Something Seems Phishy

How to prevent computer attacks and identity theft.

BY MARK BASSINGTHWAIGHTE

Some time ago, I was stunned by a discussion with a law firm that had almost been scammed into sending several hundred thousand dollars overseas. The incident involved what turned out to be a fraudulent check from a "client" and a request for the firm to transfer funds.

What floored me was the firm's response to the situation. As we talked about what had happened, the lawyers recognized that they were fortunate to have listened to their firm administrator's advice to not release any funds until the deposited check cleared. But even after the check bounced, they felt unable to do anything about it, or have the situation investigated, because of a perceived attorney-client relationship and the loyalties they believed flew from that. The scammers had invested enough time in becoming involved with the firm that, even after nearly being taken in, the lawyers felt that confidentiality trumped. Wow. Whoever was behind that scam knew what he or she was doing.

I wish I could say that this particular story was unusual—but I can't. In the years since, these types of scams have only become more frequent and sophisticated, and it all owes to social engineering.

The Psychological Manipulation

Social engineering, in the context of cybercrime, is about the non-technical aspects of the offense. It's the use of psychological manipulation to trick people into doing something that isn't in their best interests. The goal may be to obtain confidential information, steal personal identities or money, gain access to computer network resources—the list goes on.

These attackers have a number of methods at their disposal. If the goal is to transfer some rogue software to your computer network, perhaps they leave a flash drive in the parking lot or send a free digital music player to a "lucky winner," who happens to be a member of your staff. Of course, once the device is connected—in an attempt to see what's on the flash drive or to start enjoying that unexpected prize—your network is compromised. This type of attack is called baiting.

Other methods include, but are by no means limited to, fake callbacks from technical support, where the attacker randomly calls numbers at a business until someone falls prey; pretexting, where the scammer impersonates a bank employee, tax authority, insurance investigator, or the like to trick someone into disclosing information; and phishing, which is something we all need to know more about because of the high number of attacks.

Phishing Basics

Phishing is the criminal attempt to

TECHGEAR

The Nokia Lumia Icon (from $199.99 with contract) features a 2.2 GHz quad-core processor, 2 GB RAM, and 32 GB of storage. The Windows phone has four high-performance microphones to minimize background noise, a full HD 1080-pixel display, and a 20-mega-pixel camera with optical image stabilization.

WEBLINKS

DAVID GAIR is a board certified tax attorney in Dallas. Gair focuses on tax matters and tax litigation in the United States Tax Court, U.S. Court of Federal Claims, U.S. bankruptcy courts, and U.S. district courts, including representation in complex international and domestic civil and criminal matters. He covers tax issues on his blog, texastaxtalk.com.

flipboard.com
I am a news junkie, so one of my favorite apps is Flipboard, which takes content from popular news websites and my own RSS feeds and presents it in an easy-to-navigate magazine format. It is convenient to have a single location where I can read various blogs.

federaltaxcrimes.blogspot.com
Jack Townsend does a great job of presenting current criminal tax issues. This blog is written principally for tax professionals and tax students and offers lots of practical advice.

txsaltlaw.com
This is a great state and local tax law blog with insight and commentary on developments in Texas.

dontmesswithtaxes.typepad.com
This blog is written by a professional journalist and self-proclaimed "tax geek." Articles are rich with practical content and also humor and entertainment.

forbes.com/taxes
Forbes is a valuable news source, with articles that include good legal information. The magazine recruits professionals from across the country to opine on tax matters.

trick another person into providing personal or sensitive information—such as a birth date, address, credit card number, username, or account password—by requesting a response to an email or text message. Many of us have a sense of this general approach and would delete an email that says our bank account will be closed unless we open the attachment, or unless we click on some link to verify our login credentials, simply because the email obviously didn't come from our bank. But what if the email does purport to be from the correct bank, replicates the look of the bank's website, and features all the correct, official logos? What if, instead of asking you to verify login credentials online, the email instructs you to call a number and an automated system then asks for your credentials?

Phishing attacks have become very sophisticated. Not only are the above examples real, there are many other approaches out there. I personally have received an email supposedly from a close friend, stating that he had his wallet stolen, was stuck in London, and was hoping I would wire some money to help him return to the States. I have received an email that claimed to be from Microsoft, informing me about a serious security problem in its software and advising that I immediately click a link to download the necessary update so that I would remain secure. Honestly, I almost fell for that last one; the email's level of ingenuity was that good.

In truth, the possible variations on phishing attacks seem to be limited only by the imagination and programming skills of the criminals behind them. Unfortunately, we'll keep seeing these attacks, and they'll continue to evolve, because they work.

Training and Other Prevention Tips

Hopefully, you now have a sense of how ugly the situation has become. The upshot is that it's time to get in front of the problem because no one else is going to take care of it for you. It simply isn't possible for your IT support to protect your systems from all phishing attacks because the attacks are directed not at hardware but at the people who use your systems—including you.

The good news is there are a few things all of us can do to protect our personal information—as well as our client confidences—and it begins with training. Everyone in your firm should be made aware of the nature of phishing attacks and learn how to spot them. You can use online resources as training tools, such as the Microsoft Safety & Security Center (microsoft.com/security), Wikipedia, and TechRepublic.com. If you have in-house IT, ask them to provide a seminar on phishing and other online hazards.

In addition, here are other precautionary steps:

- Keep all software updated with critical security patches as they become available.

- Use reputable antivirus tools as well as spyware identification and removal tools on all computers that are part of the office network—and don't overlook remote and mobile computers such as home computers, personal laptops, and computer tablets.

- Check with your IT staff or consultant to see if you are running the most current version of your Internet browser. If your browser has anti-phishing capabilities built in, make certain this functionality is enabled on all devices that are on the network or that log in to the network remotely.

That said, the most important piece of advice is to remember that no matter how sophisticated your security systems and tools are, the user will always remain vulnerable. Awareness and training will continue to be key and should occur on a semiannual basis to keep the issue front and center. Everyone in your firm needs to be on the lookout for phishing emails or text messages because law organizations have a significant amount of valuable data on their computer systems that scammers want.

Yes, lawyers can be a trusting bunch; but as I shared at the beginning of this article, that attribute doesn't always serve us well. **TBJ**

MARK BASSINGTHWAIGHTE *is risk manager for ALPS Property & Casualty Insurance Company, a provider of Lawyers' Professional Liability Insurance. He conducts law firm risk management assessment visits, presents CLE seminars, and writes extensively on risk management and technology topics. Bassingthwaighte received his J.D. from Drake University Law School. Contact him at mbass@alpsnet.com.*

This article originally appeared on attorneyatwork.com and is reprinted with permission of the author.