nachman NETWORKS

PHISHING
AND SPEAR PHISHING SCAMS

Don't Get Caught In Their Nets

What is Phishing?

Phishing is tech language for fishing over the Internet for confidential business and personal information such as credit card numbers, personal identification, usernames and passwords. The first phishing scam occurred in 1996.

It uses social engineering techniques and computer programming to lure email recipients and Internet users into believing that a fraudulent website is legitimate. When the phishing victim clicks the phishing link, they find that their personal identity vital information, and even money have been stolen.

What's the Difference Between Phishing and Spear Phishing?

Phishing emails are sent to the general public. They often impersonate a government agency, bank, the IRS, social networking site or store like Amazon.

Spear Phishing emails target specific individuals. They are personalized with facts about you or your business to draw you in. And they appear to come from a company or person you do business with. It could come in the form of an email from your CEO.

A PHISHING OR SPEAR PHISHING EMAIL:

- Is one that you didn't initiate
- May contain strange URLs and email addresses
- Often uses improper grammar and misspellings
- Typically contains attachments that you don't recognize as legitimate
- Contains a link or email address that you don't recognize
- May use language that is urgent or threatening

PHISHING AND SPEAR PHISHING ARE POPULAR AMONG CYBERCRIMINALS BECAUSE THEY USUALLY SUCCEED.

10 messages have a better than:

- 90% chance of getting a click
- 8% chance of users clicking on an attachment
- 8% chance users will fill out a web form
- 18% chance that users will click a malicious link in an email

Even high-level executives get spoofed and share usernames and passwords.

THE AVERAGE COST OF A PHISHING SCAM IS $1.6 MILLION. IT'S A TOP SECURITY CONCERN FOR BUSINESSES TODAY:

- 1 in 3 companies are affected
- 30% of Phishing emails get opened
- Phishing is now the #1 vehicle for ransomware and other forms of malware

PREVENT BEING A VICTIM OF PHISHING OR SPEAR PHISHING.

Here are 8 important things to remember:

1. Stay informed about phishing techniques.

Different phishing scams are being sent out every day. Ongoing security awareness training should be a top priority for your organization. Contact Nachman Networks at (703) 600-3301 or sales@nachnet.com. We can help.

2. Think before you click a link.

Don't click on links from random emails or text messages. Hover your mouse arrow over a link to see who sent it. Most phishing emails begin with "Dear Customer" so watch out for these. Verify the website's phone number before placing any calls. Remember, secure website always starts with "https."

3. Never divulge personal information requested by email, such as your name or credit card number.

Typically, phishing emails will direct you to a webpage to enter your financial or personal information. When in doubt, visit the main website of the company in the email, and give them a call. And, never send sensitive information in an email to anyone. (A secure website always starts with "https".)

4. Consider installing an anti-phishing toolbar and security tools.

Some Internet browsers offer free, anti-phishing toolbars that can run quick checks on the sites you visit. If a malicious site shows up, the toolbar will alert you. Be sure to ask Nachman Networks about updated computer security tools, such as anti-virus software, spyware and firewalls. They will drastically reduce the chances of hackers and phishers infiltrating your computer or your network.

5. Never download files from suspicious emails or websites.

Double check the website URL for legitimacy by typing the actual address into your Web browser. Check the site's security certificate. Also, beware of pop-ups as they may be phishing attempts. Your browser settings allow you to block pop-ups, where you can allow them on a case-by-case basis. If one gets through, don't click on the "cancel" button as this is a ploy to lead you to a phishing site. Click the small "x" in the upper corner of the window, instead.

6. Get into the habit of changing your passwords often.

You can also use a password manager like Dashlane or Last Pass that will automatically insert new, hard-to-crack passwords for you.

7. Regularly check your online bank and credit card accounts.

To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

8. Update your browsers to the latest version.

Security patches are released in response to the vulnerabilities that phishers and hackers exploit. Don't ignore messages to update your browsers, and download the updates as soon as they're available.

Protect your confidential information and your business.

Nachman Networks will train you and your staff to recognize and block Phishing and Spear Phishing Scams. Contact us at (703) 600-3301 or sales@nachnet.com.