Thank you for your interest in e-Safety, and for teaching safe and responsible Internet use to your students. Educators are invited to access and download i-SAFE© curriculum AT NO CHARGE under the following conditions:

Only educators who have attended an i-SAFE© Professional Development Program and are "i-SAFE© Certified" are allowed to access this i-SAFE© grade-specific lesson plan PDF file.

Further, clicking on the button (below) means i-SAFE© Certified educators agree that:

- i-SAFE© lessons may only be taught by i-SAFE© Certified educators.
- i-SAFE© lessons may NOT be shared with other educators.
- i-SAFE© lessons may NOT be duplicated for any reason except for classroom use.
- i-SAFE© lesson hand-outs may be printed for students ONLY for current classroom use.

Duplication and/or selling of the i-SAFE copyrighted materials, or any other form of unauthorized use of this material, is against the law.

(I agree to above Terms of Use)

Agree and Print

LESSON—Phishing and Pharming Scams

Suggested grade level 9-12

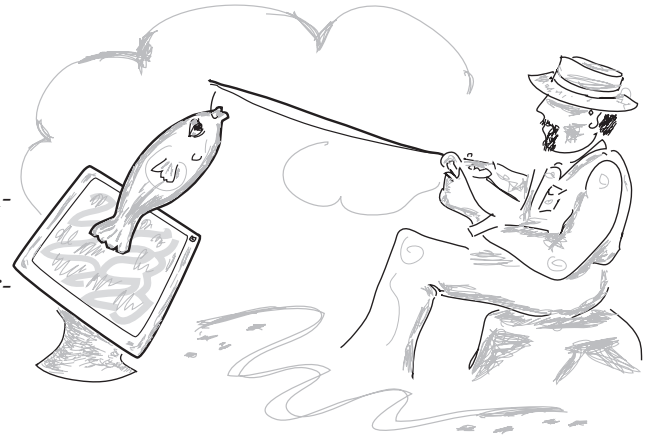
Lesson Guide

Learners will understand the terms "pharming" and "phishing," and how to prevent these types of malicious attacks.

Learning Objectives

Students will:

- be able to define the term "pharming"
- be able to define the term "phishing"
- understand basic online prevention for pharming and phishing attacks
- create a flyer to inform others about risks to personal information security through phishing and pharming



Materials/Preparation

- a copy of reference for each student
- materials to create flyers or brochures

Procedures

Discussion

Ensure that all students have printouts of the reference page.

Use the reference page and the following questions as a guide to discuss online phishing and pharming.

- Have any of the students received phishing e-mails?
- Have students describe phishing scams they have seen.
- Which age groups might be especially vulnerable to phishing scams and why?
- Who might be especially vulnerable to pharming scams and why?
- Have students think about their parents' vulnerability to this threat. (Students may be more aware of cyber security issues than their parents.)

Activity

Develop a strategy to create flyers or informational brochures about phishing and pharming scams to provide awareness and prevention techniques.

- Use the discussion as a guide. What age group or groups will be targeted?
- Who will copy the flyers?
- Where will the flyers be distributed?

Distribute the flyers created in the activity.

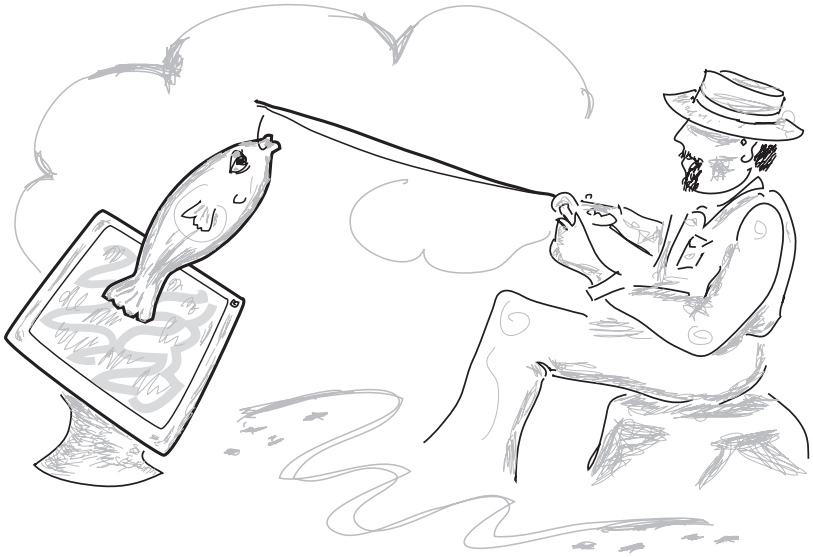
Have students take home copies of the flyers to discuss and share with their families.

If parents use e-mail, have students look for phishing e-mails to provide direct examples.

REFERENCE—Phishing for Your Identity

Phishing is a type of scam designed to steal your identity. Online phishing occurs through spam e-mail or pop-up windows by using false pretenses to try to get you to disclose valuable personal information, such as credit card numbers, passwords, account data, or other information.

Take a Closer Look at That E-mail . . .



E-mail phishing scams may appear to be e-mail messages from popular Web sites or sites that you trust, like your bank or credit card company. Usually these fake e-mails, which may contain official-looking logos and information from real organizations, will link to pop-up windows or Web sites that appear to be the real thing—but are not! Unfortunately, unsuspecting people all too often respond to these requests for their credit-card numbers, passwords, account information, or other personal data. Once given, the personal information can be used for illegal purposes like identity theft and monetary theft.

Be alert to possible phishing scams in e-mail.

The following phrases in e-mail probably indicate that someone is phishing in your inbox:

- "Verify your account."
- "Dear Valued Customer:"
- "If you don't respond within 48 hours, your account will be closed."
- "Click on the link to gain access to your account."

Legitimate businesses are aware of phishing scams. Most will not ask you to provide personal information via e-mail.

Guidelines for Protection From Phishing

- **Do not respond to suspicious e-mail—delete them immediately**.
- **Report suspicious e-mail**. Call the organization directly—don't use the e-mail you received—and ask for confirmation of the e-mail being sent.
- **Avoid clicking on links in e-mail messages unless you are absolutely sure of the destination**. Scam artists are able to display a fake URL in the address bar on your browser.
- **Do type addresses directly into your browser or use your personal bookmarks**. When performing transactions like updating account information or changing your password, visit the Web site by using your personal bookmark or by typing the URL directly into your browser.
- **Don't enter personal or financial information into pop-up windows**.
- **Update your operating system (OS) when prompted**.
- **Check the security certificate when you are entering personal or financial information into a Web site**. One example of a secure site is a lock icon on the lower bar. If the lock is closed, the site uses encryption.

Pharming

Although not as prevalent as e-mail phishing scams, pharming is the act of redirecting Internet traffic from one Web site to a different, identical-looking site in order to trick the user into entering a user name and password into the database on the fake site.

Banking or similar financial sites are often the targets of these attacks.

Criminals use these sites to acquire personal information in order to steal your identity or commit other kinds of fraud in your name.

The real danger to understand about pharming is that, unlike a phishing e-mail, which requires the victim to act, a pharming victim may be redirected to a fake Web site without any participation or knowledge.