Cyber Liability

Spear Phishing

"Phishing," a type of cyberattack in which a hacker disguises him- or herself as a trusted source online in order to acquire sensitive information, is a common and technologically simple scam that can put your employees and business at risk. However, more resourceful criminals are resorting to a modified and more sophisticated technique called "spear phishing," in which they use personal information to pose as colleagues or other sources specific to individuals or businesses.

A spear phishing attack is often disguised as a message from a close friend or business partner and is more convincing than a normal phishing attempt; when messages contain personal information, they are much more difficult to identify as malicious.

For businesses, the potential risk of spear phishing is monumental. A report released by the Internet Crime Complaint Center (IC3) stated that there were over 120,000 cybercrime-related complaints against businesses last year, resulting in over $800 million lost. A large majority of these attacks can be attributed to spear phishing, since the messages are designed and customized to make victims feel safe and secure.

The Basics of Spear Phishing

Any personal information that is posted online can potentially be used as bait in a spear phishing attack. The more a criminal learns about a potential victim, the more trustworthy he or she will seem during an attack. Once the apparent source gains the victim's trust, and there is information within the message that supports the message's validity, the hacker will usually make a reasonable request, such as following a URL link, supplying usernames and/or passwords, or opening an attachment.

Even if spear phishing perpetrators target just one of your employees, it can put your entire business at risk. Falling for a spear phishing attack can give a hacker access to personal and financial information across an entire network. And, successful spear phishing attacks oftentimes go unnoticed, which increases the risk of large and continued losses.

How to Protect Your Business

Though it is difficult to completely avoid the risk that spear phishing attacks pose, there are ways to prevent further damage to your business. Make sure that your employees are aware of these simple techniques:

- Never send financial or personal information electronically, even if you know the recipient well. It may be possible for a third party to intercept this information, especially if the recipient is later subject to a spear phishing attack.
- Be cautious when you are asked to divulge personal information in an email. Even if it appears to be from a trusted source, it could be a hacker impersonating another person or group.
- Only share personal information on secure websites or over the phone. When in a Web browser, you can ensure a website is secure when you see a lock icon in the URL bar, or when an "s" is present in the "https" of a URL. The "s" stands for "secure" at the end of the normal "http".
- Some spear-phishing schemes use telephone numbers, so be sure to never share information over the phone unless you initiate the call to a trusted number.
- Never click on links or open attachments from unknown sources. Even opening a file that seems familiar can give a spear phishing attacker access to personal information stored on your device.
- Ensure that your company's security software is up to date. Firewalls and anti-virus software can help protect against spear phishing attacks.
- Encourage employees to think twice about what they post online. Spear phishing hackers often attain personal information through social media sites. Make sure that employees know how to keep this information private to protect their own security as well as that of your business.
- Regularly check all online accounts and bank statements to ensure that no one has accessed them without authorization.
- Never enter any personal or financial information into a pop-up window or a Web browser.

What to Do If You Suspect a Spear Phishing Attack

If you believe that your business has been the target of a spear phishing attack, it is important to act quickly to limit your potential losses. The first step should be to immediately change the passwords of any accounts connected to the personal or financial information of your business or its clients, and to obtain a list of recent and pending transactions. It may also be necessary to contact law enforcement.

Next, an internal or third-party IT expert should consulted to pinpoint any vulnerabilities that remain in your business' network, and he or she can advise you on how to avoid future attacks.

If you have further questions about spear phishing or other types of cyberattacks, or if you would like to discuss potential coverage options to further protect your business, contact Medical Society of Virginia Insurance Agency today.