HIGHTOWER
THE ANDRIOLE GROUP

SHARING OUR THOUGHTS ON CYBERSECURITY

In 2017, 16.7 million people were victims of identity fraud, according to Javelin Strategy & Research. According to the same study, financial fraud due to account takeover cost consumers a total of $5.1 billion during the year. This was three times the total stolen in 2016. While the sheer frequency of data breaches might feel like the new normal, complacency should not be your cyber security strategy. Here are six ways to help protect yourself.

Pay Attention to your Passwords

Many people have had the unfortunate experience of having their email hacked. When a fraudster breaks into your email, they are not after your address book. They are looking for personal information that can help them get to your money. A strong password is your first defense. Generally, the more variables present in the password, the safer you are. Ideal passwords use longer words or phrases, special characters, numbers, and a combination of upper and lowercase letters. Try to avoid common words, grammatically correct capitalizations, or obvious substitutions of numbers for letters. You can also consider using a passphrase, which is a sequence of words, as your password. Passphrases are presently considered more secure than a password. Using a different password for every account is also key, and thankfully, you no longer have to remember all of your passwords for all of your websites. Using a password manager such as Dashlane or LastPass can help you generate and store strong passwords in a safe place.

Use Two-Factor Authentication where Possible

Many organizations now offer their users two-factor authentication. Two-factor authentication offers an additional level of security during the sign-in process. When you try to sign in a code is sent to your phone. After entering your user name and password you must also provide the code. This ensures that somebody cannot access your account without also having your personal mobile device.

Be Aware of Suspicious Emails

A legitimate organization will never send you an email with a link to reset your password or update your personal information. Emails asking you to do these things might appear legitimate at first, but when you click the link it will take you to a site that is fake. This is called Phishing. Entering your personal information or password into the fake website will send the information directly to hackers. If you receive such an email, delete it. If you receive an email from someone you don't know asking you to click on a link or open an attachment, delete it. Clicking on the link or opening attachments in an unknown email may give fraudsters a direct line into your computer and everything on it by infecting you with malware.

Use Antivirus Software

Malware is a term that describes any type of software designed to cause damage. These types of software can hide on your computer and send sensitive information such as account numbers to cyber criminals. The best way to combat malware is to install antivirus software. Many companies' software packages will do more than scan and quarantine viruses or malware on your computer, they will also help you by blocking suspicious sites and Phishing attacks.

Be Social Media Savvy

Many people overshare on social media. This practice can be downright dangerous to your security. Stop and think a moment about the security questions you set up when establishing a new online user name and password with a service provider. In what city were you born? Where did you meet your spouse? What is your favorite hobby? Where is your favorite place to vacation? What is your daughter's name? How many times have you provided hints to what this information might be via social media outlets? Every day, people post about their lives or click on links to take popular quizzes that ask for this information. Always remember, nothing you do online is ever truly private. Don't give away answers to your security questions on social media and, when possible, choose uncommon questions for your security questions.

Update Your Programs

Icons prompting us to update our systems and apps are constantly popping up on our tablets, laptops, and smartphones. Ignoring these prompts is a bad idea. Companies that design and create our apps and operating systems are constantly testing their products' security. When a tester discovers a weakness, the company fixes it and sends out an update to users. Delaying installation could leave you vulnerable to a recently discovered "easy in" for cyber criminals. However, when updating programs, always make sure that the update is from the vendor, as there have been updates that are produced maliciously by others. For example, only update Windows if you receive the update from Windows, and Adobe if the update is received by Adobe.

Your advisors at The Andriole Group are dedicated to your cyber security. Team members regularly participate in cyber security training and engage in client authentication protocol before executing client requests. We urge all of our clients to be personally vigilant when protecting their security. Talk to us today about enacting two-factor authentication for your HighTower accounts and other ways we can work together to make you safer. The way to start the journey is to start a conversation.