Name: _____ Date: _____ Score: _____

Cybersecurity Basics & Online Threat Prevention

Cybersecurity threats, network firewalls, multi-factor authentication, security frameworks

CYBERSECURITY BASICS 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 the fundamental principles of Cybersecurity Basics & Online Threat Prevention. You will explore malware threats, multi-factor authentication, network firewalls, and incident response frameworks.

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/

Your Cybersecurity Basics Learning Roadmap

- Identify common vectors of malware, phishing, and corporate network intrusion.
- Implement standard cybersecurity controls including MFA, firewalls, and endpoint defense.
- Evaluate incident response procedures for mitigating data breach impacts.
- Analyze organizational risk factors and security alignment under NIST guidelines.
- Configure security hygiene practices to mitigate automated credential stuffing.

CYBERSECURITY 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 threat prevention.

CYBERSECURITY BASICS & THREAT PREVENTION (INTRODUCTION)

Cybersecurity protects networks, systems, and data from unauthorized digital attacks. Developing robust security habits, configuring firewalls, requiring multi-factor authentication, and training staff in threat recognition are essential components of corporate network defense.

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

Checkpoint 1: Multiple Choice Challenge

1 **What is the primary objective of a phishing attack?**

- ◯ A. Stealing credentials and sensitive user data
- ◯ B. Enhancing website search engine visibility
- ◯ C. Increasing network bandwidth capacity
- ◯ D. Managing backup data center replication

2 **Which mechanism provides the strongest account protection?**

- ◯ A. Multi-factor authentication using hardware keys
- ◯ B. Complex passwords updated every thirty days
- ◯ C. Restricting account login to business hours
- ◯ D. Hiding the account username from public directories

3 **What defines a ransomware infection payload?**

- ◯ A. Encrypting system files and demanding payment
- ◯ B. Silently logging keystrokes to remote servers
- ◯ C. Injecting unauthorized advertising into browsers
- ◯ D. Using local CPU resources to mine cryptocurrency

4 **How does a zero-day exploit impact security defenses?**

- ◯ A. It targets unpatched, unknown vulnerabilities
- ◯ B. It automatically disables the corporate firewall
- ◯ C. It forces the system to perform a hard reboot
- ◯ D. It requires zero budget to remediate

5 **Which framework governs corporate security controls?**

- ◯ A. NIST Cybersecurity Framework guidelines
- ◯ B. W3C HTML5 document schema specifications
- ◯ C. ICANN registry transfer policy models
- ◯ D. IETF routing protocol definitions

Checkpoint 2: True or False Challenge

6 Question tf1

Phishing attacks only target personal email accounts.

◯ True ◯ False

7 Question tf2

Multi-factor authentication prevents credential stuffing exploits.

◯ True ◯ False

8 Question tf3

Firewalls inspect network traffic to block unauthorized port access.

◯ True ◯ False

9 Question tf4

Remediation of zero-day exploits requires standard anti-virus definition updates.

◯ True ◯ False

10 Question tf5

A honeypot is a decoy server used to lure cyber criminals.

◯ 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. Network administrators install a _____ to filter incoming traffic.
2. An attacker uses a zero-day _____ to bypass system patches.
3. Attackers send spoofed emails to conduct _____ campaigns against employees.
4. Ransomware is a destructive form of _____ that locks user data.
5. Establishing strong password _____ mitigates credential theft risks.
6. To protect sensitive communications, users apply _____ protocols.

VOCABULARY WORD BANK

MALWARE	PHISHING	FIREWALL	ENCRYPTION
HONEYPOT	EXPLOIT	INCIDENT	HYGIENE

Write your answers here:

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

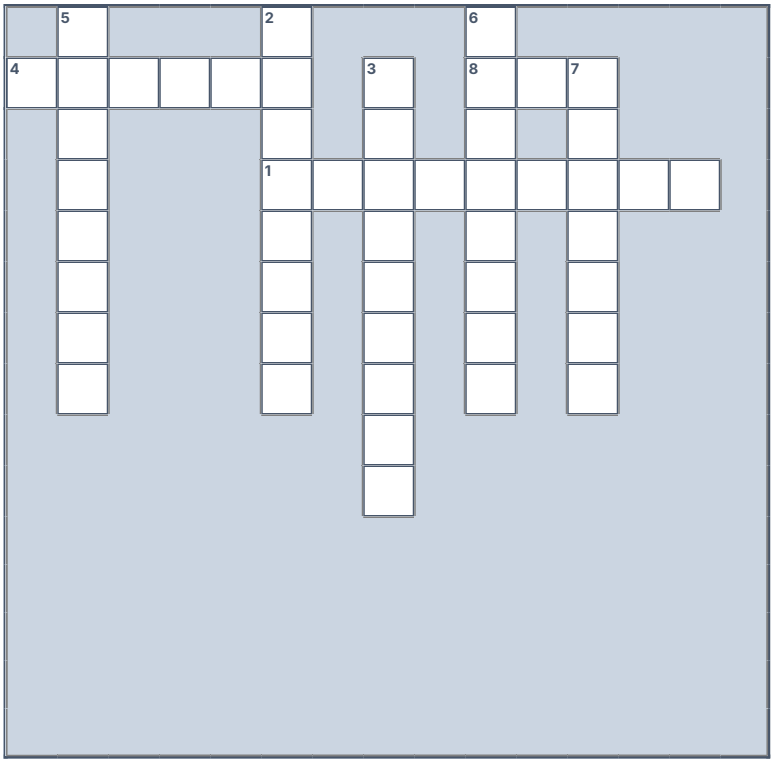
Checkpoint 4: Security Concept Match

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.

1. Ransomware Threat	**A** Malware encrypting data and demanding financial payment for decryption.
2. Multi-Factor Auth	**B** Security validation requiring two or more authentication factors.
3. Zero-Day Exploit	**C** Vulnerability exploit targeted before a vendor patch is released.
4. Decoy Honeypot	**D** Decoy system set up to lure and analyze malicious actors.
5. Intrusion Firewall	**E** Network barrier filtering traffic based on security rules.
6. Incident Response	**F** Structured plan for handling and mitigating security breaches.
7. Password Hygiene	**G** Best practices for managing credentials and authentication keys.
8. Security Framework	**H** Structured guidelines like NIST used to manage cyber risks.

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: Wrapping data packets inside secure transport protocols. (9 letters):

4 Across: Network node acting as hosting anchor for virtual links. (6 letters):

8 Across: ISP gateway provider controlling endpoint routing links. (3 letters):

DOWN CLUES

2 Down: Standard formatting protocol governing online transmissions. (8 letters):

3 Down: Total transmission volume processed through physical links. (9 letters):

5 Down: Restricting resource availability by tracking geographic IP ranges. (8 letters):

6 Down: Intrusion protection system filtering local traffic segments. (8 letters):

7 Down: Confidential asset state shielded from public exposure. (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.

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

VOCABULARY WORD LIST

MALWARE	PHISHING	FIREWALL	HONEYPOT
EXPLOIT	INCIDENT	HYGIENE	ENCRYPTION

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. MALWARE
B. PHISHING
C. FIREWALL
D. HONEYPOT
E. EXPLOIT
F. INCIDENT
G. HYGIENE
H. ENCRYPTION

DEFINITIONS & MATCH FIELDS

_____ 1. Malware encrypting data and demanding financial payment for decryption.

_____ 2. Security validation requiring two or more authentication factors.

_____ 3. Vulnerability exploit targeted before a vendor patch is released.

_____ 4. Decoy system set up to lure and analyze malicious actors.

_____ 5. Network barrier filtering traffic based on security rules.

_____ 6. Structured plan for handling and mitigating security breaches.

_____ 7. Best practices for managing credentials and authentication keys.

_____ 8. Structured guidelines like NIST used to manage cyber risks.

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. E R A W L A M

2. I N G S H I H P

3. L A W E R I F L

4. P O T Y E N O H

5. P L O I T E X

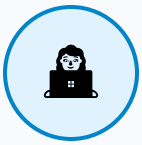
6. D E N T I C I N

7. E N E I G Y H

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

Checkpoint 8: Cybersecurity Case Studies

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



CASE STUDY 1: RANSOMWARE RECOVERY STRATEGY

Scenario: A corporate network is infected with ransomware, locking critical databases. The attackers demand a $100,000 cryptocurrency payout. The company has offline backups from 24 hours ago.

Discussion Question: Analyze the risks of paying, and evaluate the recovery strategy.

CASE STUDY 2: CREDENTIAL STUFFING DEFENSES

Scenario: An online service experiences a credential stuffing attack, with hackers testing millions of username/password pairs stolen from other sites.

Discussion Question: Detail the mechanism of this attack, and outline two defense systems.

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

19	5	3	21	18	5	25	15	21	18

19	25	19	20	5	13	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 the main objective of cybersecurity?

The main objective is protecting networks, devices, and data from unauthorized access, attacks, and accidental damage.

Q2: How does phishing differ from spear phishing?

Phishing is a broad email campaign targeting random users, while spear phishing targets specific individuals using personalized data.

Q3: What is a network firewall?

A firewall is a network security system that monitors and filters incoming and outgoing traffic based on pre-defined security rules.

Q4: Why is multi-factor authentication (MFA) necessary?

MFA adds a critical layer of defense, preventing access even if attackers steal or crack the primary password credentials.

Q5: What defines a computer virus?

A virus is self-replicating malware that attaches itself to clean files and spreads across systems once executed.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: How does ransomware lock local data?

Ransomware uses cryptographic algorithms to encrypt user files, rendering them unreadable until a decryption key is applied.

Q7: What is a zero-day vulnerability?

A zero-day is a security flaw in software that is unknown to the vendor, leaving no time for patch development before exploit.

Q8: What is the role of the NIST framework?

The NIST framework provides voluntary guidelines and standards to help organizations manage and reduce cybersecurity risks.

Q9: What is a security incident response plan?

It is a documented set of procedures for detecting, containing, and recovering from security breaches and network compromise.

Q10: How does social engineering exploit users?

Social engineering uses psychological manipulation to trick employees into revealing passwords or downloading malicious files.

Checkpoint 11: Advanced Security FAQs (Part A)

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

Q1: How does a DDoS attack overwhelm web servers?

A DDoS attack coordinates millions of compromised botnet devices to flood a server with traffic, exhausting bandwidth and CPU limits.

Q2: What is the difference between symmetric and asymmetric encryption?

Symmetric encryption uses a single key for encryption and decryption, while asymmetric encryption uses a public and private key pair.

Q3: How do hackers execute SQL injection attacks?

Attackers input malicious SQL commands into form fields, tricking the backend database into releasing unauthorized user records.

Q4: What is lateral movement in network intrusions?

It is the technique where attackers exploit initial server access to compromise other interconnected systems on the internal network.

Q5: How does DNS spoofing redirect web traffic?

DNS spoofing alters nameserver cache records, routing legitimate users to malicious lookalike websites instead of target domains.

Checkpoint 11: Advanced Security FAQs (Part B)

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

Q6: What is a hardware security token?

It is a physical device (like a YubiKey) generating cryptographic authentication proofs, offering maximum defense against remote phishing.

Q7: How do security teams use decoy honeypots?

Teams deploy non-production decoy servers to detect intrusions early and analyze the attack patterns of unauthorized actors.

Q8: What is the principle of least privilege?

It is the security standard of restricting user access rights to the absolute minimum necessary to perform their work roles.

Q9: How does a Man-in-the-Middle attack exploit connections?

An attacker intercepts and alters communications between two devices on unencrypted networks, stealing session tokens and credentials.

Q10: What are indicators of compromise (IOCs)?

IOCs are forensic data clues, such as unusual registry modifications or rogue IP traffic, showing a system was breached.

Part 11: 10 Real-World Cybersecurity Facts & Insights

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

1. SECURITY INSIGHT

Cybersecurity attacks occur globally every 39 seconds, targeting vulnerable network servers and employee inboxes.

2. SECURITY INSIGHT

Human error, including clicking phishing links, accounts for over 90% of documented corporate data breaches.

3. SECURITY INSIGHT

The average cost of a corporate data breach exceeds $4 million, including legal fines, customer churn, and repair costs.

4. SECURITY INSIGHT

Hardware-based MFA tokens prevent 100% of automated bot takeovers and bulk phishing credential theft attempts.

5. SECURITY INSIGHT

Ransomware threat volume has grown over 200% annually, becoming the primary threat vector for enterprise networks.

6. SECURITY INSIGHT

The NIST Cybersecurity Framework is divided into five core functions: Identify, Protect, Detect, Respond, and Recover.

7. SECURITY INSIGHT

Credential stuffing bots test billions of leaked username pairs daily against corporate banking and ecommerce login portals.

8. SECURITY INSIGHT

Zero-day exploit markets operate globally, with high-severity vulnerabilities trading for millions of dollars among actors.

9. SECURITY INSIGHT

A honeypot decoy system reports intrusion alerts immediately since legitimate users have no reason to access it.

10. SECURITY INSIGHT

Transport Layer Security (TLS) encrypts browser sessions, preventing packet sniffing on public Wi-Fi networks.

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 Phishing Attacks PHISHING Correct Answer: A

TEACHING NOTE

Phishing campaigns attempt to steal credentials and sensitive user data using spoofed emails.

Citation: OWASP Secure Configuration [Ref 10].

2 Account Protection MFA KEY Correct Answer: A

TEACHING NOTE

Multi-factor authentication (MFA) utilizing hardware tokens provides the strongest account access defense.

Citation: NIST Digital Identity [Ref 9].

3 Ransomware Threat RANSOMWARE Correct Answer: A

TEACHING NOTE

Ransomware encrypts critical systems and data, demanding cryptocurrency payment for decryption keys.

Citation: Center for Internet Security (CIS) [Ref 8].

4 Zero-Day Vulnerability ZERO-DAY Correct Answer: A

TEACHING NOTE

Zero-day threats exploit unpatched, unknown security flaws before a vendor patch is made available.

Citation: OWASP Secure Configuration [Ref 10].

5 Security Frameworks FRAMEWORKS Correct Answer: A

TEACHING NOTE

Frameworks like NIST provide structured guidelines to help organizations manage and reduce cyber risks.

Citation: NIST Digital Identity [Ref 9].

Answer Key: Checkpoint 2 - True or False

6 Target Phishing PHISHING — Correct Answer: False

TEACHING NOTE

Phishing attacks target both corporate networks and personal accounts to expand exploit vectors.

Citation: OWASP Secure Configuration [Ref 10].

7 MFA Protections MFA KEY — Correct Answer: True

TEACHING NOTE

Multi-factor authentication prevents credential stuffing since logins require physical token proof.

Citation: NIST Digital Identity [Ref 9].

8 Traffic Firewall FIREWALL — Correct Answer: True

TEACHING NOTE

Firewalls inspect and block traffic on specific network ports to filter out unauthorized connections.

Citation: Center for Internet Security (CIS) [Ref 8].

9 Zero-Day Response ZERO-DAY — Correct Answer: False

TEACHING NOTE

Remediating zero-day flaws requires code patches and WAF filtering since signatures do not exist yet.

Citation: OWASP Secure Configuration [Ref 10].

10 Decoy Honeypots HONEYPOT — Correct Answer: True

TEACHING NOTE

Honeypots are deceptive servers used by security teams to lure, alert, and study malicious actors.

Citation: Center for Internet Security (CIS) [Ref 8].

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 1. Ransomware Threat	B 2. Multi-Factor Auth	C 3. Zero-Day Exploit	D 4. Decoy Honeypot
E 5. Intrusion Firewall	F 6. Incident Response	G 7. Password Hygiene	H 8. Security Framework

CHECKPOINT 3: KEY TERM KEY

1 FIREWALL	2 EXPLOIT	3 PHISHING
4 MALWARE	5 HYGIENE	6 ENCRYPTION

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:

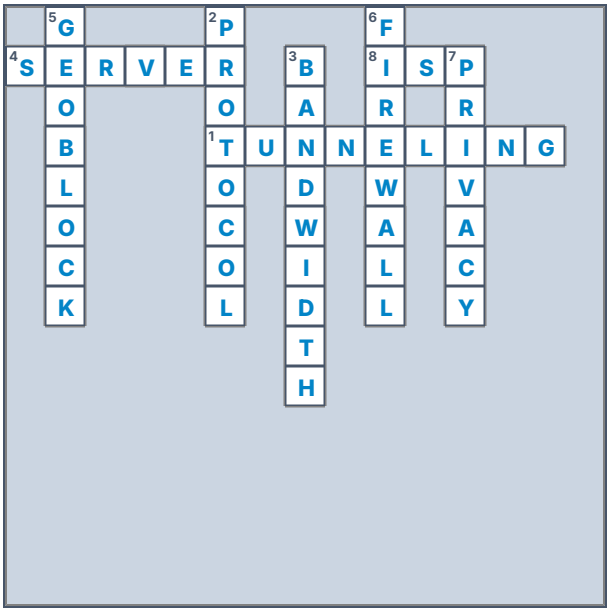
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. E R A W L A M
   MALWARE

2. I N G S H I H P
   PHISHING

3. L A W E R I F L
   FIREWALL

4. P O T Y E N O H
   HONEYPOT

5. P L O I T E X
   EXPLOIT

6. D E N T I C I N
   INCIDENT

7. E N E I G Y H
   HYGIENE

8. I R C O P T N Y E N
   ENCRYPTION

SECRET CIPHER CHALLENGE KEY

"SECURE YOUR SYSTEM WITH MULTI FACTOR AUTHENTICATION"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Ransomware Recovery Strategy

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A corporate network is infected with ransomware, locking critical databases. The attackers demand a $100,000 cryptocurrency payout. The company has offline backups from 24 hours ago.
- **Recommended Strategy & Solution:** Risks of Paying: Paying does not guarantee file decryption, labels the company as a paying target, and funds criminal activity. Recovery Strategy: The team should isolate infected hosts, wipe compromised servers, and restore data from offline backups. They must patch the initial access vector (phishing or exploit) to prevent immediate reinfection.

B Case Study 2: Credential Stuffing Defenses

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An online service experiences a credential stuffing attack, with hackers testing millions of username/password pairs stolen from other sites.
- **Recommended Strategy & Solution:** Mechanism: Attackers leverage password reuse across sites using automated bots to log into user accounts. Defenses: 1. Multi-factor authentication (MFA) blocks login attempts even if password is correct. 2. Implementing rate-limiting and CAPTCHAs blocks automated bot traffic from spamming login endpoints.