MEL CYBER TASK FORCE UPDATE

Concerned About Cyber? 4 Easy Steps for Staying Secure in 2022

Cybersecurity has become one of the biggest hot topics both inside and outside of technology circles over the last two years. From securing learning devices due to a rise in digital learning during the COVID-19 pandemic, to coping with the fallout of high-profile breaches of national infrastructure such as the Colonial Pipeline, there is a seemingly endless news cycle dedicated to cybersecurity mishaps and concerns.

And with this onslaught of negative news, it can be easy for everyday individuals to become overwhelmed and to feel powerless in the face of the "insurmountable" threats posed by cybersecurity. But nothing could be further from the truth.

With all the jargon that is typically thrown around in relation to cybersecurity there is a longstanding misperception that cybersecurity is beyond everyday people and that it should be left to the professionals. Moreover, there is a prevailing sense among the public that breaches are simply a fact of life and that we should just learn to deal with them. But this just isn't true. In fact, everyday people have a huge role to play in cybersecurity threat prevention, detection, and remediation. For example, according to IBM, **95% of breaches have human error as a main cause**. Therefore, everyday day technology users are very much the first line of defense when it comes to thwarting cybercrime. Unfortunately, though, many individuals are not aware of some of the best practices for boosting cybersecurity and how easy they are to use.

With that, here are a few key best practices that everyday people can implement today to enhance their own cybersecurity and create a more secure world for everyone.

Watch Out for Phishing

Phishing – when a cybercriminal poses as a legitimate party in hopes of getting individuals to engage with malicious content or links – remains one of the most popular tactics among cybercriminals today. In fact, 80% of cybersecurity incidents stem from a phishing attempt. However, while phishing has gotten more sophisticated, keeping an eye out for typos, poor graphics and other suspicious characteristics can be a telltale sign that the content is potentially coming from a "phish." In addition, if you think you have spotted a phishing attempt be sure to report the incident so that internal IT teams and service providers can remediate the situation and prevent others from possibly becoming victims.

MEL CYBER TASK FORCE UPDATE

Update Your Passwords and Use a Password Manager

Having unique, long and complex passwords is one of the best ways to immediately boost your cybersecurity. Yet, only 43% of the public say that they "always" or "very often" use strong passwords. Password cracking is one of the go-to tactics that cybercriminals turn to in order to access sensitive information. And if you are a "password repeater," once a cybercriminal has hacked one of your accounts, they can easily do the same across all of your accounts.

One of the biggest reasons that individuals repeat passwords is that it can be tough to remember all the passwords you have. Fortunately, by using a password manager, individuals can securely store all their unique passwords in one place. Meaning, people only have to remember one password. In addition, password managers are incredibly easy to use and can automatically plug-in stored passwords when you visit a site.

Enable MFA

Enabling multi-factor authentication (MFA) – which prompts a user to input a second set of verifying information such as a secure code sent to a mobile device or to sign-in via an authenticator app – is a hugely effective measure that anyone can use to drastically reduce the chances of a cybersecurity breach. In fact, according to Microsoft, MFA is 99.9 percent effective in preventing breaches. Therefore, it is a must for any individual that is looking to secure their devices and accounts.

Activate Automatic Updates

Making sure devices are always up to date with the most recent versions is essential to preventing cybersecurity issues from cropping up. Cybersecurity is an ongoing effort, and updates are hugely important in helping to address vulnerabilities that have been uncovered as well as in providing ongoing maintenance. Therefore, instead of trying to remember to check for updates or closing out of update notifications, enable automatic update installations whenever possible.

For more information about cyber risk control, model policies, cyber insurance, news, tips and best practices visit NJMEL.org.

For details, contact the MEL Underwriting Manager or your local JIF Executive Director

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL · MEL