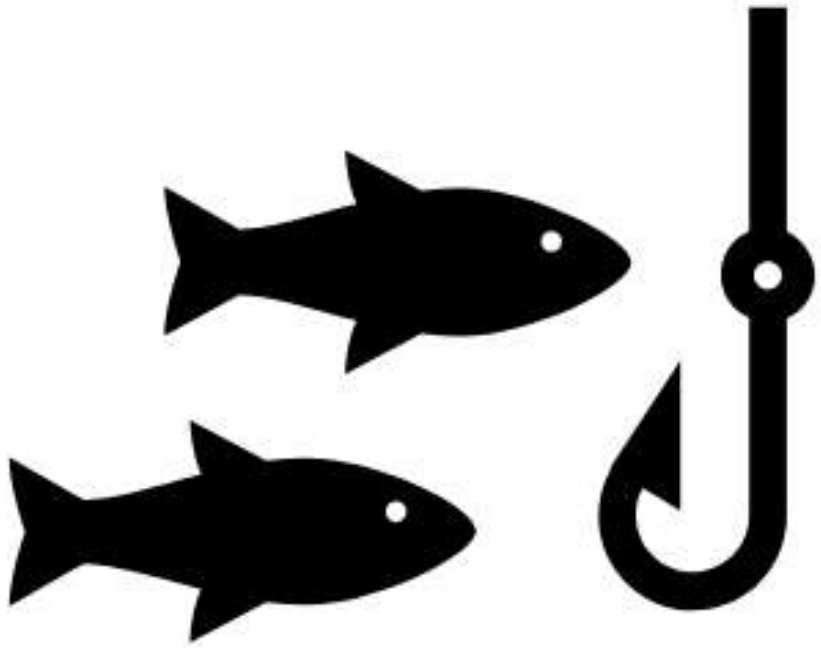
Let's NOT Go Phishing!

WLS CYBER SMARTS SERIES

Agenda

Today we'll dive into

- What phishing is
- Types of phishing
- How to recognize phishing
- How not to get caught

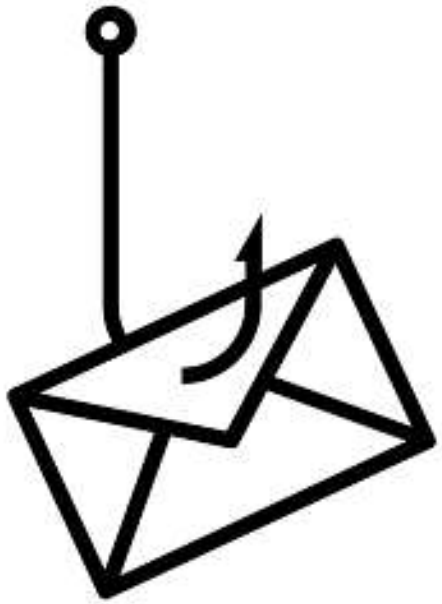


Quiz #1

What phishing is

Counterfeit communications – usually email - that have a "lure"

- appear to come from a trustworthy source
- try to fool the victim into providing confidential information
- provide access to online accounts, personal data, or permissions to access systems or can hijack or infect networks with ransomeware
- Another Phishing quiz https://www.intradyn.com/phishing-quiz/



Types of phishing

95 percent of all attacks on enterprise networks start with phishing

- **Spoofing** Any identity disguise
- **Spear Phishing** targets specific individuals
- **Whaling** targets a "big fish" like a CEO
- **Business Email Compromise (BEC) Attacks** impersonate a company executive vendor or supplier
- **Social media phishing** uses social media information to target a victim
- **Pharming** has two stages
  - install malicious code on your computer
  - the code sends you to a fake website automatically

Other types of phishing

- **Smishing** any kind of phishing that involves a text message
- **Vishing** Voice phishing, uses a phone call to obtain sensitive information

smishing by Jorge Reyes
from the Noun Project

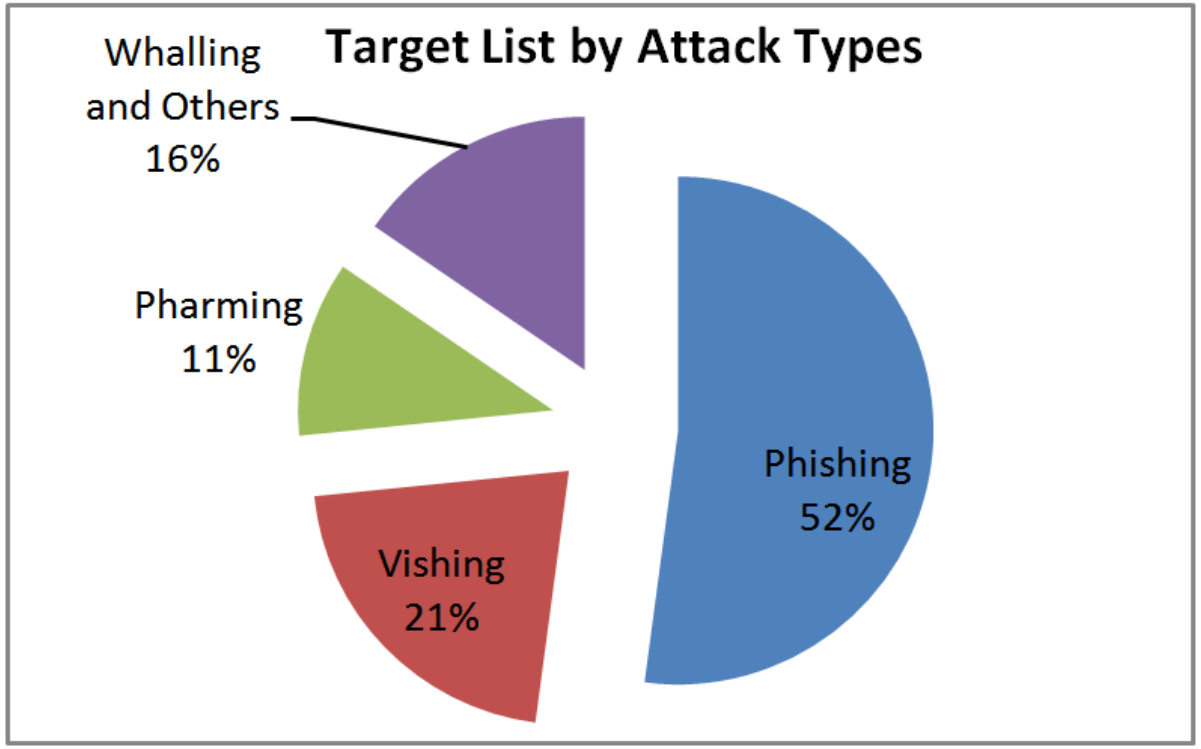
vishing by Jorge Reyes
from the Noun Project

Does it work?

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Why does it work?

- Social Engineering Attacks
- Count on human psychology
- Use fear, curiosity, urgency, and greed to compel recipients
- Appear legitimate by using information gotten through social media



How not to get "socially engineered"

- ✓ **Beware urgency!**
- ✓ **Verify urgent messages with their source** by calling, texting, or ***separately*** emailing the source

Security experts consider people's minds and habits the most vulnerable part of digital security.

Source

How to recognize a safe URL

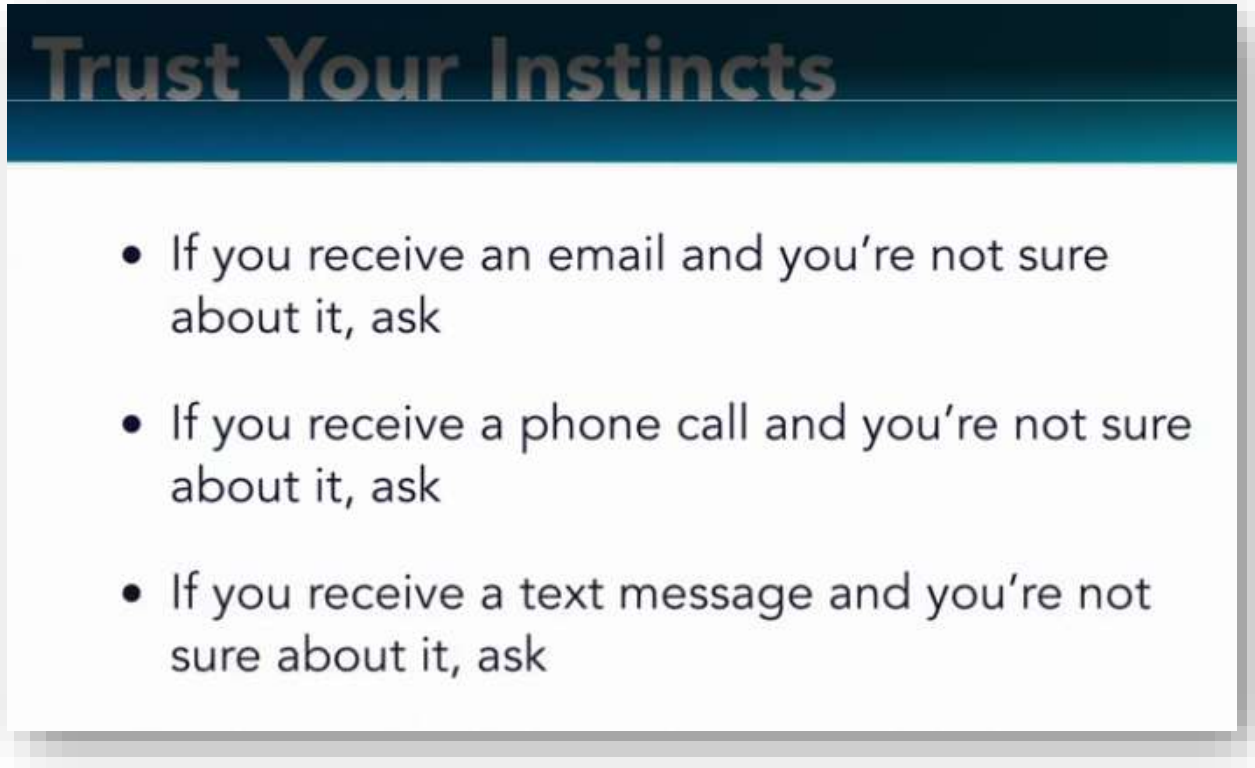
https://securityinabox.org/media/en/malware/how_to_read_urls.gif

Do not click an unknown link!

1. After "https://" , travel right to the next "/".
2. Then travel left to the previous "." and the word right before it. Your browser will usually highlight this part for you.
3. **Does it look like the site you expected to go to?** If not, someone may be trying to trick you.

How not to get caught when you click

- ✓**Pause before you click**
- ✓**Use caution when opening attachments**
- ✓**Do not click an unknown link!**
  Copy and paste it into a URL verifying website
  - https://www.virustotal.com
  - https://www.phishtank.com

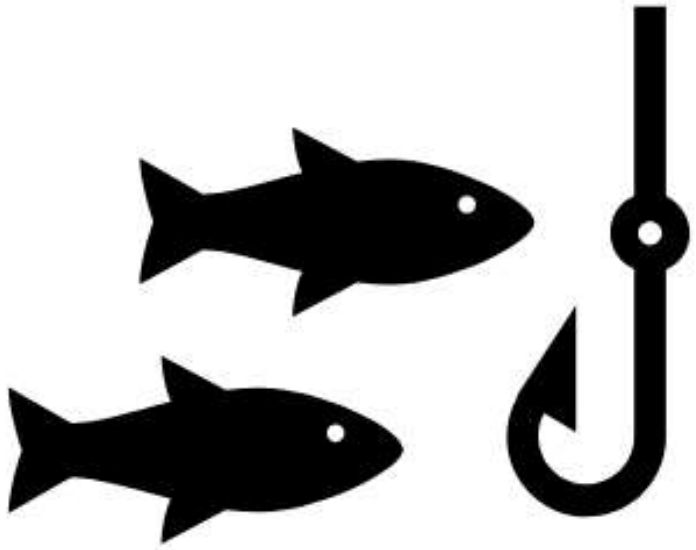


How not to get caught when you log in

- ✓ **Use Multi-factor Authentication**
  - ✓ extra set of credentials
  - ✓ the phisher won't have the code to get further
  - ✓ two-fold purpose: prevent the attacker from getting to your accounts and alerts you that something is wrong

Quiz#2

Let's review!



Cybersecurity Essentials

Keep your mobile devices and work area secure.

Keep software updated and on.

Use Multi-factor Authentication, strong passwords, and a password manager.

Know your library's data and digital standards policies.

You control the human factor. Trust your instincts – if something seems off or suspicious, contact your IT team or WLS IT.

Try out PKF O'Connor Davies Cybersecurity Newsletter

Recent Article

Links & Support

- FTC Cybersecurity For Small Business – Phishing
  https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing.pdf
- Cisco Phishing Information - focuses on business phishing
- Security In a Box
- Microsoft Protect Yourself From Phishing
- Norton Security - Smishing
- Kaspersky - Pharming
- The Tech Hacker – Phishing and MFA
- https://www.phishing.org/

Allison Midgley
- Training@wlsmail.org
- Support@wlsmail.org