SOCIAL ENGINEERING, PHISHING ATTACKS, AND ONLINE SCAMS

Social engineering is a method cyber attackers use to deceive victims into performing an action that compromises information technology, such as opening malicious webpages or downloading malicious file attachments. Attackers use human interaction and social skills to obtain or compromise personal data or information about an organization and its computer systems. Attackers might seem unassuming and respectable, claiming to be new employees, support personnel, or researchers. Some attackers even provide fraudulent credentials to support their identity. By interacting with their victims and asking questions, attackers can possibly piece together enough information to infiltrate an organization's network, steal or compromise personal, financial, and/or other sensitive data. When attacking an organization, multiple employees might be targeted in order to obtain all of the necessary information.[1]

PHISHING ATTACKS

Phishing, a form of social engineering, is the processes of deceiving recipients into sharing sensitive information with an unknown third-party, or cyber attacker, typically through email; however, websites and internet pop-up ads are also used.[2] When using email, it is difficult to know exactly with whom you are communicating. Scammers utilize this uncertainty to pose as legitimate businesses, organizations, or individuals to gain the trust of users and compromise their personal, financial, or other sensitive information. Scammers appear to represent legitimate businesses or organizations by spoofing email addresses, creating fake websites with legitimate logos, and providing phone numbers to illegitimate customer service centers or tech support centers operated by attackers. The two most common types of phishing attacks include phishing scams and spear-phishing.

> **Spoofing occurs when a malicious party impersonates another device or user on a network in order to steal data, spread malware, or bypasses access controls.**

Phishing scams are perhaps the best-known forms of email scams. An example of this type of scam involves an attacker pretending to have a fortune that he or she is incapable of accessing without the assistance of someone trustworthy. Attackers will attempt to obtain your financial information using the promise of sharing the wealth in exchange for your help. Phishing emails have also come from attackers impersonating university staff, tech support companies, utility companies, and charities. Attackers often take advantage of holidays or current events (i.e., natural disasters, epidemics and health scares, economic concerns, and political elections).[1]

- In February 2015, Apple users reported a phishing scam campaign. Attackers sent out spoofed emails claiming that a customer's Apple ID, iCloud, or iTunes account had been compromised and asked for personal information from the customer to fix the problem. Because many Apple users also use iCloud accounts to back up their mobile devices, the hackers could use the stolen information to access more personal information.[4]

- The 419 Scam, or Spanish Prisoner scam, is one of the most popular phishing scams. The scam actually dates back several hundred years, long before email was invented. The table below illustrates how the scam works – choose one from each column:

You are contacted by a:	Who needs help with getting large amounts of _____ out of the country:	The problem (or why your help is needed) is:	Victims eventually:
- Prince - General - Family member of deposed leader - Wealthy businessman - Doctor	"Forgotten" government money - Diamonds - Personal wealth - Excess money from over-invoiced contracts	- A banker will not transfer the money without a bribe - There are taxes on the transfer - Export fees are needed - The money is marked and must be "cleaned"	- Gave up after paying "fees" and receiving nothing in return - Traveled to the country and paid further fees - Traveled to the country and were kidnapped for ransom - Traveled to the country and were killed - Were contacted by a "Government recovery agency" who asked for a fee to recover their money

- In 1999, a Norwegian millionaire traveled to South Africa as part of the 419 scam and was kidnapped and eventually murdered. The same year, a Romanian businessman was kidnapped and held for a half-million dollar ransom. Police arrested five Nigerians and two South Africans for both the kidnappings and murders.[5]

Spear-fishing attacks are a more targeted form of phishing attacks. These attacks target a specific individual, or individuals within a particular organization. Attackers utilize email addresses similar to the target's acquaintances to entice users into revealing sensitive information or downloading malicious files. This type of attack requires the gathering of a significant amount of information about the targets.[1] Spear-phishing attacks are an increasing concern for banks and other financial institutions whose organizations and customers are frequently targeted by these types of attacks.

- On 02/23/2015, Cornell University reported a phishing email that was sent to *cornell.edu* users. The email stated that the user's account is no longer active and is scheduled to be deleted on a future date. The message then prompted users to reply with their user name and password to keep their account active and subscribed to *cornell.edu's* database.[6]

- In 2014, JPMorgan Chase accounts were compromised. The attack began when a Chase employee's credentials were accessed through a spear-phishing attack. After the credentials were obtained, attackers gained access to a third-party website used by Chase and eventually accessed more than 90 internal bank servers. The attack, which started in the spring, was detected and blocked by the bank in August 2014.[7]
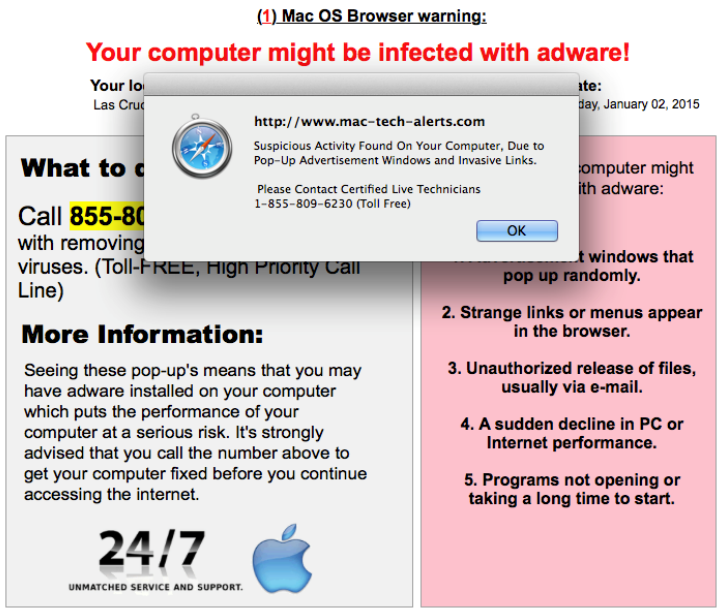
ONLINE SCAMS

The Internet has been overrun with varieties of online scams since its inception. Although it is not new, the fake tech support scam has experienced an upswing in recent months. A typical tech support scam presents itself to users who are browsing the Internet. The user will get a pop-up message stating that a virus or "suspicious activity" has been detected on the user's machine. The pop-up will contain a website and a phone number for the user to call to rectify the problem. When the number is called, attackers posing as tech support will offer to fix the machine for a fee. These pop-ups are typically the result of visiting a page that is either malicious, hacked, or contains advertising from a hacked ad feed. The page contains malicious code that either displays a pop-up, or redirects to a malicious webpage that then displays the pop-up.[8]

(1) Mac OS Browser warning:

Your computer might be infected with adware!

http://www.mac-tech-alerts.com

Suspicious Activity Found On Your Computer, Due to Pop-Up Advertisement Windows and Invasive Links.

Please Contact Certified Live Technicians
1-855-809-6230 (Toll Free)

OK

What to do

Call 855-80...
with removing...
viruses. (Toll-FREE, High Priority Call Line)

More Information:

Seeing these pop-up's means that you may have adware installed on your computer which puts the performance of your computer at a serious risk. It's strongly advised that you call the number above to get your computer fixed before you continue accessing the internet.

24/7
UNMATCHED SERVICE AND SUPPORT.

...computer might ...th adware:

...t windows that pop up randomly.

2. Strange links or menus appear in the browser.

3. Unauthorized release of files, usually via e-mail.

4. A sudden decline in PC or Internet performance.

5. Programs not opening or taking a long time to start.

It is important to understand that these messages are not caused by a virus or any other form of malware. The malware is contained within the webpage that was visited, not the user's computer. The above illustration is an example of a webpage and pop-up that user's might see as part of a tech support scam. The webpage states "you may have adware installed on your computer" leading many people to believe that their machine is infected. Many people's reactions to these pop-ups is to download anti-virus software; however, anti-virus software will not solve the problem. Additionally, it is important to know that *no website can scan your machine for malware or suspicious activity*, meaning these pop-ups claiming to have detected items on your computer are fictitious.[8]

> **It is important to distinguish the difference between a website and anti-virus software scanning your machine for adware.**
>
> - **Malicious websites CAN install malware and adware on your machine; however, they CANNOT scan your computer for adware or suspicious activity.**
> - **Anti-virus software is a program downloaded onto your machine to scan and detect malware.**

Recommendations

The Pennsylvania Criminal Intelligence Center (PaCIC) is providing this information for situational awareness purposes. These types of cyber-attacks, as well as many others, occur every day. The following recommendations are provided to help protect you from experiencing unwanted intrusions:

- Be mindful and observant of potential traps and scams. Be cautious of all communication you receive, including those claiming to be from "trusted entities" and be wary of clicking links within those messages. Do not open
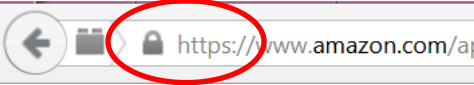
emails from unknown sources. If you are unsure of the origin of the message, do not click on any links or download any files within the message. Additionally, check the return email address listed after the name of the sender in the message. Oftentimes, the return email address will assist in determining if the email is legitimate.

- Do not respond to spam emails.
- Do not send any of your personal information via email. Legitimate businesses will not ask customers to send personal information via email. If you receive an email from a business asking for personal information, look up the business phone number and call them to ensure the message is legitimate. Do not use phone numbers contained within the message as these numbers might be answered by attackers.
- Never enter personal information into a pop-up. Often, enticing offers are advertised through pop-up ads that ask for customers' information to be input directly into the pop-up. If you are interested in an offer, contact the retailer through their homepage, or by other legitimate contact methods. If you are unable to determine if the webpage is legitimate, call the business directly.
- Be observant. Scammers rely on deception to entice users to willingly comply. These types of scams can be difficult to identity; however, there are signs that indicate a phishing scam, including: poor spelling or grammar within the message, the use of threats or incredible offers intended to cloud a user's judgment.
- Ensure that all transactions are completed in a secured browser. Look for a lock icon depicted in the URL and for the website to display "https" instead of "http," as pictured on the right. Additionally, ensure that the URL provided matches the URL of the legitimate business website. Attackers cannot use the same URL associated with legitimate websites so they often spoof web addresses to look legitimate. Examples of this include using a different domain name (e.g., .com vs .net) or using variations of the spelling of the actual address. The latest versions of web browsers include features which point out whether the site you are visiting is legitimate or not.

- Be aware of email attachments and do not trust a file based on its extension. An attacker often uses a second extension to ensure the file looks like a regular PDF, but contains an executable file. Executable files have an .exe extension. To help identify double extensions, you can turn off the "hide extensions for known files" option on your operating system. The following websites provide instructions on disabling this option:
    - Windows users: http://support.microsoft.com/kb/865219
    - Mac users: https://support.apple.com/kb/PH10845?locale=en_US
- Be cautious when dealing with container files, such as .zip files. Any type or number of files can be packaged within these container files.
- Finally, make sure an up-to-date anti-virus software program is installed on your machine. Enable the anti-virus program to scan attachments before downloading and saving them to your computer.[1]

[1] McDowell, M. (2013, February 6). Security tip st04-014 – Avoiding social engineering and phishing attacks. *United States Computer Emergency Readiness Team.* Retrieved 03/12/2015 from https://www.us-cert.gov/ncas/tips/ST04-014.

[2] Cyber crime: A technical desk reference. (2013). *Center for Internet Security*. Retrieved 03/12/2015.

[3] DuPaul, N. (n.d.). Spooking attack: IP, dns & arp. *Veracode.* Retrieved 03/12/2015 http://www.veracode.com/security/spoofing-attack.

[4] AG: Phising scam targets apple users. (2015, February 23). *WTVA*. Retrieved 03/12/2015 from http://www.wtva.com/content/news/mississippi/story/AG-Phishing-scam-targets-Apple-users/EHbv8w0fkEKajNusfNf0Rg.cspx.

[5] Cassidy, K. (2002, February 8). The 419 scam, or why a nigerian prince wants to give you two million dollars. *Informit*. Retrieved 03/12/2015 from http://www.informit.com/articles/article.aspx?p=25269/.

[6] Example of a "phishing email." (n.d.). *Cornell University*. Retrieved 03/12/2015 from http://www.it.cornell.edu/security/phish.cfm?doc=591.

[7] Kitten, T. & Schwartz, M. (2014, December 24). Chase attackers exploited basic flaws. *Bank Info Security*. Retrieved 03/12/2015 from http://www.bankinfosecurity.com/chase-attackers-exploited-basic-flaws-a-7717.

[8] Tech support scam pop-ups. (2015, January 6). *The Safe Mac*. Retrieved 03/12/2015 from http://www.thesafemac.com/tech-support-scam-pop-ups/.