* **Phish or Legit?**

Phishing Prevention Guide

Tammy Le

Secretary for WiCys Student Chapter

University of Washington

2023-2024

**What is Phishing?**

Phishing is when cybercriminals pretend to be trustworthy sources to trick people into sharing sensitive information like usernames, passwords, or financial details. These attacks can come through emails, text messages, phone calls, or fake websites. By knowing what to watch for, you can help protect yourself and our organization from these threats.

**Spotting Phishing Attempts**

*What to Look For:*

* Unusual Email Addresses: Phishing emails often come from addresses that look almost right but have slight misspellings or extra characters.
* Generic Greetings: Phishers may address you as “Customer” or “Account Holder” instead of using your name.
* Urgent or Threatening Language: Phishing messages often create a sense of urgency to pressure you into acting quickly.
* Unexpected Attachments or Links: Be wary of attachments or links you didn’t expect, especially if they’re out of context.

*Common Types of Phishing:*

* Email Phishing: Mass emails that look official but aim to steal your information.
* Spear Phishing: More targeted emails that may use your name or other details to seem convincing.
* Smishing and Vishing: Phishing through text messages (SMS) or phone calls, often pretending to be from customer service or tech support.

*Examples and Red Flags*

* Watch for links that don’t match official *URLs (hover over them to check).* Also, be alert for grammar mistakes or anything that feels out of place.

**Staying Safe**

*Best Practices for Email Security*

1. Only click links or open attachments from trusted sources. If unsure, verify directly with the sender.
2. Check the sender’s email address closely; phishers often use similar-looking addresses.
3. Hover over links before clicking to preview where they lead.
4. Strengthen Your Passwords
5. Use strong, unique passwords for every account and enable two-factor authentication (2FA) where possible.
6. Consider using a password manager to securely organize and store passwords.
7. Keep Your Software Up to Date
8. Regular updates to your operating system, software, and antivirus tools are crucial. These updates protect against known security vulnerabilities.
9. Enable Multi-Factor Authentication (MFA)
10. MFA is a strong defense against phishing because it requires extra verification beyond just a password. Set up MFA on your accounts whenever possible.

*How Organization(s) Protects Against Phishing*

1. Reporting Suspicious Messages

If you see something suspicious, report it to our IT security team. Reporting helps us investigate potential threats and protect others.

1. Staying Informed

Organizations should provide regular phishing awareness training and simulations. By staying informed, you’ll be better prepared to recognize phishing attempts and stay secure.

**What To Do if You Think You’ve Been Phished**

*Immediate Steps*

If you believe you may have clicked on a phishing link or shared sensitive information:

* Disconnect from the internet to stop any potential malware.
* Change your passwords, especially on sensitive accounts.
* Report the incident to any IT or security team for further support (in that organization)

*Securing Compromised Accounts*

* Update your passwords, enable two-factor authentication, and review your account activity for anything unusual. Run a virus scan on your device to check for malware.

**Additional Resources**

* Cybersecurity & Infrastructure Security Agency (CISA) – Resources and alerts on cybersecurity.
* Federal Trade Commission (FTC) – Tips on recognizing and avoiding phishing.

**Citations**

Cybersecurity and Infrastructure Security Agency (CISA). "Phishing: Avoid Phishing Scams." U.S. Department of Homeland Security, [www.cisa.gov/topics/cybersecurity-threats/phishing](http://www.cisa.gov/topics/cybersecurity-threats/phishing). Accessed 6 Nov. 2024.

Federal Trade Commission. "How to Recognize and Avoid Phishing Scams." Federal Trade Commission, 12 May 2023, www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

"Common Scams and Crimes: Phishing." Federal Bureau of Investigation, U.S. Department of Justice, www.fbi.gov/scams-and-safety/common-scams-and-crimes/phishing. Accessed 6 Nov. 2024.

Krebs, Brian. "The ABCs of Phishing Prevention." Krebs on Security, [www.krebsonsecurity.com/the-](http://www.krebsonsecurity.com/the-) abcs-of-phishing-prevention/. Accessed 6 Nov. 2024.

National Cyber Security Centre. "Phishing Attacks: Protecting Your Organization from Malware, Data Breaches, and Fraud." NCSC, United Kingdom Government, 23 Sept. 2023, www.ncsc.gov.uk/guidance/phishing.

Newman, Lily Hay. "How to Avoid Phishing Scams." Wired, Condé Nast, 15 July 2023, www.wired.com/story/how-to-avoid-phishing-scams/.

Tischer, Marc, and Steven Furnell. "Phishing Prevention Practices in Organizations." Journal of Cybersecurity, vol. 9, no. 2, 2022, pp. 99-115.