Vol. 15 No. 8
August 2023

BUSINESS*insights*

What is Phishing? Identifying and Protecting Your Business from Phishing Attacks

For most businesses, email is a convenient and effective communication tool inside and outside of their organization. Unfortunately, it is also the primary avenue used by scammers for phishing attacks. Cybercriminals use emails to distribute malware, phishing, and other attacks designed to defraud individuals and corporations. Phishing attacks use a combination of email and fictitious websites to fool users into disclosing sensitive information. With many employees working from home, attackers have gained an advantage. To protect yourself and your business from these scams, it is critical to understand what they are and how to avoid them.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, credit card details, and other pertinent personal information. These messages usually appear as if the user is receiving a legitimate email or phone call from a trusted entity, such as a bank or someone in their company, and typically directs them to click a link, download an attachment, or provide financial information over the phone.

The are many different types of phishing schemes. Understanding and educating your employees about these schemes is key to protecting your business from falling victim to them.

Spear Phishing

Spelling mistakes and poor grammar used to be the tell-tale sign of a phishing attempt. Over the years, phishing has evolved into a much more sophisticated cyber-crime as scammers began to use targeted phishing schemes. Spear phishing targets specific individuals and it’s often difficult to distinguish these emails from legitimate messages, which is part of the reason these cyber scams are so successful.

Before the scammer sends you any communication, they already know some of your personal information. They’ve researched and learned about your business to pose as someone you do business with, or they’ve monitored your social media for tidbits about your life, i.e. did you post on social media about that big purchase you just made? Once armed with this information, they can craft a carefully worded message that will seem very believable to its targeted recipient.

IDeACOM® NETWORK

P.O. Box 1336
Blue Ridge, GA 30513
1-866-IDEACOM (433-2266)
www.ideacom.org

Whaling

Whaling, or CEO Phishing, is another form of phishing that targets high-level executives and managers. The attackers, in this case, are looking to gain access to their target's email account. Once they've gained access, their possibilities are limitless. They can access personnel files, initiate wire transfers, or gain access to any other information they'd like.

Pharming

Pharming is a type of cyber-attack that involves manipulating the domain name system (DNS) to redirect users to fraudulent websites without their knowledge or consent. Unlike phishing, which relies on social engineering techniques to trick individuals into revealing sensitive information, pharming takes advantage of DNS vulnerabilities to automatically reroute users to malicious websites, even if they enter the correct website address (URL) in their web browser.

Ransomware Phishing

A ransomware phishing attack will typically be an email that appears to be coming from someone known to the recipient asking them to click on a link or open a file. Once the link is clicked or the file is opened, ransomware is loaded. The file may even appear to be legitimate - maybe it has the company logo – so the target may not realize what has happened until the attacker has locked all files and sent a ransom demand.

Vishing

Phishing is not just limited to email messages. Just as people use email and other technologies for criminal purposes, they've also found a way to use your VoIP phone systems to scam businesses and consumers by faking Caller ID.

A typical vishing scam involves using VoIP with a modem to call phone numbers in a given area. When a person answers the phone, an automated recording states that the person's credit card is showing fraudulent activity. The person is directed to call a specific toll-free or local phone number immediately. The number dialed may show a spoofed caller ID for the financial company the scammer is pretending to represent. When the call is made, the recording on the other line asks you to enter your credit card number and three-digit code, which is exactly what the scammers are after.

Smishing

Smishing is also done over the phone using text messaging. Scammers use text messages to try and trick people into giving them personal and financial information via text message by posing as a bank or credit card company. Often times there is a link to click on or a phone number they are asking you to call where they will try and obtain the information they are after.

Protect Yourself and Your Organization. There are many steps you can take to prevent or reduce the risks associated with phishing attacks:

1. **Educate your employees.** Implement security awareness training and teach your employees how to recognize phishing attacks.
   - If you spot a spelling error or poor grammar, it is very likely the message you received was not sent by the organization it claims to be from.
   - Think before you click. Before you download an attachment, always stop to evaluate whether it is from a legitimate sender. It is easy to make an email appear as if it came from your bank or other financial institutions. Check the actual email address of the sender to be sure they are whom they say they are.
   - If a call appears to be from a bank, credit card company, or other official business and requests financial information, end the call. Look up the official number of that business and call them back on that number. Never provide company credit card or other financial information over the phone unless you are already acquainted with the representative calling.

2. **Filter your email.** Most email security solutions include spam and virus filters. Anti-phishing protection solutions should check for domain spoofing and be able to flag questionable content.

3. **Frequent backups.** Because most phishing emails contain some sort of ransomware, it is important to keep your system consistently backed up. This will allow you to get employees back to work quickly by getting them access to the latest versions of their uninfected files.

4. **Keep software up-to-date.** Regularly updating your operating system and security software helps to fix security vulnerabilities being taken advantage of by hackers. A virus can spread across your network using gaps in security caused by out-of-date software.

5. **Encourage reporting.** Promote a culture where employees feel comfortable reporting suspicious emails or incidents promptly.

Investing in technology and training your employees will considerably reduce your risk and the impact a cyber-attack could have on your business. Contact your Ideacom Network provider to learn more about the options available to protect your business and help you stay better prepared.

IDEACOM® NETWORK
P.O. Box 1336
Blue Ridge, GA 30513
1-866-IDEACOM (433-2266)
www.ideacom.org