Cyber Liability

Watch for These 6 Phishing Scams

Phishing is a type of cyberfraud that utilizes deceptive emails or other electronic communication to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. While emails are the most common delivery method of phishing attempts, cybercriminals may also use text messages, social media messages, fake or misleading websites, voicemails or even live phone calls. This article describes six common types of phishing scams to watch out for and provides actionable suggestions for how to mitigate them.

Types of Phishing Scams

Many significant cyberattacks have included a phishing component. In fact, in its 2021 Data Breach Investigation Report, Verizon noted that phishing played a role in approximately one-third of all breaches analyzed. The following are six of the most common types of phishing scams:

1. **Deceptive phishing**—Deceptive phishing is when a cybercriminal impersonates a recognized sender to steal personal data and login credentials. These emails often trick victims by asking them to verify account information, change a password or make a payment.
2. **Spear phishing**—A spear-phishing scheme is typically aimed at specific individuals or companies and uses personalized information to convince victims to share their data. In these instances, cybercriminals will research a victim's online behavior—such as where they shop or what they share on social media—to collect personal details that make them seem legitimate.
3. **Whaling**—Whaling aims to trick high-profile targets such as CEOs, chief financial officers and chief operating officers into revealing sensitive information, including payroll data or intellectual property. Since many executives fail to attend company security trainings, they are often vulnerable to whaling scams.
4. **Vishing**—Vishing, or "voice phishing," occurs when a criminal calls a target's phone to get them to share personal or financial information. These scammers often disguise themselves as trusted sources, such as a bank or the IRS, and rely on creating a sense of urgency or fear to trick a victim into giving up sensitive information.
5. **Smishing**—Smishing refers to "SMS phishing" and incorporates malicious links into SMS text messages. These messages often appear to be from a trustworthy source and lure victims in by offering a coupon code or a chance to win a free prize.
6. **Pharming**—Pharming is a sophisticated method of phishing that redirects a victim to a site of the cybercriminal's choosing by installing a malicious program onto their computer. The goal is to have users input their login credentials or personal information, such as credit card numbers, on the fraudulent site.

How to Protect Against Phishing Scams

As more criminals turn to online scams to steal personal and company information, business leaders and employees must remain vigilant in their cybersecurity efforts. While no single cybersecurity solution can avert all phishing attacks, the following actions can minimize their frequency and severity:

- **Stay informed about phishing techniques.** IT administrators should constantly monitor for new phishing scams and implement employee training accordingly. Utilizing mock phishing scenarios can help prepare employees for real attempts.
- **Examine a message before clicking.** Phishing scams often contain off-kilter URLs, so inspect the web address before

clicking on the website. A secure website always starts with "https." When in doubt, go directly to the source rather than clicking a potentially dangerous link. In addition, phishing scams depend on emotional lures to attract victims, so be wary of messages that incite an emotional or fearful response.

- **Keep computer systems up to date.** Security patches are released for computer systems to secure loopholes that cybercriminals inevitably discover and exploit. Download and install new software as soon as it's available, including browser updates.
- **Never give out personal information.** As a general rule, never share personal or financially sensitive information over the internet. When in doubt, go to the company's direct webpage and call to see if the request is legitimate.
- **Use antivirus software.** Implement antivirus software on all work systems to detect and prevent phishing attacks.
- **Back up data regularly.** Since phishing attacks often leave behind malware, including ransomware, companies should have a robust data backup program so attacks don't hinder the organization's productivity.

Phishing scams are becoming more sophisticated and severe. By taking the proper precautions, organizations can minimize their damage. For additional risk management guidance and insurance solutions, contact us today.