The INFormer—Security Edition

Volume 1, Issue 3 October 1, 2013

INtegrity First Corporation

Phishing for Dollars—Law Firm Attacked

In the previous issue of the Security IN-Former, different types of hypothetical phishing and social engineering attacks were discussed in detail. In this issue, we will specifically discuss the Trojan Banker virus, which has hit at least ***two*** law firms to date and many other companies. The law firms wish to remain anonymous for the sake of their reputations.

How it Happened: The bookkeeper at the firm was reading emails and clicked on a link that was infected by a phishing scheme which installed the Trojan Banker virus. The virus protection on the bookkeeper's computer did not catch it and the Trojan Banker virus was installed on the bookkeeper's computer. The virus was then able to capture everything that was typed on the keyboard and then sent the information back to the hacker or hackers responsible for the phishing scheme.

Later that day, she went to the firm's trust account online, typing in the username and password to enter the site. This gave the hackers knowledge of the username and password for the law firm's trust account. Once they saw that she was in the account, they used social engineering tactics and called the law firm to speak with the bookkeeper, pretending to be someone from the bank. They told her that they noticed activity from the account, that something looked wrong, and that they could help her fix it if she supplied them with the more secure second password.

In the case of this trust account, a second password was required to make wire transfers. Because the bookkeeper did not know that they were not from the bank, she gave them the password and they told her that they would "fix" the account. Of course, there was nothing to fix. They used the second password, along with the knowledge of the first password and username, to transfer six figures from the account to an overseas bank. Because it was a trust account, the law firm itself immediately had to come up with the money to put back into the account. Additionally, they had to hire computer technicians to inspect their entire system to find and ***FIX*** the security breach.

Lessons Learned: Firstly, all security software should be up to date on your system because approximately 57,000 new malicious pieces of software are released weekly. Secondly, the virus would have been making her computer run fairly slowly. If you notice that your computer is running slowly, this *may* be a sign that something is wrong. Thirdly, when using services like online banking, disable any functionality that you do not use. Finally, if someone asks you for a password over the phone or email, ***NEVER*** give it out. There are other ways of verifying an identity and companies should not ask for passwords over the phone. These lessons and more are covered in INF's Secure-A-Day, a seminar that walks you through your day through the eyes of a hacker. ***Informed employees are a company's first line of defense against security breaches.***

Inside this issue:

Phishing for Dollars—Law Firm Attacked. 1

Secure-A-Day..... 2

Coulda, Woulda, Shoulda..... 2

Special points of interest:

- October is Cyber Security Awareness Month! Are you protected?
- Secure-A-Day is offered by INF to advise on security risks and comes with FREE Action Plans

INtegrity First Corporation

3633 Poplar Avenue
Pittsburgh, PA 15234

Phone: 412.563.2106
Fax: 412.563.6109
Email: info@integrityfirstins.biz
Web: www.integrityfirstins.biz

Secure-A-Day

Secure-A-Day is a virtual walk-through of your typical day through the eyes of a security professional in your own office environment. We review typical security exposures found in the office, while away at meetings, and at home. For more information on this class, visit: http://integrityfirstins.biz/Home/SecureADayDetails or email sivol@integrityfirstins.biz.

This class is offered by Stacey Ivol. Stacey has her Bachelor of Engineering degree from the University of South Carolina in Computer Engineering as well as her Masters of Science degree from Carnegie-Mellon University in Computer Engineering, with a focus on cryptography. She is the Vice President of the Privacy/Data Breach Unit for INF, Web Master for multiple companies and does security consulting for businesses.

October is Cyber Security Awareness Month!

Coulda, Woulda, Shoulda...Now I've Been Compromised

Most people look at a computer and think, "Why would anyone hack into that?" Hackers, however, think, "Why not?" It is a common belief that computer security only includes having updated virus protection, when it is so much more than that.

Your office should always have the proper physical protection via locks and alarm systems as well as key management. You can purchase a laptop lock or a desktop lock for under $30.00. This makes it more difficult for a grab-and-go thief to take off with your computer.

If your machine is stolen, there are a number of things that you can do to protect yourself preemptively. You can install a "poison pill" program that, when activated, will destroy all of the data on it the next time that it is connected to the internet. You could also encrypt your hard drive because there are commercially available programs that can crack your Windows password in less than two hours. In order to read any of the encrypted files, you have to have the hard drive password.

This leads into the importance of passwords. ***You should never use the same password for more than one account***. Please refer to the Security INFormer, Volume 1 Issue 1 for password creation tips (*http://integrityfirstins.biz/Content/Security-INFormer1-1.pdf*).

Keeping your computer physically safe is Step One of the process. Keeping it safe while connected to the internet is an entirely separate set of rules.

Your line of defense in this case will be virus protection, malware protection, and firewalls. Make sure your virus and malware protection updates daily and runs a full scan of your computer once a week. Update your software regularly on your computer. Do not ignore these weekly updates as some of them are security updates that fix a recently discovered exploit.

You can have the best security in the world, but if your employees do not use it, then it is moot. Educating your employees about the importance of security will go a long way in preventing your systems from being compromised. Make sure they know the ramifications to themselves and to the company if a data breach occurs. To protect your company, there should be a Computer Use Policy and a Security Policy that they must review on a regular basis.

In case of a data breach, you should have a plan in place to deal with it quickly and efficiently. The faster that you deal with a compromised system, the less time it has to balloon into a large problem and the less data you could possibly lose.

INF's Secure-A-Day Seminar offers **FREE** Data Breach Plans that will guide you through the process. It also offers FREE sample Computer Use and Security Policies that you can tailor to your company's needs.

I've been compromised, now what?

If, despite your best efforts, you have been compromised, you should notify the individuals that are affected via e-mail or regular mail. If the breach affects more than 1000 individuals, the nationwide credit reporting agencies should be notified. Depending upon the situation, state and federal law enforcement may need to be notified. If your business is located in Pennsylvania, you should consult Pennsylvania Statutes 73 § 43-2303 for more complete information.