May 2015
Volume 10, Issue 5

Don't Take the Bait on Phishing Scams

More than 200 billion emails are sent and received worldwide each day.[i] That represents a lot of opportunity for phishing scams, in which scammers distribute emails that appear to come from legitimate organizations or individuals and try to entice the recipient into clicking on malicious links or attachments. Spear-phishing is a more targeted type of phishing in which a specific organization or person is the target. The typical goal of phishing attacks is to get the victim to give up sensitive information such as a Social Security number or financial information. Phishing is also used as a way for attackers to get inside an organization's network for cyber espionage or other malicious activity.

Scammers will use spoofed email addresses, phony websites with legitimate logos, or phone numbers to fake customer service centers operated by the scammers. Last year phishing attacks cost organizations $4.5 billion in losses.[ii]

Common Phishing Scams

When it comes to phishing, the best line of defense is you. If you pay attention to potential phishing traps and watch for telltale signs of a scam, you can minimize your risk of becoming a victim. Here are some scenarios you may encounter:

- An email appearing to be from a bank, credit card company, or other financial institution requests that you "confirm" your personal account information. Supposedly, your information has been lost, or your account is going to be closed, so it is "urgent" that you respond immediately.

- A phony email from the "fraud department" of a well-known company asks you to verify your information because they suspect you may be a victim of identity theft.

- An email may take advantage of a current event, such as the Anthem data breach, which scammers used to send phishing emails with malicious links for "free credit reporting."

- An email claiming to be from a state lottery commission requests your banking information to deposit the "winnings" into your accounts.

- A scammer pretends to have a large sum of money and needs "someone trustworthy" to help access it. The scammer promises to share the wealth in exchange for your help - specifically, your financial information.

Easy Tips to Protect Yourself from Phishing

- Do not send any sensitive personal information via email. Legitimate organizations will not ask users to send information this way.

- Visit banking or financial websites by typing the address into the address bar. Do not follow links embedded in an unsolicited email.

- Only open an email attachment if you're expecting it and know what it contains. Be cautious about container files, such as .zip files, as malicious files could be packed inside.

- If you want to verify a suspicious email, contact the organization directly – but don't call the number which is provided in the email.

- Use discretion when posting personal information on social media. This information is a treasure-trove to spear phishers who will use it to feign trustworthiness.

- Use antivirus software to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails. Keep your Internet browser updated with the latest security patches.

For More Information

- Anti-Phishing Working Group: www.antiphishing.org
- Internet Crime Complaint Center (IC3): www.ic3.gov/default.aspx
- Federal Trade Commission: https://www.consumer.ftc.gov/articles/0003-phishing

---

Provided By:

Center for Internet Security | STOP | THINK | CONNECT

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.

---

[i] http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf
[ii] http://www.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm