

Cyber Elementary School

3rd Grade Lesson Plan Book

Lesson 3: Recognizing Phishing Emails and Messages: Don't Take the Bait

Lesson Title: Recognizing Phishing Emails and Messages: Don't Take the Bait

Lesson Number: 3 of 36

Grade/Age: Elementary School (Grade 3)

Subject: Cyber Security and Safety

Duration: 30–40 Minutes

Learning Objectives

- Students will be able to define phishing and explain why attackers use fake messages to trick people.
- Students will be able to identify at least three warning signs of a phishing email or message.
- Students will be able to describe the safe action to take when they receive a suspicious message.
- Students will be able to explain why it's dangerous to click links or download attachments from unknown senders.

Skills

Digital literacy, critical thinking, careful reading, skepticism toward unknown sources, decision-making under uncertainty.

Warm-Up / Hook (5 minutes)

"Fishing for Clues" Game. Show students a fishing hook with bait on it (a picture or a simple drawing). Ask: "Why does the fisherman put yummy bait on the hook instead of just a bare hook?" Students will say to trick the fish into biting. Explain that "phishing" (spelled with a "ph" like the word "fish") works the same way — a scammer dangles something tempting or scary in a message (a prize, a warning, an urgent request) to trick someone into clicking a link or giving away information, just like bait hides a hook.

Recommended Teacher Talking Points (Introduction)

- Phishing is when someone sends a fake email, text, or message pretending to be someone they're not — like a company, a game you use, or even a friend — to trick you into clicking a link or sharing information.
 - Phishing messages often try to make you feel excited ("You won a prize!") or scared ("Your account will be deleted!") so you react quickly without thinking.
 - The goal of a phishing message is usually to get your password, personal information, or to get you to click a bad link or download something harmful.
 - Today we'll learn the warning signs of phishing and what to do if you ever get a suspicious message.
-
-
-

Direct Instruction with Recommended Teacher Talking Points

Core Concept:

- Phishing messages often have warning signs: strange or misspelled sender addresses, urgent or scary language, offers that seem too good to be true, and requests for personal information or passwords.
- A real company or school will almost never ask you to send your password through email or a message.
- If a message asks you to click a link or download a file and you're not 100% sure who it's from, don't click it — tell a trusted adult first.
- It's always okay to pause, ask an adult, and check before clicking anything you're unsure about.

Guided Practice — 3rd Grade Skill Activity

(Skill activity to complement the learning objective)

Spot the Fishy Message

- In pairs, students review two side-by-side sample messages (one real-looking school announcement, one phishing attempt with an urgent prize claim) and circle the parts of the fake one that seem "fishy."

Independent Practice or Homework Handout — 3rd Grade Worksheet

"Don't Take the Bait!"

- Circle the message that is phishing out of two examples shown.
- List two warning signs that helped you decide.
- Write one rule about what to do if you get a message that seems fishy.

Closure (5 minutes)

Bring the class back together and ask 2–3 volunteers to share one phishing warning sign they learned. Reinforce the key takeaway: "If a message feels urgent, scary, or too good to be true, slow down, don't click, and check with a trusted adult." Preview that the next lesson will look at malware and viruses — the harmful programs that phishing links sometimes try to install.

Assessment — 3rd Grade Quiz

4 questions

1. What is phishing? a) A fun online game b) A fake message trying to trick you c) A type of computer d) A strong password
2. True or False: If a message says you won a prize you didn't enter for, it's probably safe to click.
3. If you get a message that seems fishy, you should: a) Click the link right away b) Tell a trusted adult c) Reply with your password
4. Name one warning sign of a phishing message.

Answer Key (Teacher Use) — 3rd Grade

1. b) A fake message trying to trick you.
2. False — it's a common phishing trick; you should not click and should tell an adult.
3. b) Tell a trusted adult.

4. Open-ended — accept answers like urgent language, spelling mistakes, unknown sender, or an offer that seems too good to be true.

Teacher Reflection / Notes

- What worked well in this lesson? _____
- Which grade level needed more scaffolding or support? _____
- Did students grasp the "bait and hook" analogy for phishing? _____
- Adjustments for next time: _____