Nome: _____ Data: _____ Pontuação: _____

Segurança e encriptação do Wi-Fi público

Ataques man-in-the-middle, pontos de acesso falsos, captura de pacotes, túneis VPN e encriptação HTTPS.

VISÃO GERAL DA APRENDIZAGEM SOBRE SEGURANÇA DO WI-FI PÚBLICO

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 segurança do Wi-Fi público. Vais explorar redes não encriptadas, ataques man-in-the-middle (MitM), pontos de acesso falsos, packet sniffing, túneis VPN e a segurança do trânsito HTTPS.

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/seguranca-wifi-publico/

O teu roteiro de aprendizagem sobre segurança em Wi-Fi público

- Identifica os riscos comuns do Wi-Fi público, incluindo a captura de pacotes e os pontos de acesso falsos.
- Implementa túneis de encriptação VPN para proteger os dados em trânsito.
- Impõe HTTPS e definições seguras de navegador para os trabalhadores remotos.

INSTRUÇÕES DO GUIA DE SEGURANÇA DO WI-FI PÚBLICO

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 segurança do acesso remoto. Termina com a atividade bónus Pensa rápido.

SEGURANÇA DO WI-FI PÚBLICO E PROTEÇÃO EM TRÂNSITO (INTRODUÇÃO)

Os pontos de acesso Wi-Fi públicos não encriptados deixam o tráfego de rede exposto a packet sniffing e a ataques de falsificação Evil Twin. Forçar o tráfego através de túneis seguros de encriptação VPN e impor regras HSTS apenas HTTPS protege as sessões contra a interceção na rede local.

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 um ataque Man-in-the-Middle (MitM)?

- A. Intercetar e alterar as comunicações entre duas partes numa rede partilhada
- B. Uma técnica de extração de bases de dados dirigida a registos de utilizadores
- C. Sobrecarregar servidores web com pedidos de tráfego de rede
- D. Apagar volumes de armazenamento do disco rígido local

2. O que é um ponto de acesso falso (Evil Twin)?

- A. Um ponto de acesso Wi-Fi malicioso configurado com o mesmo SSID de uma rede legítima
- B. Uma ferramenta administrativa usada para monitorizar cópias de segurança de bases de dados
- C. Uma configuração de gateway VPN segura
- D. Um registo DNS que mapeia os servidores de correio autorizados

3. Como protege uma VPN o tráfego em Wi-Fi público?

- A. Envolve todos os pacotes de rede num túnel encriptado, tornando-os ilegíveis para os sniffers
- B. Bloqueia automaticamente todos os pedidos de ligação de entrada
- C. Altera o endereço MAC da placa de rede física
- D. Elimina os cookies em cache do navegador

4. O que é o packet sniffing?

- A. Usar ferramentas de hardware ou software para capturar e registar pacotes de rede
- B. Analisar diretórios locais à procura de ficheiros duplicados
- C. Restringir os privilégios de leitura da base de dados com base nas funções dos utilizadores
- D. Encriptar unidades de armazenamento com chaves AES-256

5. Qual é o papel do HTTPS?

- A. Encriptar o tráfego da sessão entre o navegador e o servidor Web
- B. Filtrar as mensagens de email recebidas na gateway
- C. Comprimir imagens para carregamentos de página mais rápidos
- D. Gerir estruturas de ficheiros em armazenamento ligado à rede

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Os utilizadores ligados podem facilmente capturar dados em texto simples em redes Wi-Fi públicas abertas.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Os pontos de acesso fraudulentos (Evil Twins) são sempre autorizados pelos administradores de rede.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Uma VPN é ineficaz a proteger o tráfego contra a captura de pacotes em redes públicas.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. O HTTPS encripta apenas o caminho do URL, deixando a carga útil dos pacotes em texto simples.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. As redes Wi-Fi com segurança WPA3 oferecem uma proteção mais forte do que as redes abertas e sem palavra-passe.

○ 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. Capturar palavras-passe privadas numa rede Wi-Fi pública é _____ de comunicações.

2. Analisar pacotes em bruto numa rede local recorre ao _____ de pacotes.

3. Um hotspot falso que imita o Wi-Fi de um hotel é um _____ .

4. Proteger o trânsito do tráfego web exige encriptar com _____ .

5. Encriptar todas as saídas da rede recorre a um cliente _____ .

6. Um caminho de comunicação encriptado através de redes públicas é um _____ .

BANCO DE PALAVRAS DE VOCABULÁRIO

EVIL TWIN FIREWALL HTTPS INTERCEÇÃO NORMA WPA SNIFFING TÚNEL VPN

Escreve aqui as tuas respostas:

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

Ponto de controlo 4: Associação de conceitos de segurança

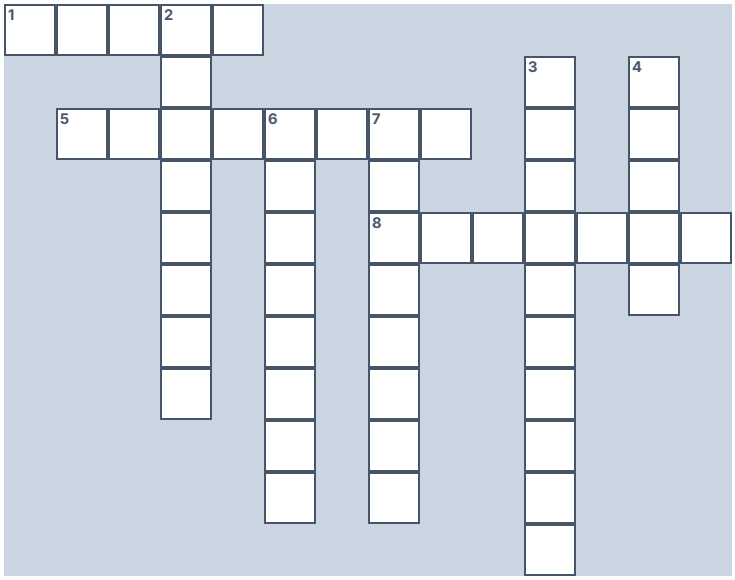
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. INTERCEÇÃO	A	Norma moderna de segurança Wi-Fi.
☐	2. SNIFFING	B	Caminho de dados seguro em trânsito.
☐	3. GÉMEO MAU	C	Filtrar o tráfego de entrada.
☐	4. HTTPS	D	Hotspot fraudulento que imita o Wi-Fi.
☐	5. VPN	E	Ler o tráfego em trânsito.
☐	6. TÚNEL	F	Captura de pacotes de dados da rede.
☐	7. WPA3	G	Rede privada virtual encriptada.
☐	8. FIREWALL	H	Transmissão web segura.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

1. Caminho seguro para os dados em trânsito. (5)

5. Captura de pacotes de dados da rede. (8)

8. Rede privada virtual encriptada. (7)

VERTICAIS

2. Hotspot falso que imita um Wi-Fi. (8)

3. Leitura do tráfego em trânsito. (10)

4. Transmissão web segura. (5)

6. Filtragem do tráfego de entrada. (8)

7. Norma moderna de segurança Wi-Fi. (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: Caminho seguro para os dados em trânsito. (5 letras):

5 horizontal: Captura de pacotes de dados da rede. (8 letras):

8 horizontal: Rede privada virtual encriptada. (7 letras):

VERTICAIS

2 vertical: Hotspot falso que imita um Wi-Fi. (8 letras):

3 vertical: Leitura do tráfego em trânsito. (10 letras):

4 vertical: Transmissão web segura. (5 letras):

6 vertical: Filtragem do tráfego de entrada. (8 letras):

7 vertical: Norma moderna de segurança Wi-Fi. (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 R I G N R M P X Q O C U S T
E L J B A B C P X L R K Y K X
T K D Q M J D I N N E K Q P G
M L L A W E R I F M D Q R S T
N T G C S I Q O H S E B W D S
I Z V C Z N W S F S V K H Z D
W N D Q X T P C N U P B A Z N
T D K A D E O D O I N T F H I
L D R Q M R E I R R F Z T S F
I Q V F A C T A M Q O F N H P
V T X Q K E U R A U S D I N Y
E B F S X C N W W J A R Z N Y
Y L G I M A E R P J M L T O G
H Q Q H Z O L A A O V G U B Y
R Y B H L Z G J O P N W C M Z

LISTA DE PALAVRAS DE VOCABULÁRIO

INTERCECAO SNIFFING EVILTWIN HTTPS REDEVPN TUNEL NORMAWPA FIREWALL

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. INTERCECAO**
- **B. SNIFFING**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. REDEVPN**
- **F. TUNEL**
- **G. NORMAWPA**
- **H. FIREWALL**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Norma moderna de segurança Wi-Fi.

_____ 2. Hotspot falso que imita um Wi-Fi.

_____ 3. Captura de pacotes de dados da rede.

_____ 4. Caminho seguro para os dados em trânsito.

_____ 5. Filtragem do tráfego de entrada.

_____ 6. Leitura do tráfego em trânsito.

_____ 7. Rede privada virtual encriptada.

_____ 8. Transmissão web segura.

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. AECRNICOET
2. LENVIWTI
3. ERVNDPE
4. MPAWANOR
5. FINGFSNI
6. PHTST
7. ELTNU
8. EIWLFLAR

Atividade bónus: Pensa rápido

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

1	Razões para atualizar o software			
2	Dispositivos que se ligam automaticamente ao Wi-Fi			
3	Informações que nunca deves partilhar			
4	Hábitos seguros que podes começar hoje			
5	Formas de estar seguro num café			
6	Dispositivos que podem ser hackeados			
7	Coisas que um hacker consegue ver num Wi-Fi aberto			
8	Sinais de uma rede Wi-Fi falsa			
9	Alternativas ao Wi-Fi público			
10	Sinais de alerta num email			
11	Coisas que não fazes em Wi-Fi público			
12	Locais com Wi-Fi gratuito			
13	Formas de proteger as tuas contas			
14	Sinais de que um computador está infetado			
15	Nomes de Wi-Fi que parecem suspeitos			

Ponto de controlo 8: Estudos de caso de cibersegurança

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

ESTUDO DE CASO 1: CONTENÇÃO DA INTERCEÇÃO DE PACOTES EM WI-FI PÚBLICO

👷

Cenário: Um executivo de vendas remoto, ligado à rede Wi-Fi pública de um aeroporto, repara que vários emails de negócios sensíveis foram divulgados pouco depois de os enviar em texto simples.

Questão para debate: Analisa os riscos das redes públicas e descreve uma solução de encriptação de tráfego.

ESTUDO DE CASO 2: DEFESA CONTRA HOTSPOTS FALSOS EVIL TWIN

👷

Cenário: Atacantes implementam um ponto de acesso sem fios falso chamado "CoffeeShop_Guest", que imita o hotspot legítimo de um café e captura o tráfego de rede de clientes desprevenidos.

Questão para debate: Detalha os passos de verificação para detetar e bloquear pontos de acesso falsos.

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

5	14	3	18	9	16	20	1		15		20	18	1	6	5	7	15		4	15
23	9	6	9		16	21	2	12	9	3	15		3	15	13		21	13	1	
								22	16	14										

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: Porque é inseguro o Wi-Fi público?

O Wi-Fi público aberto não encripta o tráfego no ar, pelo que outras pessoas próximas podem capturar quaisquer dados desprotegidos. [2]

Q2: O que é a captura de pacotes (packet sniffing)?

Um packet sniffer captura os dados brutos que circulam numa interface de rede, expondo palavras-passe em texto simples e detalhes do tráfego.

Q3: O que é um Evil Twin?

Um ponto de acesso falso criado por hackers que imita o nome e as definições de um ponto de acesso Wi-Fi local de confiança.

Q4: Como me protege uma VPN?

Encaminha o teu tráfego por um túnel encriptado, ocultando a tua atividade de navegação de sniffers da rede local.

Q5: O HTTPS protege-me em Wi-Fi público?

Sim, cifra os dados trocados entre o teu navegador e o site, e uma VPN acrescenta mais uma camada de proteção.

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 WPA3?

A norma moderna Wi-Fi Protected Access, que oferece encriptação mais forte e proteção contra ataques de dicionário offline. [1]

Q7: O Wi-Fi público pode distribuir software malicioso?

Sim, os atacantes podem intercetar o tráfego e injetar pedidos de descarregamento maliciosos (drive-by downloads) na tua sessão do navegador.

Q8: Qual é o risco da partilha de ficheiros?

Se a partilha de ficheiros estiver ativada, outros utilizadores da rede pública podem ler ou modificar o diretório da tua pasta local.

Q9: O que é um portal cativo?

A página de início de sessão que as redes de hotéis ou cafés usam para conceder acesso à internet, e que por vezes pode ser falsificada por atacantes.

Q10: Devo desligar o Wi-Fi quando não o estiver a usar?

Sim, desativar o Wi-Fi impede que o teu dispositivo se ligue automaticamente a redes não fiáveis.

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 é que um ataque Man-in-the-Middle explora o DNS?

Usando DNS spoofing num router malicioso para dirigir os browsers visados para páginas de destino de phishing semelhantes em vez dos domínios visados.

Q2: O que é o sequestro de sessão?

Um atacante que captura um cookie de sessão não encriptado numa rede Wi-Fi pública e o importa para contornar os inícios de sessão com credenciais.

Q3: O que é o SSL stripping?

Um ataque MitM em que o atacante faz o downgrade do pedido HTTPS seguro de um utilizador para HTTP não encriptado, capturando credenciais em texto simples.

Q4: Como protege o HSTS contra o SSL stripping?

O HTTP Strict Transport Security obriga os navegadores a ligarem-se apenas por HTTPS, recusando recursos a HTTP não encriptado. [3]

Q5: O que é uma VPN com split tunneling?

Uma configuração que encaminha apenas o tráfego empresarial pela VPN e envia os dados da Internet pública diretamente, o que pode arriscar a exposição por caminhos de fuga.

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: Porque é o WPA2 vulnerável ao KRACK?

O Key Reinstallation Attack explora o handshake de quatro vias do WPA2 para desencriptar pacotes sem a palavra-passe do Wi-Fi.

Q7: O que é o isolamento de clientes?

Uma definição de segurança do router que impede os dispositivos Wi-Fi ligados de comunicarem diretamente entre si, bloqueando a captura de tráfego local.

Q8: Como usam os atacantes servidores DNS falsos?

Configuram routers falsos para atribuir servidores DNS falsos aos clientes, o que lhes permite intercetar e reescrever todas as pesquisas web.

Q9: Uma VPN pode esconder o meu endereço MAC local?

Não. Os endereços MAC são identificadores locais da camada 2; usa antes a definição integrada de aleatorização de MAC (endereço privado) do teu dispositivo.

Q10: O que é um ataque de falsificação de captive portal?

Um atacante que aloja um portal de autenticação falso num ponto de acesso falso para roubar credenciais sob a aparência de acesso Wi-Fi gratuito.

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

Os trabalhadores remotos usam frequentemente Wi-Fi em cafés, hotéis e aeroportos, onde não podem controlar a segurança da rede.

2. PERSPETIVA SOBRE SEGURANÇA

Um ponto de acesso falso Evil Twin pode copiar o nome e o endereço MAC exatos de uma rede de confiança, confundindo os dispositivos.

3. PERSPETIVA SOBRE SEGURANÇA

O software de captura de pacotes, como o Wireshark, é gratuito e pode mostrar em texto simples palavras-passe HTTP não encriptadas.

4. PERSPETIVA SOBRE SEGURANÇA

A segurança WPA3 utiliza a Autenticação Simultânea de Iguais (SAE) para proteger contra ataques locais de força bruta.

5. PERSPETIVA SOBRE SEGURANÇA

Os ataques de SSL stripping contornam as proteções HTTPS básicas ao intercetar na gateway os redirecionamentos HTTP iniciais.

6. PERSPETIVA SOBRE SEGURANÇA

Os cabeçalhos de resposta HTTP Strict Transport Security (HSTS) impedem os navegadores de recorrerem a ligações HTTP não encriptadas. [3]

7. PERSPETIVA SOBRE SEGURANÇA

Desativar o «Auto-Connect» impede que os smartphones se liguem a redes falsas semelhantes em espaços públicos.

8. PERSPETIVA SOBRE SEGURANÇA

As configurações de VPN 'always-on' empresariais forçam todo o tráfego de rede dos trabalhadores remotos a passar pelas firewalls da empresa.

9. PERSPETIVA SOBRE SEGURANÇA

Os pontos de acesso fraudulentos podem fornecer respostas DNS falsificadas, redirecionando domínios-alvo para servidores de phishing.

10. PERSPETIVA SOBRE SEGURANÇA

Sem uma VPN, outros utilizadores de um hotspot aberto podem ver quais os sites e servidores com que o teu dispositivo comunica.

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] Wi-Fi Alliance. (n.d.). Security.
https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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 um ataque Man-in-the-Middle (MitM)? → Intercetar e alterar as comunicações entre duas partes numa rede partilhada

2 Pergunta 2 — **Resposta correta: A**

NOTA PARA O PROFESSOR

O que é um ponto de acesso falso (Evil Twin)? → Um ponto de acesso Wi-Fi malicioso configurado com o mesmo SSID de uma rede legítima

3 Pergunta 3 — **Resposta correta: A**

NOTA PARA O PROFESSOR

Como protege uma VPN o tráfego em Wi-Fi público? → Envolve todos os pacotes de rede num túnel encriptado, tornando-os ilegíveis para os sniffers

4 Pergunta 4 — **Resposta correta: A**

NOTA PARA O PROFESSOR

O que é o packet sniffing? → Usar ferramentas de hardware ou software para capturar e registar pacotes de rede

5 Pergunta 5 — **Resposta correta: A**

NOTA PARA O PROFESSOR

Qual é o papel do HTTPS? → Encriptar o tráfego da sessão entre o navegador e o servidor Web

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os utilizadores ligados podem facilmente capturar dados em texto simples em redes Wi-Fi públicas abertas.

7 **Pergunta 7** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Falso: um Evil Twin é um hotspot não autorizado montado por um atacante para imitar um verdadeiro.

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

NOTA PARA O PROFESSOR

Falso: uma VPN encripta o tráfego num túnel, pelo que os sniffers locais não o conseguem ler.

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

NOTA PARA O PROFESSOR

Falso: o HTTPS encripta toda a troca HTTP, incluindo o caminho do URL e o conteúdo da página.

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

NOTA PARA O PROFESSOR

As redes Wi-Fi com segurança WPA3 oferecem uma proteção mais forte do que as redes abertas e sem palavra-passe.

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

E 1. INTERCEÇÃO	F 2. SNIFFING	D 3. GÉMEO MAU	H 4. HTTPS
G 5. VPN	B 6. TÚNEL	A 7. WPA3	C 8. FIREWALL

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 INTERCEÇÃO	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 VPN	6 TÚNEL		

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

1 G – NORMAWPA	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNEL
5 H – FIREWALL	6 A – INTERCECAO	7 E – REDEVPN	8 D – HTTPS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar INTERCEÇÃO, SNIFFING e GÉMEO MAU 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.

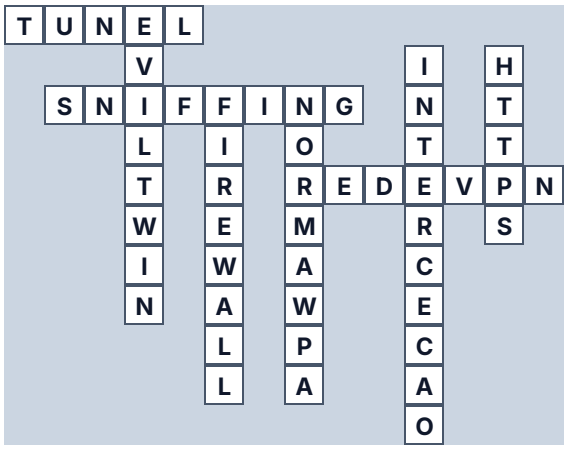
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: TUNEL Caminho seguro para os dados em trânsito. (5 letras)

5 horizontal: SNIFFING Captura de pacotes de dados da rede. (8 letras)

8 horizontal: REDEVPN Rede privada virtual encriptada. (7 letras)

VERTICAIS

2 vertical: EVILTWIN Hotspot falso que imita um Wi-Fi. (8 letras)

3 vertical: INTERCECAO Leitura do tráfego em trânsito. (10 letras)

4 vertical: HTTPS Transmissão web segura. (5 letras)

6 vertical: FIREWALL Filtragem do tráfego de entrada. (8 letras)

7 vertical: NORMAWPA Norma moderna de segurança Wi-Fi. (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. AECRNICOET — **INTERCECAO**
2. LENVIWTI — **EVILTWIN**
3. ERVNDPE — **REDEVPN**
4. MPAWANOR — **NORMAWPA**
5. FINGFSNI — **SNIFFING**
6. PHTST — **HTTPS**
7. ELTNU — **TUNEL**
8. EIWLFLAR — **FIREWALL**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"ENCRIPTA O TRAFEGO DO WIFI PUBLICO COM UMA VPN"

Soluções dos estudos de caso

A Estudo de caso 1: Contenção da interceção de pacotes em Wi-Fi público

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um executivo de vendas remoto ligado a uma rede Wi-Fi pública de aeroporto repara que vários emails de negócios sensíveis são divulgados pouco depois de os enviar em texto simples.
- Estratégia e solução recomendadas: Tornar obrigatório o uso de um cliente VPN empresarial em todos os postos de trabalho remotos. Aplicar extensões de navegador apenas HTTPS e bloquear protocolos não encriptados (como HTTP e FTP) na firewall do cliente.

B Estudo de caso 2: Defesa contra hotspots falsos Evil Twin

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Atacantes instalam um ponto de acesso sem fios falso chamado «CoffeeShop_Guest», que imita o ponto de acesso legítimo de um café, e capturam o tráfego de rede de convidados desprevenidos.
- Estratégia e solução recomendadas: Auditar os endereços MAC BSSID dos pontos de acesso para verificar a autenticidade da rede. Impor a validação da postura do cliente para bloquear a ligação a redes abertas e exigir pontos de acesso móveis (hotspots) para trabalho sensível.