MILES SMITH INSURANCE GROUP

Trade Association Forum
OFFICIAL PARTNER
the association of associations

CYBER TRAINING MANUAL

One of the most important aspects of cyber security is a well-trained workforce. Use this employee cyber training manual to educate your members employees about common cyber threats and the best practices to defend against them.

EMPLOYEE CYBER TRAINING MANUAL

WE HAVE PUT TOGETHER THIS DOCUMENT TO HELP RAISE AWARENESS OF CYBER-SECURITY VULNERABILITIES AND TO GIVE YOU THE KNOWLEDGE TO PROTECT YOURSELF BOTH AT HOME AND IN THE WORKPLACE.

Although some of the topics outlined may not apply to you directly, it is important to gain a background in cyber-security procedures as well as the measures that are specific to your business.

1. SOFTWARE UPDATES

When using devices, such as laptops, desktop computers, smartphones and tablets, you may see a small window pop up on the screen asking you to update your operating system (OS) or anti-virus protection. Although these can be frustrating and are easy to ignore, they play a critical role in cyber-security, and making your employees aware of this is vital.

Device manufacturers and software developers use the 'always connected' nature of todays world to constantly adapt to new cyber-threats and push updates out to their users. Companies like Apple, Microsoft and Google can respond to a hole in their software and release a patch to fix it within a few days. In addition, there is a bonus for you; these patches often include new features that will make your devices more capable.

Simple security tips:

- Update the software on your computer and mobile devices whenever you are prompted
- Check your programs and applications regularly to ensure you are using the most up-to-date version. If you are not, be sure to download updates only from the official developer
- If you have installed anti-virus software, be sure to run sweeps of your device regularly to check for malware and viruses, these can be set to run automatically and at regular intervals, for example weekly.

Trying to figure out how to update your device and finding a time to do it can be harder than it sounds. However, many devices now support automatic updating. This means that when you are not likely to be using your device, such as in the middle of the night, your device will automatically download any available software updates and restart.

2. SAFE INTERNET BROWSING

It is easy to assume that all websites are safe to browse, especially when you are using smartphones or other mobile devices. However, malicious sites can use tactics, such as internet cookies and phishing schemes, to gain access to your device or important personal and professional information.

Simple security tips:

- When using a web browser, check the URL for a small lock icon to be sure that a site is secure
- Additionally, a secure website will have an 's' in the 'https://' that comes before the full URL
- Never type personal or professional information, such as usernames, passwords, telephone numbers or addresses, into a pop-up window
- If you ever suspect that a website is not what it seems, close your browser immediately.

3. SECURE PASSWORDS

Making a new password can be one of the most frustrating and important things you do online. Every website and service seems to have different rules about length and complexity, and then you have to add your password to an ever-growing list in your memory. However, knowing the details of what goes into creating a password can give you the insight you need to make a password that is both secure and easy to remember.

When you make a password, the service or website you are signing up for usually encrypts the password before storing it on its servers. That way, even if a hacker were to gain access to your password

through a cyber-attack, he or she still will not have access to the text that makes up your password. Websites often require passwords to include upper-case letters, numbers and symbols because these special characters exponentially increase the number of possibilities that hackers will have to try in order to figure out your password.

The next time you are required to make a password, try typing in a favourite quote from a book, or a saying that is familiar to you. If you can also add a capital letter or special character, the password will be that much stronger.

Simple security tips:

- Make sure that your passwords include an upper-case letter, a number and a special character
- Never keep your password written down somewhere, especially around the devices you use to access your online account
- If you use a number of online accounts, consider using a password management tool. These websites and services require a single login and will manage and save your passwords for you. However, be sure to research a service before you use it, as some have better reputations than others do.

4. INSTALLING SOFTWARE

Software, such as apps and computer programs, make it easy to do work and access social media and other forms of entertainment. However, hackers can use malicious software to access your messages, contacts, emails and even your location based on GPS data.

Simple security tips:

- When you download a piece of software, make sure to check how much access it has, and that a reputable developer made it. Many apps and programs ask for more access to your computer or mobile device than is required
- Always be sure to download an app from your device manufacturer's official store. Cyber criminals often make fraudulent apps that are deliberately designed to look like legitimate apps, but will harvest your information for illegitimate reasons.

5. SOCIAL MEDIA

Social media sites like Facebook, LinkedIn and Twitter allow us to connect easily with family and friends. However, they can also give hackers access to your personal information for phishing schemes. It is completely normal to check social media during the working day, but you should keep some best practices in mind.

Simple security tips:

- Never talk about your work in social media posts without clearing it with a manager first. Even if you think something is innocent, it could give potential criminals an idea for cyber-attacks against your employer or co-workers
- Do not update social media when you are away. Although it can be tempting to post pictures and update your location for friends and family members, this will give everyone a clear picture of when you are out of the house and office. Then, anyone could use this information as a means to attempt to steal from your home or office
- Go into the settings of your social media accounts and check that your security settings are to your liking. Most social media sites allow you to block strangers and members of the public from viewing your information without your consent.

CYBER INSURANCE

As reliance on technology continues to increase, new exposures continue to emerge. As your business grows, it is vital to make sure your cyber liability insurance cover grows with it.

A cyber insurance policy is designed to provide support and protect you and your members business if it is subject to a data breach or an attack by a hacker. Miles Smith can arrange comprehensive cyber cover and we can help with reputation management should you need it.

To find out more about how working with Miles Smith can benefit you, please contact Ian Cook, Interim Managing Director of Miles Smith Insurance Solutions - icook@milessmith.co.uk or call him on 020 7977 4800.

Provided by Miles Smith Insurance Group