Cyber Security

By: Rhonda L. Duddy, Esq.

With the increased convenience of technology comes an increased risk. No one is immune from cybercrime. For example, as we have recently heard, millions of people have been affected by the Equifax data breach. The list of corporations with data breaches is growing, but small business and individuals face harmful hacking and scamming schemes as well.

National Cyber Security Awareness Month occurs every October and is designed to educate people and bring awareness to the growing problem of cybercrime. The following are a few ways to identify types of cyber attacks so we can all make an effort to be safer and more secure on line.

Cyber criminals continue to look for ways to hack into our computer systems and have become more creative and sophisticated in their strategies. One danger to be aware of is ransomware. Ransomware targets everyone from home users to businesses and government networks and can lead to temporary or permanent loss of sensitive information, disruption of business, and financial loss.

Ransomware is defined as a type of malicious software designed to block access to a computer system until a sum of money is paid to unlock the data. Paying the ransom does not guarantee you will regain access to your data. The Tewksbury Police Department had found themselves victims of a cyber attack and decided to pay the $500.00 ransom to get their data back, but some organizations have paid the ransom, sometimes in bitcoin, and were never provided with information to release their information.

Another cybercrime concern is phishing. Phishing is an attack used by cyber criminals to trick you into giving up information. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well known store. These messages then encourage you to take an action, such as clicking on a malicious link or opening an infected attachment.

Cyber criminals craft these convincing looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. Some Verizon customers were victims when they were targeted earlier this year and received legitimate looking emails attempting to lure them to a fraudulent website to input personal information or download a virus infected program.

There is an even more targeted type of phishing to be aware of known as spear phishing. Spear phishing is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. The attackers research their intended targets such as by reading the intended victims' Linkedin account, Facebook account, or company websites, as well as any messages they post on public blogs or forums. Based on their research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

Cybercriminals know the best strategies for gaining access to our sensitive data, but here are some steps to take to protect ourselves from cyber attacks:

- Be suspicious of emails with grammar or spelling mistakes. Most legitimate businesses proofread their messages carefully before sending them.
- Use strong passwords and change them every few months. A strong password would be a phrase or something that would be difficult for a hacker to guess. It would be prudent to not use common passwords, such as "123456" or "password." You should keep a list of your passwords on a piece of paper, not on your computer.
- Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it.
- Be suspicious of attachments. Only click on those you are expecting. If it looks suspicious, even if you know the source, it's best to delete the email or avoid clicking on the advertisement.
- If you get a suspicious email from a trusted friend call them as their computer may have been infected or their account may be compromised.
- Don't click pop ups or suspicious links.
- Don't "click here". Log in to the company's actual website instead.
- Limit the type of business you conduct on public wi-fi networks as they are not secure.
- Regularly update your antivirus software and use a firewall to block access to known malicious addresses.
- Enable spam filters to prevent phishing emails from reaching you.
- Back up your data regularly and test those backups to verify they are working properly.
- Exercise caution when using email providers such as AOL, Google, Yahoo, Hotmail as they are highly targeted accounts.
- Be careful what you download.
- Stay up to date and aware of emerging cyber threats.

You may not be able to prevent a cyber attack, but you can take these steps to maximize defenses and minimize the impact.