withum

AUDIT TAX ADVISORY

# 8 TIPS TO BECOMING CYBER SECURE

**With the ever changing technologies of today, data breaches and cybersecurity are at the forefront of our minds, and rightfully so. The number of successful cyberattacks in the U.S. has grown 144% in the past four years. Attacks are happening daily, with 62% of these attacks targeting small to midsized businesses.**

Do you have a data security policy in place? If you answered yes, you're among the 36% of SMBs that have a data security policy in place. If you answered no, you're at risk of losing a lot should a breach or attack happen. Breaches are costly, impacting revenues, your reputation and branding, and your valued clients.

So what are some quick tips you can do to start protecting you and your organization?

## TIP 1 Create complex passwords that are east to remember

Sure, you've heard this before – make your passwords complex and use a different one for every website and application. The longer and more complex the password, the more difficult it is to hack. Choose something that is easy to remember, like your favorite song lyric, so that you won't easily forget it.
Suggestions: Take the first letter from each word of that song lyric to get 8-9 letters for your password. Then add a number and special character to it.
Interested in testing how secure your passwords really are? Go to howsecureismypassword.net and test it out! But wait; don't try your actual password. Use one that is of a similar length and nature. Giving your actual password out to a third party website, just to test its strength... not a good idea!

## TIP 2 Think before you click

Don't fall for a "phishing attack". Never click a link or open an attachment that you did not expect to receive. Scams today look very convincing, coming in the form of voicemails, eFaxes, invoices, social media, ADP theme, or from the IRS. If you're not expecting something or have to think twice about the contents, don't open it. If you do, you're opening hackers to the contents of your computer. Contact your IT department if you think an email is suspect, or just delete it and report it as SPAM.

## TIP 3 Prevent email fraud

Since January 2015, there has been a 270% increase in email fraud instances. There have been over 17,642 victims and $2.3 billion in losses between October 2013 and February 2016, with the most prominent one being Ubiquity Networks that became a victim of a $46.7 million "CEO email fraud".
Scam emails aren't as obvious as ALL CAPS or with $$$ saying "YOU WON CA$H $$$$". Emails today can be very convincing. Be cautious of mimicked email addresses. Be wary of email-only wire transfer requests and requests involving urgency. If it's something you're not expecting or the address look a little off, it probably is a fake. Don't hesitate to pick up the phone and call to verify legitimate business partners and reasons. Being conscientious of what you're opening and who is sending you emails can help you avoid a $25,000 to $75,000 loss, which is the average loss per scam.

## TIP 4 Protect your computer environment against viruses and Malware

Does your computer have security programs on it? Are they up to date? The best ways to steer clear of viruses and malware are to use an industry-leading anti-virus software solution. There are many types out there, and they don't have to break the bank, but having a level of defense can go a long way.
On your anti-virus software, enable the "auto update", "auto-protect" and "personal firewall" to ensure you always have protection in the background and that it stays updated. Also, when possible use "whitelisting" solutions. Unlike most of the anti-virus solutions that use a "blacklist" to identify malicious files, these solutions allows you to create a "whitelist" of programs and applications that you explicitly allow to run for your day to day business. Everything else is automatically blocked providing a higher level of security.

withum
AUDIT TAX ADVISORY

## TIP 5 Make your systems less "vulnerable"

Did you know that majority of attacks rely on un-patched operating system vulnerabilities? Protection your computers against such attacks and making them is as simple as turning on "auto updates" for your computers operating system. If you use Microsoft Windows, this can be done by choosing to "automate installation" of all "important updates".

## TIP 6 Don't fall for 'free' USB drives

Who doesn't like free stuff! It is nearly impossible to go around a trade fair today without walking out with a bag full of "free" USB drives. While there is no harm in collecting them and handing them over to your kids as a toy, it might not be a very good idea to actually plug them in your home or work computer. If you don't trust the source of the USB drive, don't plug it in. These drives can very easily be used to carry and deliver a malware or virus onto your computer, allowing someone else access to your important information. In fact, this technique was used to perpetrate the "worst breach of U.S. military computers in history". It started in 2008, with a USB flash drive infected by a foreign intelligence agency left in the parking lot of a Department of Defense facility at a base in the Middle East and impacted the network of United States Central Command. It took 14 months to clean the network and the systems. A recent study was done to determine the success rate of this attack vector. They dropped USB drives in a public parking lot of government buildings and private contractors. 60% of the people that picked one up plugged the device into their office computers. If it had a logo on it, 90% plugged them in. These people didn't know where the drives came from but used them anyway. Thankfully it was just a study, but can you imagine if the impact if it were an actual attack?

## TIP 7 Avoid being ransomed by "Ransomware"

Have you or someone you know been a victim of "Ransomware"? As the name suggests, "Ransomware" is a computer malware that "locks" all your data on your computer by encrypting it and demands a ransom payment to restore it. Usually the ransom amount is a few hundred dollars, unless you are an institution like a hospital, a local police department, etc. in which case the ransom amount can run to thousands of dollars. Just in the first three months of 2016, these attacks increased tenfold over the total entire previous year, costing victims more than $200 million.The easiest way to minimize the impact of a "Ransomware" attack is to immediately disconnect the infected machine(s) from the network, reinstall the operating system (yes just cleaning with an anti-malware software is not recommended) and restore from your last good backup copy. That brings us to the key question: Do you backup your laptop or desktop daily? It's never too late to start. How else can you protect yourself from Ransomware? And, if necessary, pay the ransom to get your files back.

## TIP 8 Is public Wi-Fi really safe?

Public Wi-Fi is great. You can sign on while on the go – from the coffee shop, hotel or airport. But, using unsecured, public Wi-Fi can come with risks. Hackers can act as the "middle man" between you and the connection point, seeing all traffic and files you're sharing. How can you stay secure?

- Always use VPN connection when possible. This will ensure a secure connection.
- Avoid accessing sensitive websites like banks.
- Always choose the connection type as "public". This will turn off network file sharing.
- Double check that your email application like Outlook has been setup to encrypt communication with Exchange when outside of your corporate network.

These eight tips that can get you started in keeping you and your precious data protected. Don't want until you've already been breached, start taking the precautions today.

**Anurag Sharma, CISA, CISSP, CRISC, MBA**
Principal, Team Member, Cyber Secure Services
T (609) 520 1188
asharma@withum.com