Name: _____ Date: _____ Score: _____

# Online Scams & Social Engineering Protection Guide

Email phishing, spoofed domains, vishing, support scams, out-of-band verification, BEC

## ONLINE SCAMS 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 online scam defense. You will explore fake phishing websites, social engineering tactics, support scams, wire fraud vectors, and payment verification methods.

### 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/online-scams/

# Your Online Scam Protection Learning Roadmap

- Identify common indicators of support scams and typosquatting domains.
- Implement email verification protocols (SPF, DKIM, DMARC) against spoofing.
- Establish out-of-band transaction verification to prevent business wire fraud.

## ONLINE SCAMS 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 online scam protection.

## ONLINE SCAMS & SOCIAL ENGINEERING PROTECTION (INTRODUCTION)

Online scams exploit human behavior through phishing, support pop-ups, vishing, and wire fraud. Enforcing out-of-band transaction verification protocols and SPF/DKIM/DMARC domain rules stops social engineering vectors at the gateway.

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

## Checkpoint 1: Multiple Choice Challenge

**1 What is the primary indicator of a support scam?**

- A. A pop-up claiming your system is infected and demanding you call a phone number
- B. An automated security update downloaded from an official registry
- C. A password manager refusing to fill credentials on a corporate domain
- D. A background file backup running on an external drive configuration

**2 Which technique uses spoofed sender domains to steal bank details?**

- A. Email phishing
- B. Port scanning
- C. Memory injection
- D. Cryptographic shredding

**3 What represents wire transfer fraud?**

- A. Tricking victims into sending money to fake corporate accounts using social engineering
- B. Encrypting system databases using ransomware payloads
- C. Querying databases via SQL injection commands
- D. Backing up system files to offline storage disks

**4 Why do scammers create fake shopping websites?**

- A. To steal credit card details and payment credentials from buyers
- B. To host sandboxed malware analysis database tables
- C. To speed up DNS name migration reindexing cycles
- D. To bypass geoblocking rules on public Wi-Fi networks

**5 What does vishing mean?**

- A. Voice phishing scams over phone networks to steal credentials
- B. Scanning local networks for unsecured system devices
- C. Restoring system databases after an unauthorized breach
- D. Running untrusted code inside secure virtual containers

## Checkpoint 2: True or False Challenge

**6 Question 6**

Phishing scams only target end-users, never executive whaling targets.

◯ True ◯ False

**7 Question 7**

Spoofed domains often use slight typos (like amaz0n.com) to mimic trusted brands.

◯ True ◯ False

**8 Question 8**

Support scams can be resolved by granting remote access to the caller.

◯ True ◯ False

**9 Question 9**

Social engineering exploits human psychology like fear and urgency to bypass security rules.

◯ True ◯ False

**10 Question 10**

Wire transfer requests should always be verified using out-of-band communication channels.

◯ 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. Fraudulent emails tricking users are called _____.
2. Web addresses that mimic trusted brands are _____.
3. Voice scams targeting bank details are called _____.
4. A pop-up demanding money for virus removal is a support _____.
5. Confirming a payment request requires out-of-band _____.
6. Redirecting business transactions to thief accounts is _____.

**VOCABULARY WORD BANK**

| | | | |
|---|---|---|---|
| PHISHING | SPOOFED | VISHING | SCAM |
| VERIFICATION | WIRE | | |

**Write your answers here:**

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

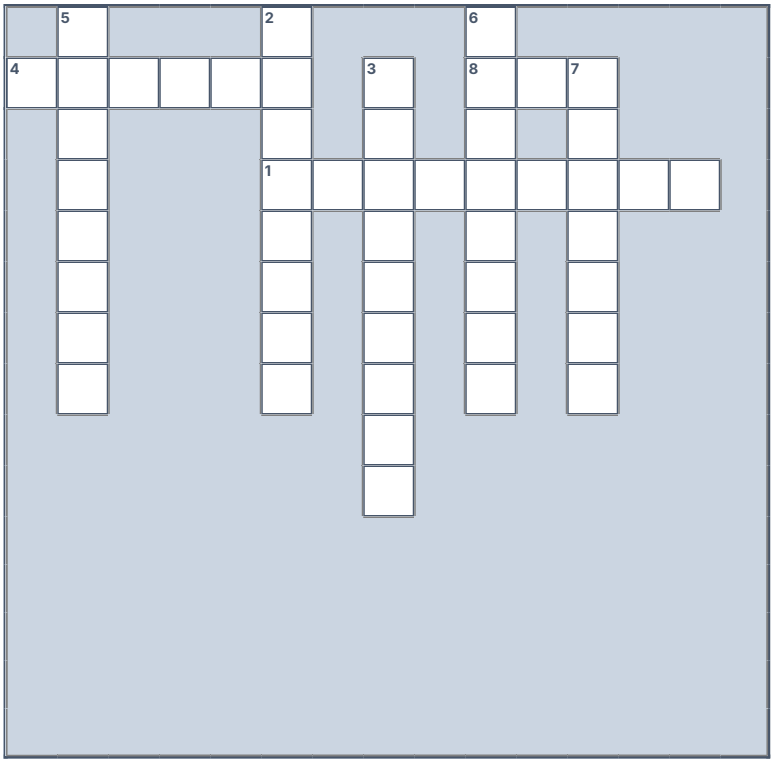
# Checkpoint 4: Security Concept Match

**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.

| | | | |
|---|---|---|---|
| ( ) | PHISHING | A | Fraudulent email campaigns designed to steal login credentials and passwords. (A) |
| ( ) | SPOOFED | B | Mimicked email sender or website address designed to look legitimate. (B) |
| ( ) | VISHING | C | Fraudulent voice calls designed to steal credentials and account details. (C) |
| ( ) | SCAM | D | Fraudulent scheme designed to steal money or access credentials from victims. (D) |
| ( ) | VERIFICATION | E | Confirming payment details using a trusted secondary contact method. (E) |
| ( ) | WIRE | F | Fraudulent redirection of bank transactions to criminal accounts. (F) |
| ( ) | WHALING | G | Targeted phishing attacks aiming to steal credentials from C-level executives. (G) |
| ( ) | SMISHING | H | Sending scam text messages to steal mobile account 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: Agency representing clients to recover domain assets hijacked in phishing scams (9 letters):**

**4 Across: Neutral safety account protecting buyers from fake escrow portal scams (6 letters):**

**8 Across: Corporate naming asset mimicked by scammers using typo-squatted domains (5 letters):**

## DOWN CLUES

**2 Down: Financial assessment of losses and recovery costs after corporate wire fraud (9 letters):**

**3 Down: Stealth registration setup used by scammers to hide WHOIS contact records (7 letters):**

**5 Down: Entity where spoofed domain names must be reported for rapid deletion (9 letters):**

**6 Down: Authorization passcode stolen by scammers to hijack domain assets (7 letters):**

**7 Down: Online bidding forum where typo-squatted trademark domains 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.

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

### VOCABULARY WORD LIST

| | | | |
|---|---|---|---|
| PHISHING | SPOOFED | VISHING | SCAM |
| VERIFICATION | WIRE | WHALING | SMISHING |

# 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.** PHISHING
**B.** SPOOFED
**C.** VISHING
**D.** SCAM
**E.** VERIFICATION
**F.** WIRE
**G.** WHALING
**H.** SMISHING

### DEFINITIONS & MATCH FIELDS

_____ 1. Fraudulent email campaigns designed to steal login credentials and passwords.

_____ 2. Mimicked email sender or website address designed to look legitimate.

_____ 3. Fraudulent voice calls designed to steal credentials and account details.

_____ 4. Fraudulent scheme designed to steal money or access credentials from victims.

_____ 5. Confirming payment details using a trusted secondary contact method.

_____ 6. Fraudulent redirection of bank transactions to criminal accounts.

_____ 7. Targeted phishing attacks aiming to steal credentials from C-level executives.

_____ 8. Sending scam text messages to steal mobile account 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. G I S H P H I N

2. O O P S E D F

3. G I S H V I N

4. M A C S

5. I F I C A N R E I O T V

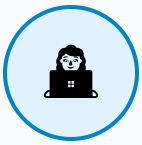
6. E R I W

7. I N G W A L H

8. G I S H M I N S

# Checkpoint 8: Cybersecurity Case Studies

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



### CASE STUDY 1: CORPORATE WIRE TRANSFER SCAM PREVENTION

**Scenario:** A finance department receives an urgent email from a spoofed vendor address, requesting that future invoice wires be directed to a new routing number.

**Discussion Question:** Outline the wire fraud verification policy, and specify email authentication blocks.

### CASE STUDY 2: EXECUTIVE WHALING PHISHING INCIDENT

**Scenario:** An executive clicked a phishing link claiming to hold a secure board-meeting document, entering their primary corporate credentials on a spoofed portal.

**Discussion Question:** Detail the incident response steps, and explain how to audit executive logins.

# 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 | | _ 25 | _ 15 | _ 21 | _ 18 |
| _ 16 | _ 8 | _ 9 | _ 19 | _ 8 | _ 9 | _ 14 | _ 7 | | _ 15 | _ 21 | _ 20 | _ 18 | _ 5 | _ 1 | _ 3 | _ 8 | | _ 23 | _ 9 | _ 20 | _ 8 |
| _ 19 | _ 3 | _ 1 | _ 14 | _ 14 | _ 5 | _ 18 | | _ 22 | _ 5 | _ 18 | _ 9 | _ 6 | _ 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 an online scam?

A fraudulent scheme using digital channels to trick victims into sending money or giving up personal credentials.

### Q2: What is the main indicator of email phishing?

A message claiming urgency (like account suspension) and directing you to a link that doesn't match the official domain.

### Q3: What is typosquatting?

Registering domains with common typos of popular brands (like amaz0n.com) to host fake phishing sites.

### Q4: What is a support scam?

A pop-up claiming your PC is infected, directing you to call a number and pay for fake cleanup software or remote access services.

### Q5: What is vishing?

Phishing attacks using voice phone calls to trick victims into giving bank account or login details.

# Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

### Q6: What does wire fraud mean?

Redirection of payment transactions to scam accounts by impersonating vendors or executives.

### Q7: What is whaling?

A highly targeted form of spear phishing aiming directly at high-value targets like C-level corporate executives.

### Q8: What is smishing?

Scam text messages sent to mobile devices, containing link prompts to fake portals or tracking updates.

### Q9: Why is out-of-band verification critical?

It confirms transaction details using a separate communication channel (like a phone call), avoiding compromised email threads.

### Q10: How does a fake escrow scam work?

Scammers create a spoofed escrow site, claiming funds are held securely, then steal the buyer's wire deposit.

# Checkpoint 11: Advanced Security FAQs (Part A)

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

### Q1: How do scammers use BEC (Business Email Compromise) to execute wire fraud?

They hijack a legitimate employee's email account, monitor invoice threads, and send updated billing details with scam bank accounts.

### Q2: What is the risk of IDN homograph attacks in online scams?

Using non-ASCII characters that look identical to normal letters (e.g., Cyrillic 'a') to register spoofed domains that mimic real brands.

### Q3: Why is email header inspection important in scam detection?

It reveals the actual origin server IP and SPF/DKIM validation status, showing if the sender domain is forged.

### Q4: How do support scammers exploit remote desktop software?

They use utilities like AnyDesk or TeamViewer to connect to the victim's device, plant malware, and steal saved passwords.

### Q5: What is the goal of advance-fee scams?

Tricking victims into paying processing fees upfront in exchange for a large financial reward that does not exist.

# Checkpoint 11: Advanced Security FAQs (Part B)

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

### Q6: How do scammers use social media profiling for targeted phishing?

They compile corporate organizational structures and employee names to draft convincing spear-phishing emails.

### Q7: Why do fake web shops offer steep discounts?

To lure buyers into entering their credit card details, capturing credentials for reuse or resale on carding forums.

### Q8: How do DMARC records block phishing scams?

DMARC instructs email servers to reject messages that fail SPF or DKIM checks, preventing spoofed emails from reaching corporate inboxes.

### Q9: What is the threat of credential harvesting portals?

Spoofed landing pages designed to look exactly like Microsoft 365 or Google workspaces, stealing login credentials as they are entered.

### Q10: How do security teams report and disable scam domains?

By submitting evidence of fraud to the registrar's abuse email, hosting provider, and Google Safe Browsing registry.

## Part 11: 10 Real-World Cybersecurity Facts & Insights

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

**1. SECURITY INSIGHT**

Phishing represents the start point for over 90% of corporate scams and network security breaches.

**2. SECURITY INSIGHT**

BEC (Business Email Compromise) wire scams account for over $2 billion in annual losses globally.

**3. SECURITY INSIGHT**

Typo-squatted domains are registered by scammers within minutes of major brand launch announcements.

**4. SECURITY INSIGHT**

Technical support scams target senior demographics, stealing millions in fake diagnostic support fees.

**5. SECURITY INSIGHT**

Homograph attacks look identical in browser address bars unless the browser displays punycode configurations.

**6. SECURITY INSIGHT**

SMS text scams (smishing) have higher open rates than email phishing, increasing the speed of credential theft.

**7. SECURITY INSIGHT**

Whaling attacks target executive emails because they control access to large payment wire transfers.

**8. SECURITY INSIGHT**

Out-of-band payment validation prevents over 95% of business email compromise wire fraud losses.

**9. SECURITY INSIGHT**

Fake escrow platforms are a leading scam vector in secondary domain transactions, capturing wires.

**10. SECURITY INSIGHT**

Google Safe Browsing flags and blocks tens of thousands of newly created scam domains daily.

# 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 PHISHING | B SPOOFED | C VISHING | D SCAM |
| E VERIFICATION | F WIRE | G WHALING | H SMISHING |

## CHECKPOINT 3: KEY TERM KEY

| | | |
|---|---|---|
| 1 PHISHING | 2 SPOOFED | 3 VISHING |
| 4 SCAM | 5 VERIFICATION | 6 WIRE |

## 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).

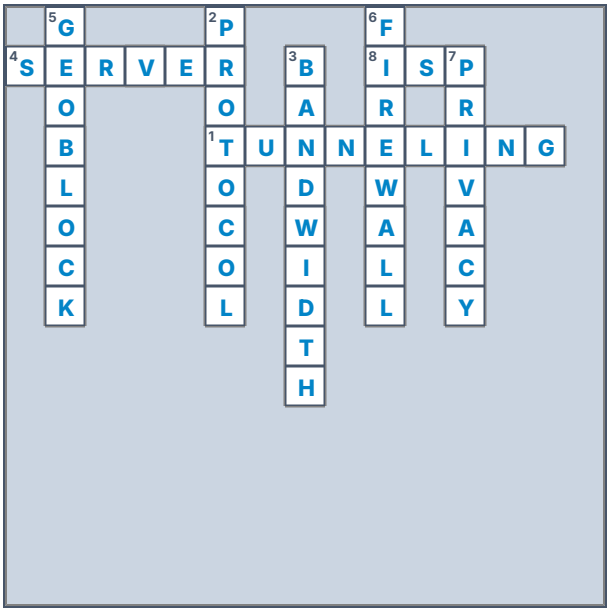
**Regulatory Compliance:**
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

# Puzzles Keys & Instructor Notes

## WORD SEARCH SOLUTION

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

2. O O P S E D F
   **SPOOFED**

3. G I S H V I N
   **VISHING**

4. M A C S
   **SCAM**

5. I F I C A N R E I O T V
   **VERIFICATION**

6. E R I W
   **WIRE**

7. I N G W A L H
   **WHALING**

8. G I S H M I N S
   **SMISHING**

**SECRET CIPHER CHALLENGE KEY**

**"DETECT YOUR PHISHING OUTREACH WITH SCANNER VERIFICATION"**

# Domain Brokerage Case Studies Solution Key

## A Case Study 1: Corporate Wire Transfer Scam Prevention

Instructor Solution

### GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A finance department receives an urgent email from a spoofed vendor address, requesting that future invoice wires be directed to a new routing number.
- **Recommended Strategy & Solution:** Enforce a dual-authorization policy for all payments. Implement out-of-band verification using a pre-saved phone number, and block spoofed domain emails at the gateway.

## B Case Study 2: Executive Whaling Phishing Incident

Instructor Solution

### GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An executive clicked a phishing link claiming to hold a secure board-meeting document, entering their primary corporate credentials on a spoofed portal.
- **Recommended Strategy & Solution:** Isolate the executive's device. Reset all corporate session tokens and credentials. Review access logs for data egress, and implement hardware MFA on all logins.