Name: _____ Date: _____ Score: _____

Phishing Attacks & Social Engineering

Spear phishing, whaling scams, SPF/DKIM/DMARC protocols, sender spoofing, and employee security training.

PHISHING ATTACKS 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 phishing attacks and social engineering. You will explore spear phishing, whaling, domain spoofing, SPF/DKIM/DMARC protocols, link safety, and employee awareness training.

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/phishing-attacks/

Your Phishing Mitigation Learning Roadmap

- Identify common phishing, vishing, and support pop-up scams.
- Implement out-of-band transaction verification procedures.
- Configure SPF, DKIM, and DMARC rules to block spoofed domains.

PHISHING ATTACKS 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 email authentication.

PHISHING ATTACKS & SOCIAL ENGINEERING (INTRODUCTION)

Phishing attacks utilize targeted messages, whaling scams, and domain spoofing to harvest user login credentials. Securing corporate systems requires deploying SPF, DKIM, and DMARC rules at the gateway alongside out-of-band approval steps.

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

Checkpoint 1: Multiple Choice Challenge

1 What is spear phishing?

- A. A targeted phishing email tailored to a specific individual or organization
- B. A broad bulk email sent to millions of random addresses
- C. A network attack that floods web servers with traffic
- D. A database extraction technique targeting user records

2 Which protocol prevents email sender spoofing by mapping authorized IP addresses in DNS?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 What is a whaling attack?

- A. A phishing campaign targeted specifically at high-profile corporate executives
- B. An SQL injection attack targeting database backups
- C. A physical theft of local area network router equipment
- D. An automated credential stuffing brute-force scan

4 What does DKIM do?

- A. Adds a cryptographic signature to emails to verify sender authenticity
- B. Blocks incoming network packet traffic at the firewall
- C. Encrypts database storage volumes at rest
- D. Scans email attachments for signature-based malware

5 What is the role of DMARC?

- A. Directing receiving email servers on how to handle failed SPF/DKIM checks
- B. Decrypting system passwords using precomputed rainbow tables
- C. Establishing secure VPN tunnels between remote offices
- D. Configuring network routing access privileges

Checkpoint 2: True or False Challenge

6 Question 6

Spear phishing relies on generic bulk emails sent to millions of random addresses.

◯ True ◯ False

7 Question 7

DMARC policies can instruct mail servers to reject unauthorized spoofed messages.

◯ True ◯ False

8 Question 8

SPF verification operates by validating the cryptographic signature of the email body.

◯ True ◯ False

9 Question 9

Whaling attacks target low-level corporate administrators to access database files.

◯ True ◯ False

10 Question 10

Enforcing out-of-band transaction verification blocks financial wire transfer scams.

◯ 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. Targeting a specific employee with personalized information is _____ phishing.
2. Forging an email header to make messages look legitimate is sender _____.
3. The DNS record list of authorized mail server IPs is _____.
4. The email signature standard providing sender verification is _____.
5. Establishing policies to reject failed SPF/DKIM checks uses _____.
6. A phishing campaign targeting C-level executives is called _____.

VOCABULARY WORD BANK

SPEAR	SPOOFING	SPF	DKIM
DMARC	WHALING		

Write your answers here:

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

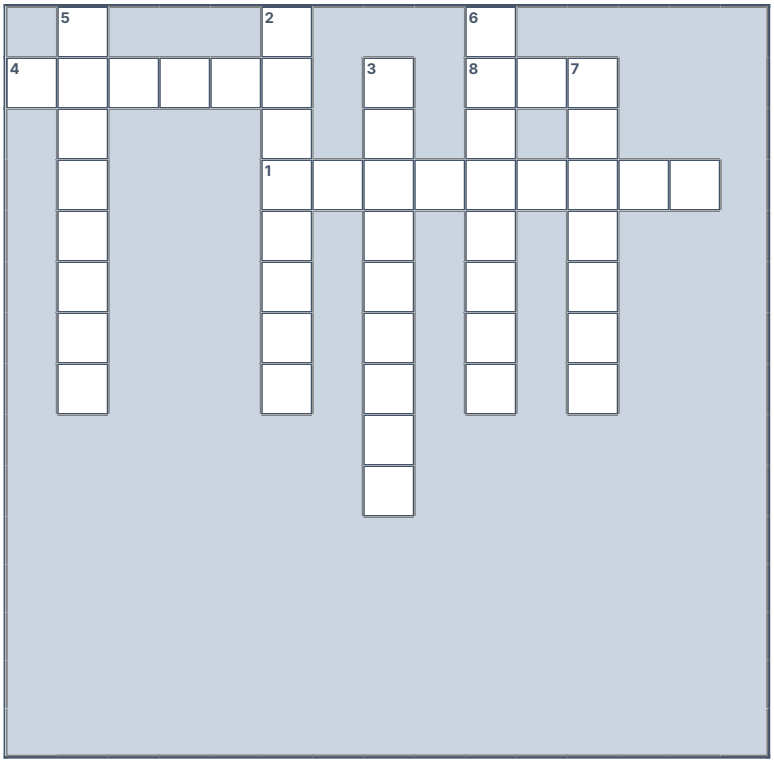
Checkpoint 4: Security Concept Match

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.

SPEAR	**A** Personalized targeted email. (A)
SPOOFING	**B** Forging sender email address. (B)
SPF	**C** DNS authorized sender IPs. (C)
DKIM	**D** Cryptographic signature in email. (D)
DMARC	**E** Policy reject instructions. (E)
WHALING	**F** Target C-level executives. (F)
PHISHING	**G** Social engineering email. (G)
VISHING	**H** Voice-based scam calls. (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: Targeted phishing email customized for a specific recipient. (5 letters):

4 Across: Forging email header details to masquerade as a trusted sender. (8 letters):

8 Across: DNS record mapping authorized sending IP addresses. (3 letters):

DOWN CLUES

2 Down: Cryptographic signature verification standard in email headers. (4 letters):

3 Down: Domain alignment policy governing SPF and DKIM failures. (5 letters):

5 Down: Phishing attacks directed specifically at corporate executives. (7 letters):

6 Down: Broad social engineering messages attempting to steal credentials. (8 letters):

7 Down: Voice-based phone scamming to harvest personal information. (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.

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

VOCABULARY WORD LIST

SPEAR	SPOOFING	SPF	DKIM
DMARC	WHALING	PHISHING	VISHING

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. SPEAR
B. SPOOFING
C. SPF
D. DKIM
E. DMARC
F. WHALING
G. PHISHING
H. VISHING

DEFINITIONS & MATCH FIELDS

_____ 1. Personalized targeted email.

_____ 2. Forging sender email address.

_____ 3. DNS authorized sender IPs.

_____ 4. Cryptographic signature in email.

_____ 5. Policy reject instructions.

_____ 6. Target C-level executives.

_____ 7. Social engineering email.

_____ 8. Voice-based scam calls.

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. R A E P S

2. G N I F O O P S

3. F P S

4. M I K D

5. C R A M D

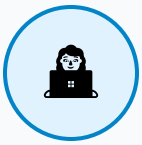
6. G N I L A H W

7. G N I H S I H P

8. G N I S H I V

Checkpoint 8: Cybersecurity Case Studies

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



CASE STUDY 1: C-SUITE WHALING ATTACK REMEDIATION

Scenario: A Chief Financial Officer receives a highly personalized email claiming to be from the CEO, requesting a rapid $50,000 wire to close a confidential domain purchase.

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

CASE STUDY 2: DEPLOYING SPF/DKIM/DMARC GATEWAY POLICIES

Scenario: An enterprise is failing security audits because outbound marketing emails are frequently flagged as spam, and hackers are actively spoofing the company's brand domain.

Discussion Question: Establish technical and administrative controls to verify email authenticity.

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

_	_	_	_	_	_		_	_	_	_	_	_		_	_	_	_		_	_	_	_	_	
4	5	20	5	3	20		19	15	3	9	1	12												
_	_	_	_	_	_	_	_	_	_	_		_	_	_	_		_	_	_	_	_			
5	14	7	9	14	5	5	18	9	14	7		23	9	20	8		5	13	1	9	12			
_	_	_	_	_	_	_	_	_		_	_	_	_	_	_	_	_	_	_	_	_	_	_	
7	1	20	5	23	1	25		1	21	4	9	20	9	14	7									

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 phishing?

Phishing is a social engineering attack where criminals send fraudulent messages to trick users into sharing sensitive data.

Q2: What is the difference between phishing and spear phishing?

Phishing targets broad groups with generic content, while spear phishing targets specific victims using customized details.

Q3: What is whaling?

Whaling is a highly targeted phishing attack aimed at high-profile executives who hold administrative power.

Q4: What is email spoofing?

Email spoofing is the creation of email messages with a forged sender address to trick the recipient into trusting the source.

Q5: How does SPF prevent spoofing?

It publishes a list of authorized sending IP addresses in DNS, allowing receiving servers to verify the mail source.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: What is DKIM?

DomainKeys Identified Mail adds a cryptographic signature to email headers, verifying that the email was sent by the domain owner.

Q7: What does DMARC stand for?

Domain-based Message Authentication, Reporting, and Conformance.

Q8: What is a DMARC policy?

A policy telling mail servers how to treat messages failing SPF/DKIM (none, quarantine, or reject).

Q9: What is vishing?

Voice phishing, where attackers use fraudulent phone calls to extract administrative or financial data.

Q10: How do link scanners help?

They scan and rewrite incoming email links to verify the safety of destination web pages at the time of click.

Checkpoint 11: Advanced Security FAQs (Part A)

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

Q1: How does a homograph attack work?

Attackers register domain names using lookalike non-ASCII Unicode characters to mimic a legitimate domain name visually.

Q2: What is a punycode representation?

A standard translating Unicode domain strings into an ASCII-compatible format starting with 'xn--' to prevent browser confusion.

Q3: Why is 'p=reject' the safest DMARC state?

It instructs receiving email systems to completely discard messages failing SPF/DKIM validation, blocking spoofed outreach.

Q4: How do attackers bypass SPF rules?

By exploiting lookalike domains (typosquatting) or using compromised accounts on legitimate third-party mail services.

Q5: What is business email compromise (BEC)?

A corporate scam where attackers hijack or impersonate business email accounts to authorize fraudulent payments.

Checkpoint 11: Advanced Security FAQs (Part B)

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

Q6: How does multi-factor authentication stop phishing?

It requires secondary tokens (such as hardware keys) that cannot be stolen through lookalike landing pages alone.

Q7: What is a credential harvesting landing page?

A lookalike login portal designed to capture entered usernames, passwords, and MFA tokens in real time.

Q8: What is subdomain hijacking?

An attacker taking control of an unused DNS subdomain pointer to host malicious phishing landing pages under a trusted parent domain.

Q9: How does DKIM alignment check work?

It verifies that the domain in the 'From' header matches the domain that cryptographically signed the message in the DKIM header.

Q10: What is the role of an email gateway?

Filtering incoming email, auditing links, sandboxing attachments, and validating SPF/DKIM/DMARC compliance.

Part 11: 10 Real-World Cybersecurity Facts & Insights

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

1. SECURITY INSIGHT

Over 90% of successful corporate cyber attacks start with a fraudulent email phishing message.

2. SECURITY INSIGHT

The average cost of a business email compromise (BEC) wire transfer scam exceeds $100,000 per incident.

3. SECURITY INSIGHT

Homograph attacks utilize Cyrillic lookalike letters to visually duplicate exact-match brand domains in browsers.

4. SECURITY INSIGHT

The 'p=reject' DMARC configuration prevents spoofed emails from ever appearing in a user's spam folder.

5. SECURITY INSIGHT

Whaling attacks targeting CEOs commonly request urgent payments for confidential mergers or domain purchases.

6. SECURITY INSIGHT

Credential harvesting portals often use dynamic scripts to validate passwords against active directories instantly.

7. SECURITY INSIGHT

NIST guides recommend continuous security awareness training and regular phishing simulations for all staff.

8. SECURITY INSIGHT

SPF records have a strict limit of 10 DNS lookups; exceeding this limit invalidates the SPF validation check.

9. SECURITY INSIGHT

FIDO2 hardware security keys provide cryptographically backed protection against remote credential harvesting.

10. SECURITY INSIGHT

The registry-level lock prevents unauthorized changes to registrar DNS records, stopping subdomain takeover vectors.

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: 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 SPEAR	B SPOOFING	C SPF	D DKIM
E DMARC	F WHALING	G PHISHING	H VISHING

CHECKPOINT 3: KEY TERM KEY

1 SPEAR	2 SPOOFING	3 SPF
4 DKIM	5 DMARC	6 WHALING

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).

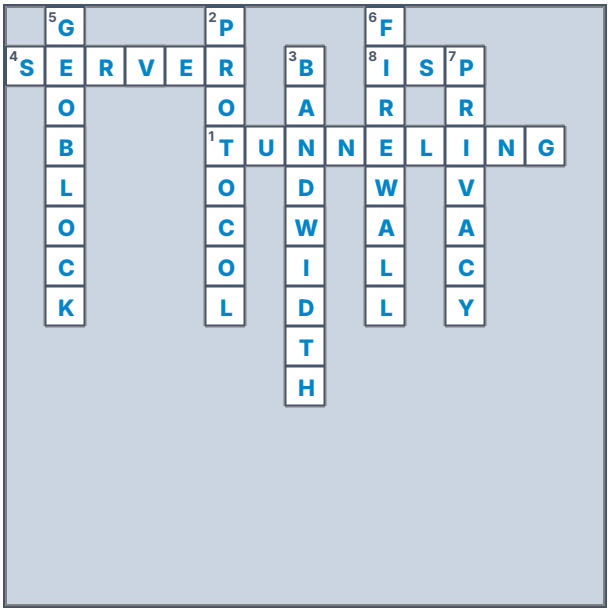
Regulatory Compliance:
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. R A E P S
   SPEAR

2. G N I F O O P S
   SPOOFING

3. F P S
   SPF

4. M I K D
   DKIM

5. C R A M D
   DMARC

6. G N I L A H W
   WHALING

7. G N I H S I H P
   PHISHING

8. G N I S H I V
   VISHING

SECRET CIPHER CHALLENGE KEY

"DETECT SOCIAL ENGINEERING WITH EMAIL GATEWAY AUDITING"

Domain Brokerage Case Studies Solution Key

A Case Study 1: C-Suite Whaling Attack Remediation

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A Chief Financial Officer receives a highly personalized email claiming to be from the CEO, requesting a rapid $50,000 wire to close a confidential domain purchase.
- **Recommended Strategy & Solution:** Configure DMARC with a 'p=reject' policy to block spoofed sender domains. Add external sender warning banners at the gateway, and require verbal, out-of-band confirmation for all financial transactions.

B Case Study 2: Deploying SPF/DKIM/DMARC Gateway Policies

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An enterprise is failing security audits because outbound marketing emails are frequently flagged as spam, and hackers are actively spoofing the company's brand domain.
- **Recommended Strategy & Solution:** Publish a TXT record for SPF detailing authorized sender IPs. Configure DKIM signing keys on outbound mail servers, and analyze incoming DMARC XML feedback reports to identify abuse.