EMPLOYEE EDUCATION: SPEAR PHISHING, TROJANS, AND SOCIAL ENGINEERING

2012
TABLE OF CONTENTS

Why would a hacker target me at work? ................................................................. 3
What kind of data do these hackers want? ......................................................... 3
What is spear phishing? ................................................................................. 3
What is a Trojan? .......................................................................................... 3
What is social engineering? ......................................................................... 3
Risks to Using your Laptop Outside of the Corporate Network ..................... 4
Best Practices for Employees to Avoid Getting Scammed .............................. 4
   Always be suspicious of unknown people or e-mail addresses you do not recognize. 4
   Be Suspecting of unexpected phone calls at work ........................................ 4
   Be wary of links ....................................................................................... 5
   Be wary of pop-up messages to update your computer ............................... 5
   Limit the amount of personal information you share online ..................... 5
   Always trust your instinct ........................................................................ 5
   Be careful of the websites you visit .......................................................... 5
Additional Resources ..................................................................................... 6
EMPLOYEE EDUCATION: SPEAR PHISHING, TROJANS, AND SOCIAL ENGINEERING

As a company concerned with combating online fraud and identity fraud, RSA periodically publishes documents as an informative resource designed to help you recognize potential scams used by hackers to target you and your company.

WHY WOULD A HACKER TARGET ME AT WORK?

The answer is simple. They want a way into your company’s IT infrastructure. Depending on your role in your company, you may have access to critical systems and sensitive data. And hackers want to use you to gain unauthorized access to the same systems and data you can access.

WHAT KIND OF DATA DO THESE HACKERS WANT?

They are often interested in intellectual property, trade secrets, source code, financial data, product roadmaps and design documents, personnel records, customer databases and personally identifiable information (such as personal or financial information that can be used to commit identity theft).

WHAT IS SPEAR PHISHING?

Many of us are familiar with the term phishing and have likely received a phishing e-mail at a personal e-mail address. Phishing is a hacker’s way of attempting to manipulate users to divulge sensitive information, such as user names, passwords and credit card details, by masquerading as a trustworthy company, most often, a bank. Most phishing attacks that are launched target massive numbers of e-mail recipients at a single time.

Spear phishing uses the same techniques as a regular phishing attack. The difference is that a spear phishing attack is targeted at a specific company or an individual within a company and is done with the intent to gain unauthorized access to the corporate network to extract confidential data. Spear phishing uses fraudulent or hoax e-mails, embedded URL links or attachments that conceal Trojans and malware. According to an industry expert, more than 800 million spear phishing e-mails are sent daily – with those numbers continuing to rise.

If your company requires you to use a security token, a hacker may try to use spear phishing as a way to get information from you such as the user name and PIN or password you use in addition to your token passcode to log in to your corporate network or other information related to your token.

WHAT IS A TROJAN?

A Trojan is malicious software that can infect your computer and has the capability to record your online activities, capture the information you type and communications you send, and collect your personal data. You can get infected with a Trojan in a variety of ways, and many times, it is through seemingly innocent activities such as visiting an online news site or browsing to a social networking site. But more often, hackers are using spear phishing e-mails as a way to infect employees with a Trojan or some form of malicious software that enables them access to your computer and your company’s network.

WHAT IS SOCIAL ENGINEERING?

Social engineering is the practice of manipulating human emotions, interests or desires to obtain a specific response. Hackers use social engineering in most of their scams to get you to respond or disclose crucial information.

E-mail is one of the most important communication tools we use in the work environment. Hackers know this and design their schemes to work against you. This is where social engineering comes into play.
When using social engineering against employees, hackers craft e-mails to look like they came from someone you know, perhaps a person inside your company or from a business you are likely to trust. The e-mail often includes insider information or a piece of public knowledge in order to avoid raising your suspicion. Another common ruse is to craft an e-mail that comes from an internal department such as IT or finance that requires you to respond to an urgent request to update a program or account information.

Like a regular phishing attack, spear phishing e-mails usually contain a link for you to click on which could:

- Lead to a phishing website that may request certain information from you such as your corporate login credentials
- Download a Trojan onto your computer that is capable of capturing what you do and intercepting your work-related communications

While email is a common way by which attacker may attempt to contact employees, using the phone for the same purpose is just as prevalent. Using Facebook and LinkedIn, a social engineer has the capability to learn employee names, job descriptions, job specific terminology, etc., and may be able to talk someone into giving out information that is not available to the general public. Their goal is to pretend to be a fellow employee or a trusted outside authority. Cybercriminals can masquerade as anyone.

RISKS TO USING YOUR LAPTOP OUTSIDE OF THE CORPORATE NETWORK

Logging into your VPN or corporate webmail from a home office or other remote location using a laptop or other device issued by your company is a typical practice for today’s mobile workers. However, such activities pose additional security challenges. Many employees also use their work-issued laptop to conduct personal business and visit or browse non-business-related websites such as social networking sites. This leaves their corporate computer more prone to a Trojan or malware infection that has the potential to record access credentials, intercept e-mail communications and capture work-related activities.

BEST PRACTICES FOR EMPLOYEES TO AVOID GETTING SCAMMED

Always be suspicious of unknown people or e-mail addresses you do not recognize.

Anyone can be anyone else in the online world, and you must always be suspicious of people or e-mail addresses that you do not recognize. Keep in mind that a hacker targeting your company has likely researched you and other employees online and could have some of your personal information in their possession (and actually use that against you in order to get you to respond). Hackers are not usually after the employee personally; they are just using employees to gain access to a company’s systems and information.

Be suspecting of unexpected phone calls at work

How do you protect against social engineering in a phone conversation?

- Ask them for their name, company and phone number – in almost every case, the caller will disconnect when asked questions or put on hold.
- Call back – An attacker pretending to be an employee can spoof (masking or faking their name and number on the caller ID) a number from inside of EMC. Validate the call back number by searching EMC's corporate directory.
- Never, under any circumstances, give out your username and/or password.
It’s important to remember that no matter who you are and what position you hold with your company, you could be susceptible to a social engineering attack.

Be wary of links
Always use extra caution before clicking on any link contained in an e-mail. In the case of spear phishing, you are likely to be directed to a fake website that requests you provide sensitive information or other sites that will attempt to infect you with a Trojan.

Be wary of pop-up messages to update your computer.
Always be careful about accepting pop-up messages to update programs such as Flash, Java and Acrobat PDF Reader. You should perform these updates only when your computer system prompts you to update them.
You will usually see these types of update prompts when turning on or restarting your computer. You should never accept a prompt to perform these types of “updates” when it is suggested by a website you visit in order to view content such as a video.

Limit the amount of personal information you share online
The growth of social networking sites has made it easier for hackers to obtain information about you. This is a way for them to gather information about you or get inside your trusted network. Be wary of the people that may attempt to “friend” you or become part of your professional network on social networking sites.

Always trust your instinct
The goal of a hacker is to create fear, anxiety, or some other emotion in order to get you to respond immediately. Legitimate messages delivered by an internal department or someone you know will not elicit this type of response. Trust your instincts. If an e-mail doesn’t feel right, you should report your suspicions to your company’s IT department immediately.

Be careful of the websites you visit
Many companies have policies in place that block employees from browsing to certain websites while they are logged into the corporate network. Many of these policies are in place because of the dangers of the Internet and the risks to the corporate network. For example, consider that 20 percent of all cyber-attacks are targeted at users of social networking sites.
If you travel often or work from home or other remote locations on a regular basis, you likely use your work-issued laptop or mobile device to do so. In addition, you likely use it to conduct personal business and visit or browse non-business related sites. It is very important to be careful while surfing the web because even legitimate sites can be exploited by hackers to infect you with a Trojan.
ADDITIONAL RESOURCES

Can you detect a phishing attack or fake website? See how savvy you are about phishing and other scams. Play this educational game\(^1\) today:

www.wombatsecurity.com/antiphishing_phil/index.html

Get more information on the latest cyber threats. StaySafeOnline offers valuable tools and resources to empower businesses and their employees to protect company resources. Visit www.staysafeonline.org for more information.

The information set forth in this RSA Educational Bulletin is based on sources and analysis that RSA Security LLC believes are reliable. It is provided only for educational purposes and for the convenience of RSA’s customers and the general public.

The information contained herein is subject to change without notice, and is provide “AS IS” without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. Statements concerning financial, regulatory or legal matters should be understood to be general observations of RSA professionals and may not be relied upon as financial, regulatory or legal advice, which RSA is not authorized to provide. All such matters should be reviewed with appropriate qualified advisors in these areas. RSA reserves the right to notify law enforcement authorities and/or other relevant agencies regarding the information RSA uncovers in the course of doing business.

\(^1\) An RSA collaboration
ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

EMC®, EMC, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. ©2012 EMC Corporation. All rights reserved. Published in the USA.