TechSpace Co., Ltd.

1112/110-111 Sukhumvit Rd., Phra khanong, Khlong Toei, Bangkok 10110
Tel: 02 381-9075 Fax: 02 713-6800

10 Cybersecurity Tips for your Business

Tip #1 - Keep software up-to-date

Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:

- Turn on Automatic Updates for your operating system.
- Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up-to-date.

Tip #2 – Utilize a strong password

We have all heard that having a strong password is important, but what classifies as a strong password?

Strong passwords:

- Should be at least 8 characters long
- Contain and mix letters, symbols, and numbers
- Avoid utilizing words, especially proper nouns
- Never include Personally Identifiable Information (PII)

If you are creating secure passwords, it can be difficult to keep track of them all. Using a password management app to store and manage your different passwords can help you keep organized in a secure fashion.

Tip #3 - Avoid Phishing scams - beware of suspicious emails and phone calls

Phishing scams are a constant threat - using various social engineering (link is external) ploys, cyber-criminals will attempt to trick you into divulging personal information such as your login ID and password, banking or credit card information.

- Phishing scams can be carried out by phone, text, or through social networking sites - but most commonly by email.
- Be suspicious of any official-looking email message or phone call that asks for personal or financial information.

Phishing attacks are a huge part of modern-day cyberattacks – some are highly personalized and may contain references to your coworkers, family members, your hobbies, and more.

The best way to mitigate this is awareness, use the **SLAM** method to help identify phishing attacks:

- Sender: Check the sender's email address
- Links: Hover and check any links before clicking
- Attachments: Don't open attachments from someone you don't know or attachments that you weren't expecting
- Message: Check the content of the message and keep an eye out for bad grammar or misspellings

Tip #4 – Utilize Multi-factor Authentication (MFA)

For both corporate applications and personal applications, it's imperative to enable MFA to validate that the person logging is who they claim to be, and to prevent malicious hackers from authenticating into your network.

Tip #5 - Be careful what you click

Avoid visiting unknown websites or downloading software from untrusted sources. These sites often host malware that will automatically install (often silently) and compromise your computer.

If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

ISO recommends using Click-to-Play(link is external) or NoScript(link is external), browser add-on features that prevent the automatic download of plug-in content (e.g., Java, Flash) and scripts that can harbor malicious code.

Tip #6 - Never leave devices unattended

The physical security of your devices is just as important as their technical security.

- If you need to leave your laptop, phone, or tablet for any length of time - lock it up so no one else can use it.
- If you keep protected data on a flash drive or external hard drive, make sure their encrypted and locked up as well.
- For desktop computers, lock your screen or shut-down the system when not in use.

Tip #7 – Use a VPN

Virtual Private Networks (VPNs) provide a great way for employees to securely access remote resources from multiple locations by connecting two private networks securely over the internet. Utilizing public Wi-Fi in airports, hotels, and coffee shops without a VPN can inadvertently give away a lot of details about what devices you have and what you're doing on the internet. In the hands of a hacker, this information can be used to formulate an attack.

Tip #8 - Use mobile devices safely

Considering how much we rely on our mobile devices and how susceptible they are to attack, you'll want to make sure you are protected:

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install apps from trusted sources (Apple AppStore, Google Play).
- Keep the device's operating system up-to-date.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most handheld devices are capable of employing data encryption - consult your device's documentation for available options.
- Use Apple's Find my iPhone(link is external) or the Android Device Manager(link is external) tools to help prevent loss or theft.

Tip #9 - Install antivirus/anti-malware protection

Only install these programs from a known and trusted source. Keep virus definitions, engines and software up-to-date to ensure your programs remains effective.

Tip #10 - Back up your data

Back up regularly - if you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system.