nLightened Thoughts

August 2012

William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

Spear Phishing: The Same Old Threat at a New Level

The message appeared to come from the IT department at Jeff's company. The IT manager, whose office is in a distant state, said that a security problem had been detected on the corporate LAN. The problem had been resolved but all users should follow the attached link to a security partner's website to confirm that their computer had not been infected. What should Jeff do?

Better yet, what would you do?

The message could be legitimate or it might be a "spear phishing" attempt. You're probably familiar with "phishing", the process of sending broadcast spams that seek to acquire information that cyber-criminals can use. Spear phishing is the smarter, more concentrated method.

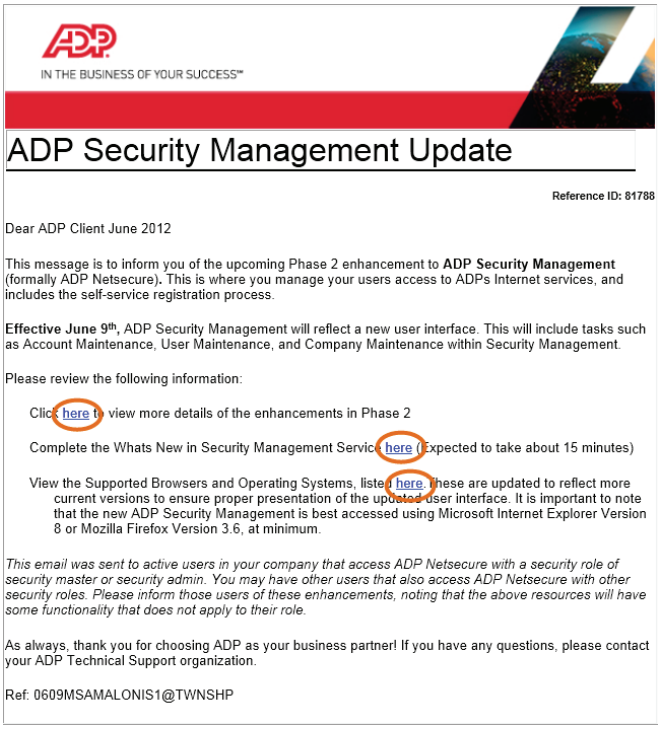
Routine phishing messages are sent to hundreds of thousands of people. As a result, I might receive a phishing message that claims to come from the Bank of America even though I've never had a BoA account. Over the years, the crooks have gotten better by picking small, local banks and sending messages to limited geographic areas.

The messages typically include graphics stolen from legitimate messages and, in recent years, the text has begun to look more like something that a reasonably intelligent native speaker of American English would write. But there's always a flaw that exposes the ruse for what it is: The message or the website that the victim is directed to will always ask for information that the sender will already have.

Spear phishing takes the threat to a new level. Customers of a telecommunications firm might receive an e-mail that says there was a problem with a recent order or a bill payment. To remedy the problem, they should visit company's website

The Legitimate Appearance of Spear Phishing

ADP is a company with some 50 thousand employees worldwide and handles payroll checks for millions of people. This message not only includes the ADP logo (conveniently linked from an ADP website) but it also looks and feels like a corporate communication.



ADP
IN THE BUSINESS OF YOUR SUCCESS℠

ADP Security Management Update

Reference ID: 81788

Dear ADP Client June 2012

This message is to inform you of the upcoming Phase 2 enhancement to **ADP Security Management** (formally ADP Netsecure). This is where you manage your users access to ADPs Internet services, and includes the self-service registration process.

Effective June 9th, ADP Security Management will reflect a new user interface. This will include tasks such as Account Maintenance, User Maintenance, and Company Maintenance within Security Management.

Please review the following information:

Click here to view more details of the enhancements in Phase 2

Complete the Whats New in Security Management Service here (Expected to take about 15 minutes)

View the Supported Browsers and Operating Systems, listed here. These are updated to reflect more current versions to ensure proper presentation of the updated user interface. It is important to note that the new ADP Security Management is best accessed using Microsoft Internet Explorer Version 8 or Mozilla Firefox Version 3.6, at minimum.

This email was sent to active users in your company that access ADP Netsecure with a security role of security master or security admin. You may have other users that also access ADP Netsecure with other security roles. Please inform those users of these enhancements, noting that the above resources will have some functionality that does not apply to their role.

As always, thank you for choosing ADP as your business partner! If you have any questions, please contact your ADP Technical Support organization.

Ref: 0609MSAMALONIS1@TWNSHP

The message is plausible in that it describes security updates that are planned and simply asks the recipient to read more about the service and then view a 15-minute program. All of these are typical requests but hovering a mouse over any of the links would reveal that they do not point to ADP websites.

Following any of the links would almost certainly result in what's called a "drive-by" malware attack but the site had been taken down before I could investigate.

Never follow a suspect link with a browser! There are ways to view the raw HTML and any other code that the site will serve. Let me know if you'd like to learn how to do this. The procedure involves using Microsoft PowerShell (installed on any Vista or Windows 7 computer and available for XP) in conjunction with a text editor.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.859.9359. On the Web at www.n-Lighten.us.

("just click this link") and respond to a few questions.

In this case, the crooks target people who have accounts with a specific cell phone company. In Jeff's case, criminals might be directing an attack at users within a specific company. The fraudulent message might not be sent to everyone. Instead, the crooks might be engaged in corporate espionage so they could be looking only for mid-level managers and above who might reasonably have accounts that would give them access to the company's proprietary information.

The FBI explains it this way: "Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, [or] order merchandise from the same website. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive."

Obtaining information the crooks can exploit is easier than you might think. Possibly they have cracked a social media site where the company's employees hang out. Or they've sifted through your public website to scrape names and e-mail addresses from the code.

When they have the information they need, the crooks send e-mails that appear legitimate to targeted victims. The message may sound urgent and legitimate so a certain number of busy employees will simply respond to the message or click the link without even thinking about the possible dangers.

Once on a phony but realistic-looking website, they will be asked to provide passwords, account numbers, user IDs, access codes, PINs, and whatever else the crooks think they can exploit.

The FBI cautions that spear phishing can also trick you into downloading malicious code or malware after you click on a link embedded in the e-mail. This is an especially useful tool in crimes like economic espionage where sensitive internal communications can be accessed and trade secrets stolen. Malware can also hijack your computer and make it part of a malevolent network that is used to send spam, house stolen software, or participate in distributed denial of service attacks.

So What Should Jeff Do?

Common sense is the best defense. Most companies, banks, and agencies, don't request personal information via e-mail.

Instead of clicking the link, pick up your phone and call the sender. Use your corporate directory, though, instead of any phone number provided in the e-mail. Those are usually just as phony as the e-mail and the website.

And never follow a link from an e-mail that warns about a security problem. Security experts will never include links. Instead, they will depend on you to know how to navigate to the bank or corporate website. Keep in mind that even legitimate-looking links might actually be frauds.

Phone Phishing

Threats can arrive by telephone, too. If you use Skype, you've probably seen "Urgent" messages that appear to come from Skype. They don't, of course, and typing the URL that the recorded message provides will lead you to a site that dispenses malware.

But a phisher might also pose as a support-team member at your ISP and send an instant message that asks for your password. You'll be told that they simply need to "verify your account" or maybe that they want to "confirm your billing information."

Once you've provided the information the thief needs, he can access your account for fraudulent purposes or spamming.

It's possible to avoid (or at least mitigate) phishing attempts by changing your browsing habits. If you receive a message that says your account needs to be "verified", simply contact the company from which the e-mail apparently originates to check that the e-mail is legitimate. Do this without using any of the contact information provided in the message.

Nearly all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to phishers. PayPal, for example, will always address you by name and not as "Dear Customer". The name PayPal uses will be the exact name that you provided when you signed up for the service.

E-mails from banks and credit card companies often include partial account numbers and thieves have figured out that many consumers don't understand the difference between the first 4 number of the account (which identify a bank) and the final 4 digits (which identify an individual). If the message calls out your credit card that begins with 4640, it's a fraud. All Visa numbers begin with 4 and 4640 identifies Chase Bank. Hundreds of thousands of people who have Amazon Visa cards will have numbers that begin with 4640.

So before Jeff does anything (or before you do anything) it's important to confirm that the request is legitimate and the only way to do that is to contact the sender using a method that has not been disclosed in the e-mail.

Be a smark fish and don't take the bait! Ω

Fast Forward

Kansas City is about to expereience the future of the Internet.

Google will use Kansas city to show what's possible by going around local cable and phone companies to provide $70-per-month gigabit Internet service using its own optical fiber in the "Fiber for Communities" broadband service.

Gigabit. 1000 megabits per second. Compare that to typical "high-speed" connection (10 Mbps in the US). A download that currently takes 5 minutes would take no more than 30 seconds.

Google is doing this to show how faster Internet service can be used. Verizon has a similar, but much slower, program. The Verizon FiOS (fiber optic) connections are available in several cities, including some parts of Manhattan, but the speed is only 15 Mbps and Verizon has stopped expanding the network because it hasn't proved to be popular with consumers. Ω