



Cyber Security

Awareness

Resource Package

Table of Contents

Page 2: Table of Contents

Page 2: Link to Webinar Recording

Page 3-4: Anti Virus Softwares

Page 5: Password Security

Page 6: Securing Devices

Page 7: Anxiety During a Cyber Scam

Page 7-8: Important Links

Page 9-12: Glossary

Page 13: HIEC & Funder Acknowledgment



Rewatch the Webinar

by clicking the image above

What to look for in an anti-virus software:

CHECKLIST:



Anti-malware:

Software created to scan devices to prevent, detect, and remove bad code that can negatively affect your data



Anti-ransomware:

Technology that protects computers from being overtaken from ransomware attacks which allows hackers full access to computer files and locks you out of your computer unless you give them money



Anti-spyware:

Program designed to avoid and remove spyware installations which gather data and forward it to a third-party without consent



Anti-adware:

Software that detects and blocks unwanted applications that could result in damages or viruses



Data protection:

Protects important files on your devices, such as your personal information and your financial documents








Secure web usage:

Being able to surf the internet without fear or fret that your computer or safety will be compromised

Top 5 most popular anti-virus software:



Note: Each program offers all of these anti-virus services, the purple circles indicate what the *basic plans* are best for.

		Security	Performance	simplicity	PC/MAC/Mobile	Privacy	Affordable	Safe Kids	Passwords	File Protection
	https://www.kaspersky.ca/	●	●	●						
	https://ca.norton.com/	●	●		●				●	●
	https://www.bitdefender.com/	●	●			●				●
	https://www.totalav.com/	●	●	●	●	●	●	●		●
	https://www.mcafee.com/	●	●	●		●		●	●	

Password Security:

Do's:

- Create a strong password
- Use different passwords for different sites
- Use a system to securely store your password
- Change your password immediately if it's been compromised

Don'ts:

- Do not share your password with anybody
- Do not store or "ask to remember" on a shared computer
Example: A public library

Criteria to build a strong password:

- At least 8 characters long
- A mixture of upper and lowercase
- A mixture of letters and numbers
- Include at least one special character (!,@.#.?.)

How to make a strong password that is easy to remember:

- Use a mnemonic device
- Replace letters or words with numbers and symbols
Example: "Dylan the UX Designer" can be...
"Dyl@nTh3UXD"

How to store your passwords securely:

- Memorize them (is easier said than done)
- Write them in a physical book (just don't lose it!)
- Save them in browser (not secure for shared passwords)

Password Managers we recommend:

- LastPass (<https://www.lastpass.com>)
- 1Password (<https://1password.com>)
- Dashlane (<https://www.dashlane.com>)
- Bitwarden (<https://bitwarden.com>)

Securing Devices:

Update your software

- Updates add new features, remove outdated features, update drivers, deliver bug fixes, and fix security holes that have been discovered.
- You can ensure your settings are enabled to automatically update software when new versions are available.

Antivirus Software

Antivirus software provides protection against cyber threats by scanning for viruses/malware/cyber threats, detecting them, and eradicating them. **Look for software that offers the following features:**

- A firewall feature helps block unauthorized access to your devices, helping to safeguard private information and financial data.
- An automatic Cloud backup feature can help protect sensitive data, photos, and other important information by enabling you to back up, store, and recover your computer files.
- Comprehensive protection for multiple devices, ranging from computers, laptops, phones and tablets.
- A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection (for example, if you are using wifi at a hotel).

Other tips for securing your devices:

- Make sure your computers, phones and tablets are locked with a password so others cannot open and use them.
- If you use shared devices, make sure you log out every time you are finished.
- Do not use USBs or other external devices unless you own them or come from a reliable source.
- Update your browser privacy and security settings. Most browsers have options that enable you to adjust the level of privacy and security while you browse.
- Avoid streaming or downloading movies, music, books, or applications that do not come from trusted sources. They may contain malware.

Anxiety During/After a Cyber Attack

By Constable Mat Rocca | Halton Regional Police

Feeling Overwhelmed?

If you end up in a state of distress, you may end up making bad decisions. Do your best to remain calm and compose yourself.

Alleviate your anxiety by taking action by...

Force closing your browser

(Press Option + Command + Escape for Apple Computers)

(Press Alt + F4 for PC Computers)

Restarting your computer in "safe mode"

Running an antivirus program

Contacting the relevant authorities

Contacting Your Local Authorities:

If it's not a crime in progress, then that would be contacting the non-emergency police line (905) 825-4777. Remember you're not alone!

Resources:

Canadian Anti-Fraud Number: 1-888-495-8501

TransUnion Consumer Relations: +1 800-663-9980

Halton Regional Non-Emergency Police Line: (905) 825-4777

CLICK THE LINK TO GO TO PAGE

The link is safe, we promise!

Important Links:

Get Cyber Safe

<https://www.getcybersafe.gc.ca/en>

The government of Canada created the Get Cyber Safe website to help educate Canadians about cyber security crime and how to prevent it from happening to you and your loved ones. They've created easy to understand step-by-step tutorials, articles, and videos that help users protect themselves online.



Learn how to stay safe online

Secure your accounts	Secure your devices	Secure your connections
		
Keep your information from being compromised.	Get tips to help you protect the devices you use every day.	Protect your Wi-Fi, Bluetooth and other connections.
Passphrases, passwords and PINs Multi-factor authentication Password managers Social media	Laptops and computers Phones and tablets Gaming systems TVs and smart devices Storage and backup System updates	Private networks (home routers) Bluetooth VPNs Firewalls Public Wi-Fi

Important Links Continued:

Canadian Centre for Cyber Security

<https://cyber.gc.ca/en/>

The Canadian Center for Cyber Security is a more academic and current resource when learning about cyber crime. The government of Canada uses this site to post up-to-date and extensive articles about the different types of virtual criminal activity that's happening around the globe, as well as alerts and advisories of potential threats. The website also features a Learning Hub where they offer courses on basic, advanced, and specialized topics about online security.



Canadian Anti-Fraud Centre

<https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>

The Canadian Anti-Fraud Center website is where you can find an extremely broad list of all the types of reported scams, from ones that just affect individuals, to scams affecting businesses. This is also the place where victims of cyber crime can report the incident and educate themselves on what to do in that situation. The website also provides lots of statistics, articles, and resources to help people understand the severity of online fraud.



Glossary

- **Anti-virus:** A software which protects your device from viruses.
- **App:** Short for “application”, it is a small computer program that performs a specific function that can include games, social networking, etc. (Ex: Candy Crush, Facebook, Youtube...)
- **Artificial intelligence (AI):** Refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.
- **Authentication:** A way for a website, account, or computer to verify that you are who you say you are. Authentication factors can include passwords, pins, and questions.
- **Backing up:** In storage technology, backup means to back up data from your hard drive to a remote server or computer for protection..
- **Browser:** A free tool that is used to view web pages and other online content on your computer or mobile device. The top used and safest browsers to use include Google Chrome, Firefox, Internet Explorer, and Safari.
- ***Cyber-attack:** A cyber-attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks.
- **Cloud:** An online service for digital storage.
- **Dox:** Search for and publish private or identifying information on the internet, typically with malicious intent.
- **Data thief:** Data theft is the act of stealing information stored on computers, servers, or other devices from an unknowing victim with the intent to compromise privacy or obtain confidential information.

Glossary

Continued...

- **Denial of Service attack (DDos):** In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
- **Domain:** Is the name of a website.
- **Exploit:** An exploit is a code that takes advantage of a software vulnerability or security flaw.
- **Encryption:** The process of converting information or data into a code, especially to prevent unauthorized access.
- **Firewall:** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- ***Hacker:** A person who uses computers to gain unauthorized access to data.
- **Http/https:** Hypertext Transfer Protocol. The S stands for secure in https. It is found at the beginning of an URL.
- **IP Address:** Short for Internet Protocol address, every computer, smartphone, and mobile device that accesses the internet is assigned one for tracking purposes.
- **Lan:** A computer network that interconnects computers within a limited area such as a residence, school.
- ***Malware:** Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Network:** A group of computers that use a set of common communication protocols over digital interconnections.

Glossary

Continued...

- **Phishing:** Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- **Password:** A secret word or phrase that must be used to gain admission to something.
- **Proxy:** A computer that acts as a gateway between a local network and a larger-scale network such as the internet.
- **Router:** A router is a device that communicates between the internet and the devices in your home that connect to the internet.
- **Ransomware:** Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- **Spam:** Unwanted messages that can be sent to your email or social media. Most "spam messages" come from companies that want you to buy their products, but some contain inappropriate images or faulty links with intent to fraud the receiver.
- **Spyware:** Spyware describes software with malicious behavior that aims to gather information about a person or organization and send such information to another entity in a way that harms the user.
- **Software:** The programs and other operating information used by a computer.
- ***Two factor authentications (2FA):** Is a method of establishing access to an online account or computer system that requires the user to provide two different types of passwords. With two-factor authentication, you will need to both provide a password and prove your identity some other way to gain access.

Glossary

Continued...

- **URL:** A “Universal resource locator” is a written address where you can find a website on the internet. Ex: <https://www.google.ca>
Phishing: Term used to describe online scams that are trying to lure you into divulging your private information, such as your identification or financial information.
 - **VPN:** A virtual private network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shielding your browsing activity from prying eyes on public Wi-Fi.
 - ***Virus:** In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates.
 - **Wi-Fi:** Wi-Fi is a wireless networking technology that allows devices such as computers, mobile devices, and other equipment to interface with the Internet.
- *represents an essential definition in relation to cyber security.*

About us

HIEC is an innovative not-for-profit social enterprise focusing on partnership, mentorship and workforce development. For almost 30 years, we've been working to build stronger connections between educators, employers and the students who will make up our future workforce.

We deliver an interactive and informative Career Awareness Program, facilitate meaningful experiential learning opportunities, host inspiring community events, and manage multiple online communities with a focus on workforce development.

We believe that students will be more successful if they are empowered to make informed and inspired career choices, connected with opportunities for experiential learning, and supported in managing their transition from school to career.

Connect with us:

Website: hiec.on.ca

Instagram: [@haltoniec](https://www.instagram.com/haltoniec)

Twitter: [@haltoniec](https://twitter.com/haltoniec)

Facebook: [/HaltonIndustryEducationCouncil](https://www.facebook.com/HaltonIndustryEducationCouncil)



Funder Acknowledgment

This project is funded by

