

CYBER HOUSE ROCK

Teacher Guide

1. Lesson Overview

Lesson Title: Protecting Your Data from Phishing Phil: Keep Your Fish Safe!

Cyber House Rock Video: <https://cyberhouserock.info/video/phishing-boat-blues/>

Topic Category: Phishing

Grade Band: 6–8

Estimated Time: 45-60 minutes per session

Lesson Type: Mini-Unit

Materials Needed:

- Video access to cyberhouserock.info
- Projector or screen
- Printed activity sheets
- Internet access
- Whiteboard / chart paper

2. Learning Objectives

By the end of this lesson, students will be able to:

1. Identify the type of sensitive personal data each “fish” represents and the common ways Phishing Phil would target it.
2. Explain at least 3 simple habits to protect personal information from phishing attempts.
3. Apply critical thinking to spot red flags in everyday scenarios.

3. Key Vocabulary

Phishing – A trick where someone pretends to be someone they are not to steal your private information.

Sensitive Data – Important personal information that phishing attacks would want to steal.

Red Flags - Warning signs that something could be a trick, such as urgent words or messages from weird senders.

Verify – Double check if something is real.

4. Background for the Teacher (1 Page Max)

Phishing Phil is a sneaky cartoon character who tries to “catch” private information (represented by different fish) through fake messages, emails or links. These fish represent real data people need to protect every day such as bank information, health info, passwords, etc. In real life, phishing is one of the most common cyber attacks. Scammers send urgent and exciting messages that play on emotion in order to get the user to fall for some sort of trick, leading to stolen money, identity theft, or hacked accounts.

A common misconception is it only happens to adults. Phishing messages have been increasingly more popular among all ages, targeting younger kids with tricks such as “Free Robux” asking for log in information and pretend alerts.

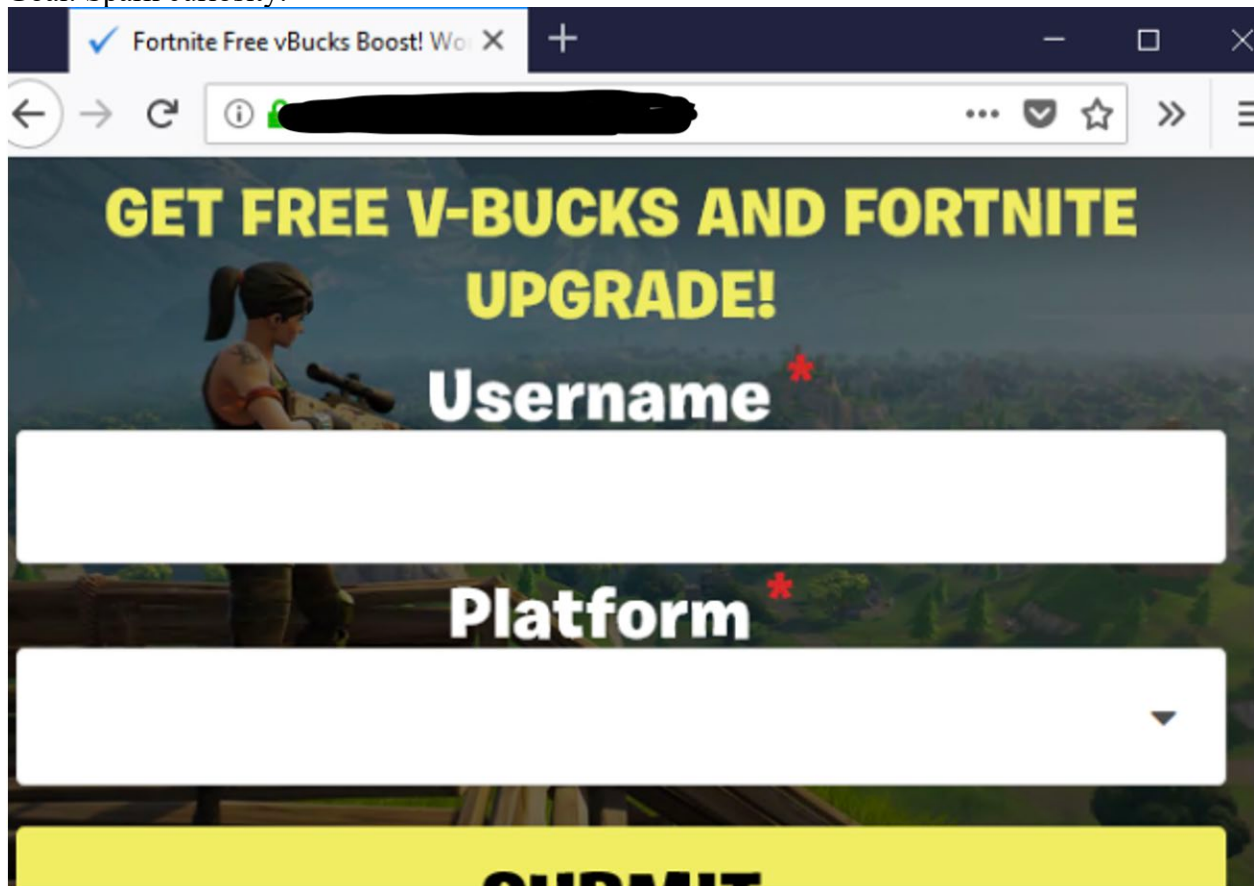
Why this matters?

This concept helps students understand small habits that can save their sensitive data, such as pausing before sharing info, checking the legitimacy of a message, and not making an emotional decision. This can help keep themselves and their families safe online. It builds lifelong skills for spotting tricks in games, social media, school, emails, and beyond.

5. Lesson Flow (Step-by-Step Plan)

A. Hook (5 minutes)

Goal: Spark curiosity.



Show this Image to the students. Ask what they would do, and if they would try it to see if it works if they came across this on their own. Take a poll, who would try it and who would ignore it. Ask if the students want to share why they chose their answer.

B. Watch the Video (3–5 minutes)

Before watching:

- Ask students to listen for how Phishing Phil tries to catch the fish, and how they can stay safe.

After watching:

- What message did you hear?
- What surprised you?
- What would you tell a friend?

C. Guided Discussion (10–15 minutes)

Provide 5–7 structured discussion prompts:

1. Why do people fall for Phishing Phils tricks?

Look for answers such as playing on emotion or causing a sense of fear.

2. What clues suggest something is unsafe?

Check sender emails, look for typos, look for urgency that is unreasonable. If something seems unreasonable, it probably is.

3. What would make this harder to detect?

If Phil knew specifics about the target, such as the specific bank they use or recent stores they shop at. Phil can craft a special message that is more believable.

4. Who is responsible for staying safe?

Kids and Adults. It is the job of every individual to spread awareness.

5. What would Personal Patty or Benny Bank say to someone looking at a potential phishing email?

Do not click on it, be aware if they are asking for personal information or bank information.

6. How does Phil target kids differently than adults?

Focuses on video games and kid activities, rather than bank accounts.

D. Interactive Activity (15–20 minutes)

Activity Name: Rank the Fish

Purpose:

Students will apply the concept by physically ranking the 9 fish by their perceived importance. This can be don't in a group or individually.

Instructions (Teacher Script-Friendly):

1. Divide students into groups of 3
2. Give each group the copy of “Phishing Phils Fish Cutout”, and scissors
3. Ask them to cut out the fish and rank them from most important to them to least important to them.
4. Debrief with the whole class and compare rankings. Discuss importance of all of them and affirm at the end that all 9 fish are important.

Materials Included:

- Printable worksheet

Activity Name: Match the Phishing Attempt

Purpose:

Students will apply the concept by analyzing short mock phishing messages and correctly match each to the specific corresponding “fish”. This helps them recognize the different kinds of phishing messages that can be sent.

Instructions (Teacher Script-Friendly):

5. Divide students into groups of 3
6. Give each group a phishing Phil matching worksheet, and scissors.
7. Ask them to cut the pieces on the dotted line. Discuss which fish Phil is targeting with each message.
8. Debrief with going through the correct answers, discussing why each would correspond.

Materials Included:

- Printable worksheet

E. Reflection / Exit Ticket (5 minutes)

Students respond:

- A tip I would give my family:

Can be paper, Google Form, or verbal.

6. Assessment Options

Formative:

- Discussion participation
- Activity responses
- Group reasoning

Summative (Optional):

- Short paragraph response
 - Describe how you would protect one fish of your choice from Phishing Phil in a real situation.

7. Extension Activities

For teachers who want more:

- Family conversation prompt:
 - Show your family your fish defense and ask if they have seen any phishing attempts.
- Create-a-poster activity
 - Make a class poster with the 9 fish.
- Write a scam from the attacker's perspective
 - Pretend to be Phil, and make a fake message to trick a fish of your choice.
- Connect to another Cyber House Rock video
 - Watch the QR code video.
https://www.youtube.com/watch?v=X6nZtmQ2DT4&list=PL33Ng3jyXO_DQyAmVcPpTAPoCuh9ACd9z&index=11
 - Connect on how a QR code can lead to stolen personal information similar to phishing.

8. Real-World Connection

Include:

- How this applies to:
 - Social media: Don't share personal information such as addresses, birthdays, etc.
 - Gaming: Fake "free item" scams are never real.
 - Banking: Urgent texts about bank accounts.
 - School platforms: Fake teacher emails asking for info (from fake email addresses)
 - AI tools: Deepfake voice/calls pretending to be family.