SMBs' GUIDE TO STAYING CYBER SAFE DURING COVID-19

During the COVID-19 pandemic, it hasn't been business-as-usual for many businesses. This disruption makes it more important than ever to make sure yours is staying cyber safe.

COVID-19 has showed us how quickly the world can change, but the need to stay cyber safe hasn't. Educating employees on cyber safe business practices is key to protecting your company from cyber attacks.

KEEP YOUR WORKPLACE SAFE WITH THESE SIMPLE STEPS

ADOPT A CYBER SECURITY POLICY

It's impossible for any employee to know every cyber threat out there, but clear cyber security rules can help everyone make better decisions when faced with one.

An effective cyber security policy should cover:

INTERNET USAGE GUIDELINES

RULES FOR EMAIL SAFETY

SOCIAL MEDIA GUIDELINES

PRACTICE SAFE PASSWORDS

All employees should use a **passphrase**, a series of at least four words and 15 characters in length.

Or use **complex passwords** with:

- At least 12 characters
- Upper and lower case letters, numbers and symbols
- No personal information

USE A DIFFERENT PASSWORD FOR EVERY ACCOUNT

NEVER SHARE YOUR PASSWORDS WITH ANYONE

CHANGE YOUR PASSWORDS IF AN ACCOUNT HAS BEEN COMPROMISED

ENABLE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) uses two or more different ways of verifying that you are who you say you are to add an extra layer of protection to your accounts and devices. We call these **authentication factors**.

Some different types of authentication factors include:

- Proof of **who you are**, like fingerprint scanners or facial recognition
- Proof of **what you know**, like a security question or password
- Proof of **what you own**, like a USB key

If many people in your business need to access business accounts or devices, make sure they all have their own ways to verify who they say they are. You can control which employees or visitors have access to your accounts.

DON'T TAKE THE BAIT

Businesses are key targets of **phishing and spear-phishing scams**, where cyber criminals, often masquerading as employees, will ask for sensitive company information, like passwords or financial info.

If you receive an unexpected email, even if it looks like it's being sent from a colleague, here's what to do:

BREATHE. Phishing messages often pressure or threaten you to respond quickly. If an email needs you to "act now", it could be a scam.

DON'T OPEN ANY LINKS OR ATTACHMENTS you're unsure of. Reach out to the sender through a different channel, like by phone, to confirm.

TALK TO TECH SUPPORT. Unsolicited messages asking you to reset a password or update account info are likely fake.

DELETE ANY MESSAGES THAT SEEM TOO GOOD TO BE TRUE, like winning a contest you didn't enter.

GET MORE TIPS TO PROTECT YOURSELF, YOUR BUSINESS AND YOUR DEVICES AT **GETCYBERSAFE.CA**

FOLLOW US ON SOCIAL MEDIA **@GETCYBERSAFE**

Communications Security Establishment
Centre de la sécurité des télécommunications
Canada