
A	T	R	A	N	S	F	E	R	E	N	C	I	A	N
F	Z	O	I	Q	T	I	P	V	U	O	U	U	K	A
E	P	V	E	R	I	F	I	C	A	C	A	O	M	K
A	N	V	G	G	P	Q	X	Y	J	K	V	J	Y	W
Y	P	J	I	Z	I	J	N	A	E	I	A	S	A	J

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: WHALING Ataques de phishing direcionados que visam roubar credenciais a executivos de topo. (7 letras)

7 horizontal: TRANSFERENCIA Redirecionamento fraudulento de transações bancárias para contas criminosas. (13 letras)

8 horizontal: SMISHING Envio de mensagens de texto fraudulentas para roubar credenciais de contas móveis. (8 letras)

VERTICAIS

1 vertical: VISHING Chamadas de voz fraudulentas concebidas para roubar credenciais e dados de contas. (7 letras)

3 vertical: FALSIFICADOS Endereço de remetente de e-mail ou de site imitado para parecer legítimo. (12 letras)

4 vertical: BURLA Esquema fraudulento concebido para roubar dinheiro ou credenciais de acesso às vítimas. (5 letras)

5 vertical: VERIFICACAO Confirmar os dados de pagamento através de um método de contacto secundário de confiança. (11 letras)

6 vertical: PHISHING Campanhas fraudulentas de e-mail concebidas para roubar credenciais de início de sessão e palavras-passe. (8 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. NSHPIHGI — **PHISHING**
2. VSGNIHI — **VISHING**
3. VCIAREAOFCI — **VERIFICACAO**
4. GHILNWA — **WHALING**
5. ADCISLIAFFOS — **FALSIFICADOS**
6. LBRAU — **BURLA**
7. NCRFTRESAIAEN — **TRANSFERENCIA**
8. SMHGSNII — **SMISHING**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"DETETA O PHISHING COM VERIFICACAO DE MENSAGENS"

Soluções dos estudos de caso

A Estudo de caso 1: Prevenção de burlas de transferências bancárias empresariais

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um departamento financeiro recebe um email urgente de um endereço de fornecedor falsificado, a pedir que as futuras transferências de faturas sejam dirigidas para um novo número de encaminhamento.
- Estratégia e solução recomendadas: Aplicar uma política de dupla autorização a todos os pagamentos. Implementar verificação fora de banda através de um número de telefone previamente guardado e bloquear na gateway os emails de domínios falsificados.

B Estudo de caso 2: Incidente de phishing de whaling contra executivos

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Um executivo clicou numa ligação de phishing que dizia conter um documento seguro de uma reunião de administração e introduziu as suas credenciais empresariais principais num portal falsificado.
- Estratégia e solução recomendadas: Isolar o dispositivo do executivo. Repor todos os tokens de sessão e credenciais da empresa. Rever os registos de acesso à procura de saída de dados e implementar MFA por hardware em todos os inícios de sessão.