OUCH! | December 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Phishing
- Protecting Yourself

Phishing

Overview

Email is one of the primary ways we communicate. We not only use it every day for work, but to stay in touch with our friends and family. In addition, email is now how most companies provide online services, such as confirmation of your online purchase or availability of your bank statements. Since so many people around the world depend on email, it has become one of the primary attack methods used by cyber criminals. In this newsletter, we explain phishing, a common email attack method, and the steps you can take to use email safely.

Guest Editor

Dr. Lance Hayden is a Managing Director for Berkeley Research Group. An expert in security culture and behavior, he is the author of People-Centric Security: Transforming Your Enterprise Security Culture from McGraw-Hill. You can find him at www.linkedin.com/in/drhayden.

Phishing

Phishing refers to an attack that uses email or a messaging service (like those on social media sites) that tricks or fools you into taking an action, such as clicking on a link or opening an attachment. By falling victim to such an attack, you risk having your highly sensitive information stolen and/or your computer infected. Attackers work hard to make their phishing emails convincing. For example, they will make their email look like it came from someone or something you know, such as a friend or a trusted company you frequently use. They will even add logos of your bank or forge the email address so the message appears more legitimate. Then the attackers send these phishing emails to millions of people. They do not know who will fall victim, all they know is the more emails they send, the greater the chance for success. Phishing is similar to using a net to catch fish; you do not know what you will catch, but the bigger the net, the more fish you will find. There are several ways attackers use phishing to get what they want:

Harvesting Information: The attacker's goal is to harvest your personal information, such as your passwords, credit card numbers or banking details. To do this, they email you a link that takes you to a website that appears legitimate. This

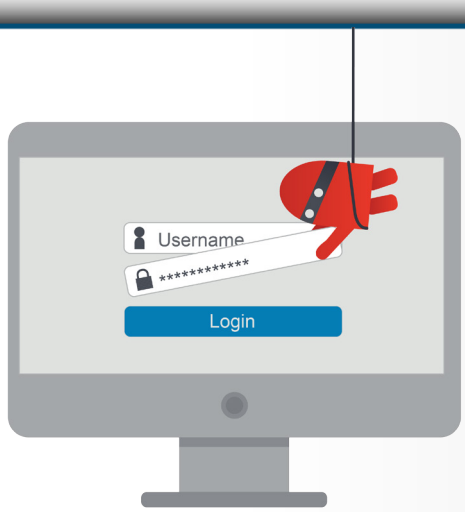
Phishing

website then asks you to provide your account information or personal data. However, the site is fake, and any information you enter goes directly to the attacker.

Malicious Links: The attacker's goal is to take control of your device. To do this, they send you an email with a link. If you click on the link, it takes you to a website that launches an attack on your device that, if successful, infects your system.

Malicious Attachments: The attacker's goal is the same, to infect and take control of your device. But instead of a link, the attacker emails you an infected file, such as a Word document. Opening the attachment triggers the attack, potentially giving the attacker control of your system.

Scams: Some phishing emails are nothing more than scams by con artists who have gone digital. They try to fool you by saying you won the lottery, pretending to be a charity needing donations or asking for your help to move millions of dollars. If you respond to any of these, they will say they first need payment for their services or access to your bank account, scamming you out of your money.



Your best defense is common sense. If an email or message is odd, suspicious or too good to be true, it may be a phishing attack.

Protecting Yourself

In almost all cases, opening and reading an email or message is fine. For a phishing attack to work, the bad guys need to trick you into doing something. Fortunately, there are clues that a message is an attack. Here are the most common ones:

- The email creates a sense of urgency, demanding "immediate action" before something bad happens, like closing your account. The attacker wants to rush you into making a mistake without thinking.
- You receive an email with an attachment that you were not expecting or the email entices you to open the attachment. Examples include an email saying it has an attachment with details of unannounced layoffs, employee salary information or a letter from the IRS saying you are being prosecuted.
- Instead of using your name, the email uses a generic salutation like "Dear Customer." Most companies or friends contacting you know your name.

Phishing

- The email requests highly sensitive information, such as your credit card number or password.
- The email says it comes from an official organization, but has poor grammar or spelling, or uses a personal email address like @gmail.com, @yahoo.com or @hotmail.com.
- The link looks odd or not official. One tip is to hover your mouse cursor over the link until a pop-up shows you where that link really takes you. If the link in the email doesn't match the pop-up destination, don't click it. On mobile devices, holding down your finger on a link gets the same pop-up. An even safer step is to copy and then paste the URL from the email into your browser or type the correct link.
- You receive a message from someone you know, but the tone or wording just does not sound like him or her. If you are suspicious, call the sender to verify they sent it. It is easy for a cyber attacker to create an email that appears to be from a friend or coworker.

If you believe an email or message is a phishing attack, simply delete it. Ultimately, common sense is your best defense.

NERC CIPv5 Cyber Security Training

Be sure to check out our free resources including the OUCH! newsletter, weekly blogs and Video of the Month. This month, we're covering CIP v5: Operating Interconnected and Interdependent BES Cyber Systems. View the video at https://www.securingthehuman.org/u/8x9.

Resources

Social Engineering:	https://www.securingthehuman.org/ouch/2014#november2014
Five Steps to Staying Secure:	https://www.securingthehuman.org/ouch/2014#october2014
I'm Hacked, Now What?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License