Phishing

Phishing is a form of social engineering that uses email or malicious websites to solicit personal information or to get you to download malicious software by posing as a trustworthy entity.

Types of Phishing

- **Spearphishing**: Phishing targeted at an individual by including key information about them
- **Whaling**: Phishing targeted at a high-profile individual to steal sensitive and high-value information
- **Vishing**: Phishing via voice communication to entice the victim to engage in conversation and build trust
- **Smishing**: Phishing via text messages to get the victim to click on a link, download files and applications, or begin a conversation

Protecting Infrastructure

- ☐ **Secure user accounts on high-value services**: Require strong passwords using a password manager and multi-factor authentication (MFA).
- ☐ **Transition on-premises email servers to a cloud-based email server**: Add advanced protection services (e.g., Microsoft Enhanced Account Protection and Google Advanced Protection service).
- ☐ **Segment your email server from other critical assets**: If you are infected it won't harm other systems.
- ☐ **Conduct Phishing Campaign Assessment (PCA)**: Determine the susceptibility of personnel to phishing attacks.

Signs of Phishing

- **Suspicious sender's address** that may imitate a legitimate business
- **Generic greetings and signature** and a lack of contact information in the signature block
- **Spoofed hyperlinks and websites** that do not match the text when hovering over them
- **Misspelling**, poor grammar or sentence structure, and inconsistent formatting
- **Suspicious attachments** or requests to download and open an attachment

As the nation's **risk advisor**, the Cybersecurity and Infrastructure Security Agency's (CISA) mission is to **ensure the security and resiliency of our critical infrastructure.**

Contact CISA at **Central@CISA.gov** for assistance with:

- Phishing Campaign Assessment (PCA)
- Obtaining a .gov Domain
- Remote Penetration Test (RPT)

Learn more about the Information Sharing and Analysis Center for your sector: **nationalisacs.org**.

Visit **cisa.gov** to learn about CISA's role in infrastructure security.

Phishing Simple Tips

- **When in doubt, report it out**: If it looks suspicious, it's best to mark it as "junk" and forward to your IT staff.
- **Think before you act**: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for PII.
- **Make passwords long and strong**: Use a password manager to ensure you have unique, long, and strong passwords for each account.
- **Use multi-factor authentication (MFA)**: Enabling MFA can help prevent adversaries from gaining access to your systems even if your password is compromised.
- **Be wary of hyperlinks**: Avoid clicking on hyperlinks in emails; hover your cursor over links in the body of the email—if the links do not match the text that appears when hovering over them, the link may be spoofed.
- **Install and update antivirus software**: Make sure all your computers are equipped with regularly updated antivirus software, firewalls, email filters, and antispyware.

Reporting Incidents

1. Notify Your IT Department

Ph: _____

E: _____

2. Follow Incident Reporting Protocols

Review CISA's guidance and resources for responding to and reporting cyber incidents: cisa.gov/cyber-incident-response

3. Report to CISA

Submit a report at us-cert.cisa.gov/report.