



Phishing Exposed: Safeguarding Your Clicks

In the ever-evolving landscape of cyber threats, phishing scams have become a very prominent weapon used by cybercriminals. These deceptive tactics prey on unsuspecting individuals by leveraging various techniques to compromise personal information, devices, and even financial assets. This week, we'll share details on common phishing tactics fraudsters use, red flags you can look for, and some tips on how to stay safe.

- **Phishing Emails:** Email remains the primary avenue for phishing attacks. Fraudsters often craft very convincing emails to impersonate reputable entities like banks, government agencies, popular online shopping platforms, and much more. These emails typically contain urgent messages, perhaps alerting you to a charge you will not recognize. These emails are designed to entice users to click on malicious links, download malicious attachments, or call phone numbers that will directly connect you with a criminal who's waiting to take control of your device.
- **Malware and Viruses:** Phishing scams frequently involve the distribution of malware and viruses. Malicious software can be hidden in seemingly harmless downloads or links, waiting to infiltrate an entire system. Once installed, malware can capture sensitive information, track keystrokes, or even take control of the entire device. Always be cautious when clicking on links or downloading attachments, especially ones you aren't expecting.
- **Information or Device Compromise:** Phishing extends beyond email, targeting users through various digital channels. Social media platforms, messaging apps, and fake websites are commonly used by fraudsters to trick victims into divulging sensitive information or even providing access to their device. To avoid a compromise, always verify the legitimacy of communication you receive before taking any action. When verifying, only use contact information you have verified on the organization's official website.
- **Fake Websites and Spoofed Domains:** Fraudsters often create fake websites that mimic legitimate ones to deceive you into providing login credentials or financial information. These spoofed domains can very closely resemble trusted sites, making it a challenge for users to discern the difference. Vigilance is crucial when entering personal information online. Always remember to check the website's URL for authenticity.
- **Text Message (SMS) Phishing:** As mobile devices play a huge role in our daily lives; fraudsters commonly exploit text messaging as another way to trick you. You may receive fraudulent text messages containing links or prompts to call a specific phone number. Like phishing emails, these messages often contain an urgent message. Clicking on the links can lead to malware installation whereas calling the phone number can lead to elaborate and very convincing social engineering attempts.