HOW TO PROTECT YOUR

Machines and Devices

One of the ways in which cyber criminals can steal your information is to infect your computer or mobile device with malicious software (malware). Keeping your devices free from dangerous software protects your information.

Use Security Software

Some malware can still cause infections. Using security software will add an additional layer of protection.

- Run quality antivirus software to conduct frequent system scans for dangerous software
- Ensure your system firewall is turned on if you have one

Stay Up to Date

Keeping your systems up to date will help prevent your machine from infection.

- Check for new updates for your computer, mobile devices, apps and software
- Turn on automatic updating for all devices, apps and software where possible

Take A Few Extra Steps

In addition to above, take the following extra steps.

- Set up a password that you have to enter to start your computer or mobile device
- Back up your information regularly to an external hard drive or via a service provider
- Use encryption software on your computer or mobile device when sending data to others

HOW TO PROTECT YOURSELF FROM

Online Scams

Phishing is a type of online scam. It refers to when a cybercriminal uses email, texts, or social media posts to convince you to give away sensitive information – usually by clicking a dangerous link, or opening an attachment.

Once you open or click on the link dangerous software is introduced to your computer and they can access your account information or other personal data.

Often these messages look like they come from legitimate sources such as a bank, government department or other well-known organization.

Learn to Spot an Online Scam and Protect Yourself

Look for poor grammar and spelling or website names that are just a little different from the reputable brands you know

- Legitimate emails won't ask for personal, sensitive or financial information (e.g., SIN or PIN numbers)
- Scam emails urge you to act quickly to avoid something bad happening
- Don't open emails, texts, or social messages from people you don't know
- Never click on links contained in emails, texts, or social messages and posts – you can search for the information online in a new window or site.

For more information

For more information contact us at
publicsafety@surrey.ca
or visit www.getcybersafe.gc.ca

17111

surrey.ca/publicsafety

CITY OF SURREY

Be Safe Online

Cyber Security Tips to Keep You Safe

PUBLIC SAFETY STRATEGY
TAKING ACTION TOGETHER

Cyber Security Outreach Program

We live in an increasingly connected online world. Protecting ourselves from cyber threats and identity theft is no longer optional. An important element of the City's Public Safety Strategy, Be Safe Online is a new cyber security outreach program that aims to provide trusted and actionable education and resources to help protect Surrey's residents and small to medium-sized businesses.

While cyber criminals are becoming better organized and more sophisticated, the following are simple things you can do today to protect your privacy and be safe online.

Personal Cyber Security Tips

Protect Your Accounts from Theft

Protect Your Devices from malicious software (malware)

Protect your personal information to prevent:

- Damage to your reputation on social networks
- Online scams
- Identity theft

HOW TO PROTECT YOUR

Accounts

Weak passwords can be cracked in minutes, giving criminals access to your activity online (e.g., bank accounts, social media accounts, and email).

Be safe online and protect your accounts by using a strong password or a passphrase and, for heightened security, use two-step verification.

Strong Passwords

- **Example:** @8jJ6eN9*jp2
- Are at least 12 characters long
- Contain a mixture of upper case, lower case, and special characters
- Do not contain common dictionary words
- Are unique for every account

Strong Passphrases

- **Example:** Bubbles smile when they fly
- Are 20 characters or longer
- Do not contain famous quotes or popular lyrics
- Should be easy to remember

Two-Step Verification

Enabling two-step verification adds an extra layer of security to your account. With two-step verification you need to provide your password or passphrase and then do one of the following:

- Enter a code sent to your phone via text
- Enter a code from an app on your phone
- Respond to a push notification to your phone

HOW TO PROTECT YOUR

Social Identity

If you use social networks, play online games, post online or chat with friends over the Internet, then you have a social identity. If you don't protect your social identity, it can be used by cyber criminals to steal your information, impersonate you or damage your reputation.

Protect Your Profile

The more personal information you share online, the more susceptible you are to cybercrime.

- Never include personal information like your age, address or phone number in your social media profile
- Enable the highest privacy settings and limit who can see your profile using the tools provided by the site or program
- Don't give others your social media password or leave the program logged in on your computer or device

Share with Care

What you post online could make you a target for those that want to hurt or manipulate you.

- Think carefully about what you will post and who might see it (including future employers)
- Ask your friends/family to think before tagging you in photos or disclosing your location without your permission
- Don't accept friend or connection requests from people you don't know

Avoid Social Media Scams

With social networking becoming more and more popular, social media scams are on the rise.

- Be wary of posts that ask you to click on a link, even from people you know.
- Don't automatically trust posts offering free gift cards or prizes
- Watch for fake friend requests asking for personal information