Name: _____ Date: _____ Score: _____

Identity Theft Prevention & Asset Security Guide

Credential leaks, MFA, dark web monitoring, credit freeze alerts, social engineering

IDENTITY THEFT PREVENTION LEARNING OVERVIEW

SECURED
DATA ENCRYPTION
256-bit AES Standard

COMPLIANT
GLOBAL STANDARDS
GDPR & CCPA Frameworks

ZERO-TRUST
ACCESS POLICY
Multi-Factor Authentication

Welcome! This activity packet guides you through identity theft prevention and mitigation. You will explore credential leaks, multi-factor authentication, dark web monitoring, credit freeze alerts, and social engineering defense.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master cybersecurity and threat prevention.
- [ ] **Part 5-7:** Solve crossword & word search puzzles.
- [ ] **Part 8-9:** Solve case studies & cipher challenge.
- [ ] **Part 10:** Review basic & advanced FAQ pages.
- [ ] **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com Cybersecurity Guide

URL: https://www.vpn.com/cybersecurity/identity-theft/

Your Identity Protection Learning Roadmap

- Understand credentials exposure risks on dark web forums.
- Implement multi-factor authentication (MFA) and credit freeze alerts.
- Design corporate security defenses against targeted social engineering scams.

IDENTITY THEFT GUIDE INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to identity protection.

IDENTITY THEFT PREVENTION & ASSET SECURITY (INTRODUCTION)

Identity theft exploits leaked credentials and weak logins to hijack personal and corporate accounts. Deploying MFA, credit freezes, dark web scanners, and SPF/DKIM/DMARC frameworks forms a critical defense against digital impersonation.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1 **What is the primary method identity thieves use to steal login credentials?**

- ◯ A. Sending fake email alerts tricking users to enter passwords on spoofed portals
- ◯ B. Listening to radio broadcasts near a user's corporate office
- ◯ C. Defragmenting a user's local server storage drive
- ◯ D. Disconnecting external network backup configurations

2 **Which security control provides the strongest defense against credential leaks?**

- ◯ A. Multi-factor authentication using hardware keys
- ◯ B. Creating long passwords using default browser formats
- ◯ C. Changing email usernames every six months
- ◯ D. Deleting stored cookie tracking browser histories

3 **What represents credit freezing?**

- ◯ A. Locking credit reports to prevent thieves from opening unauthorized loans
- ◯ B. Deleting bank account transaction histories from databases
- ◯ C. Disabling credit card magnetic swipe readers on scanners
- ◯ D. Encrypting local database hard drives at rest

4 **Why is dark web monitoring useful?**

- ◯ A. It alerts users if their leaked credentials appear on illicit databases
- ◯ B. It prevents active malware from running in virtual sandboxes
- ◯ C. It accelerates browser routing speeds on virtual networks
- ◯ D. It blocks backend database SQL injection access attempts

5 **What does social engineering mean?**

- ◯ A. Manipulating people into revealing confidential credentials voluntarily
- ◯ B. Scanning corporate server ports for active security exploits
- ◯ C. Backing up system database files to offline hard drives
- ◯ D. Routing network packets through three encrypted onion nodes

Checkpoint 2: True or False Challenge

6 Question 6

Identity theft only affects online digital accounts, not physical postal mail.

◯ True ◯ False

7 Question 7

Enforcing MFA on all personal accounts blocks most credential-stuffing bot attacks.

◯ True ◯ False

8 Question 8

A credit freeze blocks credit checks but prevents you from accessing your own bank account.

◯ True ◯ False

9 Question 9

Password managers protect users from phishing by refusing to auto-fill passwords on spoofed domains.

◯ True ◯ False

10 Question 10

Phishing emails often use urgent language to trigger emotional, fast responses.

◯ True ◯ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. Identity thieves target personal passwords and user _____.
2. Alerting users of database breaches identifies private account _____.
3. Requiring a temporary code to sign in is called _____.
4. Scanning hacker forums for stolen data is dark web _____.
5. Blocking unauthorized credit checks requires a credit _____.
6. Training employees in phishing awareness builds an active security _____.

VOCABULARY WORD BANK

CREDENTIALS	LEAKS	MFA	MONITORING
FREEZE	DEFENSE		

Write your answers here:

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

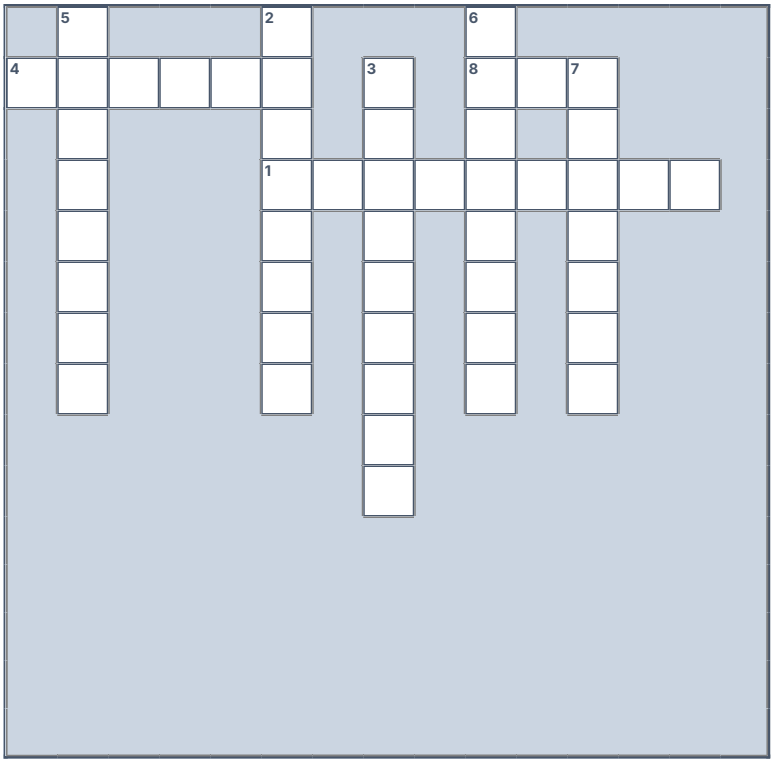
Checkpoint 4: Security Concept Match

DEFINITION MATCHING
Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

CREDENTIALS	**A**	Usernames, passwords, and private tokens used to authenticate digital identities. (A)
LEAKS	**B**	Unauthorized exposure of private databases containing personal user records. (B)
MFA	**C**	Secondary verification step (such as hardware keys) protecting account logins. (C)
MONITORING	**D**	Scanning online forums and hacker channels for stolen corporate data. (D)
FREEZE	**E**	Restricting access to credit files to prevent fraudulent loan applications. (E)
DEFENSE	**F**	Training and technical controls used to protect against identity theft. (F)
SPOOFING	**G**	Creating a fake website or email to mimic a legitimate organization. (G)
PHISHING	**H**	Sending fraudulent messages to trick users into giving up credentials. (H)

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Process of wrapping data packets inside other packets (9)

4. Remote server that routes traffic and hides your IP (6)

8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)

3. Rate of data transfer across a path (9)

5. Blocking site access based on location (8)

6. Security system that monitors and blocks traffic (8)

7. State of being free from tracking or surveillance (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Firm representing clients to negotiate domain sales after identity theft breaches (9 letters):

4 Across: Secured holding account preventing funds release until identity validation checks clear (6 letters):

8 Across: Corporate name asset targeted by thieves using spoofed email domains (5 letters):

DOWN CLUES

2 Down: Financial assessment of damages and credit recovery costs after identity theft (9 letters):

3 Down: Hidden security posture preventing public scanning of domain registrant details (7 letters):

5 Down: ICANN entity where domain WHOIS registrant contact records are locked (9 letters):

6 Down: Authorizing passcode needed to securely transfer domains to a new provider (7 letters):

7 Down: Public bidding market where recovered trademark domain names are sold (7 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

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

VOCABULARY WORD LIST

CREDENTIALS	LEAKS	MFA	MONITORING
FREEZE	DEFENSE	SPOOFING	PHISHING

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

A. CREDENTIALS
B. LEAKS
C. MFA
D. MONITORING
E. FREEZE
F. DEFENSE
G. SPOOFING
H. PHISHING

DEFINITIONS & MATCH FIELDS

_____ 1. Usernames, passwords, and private tokens used to authenticate digital identities.

_____ 2. Unauthorized exposure of private databases containing personal user records.

_____ 3. Secondary verification step

_____ 4. Scanning online forums and hacker channels for stolen corporate data.

_____ 5. Restricting access to credit files to prevent fraudulent loan applications.

_____ 6. Training and technical controls used to protect against identity theft.

_____ 7. Creating a fake website or email to mimic a legitimate organization.

_____ 8. Sending fraudulent messages to trick users into giving up credentials.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key cybersecurity concepts and terms. Write your answers in the input boxes provided.

1. C E D I L N R T A E S

2. K E A L S

3. F M A

4. M O N I I T R O N G

5. Z E E R F E

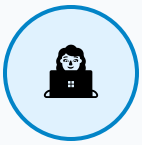
6. S E D E N E F

7. I N G F O O P S

8. G I S H P H I N

Checkpoint 8: Cybersecurity Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.



CASE STUDY 1: EXECUTIVE IDENTITY IMPERSONATION PROTECTION

Scenario: A high-profile C-suite executive has been targeted by typo-squatted domain names mimicking their personal email to defraud clients. Design a brand protection plan.

Discussion Question: Analyze the brand spoofing risks, and detail SPF/DKIM/DMARC and authentication controls.

CASE STUDY 2: CORPORATE CREDENTIALS DARK WEB EXPOSURE

Scenario: A dark web database dump contains several hundred corporate credentials belonging to system administrators of an enterprise. Design a mitigation strategy.

Discussion Question: Outline the credential cleanup process, and plan a password manager roll-out.

Final Challenge: Decrypting the Cipher

A cybersecurity professional protects network assets from online threat actors. Use the Letter-to-Number key below to decrypt the message by writing the matching letters in the blank spaces.

LETTER-TO-NUMBER ENCRYPTION KEY

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	_ 3	_ 20		_ 25	_ 15	_ 21	_ 18

_ 4	_ 9	_ 7	_ 9	_ 20	_ 1	_ 12		_ 9	_ 4	_ 5	_ 14	_ 20	_ 9	_ 20	_ 25		_ 23	_ 9	_ 20	_ 8

_ 13	_ 21	_ 12	_ 20	_ 9	_ 6	_ 1	_ 3	_ 20	_ 15	_ 18		_ 1	_ 21	_ 20	_ 8	_ 5	_ 14	_ 20	_ 9	_ 3	_ 1	_ 20	_ 9	_ 15	_ 14

Decoded cybersecurity message:

_____

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 10: Basic Cybersecurity FAQs (Part A)

Review common questions and answers regarding online threat mitigation.

Q1: What is identity theft?

A crime where an attacker steals personal records (like passwords or SSNs) to impersonate someone else for financial gain.

Q2: What is the most common cause of identity theft?

Phishing emails that trick users into entering their passwords on fake, spoofed websites.

Q3: How does multi-factor authentication (MFA) protect identities?

MFA requires a secondary proof (like a hardware key) to log in, blocking attackers even if they steal your password.

Q4: What is a credit freeze?

A free service blocking credit bureaus from sharing your credit file, stopping thieves from opening new loans in your name.

Q5: What is dark web monitoring?

Software checking hacker forums for leaked emails, passwords, and personal records, alerting you if your data is exposed.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: What does credential stuffing mean?

Automated bots testing leaked password lists across hundreds of websites to take over active accounts.

Q7: Why is email spoofing dangerous?

It allows attackers to fake the sender's name in emails, making phishing messages look like they came from trusted colleagues.

Q8: How do password managers stop identity theft?

They store complex, unique passwords for every account and refuse to auto-fill credentials on fake phishing domains.

Q9: What is spear phishing?

A highly targeted phishing attack customized with the victim's name and details to increase the chance of deception.

Q10: How does a credit alert differ from a freeze?

An alert tells lenders to verify your identity before opening accounts, while a freeze blocks access to your credit file entirely.

Checkpoint 11: Advanced Security FAQs (Part A)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q1: How does SIM swapping lead to identity theft?

Attackers convince carrier staff to transfer the victim's phone number to a new SIM card, hijacking SMS-based 2FA codes.

Q2: What is the role of DMARC in preventing identity theft?

DMARC allows domain owners to block spoofed emails from reaching inboxes, stopping fake emails from mimicking corporate domains.

Q3: Why is synthetic identity theft difficult to detect?

Thieves combine real SSNs with fake names and birthdates to build brand-new credit profiles, bypassing basic fraud alerts.

Q4: How do data brokers exploit personal identities?

Brokers collect public records, web behavior, and purchase histories to compile profile dossiers, which can be leaked or sold.

Q5: Why is SMS-based MFA considered vulnerable?

SMS traffic is vulnerable to interception, phishing, and carrier-level SIM-swapping exploits.

Checkpoint 11: Advanced Security FAQs (Part B)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q6: What is a credit file lock?

A commercial service similar to a freeze, allowing users to instantly unlock or lock their credit file via a mobile app.

Q7: How do corporate data breaches fuel identity theft?

Leaked databases expose millions of plain credentials, giving thieves the raw data needed to execute targeted identity fraud.

Q8: What is the risk of social media oversharing?

Publicly sharing pet names, birthplaces, and mother's maiden names gives thieves the answers to common account recovery questions.

Q9: How do biometric logins protect identity profiles?

Biometrics link logins to physical features (like fingerprints or face maps), which cannot be stolen in database breaches.

Q10: How does the Red Flags Rule combat identity theft?

A federal regulation requiring financial institutions to develop written programs to detect and respond to warning signs of identity theft.

Part 11: 10 Real-World Cybersecurity Facts & Insights

Review real-world facts regarding security breaches, defense mechanisms, and compliance standards.

1. SECURITY INSIGHT

Identity theft reports exceed 1.4 million annually in the United States, representing a leading consumer threat.

2. SECURITY INSIGHT

Enforcing hardware-based security keys stops 100% of automated credential hijacking attempts.

3. SECURITY INSIGHT

Over 80% of data breaches involve compromised passwords, fueling downstream identity fraud.

4. SECURITY INSIGHT

A credit freeze is free by federal law, preventing lenders from checking credit files until unlocked.

5. SECURITY INSIGHT

DMARC security records block billions of spoofed emails daily, stopping identity impersonation at the gateway.

6. SECURITY INSIGHT

SIM swapping allows hackers to bypass SMS-based two-factor authentication on banking portals.

7. SECURITY INSIGHT

Synthetic identity theft represents the fastest-growing form of financial fraud globally.

8. SECURITY INSIGHT

Over 50% of people reuse the same password across multiple online accounts, amplifying breach impacts.

9. SECURITY INSIGHT

Data brokers compile dossiers on hundreds of millions of consumers, presenting a centralized privacy risk.

10. SECURITY INSIGHT

The average time to recover from identity theft exceeds six months, requiring hundreds of hours of work.

Technical References & Sources

The study guide and interactive puzzles are compiled from global NIST, OWASP, and data privacy compliance standards.

SCHOLARLY & INDUSTRY REFERENCES

[1] CISA. (2025). Cybersecurity Alerts & Advisories. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories

[2] GDPR. (2024). General Data Protection Regulation (GDPR) Official Text. Retrieved from https://gdpr-info.eu/

[3] NIST. (2024). Special Publication 800-53: Security and Privacy Controls. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[4] NIST. (2023). Special Publication 800-61: Computer Security Incident Handling Guide. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[5] NIST. (2023). Special Publication 800-88: Guidelines for Media Sanitization. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[6] IETF. (2021). RFC 8446: Transport Layer Security (TLS) 1.3 Specification. Retrieved from https://datatracker.ietf.org/doc/rfc8446/

[7] IETF. (2022). RFC 7519: JSON Web Token (JWT) Specification. Retrieved from https://datatracker.ietf.org/doc/rfc7519/

[8] Center for Internet Security (CIS). (2024). Critical Security Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] OWASP. (2024). Top 10 Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/

[10] OWASP. (2025). Application Security Verification Standard (ASVS). Retrieved from https://owasp.org/www-project-application-security-verification-standard/

Answer Key: Checkpoint 1 - Multiple Choice

1 Brokerage Function BROKERAGE Correct Answer: A

TEACHING NOTE

Domain brokers act as confidential negotiators representing buyers and sellers to reach fair market transactions.

Citation: ICANN Transfer Policy [Ref 1].

2 Stealth Strategy STEALTH Correct Answer: A

TEACHING NOTE

Stealth acquisition conceals corporate buyer identity to prevent sellers from inflating asking prices.

Citation: Escrow.com Protocol [Ref 7].

3 Escrow Protection ESCROW Correct Answer: A

TEACHING NOTE

Licensed third-party escrow holds funds safely until ownership transfer verification is complete.

Citation: Escrow.com Protocol [Ref 7].

4 Domain Appraisal VALUATION Correct Answer: A

TEACHING NOTE

Short 2-letter and 1-word .com domains carry extreme global brand scarcity and liquidity.

Citation: WIPO UDRP Guide [Ref 3].

5 Dispute Resolution UDRP POLICY Correct Answer: A

TEACHING NOTE

ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) governs administrative trademark disputes.

Citation: WIPO Dispute Rules [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Confidential NDAs NDAS Correct Answer: False

TEACHING NOTE

Professional domain brokers operate under non-disclosure agreements to protect buyer corporate strategy.

Citation: CIS Controls [Ref 8].

7 Escrow Delivery ESCROW Correct Answer: True

TEACHING NOTE

Escrow holding accounts disburse funds only after full domain ownership transfer is verified by the buyer.

Citation: Escrow.com Protocol [Ref 7].

8 Digital Real Estate ASSETS Correct Answer: False

TEACHING NOTE

Short 2-letter and 3-letter .com domains function as high-value, liquid digital property assets.

Citation: NIST Guidelines [Ref 9].

9 Stealth Negotiation STRATEGY Correct Answer: True

TEACHING NOTE

Direct corporate buyer outreach often causes sellers to inflate asking prices significantly.

Citation: WIPO UDRP Guide [Ref 3].

10 EPP Authorization EPP CODE Correct Answer: True

TEACHING NOTE

EPP codes are unique security passcodes generated by registrars to authorize domain transfers.

Citation: IETF RFC 5730 [Ref 4].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

A CREDENTIALS	B LEAKS	C MFA	D MONITORING
E FREEZE	F DEFENSE	G SPOOFING	H PHISHING

CHECKPOINT 3: KEY TERM KEY

1 CREDENTIALS	2 LEAKS	3 MFA
4 MONITORING	5 FREEZE	6 DEFENSE

DISCUSSION NOTES FOR INSTRUCTORS

Threat Landscape:

Verify that students understand how malware, phishing, and zero-day attacks target and disrupt network defenses.

Defense Controls:

Emphasize the deployment of network firewalls, sandbox execution, behavior scanners, and multi-factor authentication (MFA).

Regulatory Compliance:

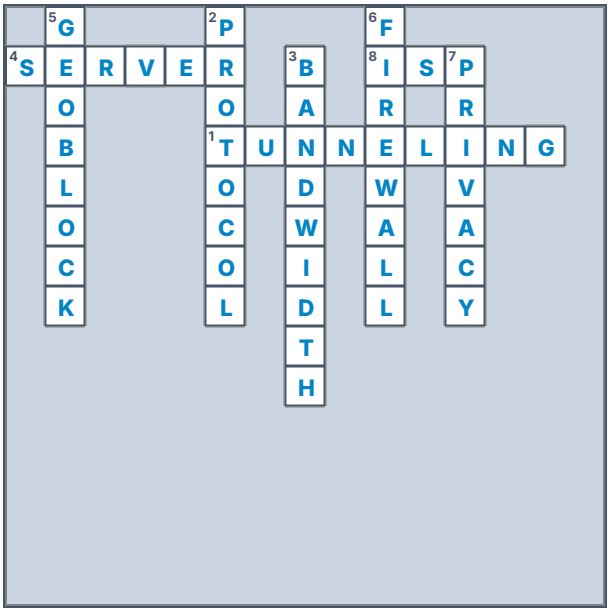
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. C E D I L N R T A E S
   CREDENTIALS

2. K E A L S
   LEAKS

3. F M A
   MFA

4. M O N I I T R O N G
   MONITORING

5. Z E E R F E
   FREEZE

6. S E D E N E F
   DEFENSE

7. I N G F O O P S
   SPOOFING

8. G I S H P H I N
   PHISHING

SECRET CIPHER CHALLENGE KEY

"PROTECT YOUR DIGITAL IDENTITY WITH MULTIFACTOR AUTHENTICATION"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Executive Identity Impersonation Protection

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A high-profile C-suite executive has been targeted by typo-squatted domain names mimicking their personal email to defraud clients. Design a brand protection plan.
- **Recommended Strategy & Solution:** Register all common spelling variants of the executive's name. Deploy email authentication protocols (DMARC, DKIM, SPF) to prevent domain spoofing. Enforce hardware MFA on all C-suite corporate logins.

B Case Study 2: Corporate Credentials Dark Web Exposure

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A dark web database dump contains several hundred corporate credentials belonging to system administrators of an enterprise. Design a mitigation strategy.
- **Recommended Strategy & Solution:** Conduct a company-wide password reset. Mandate the use of an enterprise password manager. Enforce MFA across all system portals and set up continuous automated dark web monitoring alerts.