May 2016

Phishing Emails and You

Metropolitan Government of Nashville and Davidson County

When it comes to email, we've all come across a phishing email that appeared to be a legitimate email. Phishers take advantage of the fact that it is difficult to know with absolute certainty with whom you are communicating via email. They use this uncertainty to pose as legitimate businesses, organizations, or individuals, and gain our trust, which they can leverage to convince us to willingly give up information or click on malicious links or attachments.

Be Aware of Phishing Scams

First and foremost you should utilize a spam filter (this service is should be provided by your email provider), keep all of your systems patched and your anti-virus software up to date. The second line of defense against phishing is **you**. If you are vigilant, and watch for telltale signs of a phishing email, you can minimize your risk of falling for one. Telltale signs of a potential phishing email or message include messages from companies you don't have accounts with, spelling mistakes, messages from the wrong email address (e.g. info@yourbank.fakewebsite.com instead of info@yourbank.com), generic greetings (e.g. "Dear user" instead of your name), and unexpected messages with a sense of urgency designed to prompt you into responding quickly, without checking the facts. "Resume" and "Unpaid Invoice" are popular attachments used in phishing campaigns. Here are some scenarios you may encounter:

- An email appearing to be from the "fraud department" of a well-known company that asks you to verify your information because they suspect you may be a victim of identity theft.
- An email that references a current event, such as a major data breach, with a malicious link to setup your "free credit reporting."
- An email claiming to be from a state lottery commission requests your banking information to deposit the "winnings" into your account.
- An email with a link asking you to provide your login credentials to a website from which you receive legitimate services, such as a bank, credit card company, or even your employer.
- A text message that asks you to call a number to confirm a "suspicious purchase" on

Social engineering refers to the methods attackers use to manipulate people into sharing sensitive information, or taking an action, such as downloading a file. Sometimes social engineers interact with the victim to persuade the victim to share details or perform an action, such as entering information into a login page.

your credit card. When you call, the operator will know your name and account information and ask you to confirm your ATM PIN. (This is a form of SMSishing.) What should you do?

Recommendations

- Be suspicious of unsolicited emails, text messages, and phone callers. Use discretion when providing information to unsolicited phone callers, and *never* provide sensitive personal information via email.
- If you want to verify a suspicious email, contact the organization directly with a known phone number. Do not call the number provided in the email. Or, have the company send you something through the US mail (which scammers won't do).
- Only open an email attachment if you are expecting it and know what it contains. Be cautious about container files, such as .zip files, as malicious content could be packed inside.
- Visit websites by typing the address into the address bar. Do not follow links embedded in an unsolicited 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.
- Keep all of your software patched and up-to-date. Home users should have the auto update feature enabled.
- Keep your antivirus software up-to-date to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails.

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

More information on the CIS Critical Security Control 7: Email and Web Browser Protections: https://www.cisecurity.org/critical-controls.cfm

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

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.