What is a Phishing scam, and how do you protect against it?

Understanding and Preventing Phishing Scams

Phishing (pronounced: “fishing”) is a type of online scam where criminals attempt to trick individuals into revealing sensitive personal information, such as passwords, bank details, credit card numbers, or even social security numbers. These scammers often disguise themselves as trusted entities—such as banks, email providers, government agencies, or delivery services—by sending fake messages that appear to be legitimate.

How Phishing Works

Phishing attacks typically come in the form of emails, text messages (also known as smishing), or even phone calls (vishing). The goal is to deceive the recipient into taking an action that benefits the attacker. Here’s how a typical phishing attack works:

1. **Fake Emails or Messages**: You receive an email or text that looks like it’s from a trusted company or institution. The message may claim there’s an issue with your account, a payment problem, or an urgent security alert.
2. **Deceptive Links**: The message includes a link that appears to lead to the company’s official website. However, the link actually redirects you to a fake website designed to steal your information.
3. **Information Theft**: If you enter your login details, password, or financial information on the fake site, the scammers capture your credentials and can use them for fraud or identity theft.

Common Tactics Used by Phishers

Phishing scams often use psychological manipulation to create a sense of urgency or fear. Here are some common tactics:

- **Urgency and Threats**: Messages may claim that your account will be locked or suspended unless you take immediate action.
- **Too-Good-To-Be-True Offers**: You might receive emails claiming you’ve won a prize, lottery, or gift card, urging you to click a link to claim it.
- **Impersonation of Authority Figures**: Some phishing scams pretend to be from government agencies, tax authorities, or tech support claiming that you owe money or your computer is infected with a virus.
- **Spoofed Email Addresses and Websites**: Scammers create

email addresses that look very similar to legitimate ones, often using small variations (e.g., “support@paypa1.com” instead of “support@paypal.com”).

How to Protect Yourself from Phishing

To stay safe from phishing attacks, follow these best practices:

1. **Verify the Sender**: Check the sender’s email address carefully. If it looks unusual, has misspellings, or uses a public domain like “@gmail.com” instead of an official domain, it may be a scam.
2. **Inspect Links Before Clicking**: Hover your mouse over any links to see the real URL before clicking. If the link looks suspicious or different from the official website, do not click it.
3. **Beware of Spelling and Grammar Mistakes**: Many phishing messages contain typos or awkward phrasing. Legitimate companies usually proofread their communications.
4. **Avoid Providing Personal Information**: Never enter your login credentials, bank details, or other sensitive information in response to an unsolicited message.
5. **Use Multi-Factor Authentication (MFA)**: Enabling MFA on your accounts adds an extra layer of security, making it harder for attackers to gain access even if they steal your password.
6. **Be Cautious with Attachments**: Do not download attachments from unknown or unexpected sources. They may contain malware designed to steal your data.
7. **Go Directly to Official Websites**: If you receive an email about an account issue, don’t click the link. Instead, type the official website address into your browser manually and log in from there.
8. **Report Phishing Attempts**: If you receive a suspicious email, report it to the company being impersonated and forward it to organizations like the Anti-Phishing

Working Group (reportphishing@apwg.org) or your country’s cybercrime unit.

What to Do If You Fall for a Phishing Scam

If you suspect that you’ve entered your information on a fraudulent website or clicked on a malicious link, take immediate action:

- **Change Your Passwords**: Update the passwords for any compromised accounts.
- **Enable Multi-Factor Authentication**: This adds extra security to your accounts.
- **Monitor Your Accounts**: Check your bank statements and online accounts for unauthorized activity.
- **Report the Incident**: Notify your bank, credit card provider, or any relevant service about the potential breach.
- **Run a Security Scan**: Use antivirus software to check your device for malware.

Final Thoughts

Phishing is a serious threat, but by staying vigilant and following security best practices, you can protect yourself from becoming a victim. Always think twice before clicking on links or sharing personal information, and when in doubt, go directly to the official source. Staying informed and cautious is the best way to safeguard your digital identity.

Made with the help and support of Inclusive Bytes CIC

Training | Reporting