Monthly Newsletter

August 2016 **Phishing**

In This Issue

Other Interesting Links

- US-Cert
- PhishTank
- AntiPhishing Working Group (APWG)
- OnGuardOnline
- The Latest Phishing Activity
- Recognize Phishing emails

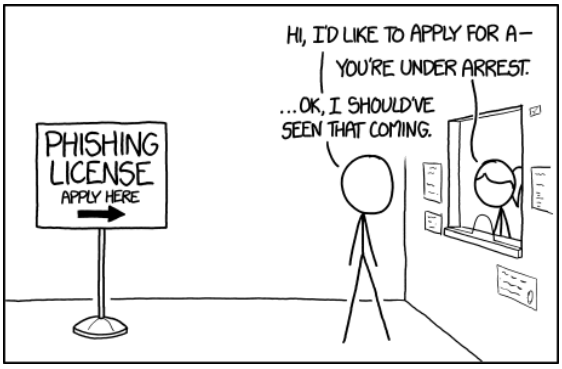
Contact Us

Cyber Security

kirk.burns@dps.texas.gov

Introduction

"Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual." (us-cert.gov)



Phishing is a very low-tech, yet highly effective method of compromising computers. This is because it is far easier to trick someone into clicking a malicious link than it is to break through computer defenses. Attackers use several techniques to perform phishing attacks. The most common technique used is to try to scare an individual into giving up confidential information; like their password. Another common technique is to send an email saying your password needs to be reset and it directs you to a website where you input the information. Because the email and the website look official, users often never question if it is legitimate and fall victim to this type of attack. Victims put in their username and password thinking they are following instructions and doing the right thing. And they are. Problem is they are doing exactly what they are supposed to do for the **attacker** to steal their information. (comic borrowed from http://www.xkcd.com)

Dangers of Phishing

The attacker's ultimate goal is what determines the actual danger. Personal and financial information, passwords, account IDs and credit card information are just some of the things that attackers attempt to acquire. The most successful phishing attempts employ the techniques of professional marketers to identify the most effective types of attacks. Phishing campaigns often happen around major yearly events such as holidays, anniversaries, etc. They can even take advantage of breaking news stories, both true and fictional. The idea is to get the user to go to a site and trick them into giving up information. While phishing attacks are often email based, they are not limited to email. Social media sites are increasingly becoming an attack vector.

Examples of dangers:

- Is the attacker trying to steal money?
    - If so, the victim will probably receive an email crafted to look like something from their bank. The purpose of this type of attack is to gain

access to the individual's bank accounts.

- Is the attacker attempting identity theft?
    - If so, the victim will most likely receive some sort of survey or specially crafted business email designed to convince the victim to give up personal information the attacker can use to impersonate the victim.
- Is the attacker attempting to gain computer access to where the victim works?
    - If so, the victim will most likely receive an email crafted to look like something official from their job which asks for confidential information.

No matter how secure a system is, if the individual can be tricked then the system can be bypassed and compromised.

Have I been Phished?

Sometimes it can be very difficult to tell. Phishing messages look like they are genuine.

They often include logos or other identifying information taken directly from a company's website. The malicious links in the message are designed to appear as if they are from the **spoofed** or **homograph spoofed** organization. Attackers will use subdomains and misspelled URLs and some attackers have even gone so far as to use JavaScript to place a picture of a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be changed by using JavaScript and other programing languages. To learn more about phishing attacks and how to report phishing attacks to your personal email, go to **us-cert.gov** or **ftc.gov**.

DPS compromise

The Department recently had a significant security breach from a successful phishing attack. A couple of months ago, an employee received an email with a link to a false password change form. The attackers used the employee's credentials to send phishing emails to approximately 1,000 Department email accounts. Thirty-four users visited the false password change form and twelve of those users were compromised. This provided the attackers with even more legitimate credentials. The attackers were able to gain access to the users' mailboxes and send additional phishing emails to targets inside and outside of DPS. Approximately 3,700 emails were blocked by our SPAM filters, but an unknown number of phishing emails were sent to email addresses outside of the DPS network (i.e. Hotmail, Yahoo, Gmail, etc.).

This compromise has promoted a change in how the Outlook Web App will be accessed in the future. The changes will happen in the near future and will be communicated in a mass email giving instructions and notification on when the procedures will go into effect.

Upcoming Cyber Projects

I want to use this part of the newsletter to notify you of upcoming Cyber related projects.

- As mentioned above, a new procedure will be implemented soon. A mass email with details and instructions will be sent out prior to implementation.
- Online mandatory yearly cyber/CJIS awareness training. The training is in place and will soon be pushed out.
    - All employees working in an IT field will receive the training first. Those employees should receive an email with instructions on how to access the training by the middle of August. IT employees will have one (1) month to complete the training.
    - All other employees will receive the email notification of required training around 1 September and will have two (2) months to complete the training.

The online cyber/CJIS awareness training is a yearly requirement. Sometime after the beginning of the new year all accounts will be reset and you will be notified on when you have to have the training completed.

For More Information

For information, tutorials and contact information about this month's topics, you can click the links on the side of the newsletter. For other Cyber Security news, please visit the Cyber Security website. Remember that security is a shared responsibility and,

"**Do Good Cyber**".

Cyber Security Training Officer

Kirk Burns is the Cyber Security Training Officer for DPS. He has a BS in Criminal Justice, a BS in Computer Science, and an MS in Digital Forensics. He is a Computer Science professor for Sam Houston State University with over 16 years of IT experience. Kirk serves as a member of the Texas Army National Guard and holds a current CISSP certification.

If you have further questions about this month's topic or any other security issue, do not hesitate to contact him. He is happy to assist. You can contact him via email at kirk.burns@dps.texas.gov, on his work phone at 512.424.5183 or on his work cell at 512.466.3151.