# A SELLER'S GUIDE TO STAYING CYBER SAFE DURING COVID-19

During the COVID-19 pandemic, it hasn't been business-as-usual for many businesses. This is especially true for brick-and-mortar stores that have had to take their shops online, opening up to a whole new crowd of customers – and a new collection of risks.

COVID-19 has showed us how quickly the world can change, but the need to stay cyber safe hasn't. Being aware of cyber safe selling practices is key to protecting your online store from cyber attacks.

## KEEP YOUR STORE SAFE WITH THESE SIMPLE STEPS

### USE A SECURE E-COMMERCE PLATFORM

When you're searching for the right platform for your online business, make sure that cyber safety plays a role in your decision. Research the security features offered by each platform, including:

**MULTI-FACTOR AUTHENTICATION**

**CUSTOMER DATA ENCRYPTION**

**REAL-TIME THREAT ALERTS**

A secure platform doesn't just keep your business safe – it keeps your customers happy too. Your customers won't be satisfied if their personal and financial information is stolen or exposed.

### 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)** adds an extra layer of protection for your accounts and devices. MFA uses two or more different ways of verifying that you are who you say you are – 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

### DON'T TAKE THE BAIT

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

**IF YOU RECEIVE AN UNEXPECTED EMAIL, EVEN IF IT LOOKS LIKE IT'S 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