Lesson Plan: Spot the Phish

Teacher Resource Audience: Teachers | Grades 8-12

Purpose

• Students learn how phishing attempts try to trick people into clicking links, opening attachments, sharing information, or taking urgent action. Students analyze fictional messages, identify red flags, and practice safe response routines.

Standards summary

• This resource may support CSF 13.1, CSF 14.1, CSF 14.2, CSF 14.3.

• Detailed alignment depends on local district pacing, approved course placement, and teacher directions.

Lesson Purpose

Students learn how phishing attempts try to trick people into clicking links, opening attachments, sharing information, or taking urgent action. Students analyze fictional messages, identify red flags, and practice safe response routines.

Learning Objectives

- Define phishing in student-friendly language.
- Identify common warning signs in suspicious messages.
- Explain why phishing threatens confidentiality, availability, and integrity.
- Choose safe responses such as pause, verify, report, and do not click.
- Reflect on how attackers use urgency, fear, rewards, authority, and curiosity.

Materials

- Spot the Phish sample messages
- Projector or shared screen
- Red flag checklist
- Exit ticket
- Optional school-approved reporting process

Lesson Flow

1. Warm-Up: Would You Click? (5 minutes)

Display a fictional message. Ask students what looks normal and what looks suspicious. Do not include real links or live examples.

2. Mini-Lesson: What Phishing Tries to Do (10 minutes)

Explain that phishing is a social engineering tactic. It often tries to create urgency, steal credentials, install malware, or collect sensitive information.

3. Red Flag Checklist (10 minutes)

Teach students to look for urgent language, mismatched sender details, unexpected attachments, suspicious links, unusual requests, poor fit with context, and requests for passwords or codes.

4. Group Analysis (15-20 minutes)

Students review fictional messages and mark red flags. They decide whether to trust, verify, report, or delete the message.

5. Safe Response Practice (5-10 minutes)

Students rewrite unsafe reactions into safe responses. Emphasize: pause, verify through a trusted channel, report if required, and never share private information.

6. Exit Ticket (5 minutes)

Students answer: One phishing red flag is... One safe response is... One thing I should never share in a message is...

Sample Fictional Messages

Scenario	Message Summary	Possible Red Flags
Urgent Password Alert	Your account will close in 10 minutes. Click this link to confirm your password.	Urgency, password request, unknown link
Prize Message	You won a free phone. Reply with your birthday and address to claim it.	Too-good-to-be-true reward, personal data request
Fake School Notice	Open the attached file to view your grade change.	Unexpected attachment, emotional trigger

Assessment

- Red flag analysis
- Safe response explanation
- Exit ticket reflection
- Class discussion participation

Teacher Notes

Keep all examples fictional and defensive. Do not use real phishing links, real student accounts, or live suspicious websites. The goal is awareness, judgment, and safe response behavior.

Detailed Tennessee Standards Connection

Tennessee Standards Connection

This lesson directly supports standards when students identify security risks, evaluate suspicious messages, explain safe responses, and connect phishing to data security and ethical technology use.

Standards source: Tennessee Department of Education, Computer Science Foundations (C10H11), May 2023. Confirm final alignment against local district pacing, approved course placement, and teacher directions.

This resource may support the following Tennessee standards when used as part of cybersecurity, digital ethics, computer science, AI literacy, or career-connected technology instruction:

- CSF 13.1 - Social, Legal, and Ethical Issues: Students research social, legal, and ethical issues encountered by IT professionals and identify responsibilities when addressing technology problems.
- CSF 14.1 - Data Security: Students explain why data security is a priority and demonstrate understanding of confidentiality, availability, and integrity.
- CSF 14.2 - Security Breaches: Students demonstrate understanding of security breaches, enterprise-level security, encryption, protocols used to secure websites, and privacy considerations.
- CSF 14.3 - Security Practices: Students identify security practices for computer and network systems, including access control, encryption techniques, BIOS features, and malware response strategies.

Item	Details
Time	45-60 minutes
Subject Fit	Cybersecurity, Computer Science Foundations, digital citizenship, advisory, business technology
Essential Question	How can I recognize suspicious messages before I click, reply, or share information?

Use guidance

- Confirm final alignment against local district pacing, approved course placement, and teacher directions.
- Keep instruction defensive, ethical, age-appropriate, and classroom-safe.