Houston Information Technology Services (HITS)
Enterprise Security

Monthly Security Tips NEWSLETTER

April 2013 Volume 8, Issue 4

Protect Yourself from Email Phishing Attacks

From the Desk of the Chief Information Security Officer (CISO)

In the pre-Internet era, con men, also known as confidence men, would gain victims' confidence through the use of deception, to defraud them. The same principles are being used today, only now to an even greater efficiency through the use of online scams. One of the most prolific means for online scamming is phishing.

"Gone Phishing"

When using the email, it is difficult to know, with certainty, with whom you are communicating. Scammers will utilize this uncertainty to pose as legitimate businesses, organizations, or individuals, and gain the trust of users. If a scammer is able to gain the trust of victims, they can leverage this trust to convince victims to willingly give up information or click on malicious links or attachments. To gain users trust, scammers will appear like legitimate businesses or organizations, by spoofing the email address, creating a fake website with legitimate logos and even providing phone numbers to an illegitimate customer service center operated by the scammers. Being mindful and observant can help you defend against scammers' deceptions by being prepared and proactive.

Two Common Types of Phishing Attacks

- *Phishing scams* are perhaps one of the best-known forms of email scams. This type of scam involves a scammer pretending to have a fortune that he or she is incapable of accessing without the help of someone trustworthy, which happens to be you! The scammers will try to obtain the user's financial information using an empty promise of sharing the wealth in exchange for their help.

- *Spear-phishing.* Spear-phishing is a targeted and personalized attack in which a specific organization or an individual is the target. These attacks will utilize information about the user email addresses, which are similar to those of their acquaintances to entice the users to either divulge sensitive information or download a malicious file. This often requires a lot of information gathering on the targets and has become one of the favored tricks used in cyber espionage.

Be Mindful

When it comes to phishing, the best line of defense is you. If you are mindful of potential phishing traps and observant of the telltale signs of a scam, you can better defend against a phishing attack. Here are some easy tips to protect yourself:

- Be cautious about all communications you receive including those purported to be from "trusted entities" and be careful when clicking links contained within those messages. If in doubt, do not click.

- Don't respond to any spam-type e-mails.

- Don't send your personal information via email. Legitimate businesses will not ask users to send their sensitive personal information through this means.

- Don't input your information in a pop-up; if you are interested in an offer that you see advertised in a pop-up ad,

contact the retailer directly through its homepage, retail outlet or other legitimate contact methods.

Be Observant

Scammers rely on their deception to entice users to willingly do what the phisher wants. Their deception is based upon resembling legitimate sites or trusted sources. These phishing scams can be very realistic and difficult to identify. However, there are some telltale signs that may indicate a phishing scam. By being observant of these, you can help minimize your risk of becoming a victim. Keep an eye out of these simple telltale signs of a phishing email:

- The email has poor spelling or grammar.
- For secure transactions, look for a lock icon in the URL.
- The use of threats or incredible offers is a common tactic that tries to elicit an emotional response to cloud the user's judgment.
- The URL does not match that of the legitimate site. Scammers cannot use the same URL associated with the legitimate websites, so they will tweak the address of their spoofed website so that at a quick glance it looks legitimate.
    - The URL may use a different domain name (e.g., .com vs .net)
    - The URL may use variations of the spelling of the actual address

Be Aware of Attachments

Don't trust a file based on its extension. There are a variety of tricks to hide the nature of the file. While the simplest solution is not to download a file from an unknown user, below are some additional things you can look for:

- Be cautious about double file extensions. One way the extension can be hidden is by adding a second extension such as "Evil.pdf.exe" so that is looks like a regular PDF, with the .exe hidden.
    - To help spot double extensions, turn off the "Hide extensions for known files" option on your computer's operating system. See: http://support.apple.com/kb/PH10845 for Mac, http://support.microsoft.com/kb/865219 for Windows
- Be wary of container files, such as.zip files. Any number of files can be packaged inside, including malicious ones!
- Beware of attached files. Malicious code can also be embedded in commonly emailed files such as .doc and pdf, giving you another reason why you should only open attachments from trusted sources!
- Do not open executable files. These are files which have a .exe extension.

Lastly, make sure you have an up-to-date anti-virus software program installed. Enable the feature to scan attachments with the anti-virus program before downloading and saving them to your computer.

For additional information about email phishing scams, please visit:

- **FTC's Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft**
- **AntiPhishing Work Group: www.antiphishing.org**
- **Microsoft - Recognize Phishing -- www.microsoft.com/security/online-privacy/phishing-symptoms.aspx**
- **Sophos – Dealing with Spear Phishing Campaigns - www.sophos.com/en-us/support/knowledgebase/37179.aspx**

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of the City'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.