Name: _____ Date: _____ Score: _____

Public Wi-Fi Security & Encryption

Man-in-the-middle attacks, rogue access points, packet sniffing, VPN tunnels, and HTTPS encryption.

PUBLIC WI-FI SECURITY 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 public Wi-Fi security. You will explore unencrypted networks, man-in-the-middle (MitM) attacks, rogue access points, packet sniffing, VPN tunnels, and HTTPS transit security.

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/public-wifi-security/

Your Public Wi-Fi Security Learning Roadmap

- Identify common public Wi-Fi risks including packet sniffing and rogue access points.
- Implement VPN encryption tunnels to secure transit data.
- Enforce HTTPS and secure web browser settings for remote workers.

PUBLIC WI-FI SECURITY 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 remote access security.

PUBLIC WI-FI SECURITY & TRANSIT PROTECTION (INTRODUCTION)

Unencrypted public Wi-Fi hotspots leave network traffic exposed to packet sniffing and Evil Twin spoofing. Forcing traffic through secure VPN encryption tunnels and enforcing HTTPS-only HSTS rules shields sessions from local network interception.

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

Checkpoint 1: Multiple Choice Challenge

1 What is a Man-in-the-Middle (MitM) attack?

- ◯ A. Intercepting and altering communications between two parties on a shared network
- ◯ B. A database extraction technique targeting user records
- ◯ C. Overwhelming web servers with network traffic requests
- ◯ D. Wiping local hard drive storage volumes

2 What is a rogue access point (Evil Twin)?

- ◯ A. A malicious Wi-Fi hotspot configured with the same SSID as a legitimate network
- ◯ B. An administrative tool used to monitor database backups
- ◯ C. A secure VPN gateway configuration
- ◯ D. A DNS record that maps authorized mail servers

3 How does a VPN protect public Wi-Fi traffic?

- ◯ A. It wraps all network packets in an encrypted tunnel, rendering them unreadable to sniffers
- ◯ B. It automatically blocks all incoming connection requests
- ◯ C. It changes the MAC address of the physical network card
- ◯ D. It deletes cached cookies in the web browser

4 What is packet sniffing?

- ◯ A. Using hardware or software tools to capture and log network packets
- ◯ B. Scanning local directories for duplicate files
- ◯ C. Restricting database read privileges based on user roles
- ◯ D. Encrypting storage drives using AES-256 keys

5 What is the role of HTTPS?

- ◯ A. Encrypting session traffic between the browser and the web server
- ◯ B. Filtering incoming email messages at the gateway
- ◯ C. Authenticating domain names in global registries
- ◯ D. Managing file structures in network-attached storage

Checkpoint 2: True or False Challenge

6 Question 6

Connected users can easily capture plaintext data on open public Wi-Fi networks.

◯ True ◯ False

7 Question 7

Rogue access points (Evil Twins) are always authorized by network administrators.

◯ True ◯ False

8 Question 8

A VPN is ineffective at protecting traffic against packet sniffing on public networks.

◯ True ◯ False

9 Question 9

HTTPS encrypts only the URL path, leaving the packet payload in plaintext.

◯ True ◯ False

10 Question 10

Wi-Fi hotspots using WPA3 security offer stronger protection than open, password-less networks.

◯ 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. Capturing private passwords on public Wi-Fi is communication _____.
2. Analyzing raw packets on a local network uses packet _____.
3. A rogue hotspot mimicking a hotel Wi-Fi is an _____.
4. Securing web traffic transit requires encrypting with _____.
5. Encrypting all network outputs uses a client _____.
6. An encrypted communication path through public networks is a _____.

VOCABULARY WORD BANK

INTERCEPTION	SNIFFING	EVILTWIN	HTTPS
VPN	TUNNEL		

Write your answers here:

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

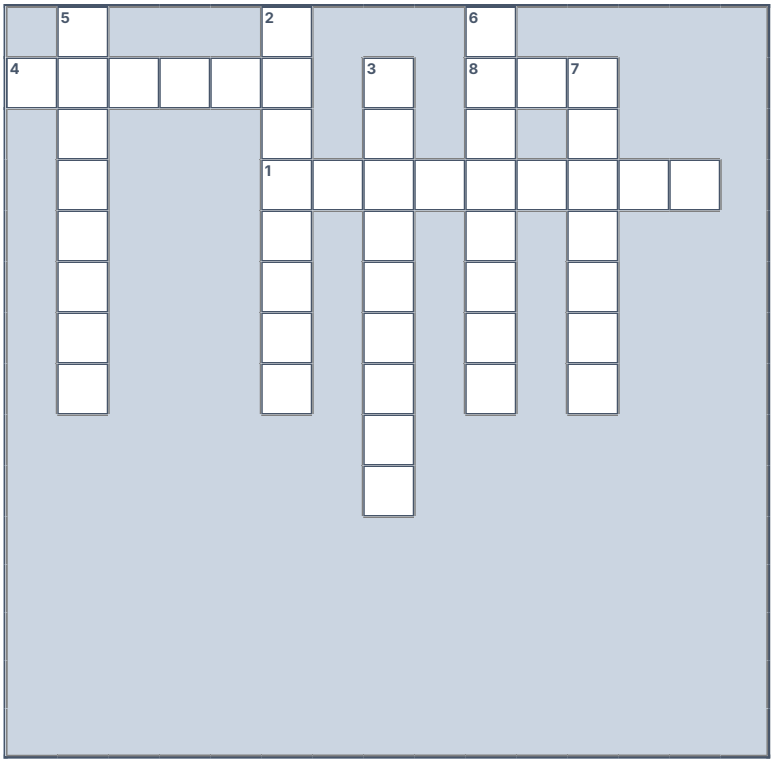
Checkpoint 4: Security Concept Match

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.

INTERCEPTION	**A** Reading traffic in transit. (A)
SNIFFING	**B** Capturing network data packets. (B)
EVILTWIN	**C** Rogue hotspot mimicking Wi-Fi. (C)
HTTPS	**D** Secure web transmission. (D)
VPN	**E** Encrypted virtual private network. (E)
TUNNEL	**F** Secure data path in transit. (F)
WPA3	**G** Modern Wi-Fi security standard. (G)
FIREWALL	**H** Filtering incoming traffic. (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: Capturing private data packets in transit on open networks. (12 letters):

4 Across: Monitoring and logging network traffic using raw capture tools. (8 letters):

8 Across: Rogue access point mimicking a legitimate Wi-Fi hotspot. (8 letters):

DOWN CLUES

2 Down: Securing web transit traffic using SSL/TLS encryption. (5 letters):

3 Down: Virtual private network client routing encrypted data tunnels. (3 letters):

5 Down: Encrypted transmission path wrapping local network packets. (6 letters):

6 Down: Modern Wi-Fi security protocol offering offline crack protection. (4 letters):

7 Down: Filtering inbound connections at the device boundary. (8 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	A	R	I	N	T	E	R	C	E	P	T	I	O	N
Q	A	G	J	C	J	Y	H	L	A	J	I	T	F	A
D	W	P	A	3	W	O	R	T	E	L	X	G	S	Y
E	O	I	R	U	B	S	G	Y	T	X	Q	J	K	C
D	B	H	O	O	K	H	N	L	U	P	O	T	C	A
K	D	F	C	V	Z	J	T	I	B	K	S	R	Y	P
R	F	T	K	E	J	I	Q	Z	F	V	I	J	K	L
Y	C	K	U	A	V	O	O	F	K	F	Q	Z	T	T
V	U	R	D	N	W	I	J	T	R	H	I	D	V	V
H	E	L	M	X	N	H	L	Q	B	F	L	N	G	M
T	I	Q	L	F	H	E	T	T	U	K	S	K	G	V
T	K	J	Y	O	R	L	L	R	W	J	W	N	O	P
A	P	G	O	S	M	F	Z	J	X	I	C	V	T	X
Y	Y	M	D	B	U	K	D	D	A	M	N	P	I	J
Y	K	T	J	F	I	R	E	W	A	L	L	N	K	Q

VOCABULARY WORD LIST

INTERCEPTION	SNIFFING	EVILTWIN	HTTPS
VPN	TUNNEL	WPA3	FIREWALL

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. INTERCEPTION
B. SNIFFING
C. EVILTWIN
D. HTTPS
E. VPN
F. TUNNEL
G. WPA3
H. FIREWALL

DEFINITIONS & MATCH FIELDS

_____ 1. Reading traffic in transit.

_____ 2. Capturing network data packets.

_____ 3. Rogue hotspot mimicking Wi-Fi.

_____ 4. Secure web transmission.

_____ 5. Encrypted virtual private network.

_____ 6. Secure data path in transit.

_____ 7. Modern Wi-Fi security standard.

_____ 8. Filtering incoming traffic.

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. N O I T P E C R E T N I

2. G N I F F I N S

3. N I W T L I V E

4. S P T T H

5. N P V

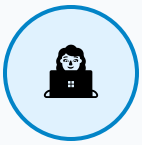
6. L E N N U T

7. 3 A P W

8. L L A W E R I F

Checkpoint 8: Cybersecurity Case Studies

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



CASE STUDY 1: PUBLIC WI-FI PACKET SNIFFING CONTAINMENT

Scenario: A remote sales executive connected to a public airport Wi-Fi network notices several sensitive business emails are leaked shortly after sending them in plaintext.

Discussion Question: Analyze public network risks, and outline a traffic encryption solution.

CASE STUDY 2: EVIL TWIN ROGUE HOTSPOT DEFENSE

Scenario: Attackers deploy a rogue wireless access point named 'CoffeeShop_Guest' mimicking a legitimate cafe hotspot, capturing network traffic from unsuspecting guests.

Discussion Question: Detail the verification steps to detect and block rogue access points.

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

5	14	3	18	25	16	20	16	21	2	12	9	3

23	9	6	9	14	5	20	23	15	18	11	20	18	1	6	6	9	3

23	9	20	8	22	16	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: Why is public Wi-Fi unsecure?

Most public Wi-Fi networks do not encrypt data packets, allowing anyone on the same network to intercept them.

Q2: What is packet sniffing?

A packet sniffer captures raw data flowing over a network interface, exposing plaintext passwords and traffic details.

Q3: What is an Evil Twin?

A rogue access point set up by hackers that mimics the name and settings of a trusted local Wi-Fi hotspot.

Q4: How does a VPN protect me?

It routes your traffic through an encrypted tunnel, hiding your browsing activity from local network sniffers.

Q5: Does HTTPS protect me on public Wi-Fi?

Yes, it encrypts the data exchanged between your browser and the website, but a VPN offers additional layout protection.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: What is WPA3?

The modern Wi-Fi Protected Access standard, offering stronger encryption and protection against offline dictionary attacks.

Q7: Can public Wi-Fi deliver malware?

Yes, attackers can intercept traffic and inject malicious download prompts (drive-by downloads) into your browser session.

Q8: What is the risk of file sharing?

If file sharing is enabled, other users on the public network can read or modify your local folder directory.

Q9: What is a captive portal?

The login page hotel or cafe networks use to grant internet access, which can sometimes be spoofed by attackers.

Q10: Should I turn off Wi-Fi when not using it?

Yes, disabling Wi-Fi prevents your device from automatically connecting to untrusted networks.

Checkpoint 11: Advanced Security FAQs (Part A)

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

Q1: How does a Man-in-the-Middle attack exploit DNS?

By using DNS spoofing on a rogue router to direct target browsers to lookalike phishing landing pages instead of target domains.

Q2: What is session hijacking?

An attacker sniffing an unencrypted session cookie over public Wi-Fi and importing it to bypass credentials logins.

Q3: What is SSL stripping?

A MitM attack where an attacker downgrades a user's secure HTTPS request to unencrypted HTTP, capturing logins in plaintext.

Q4: How does HSTS protect against SSL stripping?

HTTP Strict Transport Security forces browsers to connect only via HTTPS, refusing unencrypted HTTP fallbacks.

Q5: What is a split-tunnel VPN?

A configuration routing only corporate traffic through the VPN while sending public internet data directly, which can risk leak path exposure.

Checkpoint 11: Advanced Security FAQs (Part B)

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

Q6: Why is WPA2 vulnerable to KRACK?

The Key Reinstallation Attack exploits the WPA2 four-way handshake to decrypt packets without the Wi-Fi password.

Q7: What is client isolation?

A router security setting preventing connected Wi-Fi devices from communicating with each other directly, blocking local sniffing.

Q8: How do attackers use fake DNS servers?

They configure rogue routers to assign fake DNS servers to clients, allowing them to intercept and rewrite all web lookups.

Q9: Can a VPN hide my local MAC address?

No, MAC addresses are layer-2 identifiers used locally; you must use software-based MAC address spoofing to hide it.

Q10: What is a captive portal spoofing attack?

An attacker hosting a fake authentication portal on a rogue hotspot to steal credentials under the guise of free Wi-Fi access.

Part 11: 10 Real-World Cybersecurity Facts & Insights

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

1. SECURITY INSIGHT

Over 60% of remote workers connect their corporate devices to unsecured public Wi-Fi networks weekly.

2. SECURITY INSIGHT

An Evil Twin rogue hotspot can copy the exact name and MAC address of a trusted network, confusing devices.

3. SECURITY INSIGHT

Packet sniffing software like Wireshark is free and can display unencrypted HTTP passwords in clear text.

4. SECURITY INSIGHT

WPA3 security utilizes Simultaneous Authentication of Equals (SAE) to protect against local brute force attacks.

5. SECURITY INSIGHT

SSL stripping attacks bypass basic HTTPS protections by intercepting initial HTTP redirects at the gateway.

6. SECURITY INSIGHT

HTTP Strict Transport Security (HSTS) DNS records protect browsers from falling back to unencrypted HTTP connections.

7. SECURITY INSIGHT

Turning off 'Auto-Connect' prevents smartphones from connecting to lookalike rogue networks in public spaces.

8. SECURITY INSIGHT

Enterprise 'always-on' VPN configurations force all remote worker network traffic through corporate firewalls.

9. SECURITY INSIGHT

Rogue access points can inject malicious code into DNS caches, redirecting target domains to phishing nodes.

10. SECURITY INSIGHT

Connecting to a public Wi-Fi without a VPN exposes your active device operating system version to local hackers.

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: True

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: False

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: False

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 INTERCEPTION	B SNIFFING	C EVILTWIN	D HTTPS
E VPN	F TUNNEL	G WPA3	H FIREWALL

CHECKPOINT 3: KEY TERM KEY

1 INTERCEPTION	2 SNIFFING	3 EVILTWIN
4 HTTPS	5 VPN	6 TUNNEL

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:

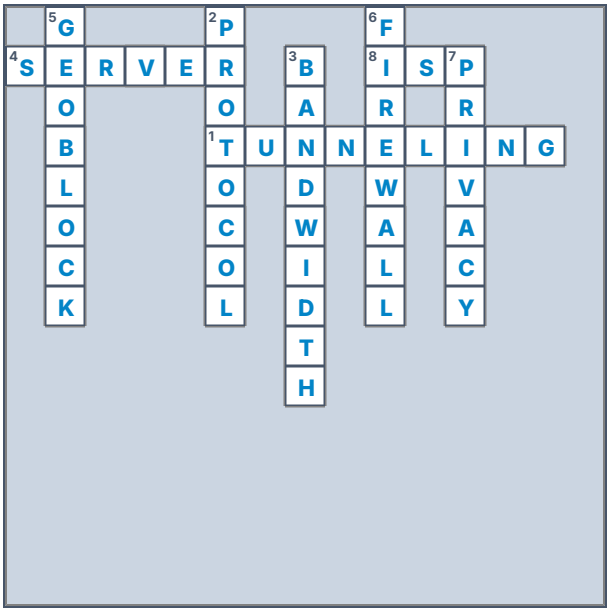
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

J	A	R	I	N	T	E	R	C	E	P	T	I	O	N
Q	A	G	J	C	J	Y	H	L	A	J	I	T	F	A
D	W	P	A	3	W	O	R	T	E	L	X	G	S	Y
E	O	I	R	U	B	S	G	Y	T	X	Q	J	K	C
D	B	H	O	O	K	H	N	L	U	P	O	T	C	A
K	D	F	C	V	Z	J	T	I	B	K	S	R	Y	P
R	F	T	K	E	J	I	Q	Z	F	V	I	J	K	L
Y	C	K	U	A	V	O	O	F	K	F	Q	Z	T	T
V	U	R	D	N	W	I	J	T	R	H	I	D	V	V
H	E	L	M	X	N	H	L	Q	B	F	L	N	G	M
T	I	Q	L	F	H	E	T	T	U	K	S	K	G	V
T	K	J	Y	O	R	L	L	R	W	J	W	N	O	P
A	P	G	O	S	M	F	Z	J	X	I	C	V	T	X
Y	Y	M	D	B	U	K	D	D	A	M	N	P	I	J
Y	K	T	J	F	I	R	E	W	A	L	L	N	K	Q

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. N O I T P E C R E T N I
   INTERCEPTION

2. G N I F F I N S
   SNIFFING

3. N I W T L I V E
   EVILTWIN

4. S P T T H
   HTTPS

5. N P V
   VPN

6. L E N N U T
   TUNNEL

7. 3 A P W
   WPA3

8. L L A W E R I F
   FIREWALL

SECRET CIPHER CHALLENGE KEY

"ENCRYPT PUBLIC WIFI NETWORK TRAFFIC WITH VPN"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Public Wi-Fi Packet Sniffing Containment

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A remote sales executive connected to a public airport Wi-Fi network notices several sensitive business emails are leaked shortly after sending them in plaintext.
- **Recommended Strategy & Solution:** Mandate the use of an enterprise VPN client on all remote workstations. Enforce HTTPS-only browser extensions, and block unencrypted protocols (like HTTP and FTP) at the client firewall.

B Case Study 2: Evil Twin Rogue Hotspot Defense

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** Attackers deploy a rogue wireless access point named 'CoffeeShop_Guest' mimicking a legitimate cafe hotspot, capturing network traffic from unsuspecting guests.
- **Recommended Strategy & Solution:** Audit access point BSSID MAC addresses to verify network authenticity. Enforce client posture validation to block connection to open networks, and mandate cellular hotspots for sensitive work.