YOUR BIGGEST SECURITY THREAT!

By Scott Guinther, I.T. Shield, LLC, Member, Small Business Resource Association

Most business owners today know they need IT security to keep their businesses safe. Antivirus/malware protection and firewalls are the basic security measures used by most businesses today. But with these necessary and valuable security measures, none of these can prevent the biggest threat to your company — Your People!

Phishing has become the easiest way for malicious individuals to gain access to your organization's data/information. Phishing is a deceptive practice to get someone in your organization to reveal confidential or personal information. There are multiple methods used to gather this information.

Phishing, in general, is the mass method of gathering information. When phishing takes place, you (and hundreds or thousands of other users) receive an email stating your account has been compromised. There is a link in the email that you are to click on immediately to correct the issue, so you do not lose any of your data. You click on the link, are directed to a website that looks legitimate and you are prompted to enter your user name and password. A lot of the time nothing happens that you can see. However, the perpetrator has already gotten the information he needs — your username and password. Hoping that you use the same username and password to log on to other sites, the perpetrator keeps trying to access sites (mostly financial) to see if the same username/password combination works.

This general phishing attack is the main method used by hackers. They also use something called Spear phishing — a targeted attack to an individual or organization using information specific to a person or company. Clone phishing is also a popular method of hacking during which an email is cloned and malicious links are added or changed before the cloned email is sent back to the senders/recipients. There is also Phone phishing, where the "target" receives a phone call from someone posing as a representative of a company (Dell, Microsoft, ATT, etc.) stating there is an issue with their account, computer or software. The goal is to get the target to reveal information (usually credit card information or username/password), but it may not be credit card information only.

YOUR BIGGEST SECURITY THREAT!

(Continued from page 55)

Calls have been placed to companies to find out the whereabouts of executives (on vacation, at a meeting, etc.). Once they have this information, they call back asking for a certain person (gathered from corporate directories) and impersonate the executive to have the victim send or give confidential information. Phone phishing can also be done using text messaging.

The size of a business is not a safe guard. According to Jeff Bardin, chief intelligence officer of cyber risk consulting firm Treadstone71, "[Forty] percent of cyberattacks are aimed at companies with 500 employees or less."[1]

How do you stop these types of attacks? Education. Companies need to train their people on how to recognize an email or a phone call that is malicious. This training needs to be done on an on-going basis as hacking methods keep evolving. I.T. Shield LLC has a program available to businesses in which test phishing emails are sent to employees. Employees can then report back indicating if the email is a phishing scam or not. It is then recorded if the user opened the email and if they clicked on any links in the email. As they report back, the user is scored on the accuracy of the user's assessment of the emails. As time goes on, the user should learn to quickly spot a phishing attack and respond correctly.

Education is the only way to combat this malicious attack on your people and organization. According to the 2018 Hiscox Small Business Cyber Risk Report[2] "Small businesses estimated their average cost for incidents in the last 12 months to be $34,604". This could be devastating for a small business. In the same 2018 Hiscox report they state "65 percent of small businesses fail to act following a cyber security incident".

I.T. Shield LLC believes that prevention is better than correction. We ask that you speak with the person or organization that handles your I.T. Security to see what methods they use to train your employees on identifying phishing threats or any other malicious attacks on your organization.

1 Debunking the 3 Cyber Risk Myths for Small and Medium-Sized Businesses - https://www.insurancejournal.com/magazines/mag-ideaexchange/2018/05/21/489533.htm

2 https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf