The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Phishing
- Scams
- Protecting Yourself

E-mail Phishing and Scams

GUEST EDITOR

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

OVERVIEW

E-mail 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 e-mail is how companies provide many products or services, such as confirmation of an online purchase or updates to our bank account. Since so many people around the world depend on e-mail, it has also become one of the primary methods cyber criminals use to attack others. In this newsletter we explain these dangers and steps you can take to protect yourself.

PHISHING

Phishing is one of the most common e-mail based attacks. It uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. Phishing was a term originally used to describe an attack designed to steal your online banking login details. However, the term has evolved and now refers to almost any cyber attack sent by e-mail. A phishing attack begins with an e-mail pretending to be from someone or something you know or trust, such as your bank or your favorite online store. These e-mails then try to entice you into taking an action, such as clicking on a link, opening an attachment, or responding to a message. Cyber criminals craft these convincing e-mails and then send them out to thousands, if not 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 e-mails they send out, the more people they may be able to fool. Phishing attacks often have one of the following objectives:

- **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 favorite color or mother's maiden name. These websites may look legitimate with exactly the same look and feel of your online bank, but they are designed to steal information that could give them access to your online account.

E-mail Phishing and Scams

- **Controlling your computer through malicious links:** Once again, the cyber attacker's goal is for you to click on a link. However, instead of harvesting your information, the 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 browser, and, if successful, these cyber criminals have full control over your computer.
- **Controlling your computer through malicious attachments**: These are phishing e-mails that have infected 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.

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

SCAMS:

Scams are nothing new; these are attempts by criminals to defraud you. Classic examples include notices that you've won the lottery (even though you never entered it) or that a dignitary needs to transfer millions of dollars into your country and would like to pay you to help with the transfer. They will then tell you that you have to pay a processing fee before you can get your money. After you pay these fees the criminals disappear, never to be heard from again.

PROTECTING YOURSELF

In most cases simply opening an e-mail is safe. For most attacks to work you have to do something after reading the e-mail (such as opening the attachment, clicking on the link, or responding to the request for information). If after reading an e-mail you think it is a phishing attack or scam, simply delete the message. Here are some indications if an e-mail is an attack.

- Be suspicious of any e-mail that requires immediate action or creates a sense of urgency. This is a common method used to trick people.
- Be suspicious of e-mails addressed to "Dear Customer" or some other generic salutation.
- Be suspicious of grammar or spelling mistakes, most businesses proofread their messages very carefully.

E-mail Phishing and Scams

- If a link in an e-mail seems suspicious, hover your mouse over the link. This will show you the true destination where you would go if you actually clicked it. The link that is written in the e-mail may be very different than where it will actually send you.
- 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. For example, if you get an email from UPS telling you your package is ready for delivery, do not click on the link. Instead, go to the UPS website and then copy and paste the tracking number.
- Be suspicious of attachments; only open attachments that you were expecting.
- Just because you got an e-mail 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 e-mail to all of your friend's contacts. If you get a suspicious e-mail from a trusted friend or colleague, call them to confirm that they sent it.

Ultimately, using e-mail 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 e-mail.

RESOURCES

Some of the links shown below 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.

How Phishing Works: http://preview.tinyurl.com/853xj85

OnGuard Online - Avoiding Scams: http://preview.tinyurl.com/6vfoljs

Anti-Phishing Working Group: http://www.apwg.org

Phishtank: http://www.phishtank.org

Security Terms & Definitions: http://preview.tinyurl.com/6wkpae5

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org