The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Overview
- Phishing Attacks
- Protecting Yourself

Email Phishing Attacks

GUEST EDITOR

Pieter Danhieux is the guest editor for this issue. He works for BAE Systems Detica in Australia (www.baesystemsdetica.com.au) and is an instructor for the penetration testing courses at the SANS Institute.

OVERVIEW

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

PHISHING ATTACKS

Phishing was a term originally used to describe email attacks that were designed to steal your online banking username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool. Phishing attacks work one of four ways:

- **Harvesting Information:** The cyber attacker's goal is to fool you into clicking on a link and taking you to a website that asks for your login and password, or perhaps your credit card or ATM number. These

Email Phishing Attacks

websites look legitimate, with exactly the same look, imagery and feel of your online bank or store, but they are fake websites designed by the cyber attacker to steal your information.

- **Infecting your computer with malicious links:** Once again, the cyber attacker's goal is for you to click on a link. However, instead of harvesting your information, their goal is to infect your computer**.** If you click on the link, you are directed to a website that silently launches an attack against your computer that if successful, will infect your system.
- **Infecting your computer with malicious attachments**: These are phishing emails that have malicious attachments, such as infected PDF files or Microsoft Office documents. If you open these attachments they attack your computer and, if successful, give the attacker complete control.
- **Scams:** These are attempts by criminals to defraud you. Classic examples include notices that you've won the lottery, charities requesting donations after a recent disaster or a dignitary that needs to transfer millions of dollars into your country and would like to pay you to help them with the transfer. Don't be fooled, these are scams created by criminals who are after your money.

PROTECTING YOURSELF

In most cases, simply opening an email is safe. For most attacks to work you have to do something after reading the email (such as opening the attachment, clicking on the link or responding to the request for information). Here are some indications if an email is an attack:

Use common sense, if an email seems odd or too good to be true, it is most likely an attack.

- Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique used by criminals to rush people into making a mistake.
- Be suspicious of emails addressed to "Dear Customer" or some other generic salutation. If it is your bank they will know your name.
- Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

Email Phishing Attacks

- Do not click on links. Instead, copy the URL from the email and paste it into your browser. Even better is to simply type the destination name into your browser.
- Hover your mouse over the link. This will show you the true destination where you would go if you actually clicked on it. If the true destination of the link is different than what is shown in the email, this may be an indication of fraud.
- Be suspicious of attachments and only open those that you were expecting.
- Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may have been compromised, and malware is sending the email to all of your friend's contacts. If you get a suspicious email from a trusted friend or colleague, call them to confirm that they sent it. Always use a telephone number that you already know or can independently verify, not one that was included in the message.

If after reading an email you think it is a phishing attack or scam, simply delete the email. Ultimately, using email safely is all about common sense. If something seems suspicious or too good to be true, it is most likely an attack. Simply delete the email.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

OnGuard Online –
http://www.onguardonline.gov/phishing

Recognizing Phishing Attacks:
http://preview.tinyurl.com/3c2axs8

OpenDNS Phishing Protect:
http://www.opendns.com/phishing-protection

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANS 2013. Over 40 security classes taught by the world's leading experts. March 08-15, 2013 in Orlando, FL. http://www.sans.org/event/sans-2013/

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner