


Digital Security Checklist

Brought to you by 

Being proactive about digital security for your business may not be at the top of your list. But with cybersecurity and fraud threats getting more sophisticated, it's critical to invest some time to avoid scams that could cause you major headaches.

You can take charge and prevent damage to your business from fraud attempts. Complete the checklist below to strengthen your digital security.

1. EMAIL AND BANK ACCOUNTS

- Review your passwords across your email, bank and other critical accounts. Make sure the passwords are strong, unique, and have not been duplicated across multiple accounts. If not, change them.



Hint

Strong pA\$\$w0rDz are often "ugly," with a mix of upper and lowercase letters, numbers and symbols.

- Set up two-factor or multi-factor authentication on your accounts when available

ONGOING



Change your passwords regularly. (Maybe set a three month reminder?) And consider setting up separate business and personal accounts to help contain the damage from any security issues that might happen.

2. SOCIAL MEDIA

- Review your data privacy settings across all platforms. When in doubt, lock it down. (For example, don't show your date of birth.)
- Enable two-/multi-factor authentication wherever it is available.
- Vet your passwords to make sure they can't be guessed from your profile or posts.



Hint

Don't use your pets' or kids' names as passwords.

- Verify the account recovery contact details on each platform you use. Make sure they're up to date, and you're in control as the business owner.
- Look at what personal details you're sharing online. Are there any that you'd rather keep out of hackers' hands?

ONGOING



Don't include sensitive business information in your posts. Be wary of any messages asking about sensitive information or about yourself or any staff or contractors you may have.

3. ELECTRONIC DEVICES

- Make sure your devices are set up to require a password to log in. (Biometrics too, if that applies.)
- Check for software and operating system updates. Make sure you're set up to download updates automatically so you'll have the latest digital security settings and all bug fixes installed.
- Consider installing anti-virus software on your devices. (Ask an IT whiz for advice if you're not sure.)

ONGOING



Change your passwords regularly. And while you may love your favourite coffee shop, avoid completing sensitive tasks on public WiFi.

4. CLOUD DATA

- Vet your cloud service providers carefully by finding out, or asking for, their data protection policies. Consider consulting an expert for advice about who's a trustworthy cloud service provider.
- If you store any client data (especially sensitive information), get advice from a lawyer to make sure you're doing everything that's required to keep the data secure.
- Be careful what you leave in the cloud. Delete old files you don't need anymore, especially if they contain sensitive information.

ONGOING



Log out of your cloud services when you're not using them.

Remember: Follow your own instincts — They're ultimately your most important line of defence!

Disclaimer: This document offers general information only and is not intended as financial, legal or other professional advice. While information presented is believed to be factual and current its accuracy is not guaranteed and it should not be regarded as a complete analysis of the subject matter discussed. No endorsement of any third parties or their advice, opinions, information, products or services is expressly given or implied by Interac Corp.