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

Prevenção do roubo de identidade e dos ativos
Fusões de segurança

Fugas de credenciais, MFA, monitorização da dark web, alertas de congelamento de crédito, engenharia social

VISÃO GERAL DE APRENDIZAGEM SOBRE PREVENÇÃO DO ROUBO DE IDENTIDADE

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 prevenção e mitigação do roubo de identidade. Vais explorar fugas de credenciais, autenticação multifator, monitorização da Dark Web, alertas de congelamento de crédito e defesa contra engenharia social.

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/roubo-identidade/

O teu roteiro de aprendizagem sobre proteção de identidade

- Compreender os riscos de exposição de credenciais em fóruns da dark web.
- Implementa a autenticação multifator (MFA) e alertas de congelamento de crédito.
- Concebe defesas de segurança empresariais contra burlas de engenharia social direcionadas.

INSTRUÇÕES DO GUIA SOBRE ROUBO DE IDENTIDADE

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 da identidade. Termina com a atividade bónus Pensa rápido.

PREVENÇÃO DO ROUBO DE IDENTIDADE E SEGURANÇA DE ATIVOS (INTRODUÇÃO)

O roubo de identidade explora credenciais divulgadas e inícios de sessão fracos para sequestrar contas pessoais e empresariais. A implementação de MFA, congelamentos de crédito, scanners da dark web e referenciais SPF/DKIM/DMARC constitui uma defesa fundamental contra a usurpação de identidade digital.

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 método que os ladrões de identidade usam para roubar credenciais de início de sessão?

- A. Enviar falsos alertas por e-mail para levar os utilizadores a introduzir palavras-passe em portais falsificados
- B. Escutar emissões de rádio perto do escritório corporativo de um utilizador
- C. Desfragmentar a unidade de armazenamento do servidor local de um utilizador
- D. Desligar configurações externas de cópias de segurança de rede

2. Que controlo de segurança oferece a defesa mais forte contra fugas de credenciais?

- A. Autenticação multifator com chaves de hardware
- B. Criar palavras-passe longas usando os formatos predefinidos do browser
- C. Alterar os nomes de utilizador do email de seis em seis meses
- D. Eliminar os históricos de rastreio de cookies armazenados no navegador

3. O que representa o congelamento de crédito?

- A. Bloquear relatórios de crédito para impedir que ladrões abram empréstimos não autorizados
- B. Eliminar históricos de transações de contas bancárias das bases de dados
- C. Desativar leitores de banda magnética de cartões de crédito em scanners
- D. Encriptar em repouso os discos rígidos das bases de dados locais

4. Porque é útil a monitorização da dark web?

- A. Alerta os utilizadores se as suas credenciais divulgadas aparecerem em bases de dados ilícitas
- B. Impede que software malicioso ativo seja executado em sandboxes virtuais
- C. Acelera a velocidade de encaminhamento do navegador em redes virtuais
- D. Bloqueia tentativas de acesso por injeção de SQL à base de dados de back-end

5. O que significa engenharia social?

- A. Manipular pessoas para que revelem voluntariamente credenciais confidenciais
- B. Analisar as portas dos servidores corporativos à procura de explorações de segurança ativas
- C. Fazer cópias de segurança dos ficheiros da base de dados do sistema para discos rígidos offline
- D. Encaminhar pacotes de rede através de três nós onion encriptados

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. O roubo de identidade afeta apenas contas digitais online, não o correio postal físico.

○ Verdadeiro ○ Falso

7 Pergunta 7

7. Impor MFA em todas as contas pessoais bloqueia a maioria dos ataques de bots de credential stuffing.

○ Verdadeiro ○ Falso

8 Pergunta 8

8. Um congelamento de crédito bloqueia as consultas de crédito, mas impede-te de aceder à tua própria conta bancária.

○ Verdadeiro ○ Falso

9 Pergunta 9

9. Os gestores de palavras-passe protegem os utilizadores contra o phishing ao recusarem preencher automaticamente palavras-passe em domínios falsificados.

○ Verdadeiro ○ Falso

10 Pergunta 10

10. Os e-mails de phishing usam frequentemente linguagem urgente para desencadear respostas emocionais e rápidas.

○ 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 ladrões de identidade visam as palavras-passe pessoais e as _____ dos utilizadores.

2. Alertar os utilizadores para violações de bases de dados identifica as _____ de contas privadas.

3. Exigir um código temporário para iniciar sessão chama-se _____ .

4. Analisar fóruns de hackers à procura de dados roubados é a _____ da dark web.

5. Bloquear consultas de crédito não autorizadas exige um _____ de crédito.

6. Formar os colaboradores em sensibilização para o phishing cria uma _____ de segurança ativa.

BANCO DE PALAVRAS DE VOCABULÁRIO

CONGELAMENTO CREDENCIAIS DEFESA FUGAS MFA MONITORIZAÇÃO PHISHING SPOOFING

Escreve aqui as tuas respostas:

1. **2.**

3. **4.**

5. **6.**

Ponto de controlo 4: Associação de conceitos de segurança

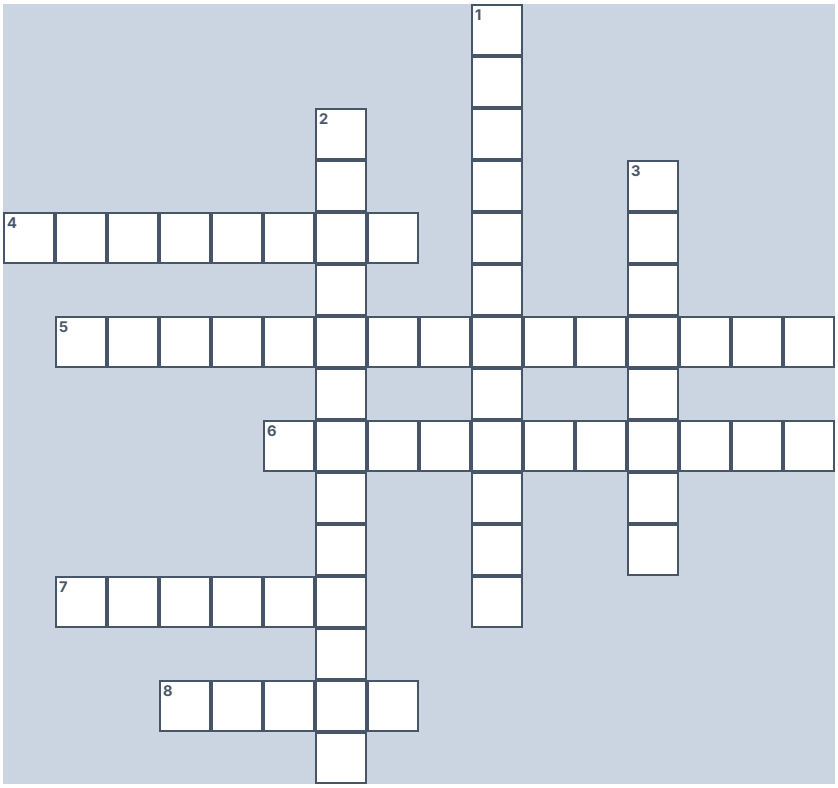
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. CREDENCIAIS	A	Passo de verificação secundário (como chaves de hardware) que protege os inícios de sessão da conta.
☐	2. FUGAS	B	Criar um site ou e-mail falso para imitar uma organização legítima.
☐	3. MFA	C	Restringir o acesso aos ficheiros de crédito para impedir pedidos de empréstimo fraudulentos.
☐	4. MONITORIZAÇÃO	D	Exposição não autorizada de bases de dados privadas que contêm registos pessoais de utilizadores.
☐	5. CONGELAR	E	Formação e controlos técnicos usados para proteger contra o roubo de identidade.
☐	6. DEFESA	F	Enviar mensagens fraudulentas para levar os utilizadores a revelar credenciais.
☐	7. SPOOFING	G	Vasculhar fóruns online e canais de hackers à procura de dados empresariais roubados.
☐	8. PHISHING	H	Nomes de utilizador, palavras-passe e tokens privados usados para autenticar identidades digitais.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

4. Envio de mensagens fraudulentas para levar os utilizadores a revelar credenciais. (8)

5. Passo de verificação secundário (como chaves de hardware) que protege os inícios de sessão. (15)

6. Nomes de utilizador, palavras-passe e tokens privados usados para autenticar identidades digitais. (11)

7. Formação e controlos técnicos usados para proteger contra o roubo de identidade. (6)

8. Exposição não autorizada de bases de dados privadas com registos pessoais de utilizadores. (5)

VERTICAIS

1. Restringir o acesso aos ficheiros de crédito para evitar pedidos de empréstimo fraudulentos. (12)

2. Análise de fóruns e canais de hackers à procura de dados corporativos roubados. (13)

3. Criar um site ou um e-mail falso para imitar uma organização legítima. (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

4 horizontal: Envio de mensagens fraudulentas para levar os utilizadores a revelar credenciais. (8 letras):

5 horizontal: Passo de verificação secundário (como chaves de hardware) que protege os inícios de sessão. (15 letras):

6 horizontal: Nomes de utilizador, palavras-passe e tokens privados usados para autenticar identidades digitais. (11 letras):

7 horizontal: Formação e controlos técnicos usados para proteger contra o roubo de identidade. (6 letras):

8 horizontal: Exposição não autorizada de bases de dados privadas com registos pessoais de utilizadores. (5 letras):

VERTICAIS

1 vertical: Restringir o acesso aos ficheiros de crédito para evitar pedidos de empréstimo fraudulentos. (12 letras):

2 vertical: Análise de fóruns e canais de hackers à procura de dados corporativos roubados. (13 letras):

3 vertical: Criar um site ou um e-mail falso para imitar uma organização legítima. (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.

A F G O K N D A N C D H I B A

O P N R L P W U T I M Y F Y S

T G I X W H F T R T O N U K R

N D H T S S L E P L N M S H K

E P S H Y A P N L W I U S N Y

M Q I Q B G A T L P T M I B D

A L H I S U F I I N O Y A B E

L Z P Z P F Y C B N R V I X F

E M C F O P W A Q Q I X C H E

G E Y C O W L C F G Z H N Z S

N W C O F R J A X X A R E K A

O Z A N I R Z O R M C G D S W

C G L W N J B M Y C A C E Y O

U Z O Z G U T F B H O V R P X

C N M H P X Y A Z X H O C I O

LISTA DE PALAVRAS DE VOCABULÁRIO

CREDENCIAIS FUGAS AUTENTICACAOMFA MONITORIZACAO CONGELAMENTO DEFESA SPOOFING PHISHING

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. CREDENCIAIS
B. FUGAS
C. AUTENTICACAOMFA
D. MONITORIZACAO
E. CONGELAMENTO
F. DEFESA
G. SPOOFING
H. PHISHING

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO
_____ 1. Envio de mensagens fraudulentas para levar os utilizadores a revelar credenciais.
_____ 2. Nomes de utilizador, palavras-passe e tokens privados usados para autenticar identidades digitais.
_____ 3. Criar um site ou um e-mail falso para imitar uma organização legítima.
_____ 4. Formação e controlos técnicos usados para proteger contra o roubo de identidade.
_____ 5. Análise de fóruns e canais de hackers à procura de dados corporativos roubados.
_____ 6. Restringir o acesso aos ficheiros de crédito para evitar pedidos de empréstimo fraudulentos.
_____ 7. Exposição não autorizada de bases de dados privadas com registos pessoais de utilizadores.
_____ 8. Passo de verificação secundário (como chaves de hardware) que protege os inícios de sessão.

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. ECIRNICAESD
5. GSFAU
2. UTCITCMAAF EAOAN
6. TAROCNAZM OIOI
3. COMATENLOE NG
7. SDEAFE
4. ONGIFSPO
8. SHHGPNII

Atividade bónus: Pensa rápido

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

1	Coisas a fazer se a tua identidade for roubada			
2	Coisas a não partilhar nas redes sociais			
3	Coisas de que fazes cópia de segurança			
4	Cartões ou documentos de identificação na tua carteira			
5	Documentos que deves proteger			
6	Coisas a fazer depois de uma fuga de dados			
7	Razões para atualizar o software			
8	Informações que um ladrão de identidade quer			
9	Dispositivos que podem ser hackeados			
10	Locais de onde os teus dados podem ser divulgados			
11	Hábitos seguros que podes começar hoje			
12	Sinais de que um computador está infetado			
13	Formas de provar quem és			
14	Sinais de roubo de identidade			
15	Sinais de alerta num email			

Ponto de controlo 8: Estudos de caso de cibersegurança

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

ESTUDO DE CASO 1: PROTEÇÃO CONTRA A USURPAÇÃO DE IDENTIDADE DE EXECUTIVOS



Cenário: Um executivo de topo de grande visibilidade foi alvo de nomes de domínio com erros de digitação (typosquatting) que imitam o seu email pessoal para burlar clientes. Cria um plano de proteção de marca.

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

ESTUDO DE CASO 2: EXPOSIÇÃO DE CREDENCIAIS EMPRESARIAIS NA DARK WEB



Cenário: Uma fuga da dark web contém várias centenas de credenciais empresariais pertencentes a administradores de sistemas de uma empresa. Cria uma estratégia de mitigação.

Questão para debate: Descreve o processo de limpeza de credenciais e planeia a implementação de um gestor de palavras-passe.

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

16	18	15	20	5	7	5		1		9	4	5	14	20	9	4	1	4	5

3	15	13		1	21	20	5	14	20	9	3	1	3	1	15

13	21	12	20	9	6	1	20	15	18

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 o roubo de identidade?

Um crime em que um atacante rouba registos pessoais (como palavras-passe ou números de segurança social) para se fazer passar por outra pessoa em benefício financeiro.

Q2: Qual é a causa mais comum de roubo de identidade?

O phishing é uma das principais formas de os ladrões obterem palavras-passe, atraindo os utilizadores para sites falsos e falsificados.

Q3: Como protege a autenticação multifator (MFA) as identidades?

A MFA exige uma segunda prova (como uma chave de hardware) para iniciar sessão, bloqueando os atacantes mesmo que roubem a tua palavra-passe.

Q4: O que é um congelamento de crédito?

Um serviço gratuito que impede as agências de crédito de partilharem o teu ficheiro de crédito, travando os ladrões de abrirem novos empréstimos em teu nome. [2]

Q5: O que é a monitorização da dark web?

Software que verifica fóruns de hackers à procura de emails, palavras-passe e registos pessoais divulgados e te alerta se os teus dados estiverem expostos.

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 credential stuffing?

Bots automatizados que testam listas de palavras-passe divulgadas em centenas de websites para tomar o controlo de contas ativas.

Q7: Porque é perigosa a falsificação de correio eletrónico?

Permite aos atacantes falsificar o nome do remetente nos emails, fazendo com que as mensagens de phishing pareçam vir de colegas de confiança.

Q8: Como impedem os gestores de palavras-passe o roubo de identidade?

Guardam palavras-passe complexas e únicas para cada conta e recusam preencher automaticamente as credenciais em domínios de phishing falsos.

Q9: O que é o spear phishing?

Um ataque de phishing altamente direcionado, personalizado com o nome e os detalhes da vítima para aumentar a probabilidade de engano.

Q10: Em que difere um alerta de crédito de um congelamento?

Um alerta indica aos credores que verifiquem a tua identidade antes de abrirem contas, ao passo que um congelamento bloqueia por completo o acesso ao teu ficheiro de crédito. [2]

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 o SIM swapping leva ao roubo de identidade?

Os atacantes convencem o pessoal da operadora a transferir o número de telemóvel da vítima para um novo cartão SIM, sequestrando os códigos 2FA enviados por SMS.

Q2: Qual é o papel do DMARC na prevenção do roubo de identidade?

O DMARC permite que os proprietários de domínios impeçam que e-mails falsificados cheguem às caixas de entrada, evitando que e-mails falsos imitem domínios empresariais.

Q3: Porque é difícil detetar o roubo de identidade sintética?

Os ladrões combinam números reais de segurança social (SSN) com nomes e datas de nascimento falsos para criar perfis de crédito totalmente novos, contornando os alertas básicos de fraude.

Q4: Como exploram os corretores de dados as identidades pessoais?

Os corretores de dados recolhem registos públicos, comportamento na web e históricos de compras para compilar dossiês de perfis, que podem ser divulgados ou vendidos.

Q5: Porque é considerada vulnerável a MFA por SMS?

O tráfego SMS é vulnerável a intercetação, phishing e explorações de troca de SIM ao nível do operador.

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: O que é um bloqueio de ficheiro de crédito?

Um serviço comercial semelhante a um congelamento, que permite bloquear ou desbloquear instantaneamente o teu ficheiro de crédito através de uma aplicação móvel.

Q7: Como alimentam as violações de dados empresariais o roubo de identidade?

As bases de dados divulgadas expõem milhões de credenciais em texto simples, dando aos ladrões os dados em bruto necessários para executar fraudes de identidade direcionadas.

Q8: Qual é o risco da partilha excessiva nas redes sociais?

Partilhar publicamente nomes de animais de estimação, locais de nascimento e apelidos de solteira da mãe dá aos ladrões as respostas às perguntas comuns de recuperação de conta.

Q9: Como protegem os inícios de sessão biométricos os perfis de identidade?

A biometria associa os inícios de sessão a caraterísticas como as impressões digitais ou o rosto; guardada no dispositivo é difícil de roubar, mas os dados biométricos armazenados podem ser divulgados.

Q10: Como é que a Red Flags Rule combate o roubo de identidade?

Um regulamento federal que obriga as instituições financeiras a desenvolver programas escritos para detetar e responder a sinais de alerta de roubo de identidade.

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 IdentityTheft.gov, gerido pela FTC, permite às vítimas nos EUA denunciar o roubo de identidade e obter um plano de recuperação personalizado. [1]

2. PERSPETIVA SOBRE SEGURANÇA

As chaves de segurança de hardware são uma MFA resistente a phishing, o tipo mais forte de MFA que a CISA recomenda. [4]

3. PERSPETIVA SOBRE SEGURANÇA

As palavras-passe comprometidas são um ponto de entrada comum em violações de dados, alimentando fraudes de identidade posteriores.

4. PERSPETIVA SOBRE SEGURANÇA

Um congelamento de crédito é gratuito por lei federal e impede os credores de consultarem os ficheiros de crédito até ser desbloqueado. [2]

5. PERSPETIVA SOBRE SEGURANÇA

O DMARC permite que os proprietários de domínios digam aos servidores de correio que rejeitem ou ponham em quarentena o e-mail falsificado que falhe as verificações. [7]

6. PERSPETIVA SOBRE SEGURANÇA

A troca de SIM (SIM swapping) permite aos hackers contornar a autenticação de dois fatores por SMS nos portais bancários.

7. PERSPETIVA SOBRE SEGURANÇA

A fraude de identidade sintética mistura dados reais e falsos, o que dificulta a sua deteção pelos credores.

8. PERSPETIVA SOBRE SEGURANÇA

Muitas pessoas reutilizam a mesma palavra-passe em várias contas online, pelo que uma única violação pode expor várias delas.

9. PERSPETIVA SOBRE SEGURANÇA

Os corretores de dados compilam dossiês detalhados sobre um grande número de consumidores, criando um risco concentrado para a privacidade.

10. PERSPETIVA SOBRE SEGURANÇA

Recuperar de um roubo de identidade pode exigir meses de trabalho, como contestar cobranças e corrigir relatórios de crédito.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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 método que os ladrões de identidade usam para roubar credenciais de início de sessão? → Enviar falsos alertas por e-mail para levar os utilizadores a introduzir palavras-passe em portais falsificados

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

Que controlo de segurança oferece a defesa mais forte contra fugas de credenciais? → Autenticação multifator com chaves de hardware

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

O que representa o congelamento de crédito? → Bloquear relatórios de crédito para impedir que ladrões abram empréstimos não autorizados

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Porque é útil a monitorização da dark web? → Alerta os utilizadores se as suas credenciais divulgadas aparecerem em bases de dados ilícitas

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que significa engenharia social? → Manipular pessoas para que revelem voluntariamente credenciais confidenciais

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Falso

NOTA PARA O PROFESSOR

O roubo de identidade também pode começar offline, por exemplo com correio ou documentos roubados.

7 Pergunta 7

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Impor MFA em todas as contas pessoais bloqueia a maioria dos ataques de bots de credential stuffing.

8 Pergunta 8

Resposta correta: Falso

NOTA PARA O PROFESSOR

Um congelamento de crédito impede novas consultas de crédito, mas não afeta as tuas contas existentes.

9 Pergunta 9

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Os gestores de palavras-passe protegem os utilizadores contra o phishing ao recusarem preencher automaticamente palavras-passe em domínios falsificados.

10 Pergunta 10

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

Os e-mails de phishing usam frequentemente linguagem urgente para desencadear respostas emocionais e rápidas.

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

H 1. CREDENCIAIS	D 2. FUGAS	A 3. MFA	G 4. MONITORIZAÇÃO
C 5. CONGELAR	E 6. DEFESA	B 7. SPOOFING	F 8. PHISHING

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 CREDENCIAIS	2 FUGAS	3 MFA	4 MONITORIZAÇÃO
5 CONGELAMENTO	6 DEFESA		

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

1 H – PHISHING	2 A – CREDENCIAIS	3 G – SPOOFING	4 F – DEFESA
5 D – MONITORIZACAO	6 E – CONGELAMENTO	7 B – FUGAS	8 C – AUTENTICACAOMFA

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar CREDENCIAIS, FUGAS e MFA 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.

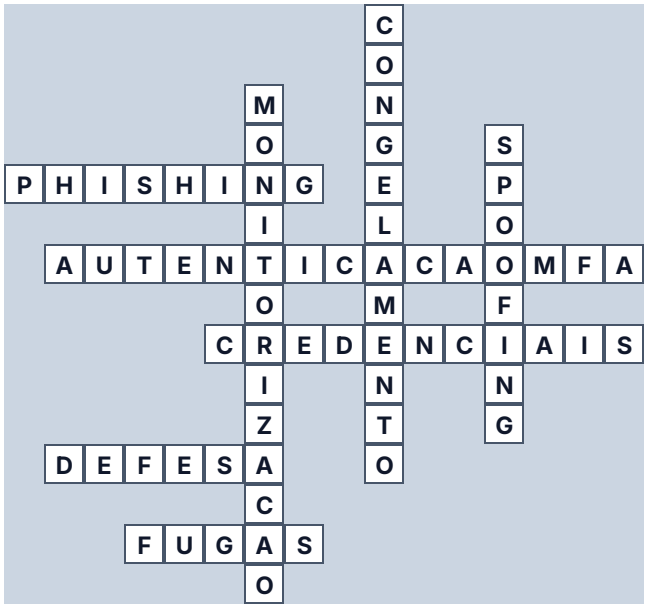
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

4 horizontal: PHISHING Envio de mensagens fraudulentas para levar os utilizadores a revelar credenciais. (8 letras)

5 horizontal: AUTENTICACAOMFA Passo de verificação secundário (como chaves de hardware) que protege os inícios de sessão. (15 letras)

6 horizontal: CREDENCIAIS Nomes de utilizador, palavras-passe e tokens privados usados para autenticar identidades digitais. (11 letras)

7 horizontal: DEFESA Formação e controlos técnicos usados para proteger contra o roubo de identidade. (6 letras)

8 horizontal: FUGAS Exposição não autorizada de bases de dados privadas com registos pessoais de utilizadores. (5 letras)

VERTICAIS

1 vertical: CONGELAMENTO Restringir o acesso aos ficheiros de crédito para evitar pedidos de empréstimo fraudulentos. (12 letras)

2 vertical: MONITORIZACAO Análise de fóruns e canais de hackers à procura de dados corporativos roubados. (13 letras)

3 vertical: SPOOFING Criar um site ou um e-mail falso para imitar uma organização legítima. (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. ECIRNICAESD — **CREDENCIAIS**
2. UTCITCMAAFEAOAN — **AUTENTICACAOMFA**
3. COMATENLOENG — **CONGELAMENTO**
4. ONGIFSPO — **SPOOFING**
5. GSFAU — **FUGAS**
6. TAROCNAZMOIOI — **MONITORIZACAO**
7. SDEAFE — **DEFESA**
8. SHHGPNII — **PHISHING**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"PROTEGE A IDENTIDADE COM AUTENTICACAO MULTIFATOR"

Soluções dos estudos de caso

A Estudo de caso 1: Proteção contra a usurpação de identidade de executivos

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um executivo de topo de uma empresa foi alvo de nomes de domínio com erros ortográficos propositados (typosquatting) que imitam o seu email pessoal para defraudar clientes. Concebe um plano de proteção da marca.
- Estratégia e solução recomendadas: Registar todas as variantes ortográficas comuns do nome do executivo. Implementar protocolos de autenticação de email (DMARC, DKIM, SPF) para impedir a falsificação de domínios. Aplicar MFA por hardware em todos os inícios de sessão da administração.

B Estudo de caso 2: Exposição de credenciais empresariais na dark web

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Uma fuga de uma base de dados na dark web contém várias centenas de credenciais empresariais pertencentes a administradores de sistemas de uma empresa. Concebe uma estratégia de mitigação.
- Estratégia e solução recomendadas: Realizar uma reposição de palavras-passe em toda a empresa. Tornar obrigatório o uso de um gestor de palavras-passe empresarial. Impor a MFA em todos os portais do sistema e configurar alertas contínuos e automatizados de monitorização da dark web.