Nome: _____ Data: _____ Pontuação: _____

# Ataques de phishing e engenharia social

Spear phishing, burlas de whaling, protocolos SPF/DKIM/DMARC, falsificação de remetente e formação de funcionários em segurança.

## VISÃO GERAL DA APRENDIZAGEM SOBRE ATAQUES DE PHISHING

**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 pelos ataques de phishing e pela engenharia social. Vais explorar spear phishing, whaling, falsificação de domínios, protocolos SPF/DKIM/DMARC, segurança de ligações e formação de sensibilização dos colaboradores.

### 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/ataques-phishing/

# O teu roteiro de aprendizagem sobre mitigação de phishing

- Identifica burlas comuns de phishing, vishing e de pop-ups de suporte.
- Implementa procedimentos de verificação de transações fora de banda.
- Configura regras SPF, DKIM e DMARC para bloquear domínios falsificados.

## INSTRUÇÕES DO GUIA SOBRE ATAQUES DE PHISHING

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 autenticação de email. Termina com a atividade bónus Pensa rápido.

## ATAQUES DE PHISHING E ENGENHARIA SOCIAL (INTRODUÇÃO)

Os ataques de phishing usam mensagens direcionadas, burlas de whaling e falsificação de domínios para recolher as credenciais de início de sessão dos utilizadores. Proteger os sistemas empresariais exige implementar regras SPF, DKIM e DMARC à entrada, juntamente com passos de aprovação fora de banda.

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

## Ponto de controlo 1: Desafio de escolha múltipla

**1. O que é o spear phishing?**

- A. Um e-mail de phishing direcionado, adaptado a uma pessoa ou organização específica
- B. Um email em massa enviado a milhões de endereços aleatórios
- C. Um ataque de rede que inunda servidores web com tráfego
- D. Uma técnica de extração de bases de dados que visa registos de utilizadores

**2. Que protocolo permite a um domínio listar em DNS os seus endereços IP de envio autorizados para combater a falsificação?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

**3. O que é um ataque de whaling?**

- A. Uma campanha de phishing dirigida especificamente a quadros executivos de empresas de grande visibilidade
- B. Um ataque de injeção de SQL dirigido a cópias de segurança de bases de dados
- C. Um furto físico de equipamento de routers de rede local
- D. Uma análise automatizada de força bruta de credential stuffing

**4. O que faz o DKIM?**

- A. Acrescenta uma assinatura criptográfica aos e-mails para verificar a autenticidade do remetente
- B. Bloqueia o tráfego de pacotes de rede de entrada na firewall
- C. Encripta volumes de armazenamento de bases de dados em repouso
- D. Analisa anexos de e-mail à procura de malware baseado em assinaturas

**5. Qual é o papel do DMARC?**

- A. Indicar aos servidores de e-mail de receção como tratar as verificações SPF/DKIM falhadas
- B. Decifrar palavras-passe do sistema usando rainbow tables pré-calculadas
- C. Comprimir anexos de email antes da entrega
- D. Configurar privilégios de acesso ao encaminhamento de rede

## Ponto de controlo 2: Desafio de verdadeiro ou falso

### 6 Pergunta 6

6. O spear phishing baseia-se em emails genéricos em massa enviados para milhões de endereços aleatórios.

- ◯ Verdadeiro
- ◯ Falso

### 7 Pergunta 7

7. As políticas DMARC podem instruir os servidores de correio a rejeitar mensagens falsificadas não autorizadas.

- ◯ Verdadeiro
- ◯ Falso

### 8 Pergunta 8

8. A verificação SPF funciona validando a assinatura criptográfica do corpo do email.

- ◯ Verdadeiro
- ◯ Falso

### 9 Pergunta 9

9. Os ataques de whaling visam administradores empresariais de baixo nível para aceder a ficheiros de bases de dados.

- ◯ Verdadeiro
- ◯ Falso

### 10 Pergunta 10

10. A verificação fora de banda dos pedidos de pagamento ajuda a travar burlas de transferências bancárias.

- ◯ 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. Visar um funcionário específico com informação personalizada é phishing _____ .
2. Falsificar um cabeçalho de e-mail para que as mensagens pareçam legítimas é _____ de remetente.
3. A lista de registos DNS dos IP de servidores de correio autorizados é o _____ .
4. A norma de assinatura de e-mail que fornece a verificação do remetente é a _____ .
5. Estabelecer regras para rejeitar verificações SPF/DKIM falhadas recorre a uma _____ .
6. Uma campanha de phishing dirigida a executivos de topo chama-se _____ .

**BANCO DE PALAVRAS DE VOCABULÁRIO**

ASSINATURA DKIM MALWARE POLÍTICA DMARC RANSOMWARE REGISTO SPF SPEAR SPOOFING WHALING

**Escreve aqui as tuas respostas:**

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

# Ponto de controlo 4: Associação de conceitos de segurança

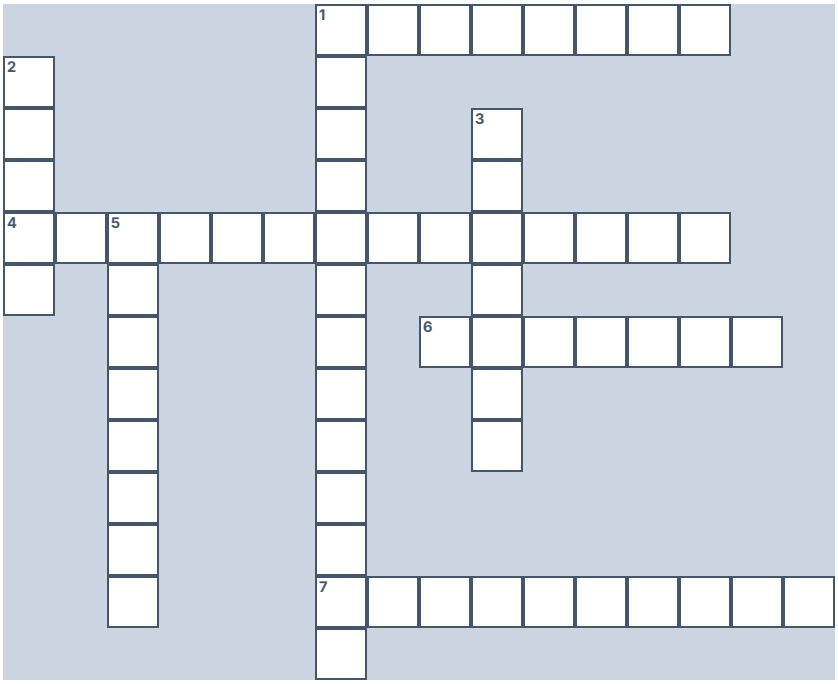
## ASSOCIAÇÃO DE DEFINIÇÕES

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

| | | | |
|---|---|---|---|
| ☐ | 1. SPEAR | A | Chamadas de burla por voz. |
| ☐ | 2. SPOOFING | B | Visar executivos de topo (C-level). |
| ☐ | 3. SPF | C | Instruções de rejeição de políticas. |
| ☐ | 4. DKIM | D | IP de remetentes autorizados por DNS. |
| ☐ | 5. DMARC | E | Email de engenharia social. |
| ☐ | 6. WHALING | F | E-mail personalizado e direcionado. |
| ☐ | 7. PHISHING | G | Falsificação do endereço de email do remetente. |
| ☐ | 8. VISHING | H | Assinatura criptográfica num e-mail. |

## Ponto de controlo 5: Palavras cruzadas

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



### HORIZONTAIS

**1. E-mail de engenharia social. (8)**

**4. Assinatura criptográfica no e-mail. (14)**

**6. Chamadas de burla por voz. (7)**

**7. IP de remetentes autorizados no DNS. (10)**

### VERTICAIS

**1. Instruções de rejeição definidas por política. (13)**

**2. E-mail personalizado e direcionado. (5)**

**3. Visa executivos de topo. (7)**

**5. Falsificação do endereço de e-mail do remetente. (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

**1 horizontal: E-mail de engenharia social. (8 letras):**

**4 horizontal: Assinatura criptográfica no e-mail. (14 letras):**

**6 horizontal: Chamadas de burla por voz. (7 letras):**

**7 horizontal: IP de remetentes autorizados no DNS. (10 letras):**

## VERTICAIS

**1 vertical: Instruções de rejeição definidas por política. (13 letras):**

**2 vertical: E-mail personalizado e direcionado. (5 letras):**

**3 vertical: Visa executivos de topo. (7 letras):**

**5 vertical: Falsificação do endereço de e-mail do remetente. (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.

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

**LISTA DE PALAVRAS DE VOCABULÁRIO**

SPEAR SPOOFING REGISTOSPF ASSINATURADKIM POLITICADMARC WHALING PHISHING VISHING

## 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 | DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO |
|---|---|
| A. SPEAR | _____ 1. Falsificação do endereço de e-mail do remetente. |
| B. SPOOFING | _____ 2. E-mail personalizado e direcionado. |
| C. REGISTOSPF | _____ 3. Chamadas de burla por voz. |
| D. ASSINATURADKIM | _____ 4. IP de remetentes autorizados no DNS. |
| E. POLITICADMARC | _____ 5. E-mail de engenharia social. |
| F. WHALING | _____ 6. Instruções de rejeição definidas por política. |
| G. PHISHING | _____ 7. Assinatura criptográfica no e-mail. |
| H. VISHING | _____ 8. Visa executivos de topo. |

## 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. AESRP
2. PIRESFOSTG
3. OPAMDRCLCTIAI
4. SNGIHPHI
5. FIPGOSNO
6. ATDNSKUIAASRMI
7. WNIGHLA
8. IHGVNIS

# Atividade bónus: Pensa rápido

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

| | | | | |
|---|---|---|---|---|
| 1 | Dispositivos que podem ser hackeados | | | |
| 2 | Sinais de um email de phishing | | | |
| 3 | Sinais de que um computador está infetado | | | |
| 4 | Palavras que criam falsa urgência | | | |
| 5 | Formas de verificar um remetente | | | |
| 6 | Pessoas a quem podes pedir ajuda de TI | | | |
| 7 | Coisas de que fazes cópia de segurança | | | |
| 8 | Peixes ou criaturas marinhas que conheces | | | |
| 9 | Empresas que os burlões fingem ser | | | |
| 10 | Hábitos seguros que podes começar hoje | | | |
| 11 | Coisas a fazer depois de clicar numa ligação falsa | | | |
| 12 | Coisas a fazer depois de uma fuga de dados | | | |
| 13 | Canais onde ocorre phishing | | | |
| 14 | Coisas que nunca envias por email | | | |
| 15 | Formas de proteger as tuas contas | | | |

# Ponto de controlo 8: Estudos de caso de cibersegurança

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

## ESTUDO DE CASO 1: CORREÇÃO DE UM ATAQUE DE WHALING A ADMINISTRADORES

👨‍💻

**Cenário:** O diretor financeiro recebe um email muito personalizado que afirma ser do CEO, a pedir uma transferência urgente de 50 000 $ para fechar a compra confidencial de um domínio.

**Questão para debate:** Analisa os riscos de falsificação de marca e detalha os controlos de autenticação SPF/DKIM/DMARC.

## ESTUDO DE CASO 2: IMPLEMENTAR POLÍTICAS DE GATEWAY SPF/DKIM/DMARC

👨‍💻

**Cenário:** Uma empresa está a falhar auditorias de segurança porque os emails de marketing enviados são frequentemente assinalados como spam, e hackers estão ativamente a falsificar o domínio da marca da empresa.

**Questão para debate:** Estabelece controlos técnicos e administrativos para verificar a autenticidade do email.

## 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 5 14 7 5 14 8 1 18 9 1

19 15 3 9 1 12 3 15 13 1 21 4 9 20 15 18 9 1

4 5 5 13 1 9 12

**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 phishing?

O phishing é um ataque de engenharia social em que os criminosos enviam mensagens fraudulentas para enganar os utilizadores e levá-los a partilhar dados sensíveis.

### Q2: Qual é a diferença entre phishing e spear phishing?

O phishing visa grupos amplos com conteúdo genérico, enquanto o spear phishing visa vítimas específicas usando detalhes personalizados.

### Q3: O que é o whaling?

O whaling é um ataque de phishing altamente direcionado a executivos de topo que têm poder administrativo.

### Q4: O que é a falsificação de correio eletrónico (email spoofing)?

A falsificação de e-mail é a criação de mensagens de e-mail com um endereço de remetente forjado para levar o destinatário a confiar na origem.

### Q5: Como evita o SPF a falsificação?

Publica no DNS uma lista de endereços IP de envio autorizados, permitindo aos servidores recetores verificar a origem do correio. [1]

# 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 é o DKIM?

O DomainKeys Identified Mail acrescenta uma assinatura criptográfica aos cabeçalhos dos e-mails, provando que um domínio assumiu a responsabilidade e que a mensagem não foi alterada.

### Q7: O que significa DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

### Q8: O que é uma política DMARC?

Uma política que indica aos servidores de correio como tratar as mensagens que falham o SPF/DKIM (nenhuma, quarentena ou rejeição). [2]

### Q9: O que é o vishing?

Phishing por voz, em que os atacantes usam chamadas telefónicas fraudulentas para obter dados administrativos ou financeiros.

### Q10: Como ajudam os verificadores de ligações?

Analisam e reescrevem as ligações dos e-mails recebidos para verificar a segurança das páginas web de destino no momento do clique.

# 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 funciona um ataque homógrafo?

Os atacantes registam nomes de domínio com carateres Unicode não ASCII semelhantes, para imitar visualmente um nome de domínio legítimo.

### Q2: O que é uma representação punycode?

Uma codificação que converte nomes de domínio Unicode em cadeias compatíveis com ASCII que começam por "xn--" para que o DNS as possa tratar.

### Q3: Porque é que 'p=reject' é o estado DMARC mais seguro?

Pede aos servidores recetores que rejeitem o correio que falhe o DMARC (SPF/DKIM alinhados) durante a sessão SMTP, bloqueando a falsificação direta. [2]

### Q4: Como contornam os atacantes as regras SPF?

Explorando domínios semelhantes (typosquatting) ou usando contas comprometidas em serviços de email legítimos de terceiros.

### Q5: O que é a fraude por comprometimento de correio eletrónico empresarial (BEC)?

Uma burla empresarial em que os atacantes sequestram ou se fazem passar por contas de e-mail de empresas para autorizar pagamentos fraudulentos.

# 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 impede a autenticação multifator o phishing?

Exige tokens secundários (como chaves de hardware) que não podem ser roubados apenas através de páginas de destino falsas.

### Q7: O que é uma página de destino de recolha de credenciais?

Um portal de início de sessão semelhante ao original, concebido para capturar em tempo real nomes de utilizador, palavras-passe e tokens de MFA introduzidos.

### Q8: O que é o sequestro de subdomínios?

Um atacante que assume o controlo de um ponteiro de subdomínio DNS não utilizado para alojar páginas de destino de phishing maliciosas sob um domínio principal de confiança.

### Q9: Como funciona a verificação de alinhamento do DKIM?

Verifica se o domínio no cabeçalho 'From' corresponde ao domínio que assinou criptograficamente a mensagem no cabeçalho DKIM.

### Q10: Qual é o papel de um gateway de e-mail?

Filtrar o e-mail recebido, auditar ligações, colocar anexos em sandbox e validar a conformidade com SPF/DKIM/DMARC.

# 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. [4]

**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. [4]

**3. PERSPETIVA SOBRE SEGURANÇA**

Os ataques homógrafos utilizam letras cirílicas semelhantes para duplicar visualmente nos navegadores domínios de marcas de correspondência exata.

**4. PERSPETIVA SOBRE SEGURANÇA**

Com «p=reject», um domínio pede aos recetores que recusem o correio que falha a verificação durante a entrega, em vez de o arquivarem como spam. [2]

**5. PERSPETIVA SOBRE SEGURANÇA**

Os ataques de whaling dirigidos a CEO pedem frequentemente pagamentos urgentes para fusões confidenciais ou compras de domínios.

**6. PERSPETIVA SOBRE SEGURANÇA**

Os portais de recolha de credenciais copiam páginas de início de sessão reais para que as vítimas introduzam as palavras-passe diretamente no formulário do atacante.

**7. PERSPETIVA SOBRE SEGURANÇA**

As orientações conjuntas da CISA sobre phishing recomendam a formação dos utilizadores a par de DMARC, SPF, DKIM e MFA resistente a phishing. [3]

**8. PERSPETIVA SOBRE SEGURANÇA**

A avaliação do SPF está limitada a 10 termos que fazem consultas DNS; exceder o limite devolve um resultado 'permerror'. [1]

**9. PERSPETIVA SOBRE SEGURANÇA**

As chaves de segurança de hardware FIDO2 proporcionam proteção com respaldo criptográfico contra a recolha remota de credenciais.

**10. PERSPETIVA SOBRE SEGURANÇA**

O phishing é uma das formas mais comuns de os atacantes entrarem pela primeira vez numa organização, razão pela qual a formação regular de sensibilização é uma defesa eficaz.

# 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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

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

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

## Soluções: Ponto de controlo 1 - Escolha múltipla

### 1 Pergunta 1

**Resposta correta: A**

#### NOTA PARA O PROFESSOR

O que é o spear phishing? → Um e-mail de phishing direcionado, adaptado a uma pessoa ou organização específica

### 2 Pergunta 2

**Resposta correta: A**

#### NOTA PARA O PROFESSOR

O SPF publica em DNS os anfitriões de envio autorizados de um domínio para que os destinatários possam verificar o remetente do envelope.

### 3 Pergunta 3

**Resposta correta: A**

#### NOTA PARA O PROFESSOR

O que é um ataque de whaling? → Uma campanha de phishing dirigida especificamente a quadros executivos de empresas de grande visibilidade

### 4 Pergunta 4

**Resposta correta: A**

#### NOTA PARA O PROFESSOR

O que faz o DKIM? → Acrescenta uma assinatura criptográfica aos e-mails para verificar a autenticidade do remetente

### 5 Pergunta 5

**Resposta correta: A**

#### NOTA PARA O PROFESSOR

Qual é o papel do DMARC? → Indicar aos servidores de e-mail de receção como tratar as verificações SPF/DKIM falhadas

## Soluções: Ponto de controlo 2 - Verdadeiro ou falso

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

### NOTA PARA O PROFESSOR

Falso: o spear phishing é feito à medida de pessoas específicas, ao contrário do phishing genérico em massa.

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

### NOTA PARA O PROFESSOR

As políticas DMARC podem instruir os servidores de correio a rejeitar mensagens falsificadas não autorizadas.

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

### NOTA PARA O PROFESSOR

Falso: o SPF verifica o IP de envio no DNS; é o DKIM que verifica uma assinatura criptográfica.

**9** **Pergunta 9** — **Resposta correta: Falso**

### NOTA PARA O PROFESSOR

Falso: o whaling visa dirigentes de topo, que podem aprovar pagamentos e aceder a dados sensíveis.

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

### NOTA PARA O PROFESSOR

Verdadeiro: confirmar pedidos de pagamento através de um canal separado e conhecido ajuda a travar fraudes de transferências bancárias.

# 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

| | | | |
|---|---|---|---|
| F 1. SPEAR | G 2. SPOOFING | D 3. SPF | H 4. DKIM |
| C 5. DMARC | B 6. WHALING | E 7. PHISHING | A 8. VISHING |

## PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

| | | | |
|---|---|---|---|
| 1 SPEAR | 2 SPOOFING | 3 REGISTO SPF | 4 ASSINATURA DKIM |
| 5 POLÍTICA DMARC | 6 WHALING | | |

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

| | | | |
|---|---|---|---|
| 1 B – SPOOFING | 2 A – SPEAR | 3 H – VISHING | 4 C – REGISTOSPF |
| 5 G – PHISHING | 6 E – POLITICADMARC | 7 D – ASSINATURADKIM | 8 F – WHALING |

### NOTAS DE DEBATE PARA PROFESSORES

**Termos-chave:**
Verifica se os alunos sabem explicar SPEAR, SPOOFING e SPF 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.

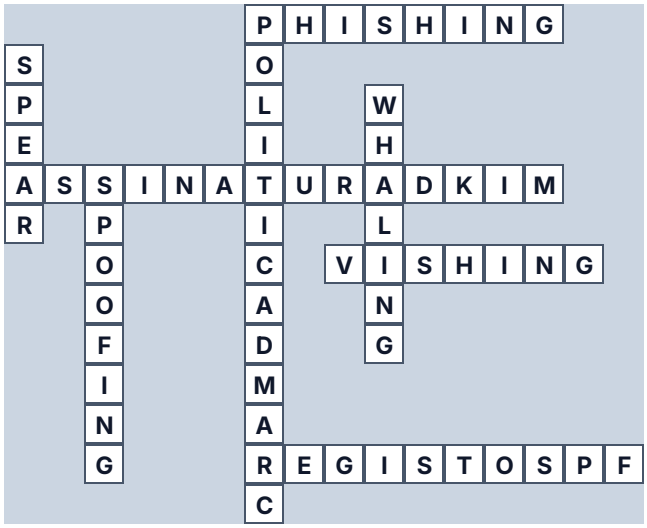
**Avaliação das fontes:**
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

# Soluções dos puzzles e notas para o professor

## SOLUÇÃO DO CAÇA-PALAVRAS

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

## SOLUÇÃO DAS PALAVRAS CRUZADAS




## GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

### HORIZONTAIS

**1 horizontal: PHISHING** E-mail de engenharia social. (8 letras)

**4 horizontal: ASSINATURADKIM** Assinatura criptográfica no e-mail. (14 letras)

**6 horizontal: VISHING** Chamadas de burla por voz. (7 letras)

**7 horizontal: REGISTOSPF** IP de remetentes autorizados no DNS. (10 letras)

### VERTICAIS

**1 vertical: POLITICADMARC** Instruções de rejeição definidas por política. (13 letras)

**2 vertical: SPEAR** E-mail personalizado e direcionado. (5 letras)

**3 vertical: WHALING** Visa executivos de topo. (7 letras)

**5 vertical: SPOOFING** Falsificação do endereço de e-mail do remetente. (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. AESRP — **SPEAR**
2. PIRESFOSTG — **REGISTOSPF**
3. OPAMDRCLCTIAI — **POLITICADMARC**
4. SNGIHPHI — **PHISHING**
5. FIPGOSNO — **SPOOFING**
6. ATDNSKUIAASRMI — **ASSINATURADKIM**
7. WNIGHLA — **WHALING**
8. IHGVNIS — **VISHING**

### CHAVE DO DESAFIO DO CÓDIGO SECRETO

**"DETETA ENGENHARIA SOCIAL COM AUDITORIA DE E MAIL"**

# Soluções dos estudos de caso

## A Estudo de caso 1: Correção de um ataque de whaling a administradores

Solução para o professor

### CRITÉRIO DE CLASSIFICAÇÃO

**As respostas dos alunos devem abranger os seguintes pontos:**

- Análise do cenário: Um diretor financeiro (CFO) recebe um email altamente personalizado que alega ser do CEO e pede uma transferência rápida de 50 000 $ para fechar uma compra confidencial de domínio.
- Estratégia e solução recomendadas: Configurar o DMARC com uma política 'p=reject' para bloquear domínios de remetente falsificados. Adicionar faixas de aviso de remetente externo no gateway e exigir confirmação verbal, fora de banda, para todas as transações financeiras.

## B Estudo de caso 2: Implementar políticas de gateway SPF/DKIM/DMARC

Solução para o professor

### CRITÉRIO DE CLASSIFICAÇÃO

**As respostas dos alunos devem abranger os seguintes pontos:**

- Análise de cenário: Uma empresa está a reprovar em auditorias de segurança porque os emails de marketing enviados são frequentemente classificados como spam e os hackers falsificam ativamente o domínio da marca da empresa.
- Estratégia e solução recomendadas: Publicar um registo TXT de SPF com os IP de remetentes autorizados. Configurar chaves de assinatura DKIM nos servidores de correio de saída e analisar os relatórios de feedback XML do DMARC recebidos para identificar abusos.