Spear Phishing

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity and respect

In the "Land of 10,000 Lakes," everybody knows what "fishing" is, and many people are also familiar with "phishing" scams. "Phishing" occurs when a criminal sends an email impersonating a financial institution, government agency, or reputable company and asks the recipient to verify his or her personal or financial information. Today's scam artists have now turned to a more sophisticated, targeted, and profitable version of the scam, known as "spear phishing."

History of "Spear Phishing"

Phishing scams have existed in one form or another since the late 1980s. Decades after the scam first appeared, people are more suspicious of questionable emails from unknown senders. Spam filters often help prevent these emails from ever reaching the intended recipient's inbox. As a result, scammers are increasingly targeting people and businesses with spear phishing scams. While "phishing" emails may be sent to thousands of people, "spear phishing" emails are much more selective.

It Happens Like This

"Chris" received an email that appeared to come from his company's human resources department. The representative asked Chris to send information from his W-2 form to her for tax purposes. Chris noticed that the tone of the email was different from other emails he had received from the human resources department and thought it was strange that the representative did not already have his W-2 information. He called the representative directly to ask about the email. When she told him she did not send the email, Chris looked more closely at the sender's email address and realized that it differed slightly from his company's email format. Chris reported the email to the company's computer specialist and the criminal authorities.

How It Works

Spear phishing occurs when a scammer poses as a company representative, often an executive or human resources representative. The scammer sends an email to an employee at the company, often from a hacked or "spoofed" email address or an address that closely resembles the company's email format. For example, if a company's email format is user@321company.com, a scammer might use user@321company.net, or user@321compny.com.

Sometimes the scam artist asks employees to provide personal information, such as Social Security numbers, tax documents, or account passwords. Other times, the scam artist asks the employee to send a wire transfer to another person or deposit a certain amount of money into an outside bank account. The scammer often creates a sense of urgency so that the employee will send the requested information or money before he or she has time to verify the legitimacy of the request.

Spear phishing is often more profitable than a basic phishing scam. First, scammers research a company to convincingly impersonate the target's boss or co-worker. People are more likely to be victimized because the email appears to come from a trusted source. Second, spear phishers may use the information they obtain to steal the identities of every employee at a business and file thousands of fake tax returns. By filing fake tax returns or selling private information to other criminals, spear phishers can make a lot of money very quickly, even if only one person falls for the scam.

Protect Yourself from Spear Phishing Attacks

The use of spear phishing attacks to steal personal information and money remains a widespread problem. There are several steps you can take to help protect yourself—and your co-workers—from spear phishing attacks, including:

Verify the email with the sender.

Call the sender directly and ask about the email. Scammers prey on people's desire to respond quickly to requests from their boss or supervisor. Taking the time to verify the email could save you and others much more time and money down the road.

Read suspicious emails carefully.

People often recognize that an email is a scam when words are spelled incorrectly or there are grammatical mistakes. Sometimes a scam email is written in a tone that is different from the one the sender usually uses, or the sender might use a different version of your name—for example, an email is addressed to "Thomas," but everyone calls you "Tom." If something seems off, verify that the email is legitimate before responding.

Check the "from" email address.

Make sure that the "from" email address matches your company's email address format. Many email programs automatically display only the name of the person sending the email, rather than the full email address. Before you send sensitive information in an email, make sure you are not sending the information to an outside email account where it is no longer secure. If the address matches your company's email format —or even the sender's real email address—you should still verify suspicious emails directly with the sender. Some scam artists hack email accounts or use technology to "spoof" their email address to make the emails look like they are coming from a legitimate source.

Guard personal information carefully.

There are often safer ways to relay sensitive information than in an email. Check with your company about its security policies.

Contact your company's technology department.

Many companies have security protocols that protect the information in their systems from attack. It can be best to refrain from "clicking" on a link or downloading an attachment in suspicious emails, as doing so could jeopardize your company's computer system. Many email programs allow users to forward emails without opening them. You may wish to ask your computer's technology department about how to safely forward any suspicious emails you receive to a specialist.

Be vigilant on the go.

Company-issued laptops and smart phones may also be vulnerable to attack. Smart phones in particular may be subject to spear phishing text messages, which can cause as much damage as an email can. Don't feel rushed by strange requests that come while you are out of the office.

Reporting Spear Phishing Attacks

You may report Internet fraud to the Federal Bureau of Investigation's Internet Crime Complaint Center online at *www.ic3.gov* or to the following agencies:

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
(763) 569-8000
www.ic3.gov

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, D.C. 20580
(877) 382-4357
TTY: (866) 653-4261
www.ftccomplaintassistant.gov