Cybersecurity Self-Assessment

If you can checkmark 7 out of 12 boxes
including the Cybersecurity Awareness Training
then you are already doing better than the average!

❑ Do you Back Up critical data at least every 7 days and store at least one backup offsite?

Data backup means duplicating information to allow retrieval of the data copies after a data loss event. If your devices catch a terrible computer virus making them unusable, your backup will enable you to quickly restore your business to an earlier point in time. You can store backups on a USB Stick but note that such a device can easily be lost or broken, losing all your data with it. A good backup practice includes storing multiple backups on different premises, including an offsite Cloud Storage.

❑ Do you provide Cybersecurity Awareness Training to employees?

All technical security measures turn obsolete if you or your employee gives an attacker access to your network. Learning what threats exist online, differences between weak and strong passwords, and spotting fraudulent content are some things taught in Cybersecurity Awareness Training. After the training, you and your employees will have good cybersecurity habits that outsmart attackers!

❑ Do you update all your devices to the latest recommended software version available ASAP?

Software updates typically provide fixes to their older versions' vulnerabilities that attackers share on the Dark Web. Staying up to date on software removes an attacker's ability to attack you using the same methods from older software. The older the software, the more time attackers have sharing vulnerabilities they find and the easier it is for them to launch a successful attack.

❑ Do you deploy commercial grade Firewall across your network?

Firewall is a ***device*** (usually a physical box that you put on the wall) that monitors and controls data and information moving to and from computers (network traffic) by deciding what to let pass through or block based on set rules that you give it. The term comes from the *physical firewall* that prevents the spread of fire between rooms. A Firewall does the same, it serves as a barrier between you and the rest of the internet

❑ Do you deploy commercial grade Antivirus on your devices?

Antivirus is a ***software*** that you install on your computer. It protects systems internally by frequently searching, spotting, and removing malicious files and viruses that have managed to enter your network. Once installed on your device, it typically runs automatically in the background to provide real-time protection against virus attacks.

❑ Do you use a Spam filter for your email?

Spam filters are used to detect unsolicited, unwanted, and virus-infested email (called spam) and stop it from getting into email inboxes. Sending spam is a lucrative business, it is estimated that 70 percent of all email sent globally is spam, so having a spam filter is a must!

Created by Victoria Gadis Torp, Cybersecurity Awareness Consultant
https://www.linkedin.com/in/victoria-gadis-torp/

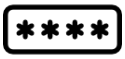
CAPITAL TEK

❑ Are your computers, servers and sensitive data files encrypted?

Encryption means that information is ciphered, making it difficult for an attacker to read what it is about even if they have access to your network or managed to steal your data. Decrypting information (making it readable again) is time-consuming, and attackers would rather find an easier target.

❑ Do you use Virtual Private Network (VPN)?

VPN is a method of accessing the internet securely and privately. VPNs create secure and controlled connections over the internet by encrypting your internet traffic and disguise your online identity, making it difficult for third parties to track your activities online and steal data. Just think of it like this: without VPN, you share sensitive business information on a loud speakerphone in public, but with a VPN, you are using earphones so that people don't hear this information.



❑ Do you use Complex Passwords?

Attacker's password-guessing program takes a long time to guess a strong (complex) password, whereas weak passwords are guessed in less than a second. Weak passwords typically use names or words (e.g. *William*, *password*, *avocados*), numbers that follow a natural order or repeat (e.g. 12345, 98765, 11111), neighbouring letters (e.g. Q-W-E-R-T-Y), and [+] or [!] as symbols. Complex passwords use random numbers, letters and symbols.

❑ Do you use a Password Manager?

A Password Manager is a computer program that allows you to generate, store and manage the multiple passwords you need to use online. It generates complex passwords for you, and you don't need to remember the passwords as you can access them all using one Master Password. However, remember to keep your one Master Password secret!

❑ Do you use Two-Factor Authentication (2FA)?

Usernames, and sometimes passwords, might remain the same for a long time, thus be easy for an attacker to take advantage of. 2FA provides an extra layer of security by asking for a second authentication factor from something you have, e.g. a phone, USB or smartcard, or a time-based PIN sent to your email or by SMS. The second factor keeps changing, so attackers have to start from scratch every time you log in.

❑ Do you have a Business Continuity Plan?

This is a plan that outlines how your business will continue operating during an unplanned service disruption. It contains a Disaster Recovery Plan with strategies for handling IT disruptions to networks, servers, PCs and mobile devices. It also typically includes data backups, identifies administrators and contact information for emergency responders and key personnel.

Need an IT expert's recommendations on how to secure your network against cyberattacks?

We would love to help you! Schedule a Free Assessment

https://capitaltek.ca/

(613) 227 – HELP (4357)

Created by Victoria Gadis Torp, Cybersecurity Awareness Consultant
https://www.linkedin.com/in/victoria-gadis-torp/