Scam Analysis Worksheet

Use this worksheet to analyze scam examples and develop educational content to help others recognize and avoid similar scams.

Scam Example

Describe the scam you're analyzing or paste the example text below:

Note: Include details like the communication method (email, text, phone call), sender information, subject line, message content, requested actions, and any images or attachments.

Scam Type Identification

Primary scam type:

- ☐ Phishing (fraudulent emails/messages to steal information)
- ☐ Spoofing (impersonating legitimate companies/individuals)
- ☐ Catfishing (fake identity to build relationships for financial gain)
- ☐ Identity theft attempt
- ☐ Investment scam/Ponzi scheme
- ☐ Tech support scam
- ☐ Government/IRS impersonation
- ☐ Employment/job scam
- ☐ Lottery/prize scam
- ☐ Advance fee fraud (Nigerian Prince type)

- ☐ Shopping/retail scam
- ☐ Charity fraud
- ☐ Romance scam
- ☐ Other: _____

Explain why you classified it this way:

Warning Signs Analysis

Identify all warning signs present in this scam:

- ☐ Urgency/pressure to act quickly
- ☐ Request for personal/financial information
- ☐ Suspicious sender address/domain
- ☐ Grammatical errors or awkward phrasing
- ☐ Generic greeting (not personalized)
- ☐ Too good to be true offer
- ☐ Request for unusual payment methods (gift cards, wire transfers, cryptocurrency)
- ☐ Suspicious links or attachments
- ☐ Inconsistencies in the message
- ☐ Mismatched URLs (link text doesn't match destination)
- ☐ Threats or consequences for not responding
- ☐ Suspicious contact information
- ☐ Other: _____
- ☐ Other: _____

For each warning sign checked above, provide the specific example from the scam:

Warning Sign	Specific Example from the Scam

Psychological Tactics Analysis

What psychological tactics does this scam use to manipulate the recipient?

- ☐ Fear/threat (loss of money, legal consequences, account closure)
- ☐ Greed/opportunity (easy money, prizes, exclusive offers)
- ☐ Authority (impersonating officials, government, IT departments)
- ☐ Scarcity/urgency (limited time, act now)
- ☐ Trust/familiarity (impersonating known brands or individuals)
- ☐ Curiosity (click to see, learn more)
- ☐ Sympathy/compassion (helping someone in need)
- ☐ Social proof (others are doing it)
- ☐ Flattery/recognition (you've been selected, you're special)
- ☐ Other:

Why might these tactics be effective? Who might be most vulnerable to this scam?

Protection Strategy

What should someone do if they receive this type of scam?

[ ]

What specific steps would help someone avoid falling for this scam?

[ ]

If someone has already responded to or fallen for this type of scam, what should they do?

[ ]

Where should this type of scam be reported?

[ ]

Educational Social Media Post

Create a social media post to warn others about this type of scam. Make it concise, educational, and engaging.

Target platform:

○ Instagram   ○ TikTok   ○ Twitter/X   ○ Facebook   ○ Other: [ ]

Target audience:

[ ]

Your Name

@yourusername

Post Title/Headline:

Post Content:

Hashtags:

Visual Element Description (what image or graphic would accompany this post):

Call to Action:

Reflection Questions

1. What was the most subtle or deceptive element of this scam that might be easy to miss?

2. How might this type of scam evolve in the future to become more convincing?

3. What is the most important takeaway for people to remember about this type of scam?