HOW TO PROTECT YOUR

Machines and Devices

One of the ways cyber criminals can steal your business data is to infect your computer or mobile device with malicious software (malware). In some cases, they will demand payment to stop them from sharing or destroying your important data (ransomware). The best defense is making your system as secure as possible.

Use Security Software

Using security software will add an additional layer of protection.

- Run quality antivirus software to conduct frequent system scans for dangerous software
- Install a system firewall and ensure it is turned on

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
- Make sure staff run updates when prompted

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 or for your most sensitive customer data or proprietary information

PROTECT YOUR BUSINESS FROM

Phishing and Online Scams

Phishing is a type of online scam. Where cybercriminals use email, texts, or social media posts to convince you to give away sensitive information – usually by clicking a dangerous link, or opening an attachment.

Often these messages appear to come from legitimate sources, such as a bank, government agency or other well-known organization. However, they can introduce dangerous software to your computer, allowing criminals to access your business accounts and other key information.

Make sure your employees know how to spot a scam

- Scams often include poor grammar and spelling or website URLs that are slightly different from legitimate sites
- Legitimate sources won't ask for sensitive or financial information
- Scams usually ask you to open an attachment or link
- Scams urge you to act quickly to avoid something bad happening

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 Your Business Safe

PUBLIC SAFETY STRATEGY
TAKING ACTION TOGETHER

Cyber Security Outreach Program

We live in an increasingly connected online world. Protecting businesses from cyber threats is no longer optional, even for small businesses. An important element of the City's Public Safety Strategy, Be Safe Online is a new cyber security outreach program that provides trusted and actionable information to help business owners protect their operations from cybercrime.

While cyber criminals are becoming better organized and more sophisticated, there are some simple things you can do today to lower your risk from cyber intrusions.

Critical Cyber Risks for Businesses

Theft of financial data and funds from business accounts

Malicious software (malware and ransomware) infecting and crashing your systems

Security of portable devices (cellphones, tablets, laptops)

Protect your business data to prevent

- Loss of trademark/proprietary information
- Release of sensitive customer data
- Damage to your brand and reputation

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 and your financial data by using a strong password or a passphrase and, for heightened security, use two-step verification.

You should also limit account access to key staff.

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. First you enter your password or passphrase and then you 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

PROTECTING YOUR

Small-Medium Size Business

The Internet has revolutionized the way we do business. It has become an essential tool in supporting day-to-day operations and the ability to thrive in today's economy.

As your small or medium sized business becomes more reliant on modern digital applications, it's important to understand the various cyber security risks so you can better protect your business and employees from cybercrime.

In a year up to two-thirds of Canadian businesses experience some kind of cyber-attack, costing them approximately $5.3 million, or about $15,000 per attack. According to the Symantec 2013 Internet Security Threat Report, the largest growth area for targeted cyber-attacks in 2012 was businesses with fewer than 250 employees — 31% of all attacks targeted them.

Achieving and maintaining cyber security is an ongoing process. Good cyber security involves the following:

- Determining what assets you need to secure (essentially, anything of value managed or owned by your business).
- Identifying the threats and risks that could affect those assets or your business overall.
- Identifying what safeguards you should put in place to deal with threats and secure assets.
- Monitoring your safeguards and assets to prevent or manage security breaches.
- Responding to cyber security issues as they occur (such as an attempt to break into business systems).
- Updating and adjusting to safeguards as needed (in response to changes in assets, threats and risks).