DIGITAL CITIZENSHIP LESSON

PHISHING

Think Before You Click!

OBJECTIVES

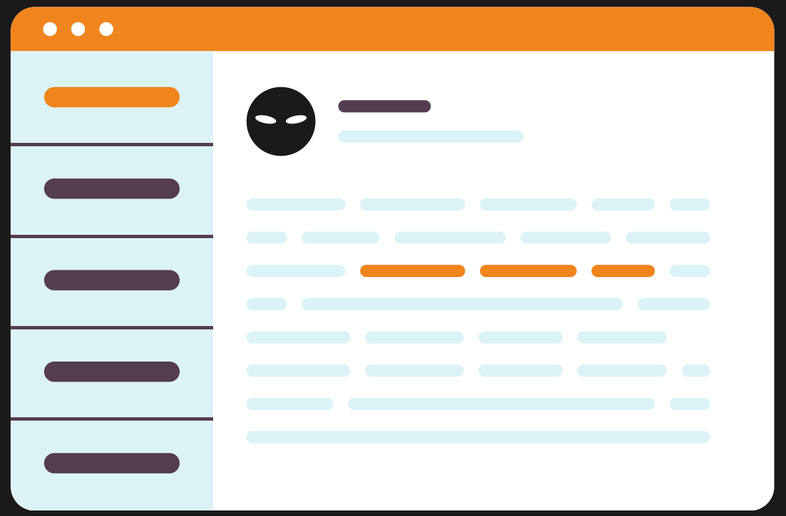
By the end of this lesson, students will be able to:

1. Define phishing, ransomware and identify common methods used by scammers
2. Recognize red flags in phishing emails, messages, or posts
3. Develop critical thinking skills to discern legitimate requests from potential phishing attempts

WHAT IS PHISHING?

Phishing is when someone tries to trick you into revealing personal information like your password, credit card numbers, or social security number.

Phishing can happen through emails, text messages, or other online platforms.



Think of an email or message you received that asked for personal information. What made it suspicious?

WHERE IS CAME FROM?

- Origin (mid-1990s on AOL): The very first phishing attacks happened on America Online (AOL) around 1995. Hackers pretended to be AOL staff and tricked users into giving up passwords and credit card details.

- Name origin: The word phishing comes from fishing — casting bait to catch victims. The “ph” spelling was influenced by hacker slang like phreaking (phone hacking)

THE HISTORY OF PHISHING

- 1990s: Simple scams on AOL, mostly fake messages asking for login details.
- 2000s: Attackers began targeting banks and financial services with fake websites and emails. Phishing kits appeared, making it easy for amateurs to launch attacks.
- 2010s: Rise of spear-phishing (targeting specific people), whaling (executives), and phishing through social media and smartphones.
- 2020s: Phishing became highly sophisticated, using AI, automation, voice cloning, and even deepfakes to trick victims.

TYPES OF PHISHING

Phishing attacks come in different forms

EMAIL PHISHING

Scammers send fake emails pretending to be a trustworthy organization

SMS PHISHING

Scammers send text messages with fake links or requests for personal information

SOCIAL MEDIA PHISHING

Scammers create fake profiles or posts to trick you into clicking on links or sharing personal informaion

EXAMPLE

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

WHAT IS RANSOMWARE ?

Ransomware is a type of malicious software (malware) that locks, encrypts or otherwise blocks access to your files or computer system and then demands a ransom payment to restore access

Keep your software updated, don't open suspicious emails, use strong passwords and use an antivirus or antimalware protection.

WHERE IS CAME FROM?

Ransomware is derived from the English word ransom, as it is the same principle as
in a kidnapping. To decrypt the information, the victim must pay the ransom.

THE HISTORY OF RANSOMWARE

The first Ransomware programm was created by Joseph Popp in 1989, it spread malware disks, with hidden files that involved encription programmms. It was known
as Aids trojan. Nowadays, it is a common program that anyone with a computer can create

EXAMPLE


Your personal files are encrypted!
Your private key will be destroyed on:
4/13/2015
Time left: 00:00
Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site
and follow the instruction.
in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.42k2bu15.com
https://34r6hq26q2h4jkzj.tor2web.blutmagie.de
Use your Bitcoin address to enter the site:
1MQrnrWHRo52jt32eUzpNcarSJM
Click to copy address to clipboard
if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.
Click for Free Decryption on site

RED FLAGS

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common read flags in phishing include:

1. Urgent or threatening language
2. Suspicious sender information
3. Requests for personal information
4. Misspellings or grammatical errors
5. Suspicious links or attachments
6. Generic greetings
7. Too good to be true

01 URGENT OR THREATENING LANGUAGE

Phishing attempts often create a sense of urgency or use threatening language to prompt immediate action. Phases like "urgent action required," "account suspended," or "your account will be deleted" may indicate a phishing attempt.

02 SUSPICIOUS SENDER INFORMATION

Check the sender's email address or social media profile. Phishing emails or messages often use generic or suspicious email addresses that do not match the legitimate entity they claim to represent.

03 REQUESTS FOR PERSONAL INFORMATION

Legitimate organizations do not request personal information, such as usernames, passwords, or credit card numbers, via email, social media, or other online means. Be cautious of any request for personal information.

04 MISSPELLINGS OR GRAMMATICAL ERRORS

Phishing emails or messages may contain misspellings, grammatical errors, or awkward phrasing. Legitimate organizations usually have professional communications and do not contain obvious errors.

05 SUSPICIOUS LINKS OR ATTACHMENTS

Be cautious of links or attachments in emails or messages from unknown or untrusted sources. Hover over links to check their actual destinations, and do not click on suspicious links or download attachments that you were not expecting.

06 GENERIC GREETINGS

Phishing emails may use generic greetings like "Dear Customer" instead of addressing you by your name. Legitimate organizations often personalize their communications with your name or other relevant information.

07 TOO GOOD TO BE TRUE

Phishing attempts may lure individuals with enticing offers, such as winning a prize or getting a huge discount. If an offer seems too good to be true, it may be a phishing attempt.

Which of the seven red flags do you think is the hardest to detect? What makes you say that?

REPORT PHISHING ATTEMPTS

If you suspect a phishing attempt, report it to a trusted adult, teacher . Please don't forward the phishing email or message to another user. You can show them on your device. Forwarding phishing emails could lead to others being phished.

Reporting phishing attempts helps protect others from falling victim to the scam.

THINK CRITICALLY

Be skeptical of emails, messages, or posts that seem too good to be true or too urgent. Remember, if it sounds too good to be true, it probably is!

Think before clicking on any links, sharing personal information online, or opening any suspicious attachments. Ask yourself if it seems legitimate and if you were expecting it.

Verify the authenticity of the sender and the information provided before taking any action. Trust your instincts and be cautious when sharing information online.

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING AND RANSOMWARE

Don't share your personal information online!