

OCTOBER 2026 / FREE FIVE-PAGE GUIDE

Protect yourself. Protect your business.

A practical guide to reducing everyday cyber risk, at home and at work.



START WITH FIVE ESSENTIALS

- ☐ Use a unique password for each important account.
- ☐ Turn on multi-factor authentication (MFA).
- ☐ Pause and verify unexpected requests.
- ☐ Install updates and keep a separate backup.
- ☐ Know who to contact if something goes wrong.

Use the next four pages as a checklist. Choose one action, complete it, then move to the next.

Protect your accounts.

Start with your main email account: it is often used to reset access to your other services.

01 Use a password manager

Give every account a unique password or a long passphrase. Let a trusted password manager generate and store passwords. Protect the manager itself with a strong master passphrase and MFA. [1]

02 Add a second sign-in check

Enable MFA wherever it is offered. Use passkeys or hardware security keys when available; these can resist phishing. Otherwise, use a supported authenticator or another available MFA method. Never approve a sign-in you did not start. [2, 12]

03 Keep recovery access safe

Check your recovery email and phone number. Store backup codes somewhere protected and separate from the device you use to sign in. Do not share passwords or verification codes with callers. [2, 10]

Pause. Verify. Then act.

An urgent invoice, a shared-file link or a message from a familiar name can still be a scam. Open the known app or type the official address yourself. Verify unusual requests through a contact method you already trust. [3]

Example: “Our bank details changed. Pay today.” Call the supplier using a number already in your records before changing payment instructions. A polished message is not proof of identity.

Secure devices and Wi-Fi.

Include computers, phones, browsers, applications and the router that connects them.

01 Install updates

Enable automatic updates where practical and complete required restarts. Use the device or app's own update settings, rather than a pop-up link. Replace or upgrade software that no longer receives security fixes. [4]

02 Use trusted software and protection

Install apps from official sources. Keep built-in security protection and the firewall enabled. For a work device, follow the IT provider's approved tools and update process. [6, 8]

03 Limit everyday access

Lock the screen when you leave. Use a standard account for routine work when practical, and reserve administrator access for approved changes. Ask IT about device encryption and recovery-key storage. [6, 8]

04 Review your Wi-Fi

Change the router's default administrator credentials and use a unique Wi-Fi password. Keep its firmware current. Use a separate guest network for visitors and smart devices where supported. [5]

STOP / VERIFY

Unexpected "support" call? Do not install a remote-control app at a stranger's request. Contact your known IT provider through its usual number. [3]

Keep a copy you can restore.

Decide what you would need after a lost laptop, a failed drive or an attack.

01 Choose what matters

List essential files, photos, business documents and cloud data. Identify who owns the backup and how much recent work you could afford to lose. Use this to choose a backup schedule. [6, 7]

02 Separate the backup

Keep more than one copy and keep a copy away from the original location. A disconnected backup can reduce exposure to ransomware. Protect cloud backup access with a unique password and MFA. [7, 9]

03 Check the result

Review failed jobs and storage warnings. Test restoring a sample file to a safe location and open it. Record the date, the result and the next check. A “completed” status alone does not prove every file is recoverable. [7]

REMEMBER

Cloud sync is not a complete recovery plan. Check version history, retention, deleted-file recovery and what happens if an account is compromised. For work data, agree independent backup coverage with your provider. [7, 8]

YOUR NEXT BACKUP CHECK

Important files or systems

Backup owner and location

Date and result of the last restore test

If you suspect an attack.

Act calmly. Use a separate trusted device to contact help if your normal device or email may be compromised.

01

Contain

For suspected malware or ransomware, disconnect the affected device from Wi-Fi, Ethernet and other networks, then stop using it. Contact IT promptly. Ask for guidance before restarting, wiping or reconnecting it; the right action depends on the incident. [9, 11]

02

Protect accounts

For a compromised account, use the provider's official recovery process from a trusted device. Reset the password, revoke sessions and review recovery details, MFA methods and email forwarding with IT or the provider. [10, 11]

03

Record and recover

Record the time, affected systems and messages safely. Keep backups isolated. Restore only into a clean environment after the cause is addressed. If financial details were exposed, contact the institution using its official channel. [9, 11]

Need help making a plan?

Talk to DITC about accounts, devices and backups. Availability, work scope and fees are agreed before an engagement.

ditc.ca | support@ditc.ca | 514 970-5667

SOURCES & FURTHER READING

- | | |
|---|---|
| 1. Passphrases and passwords | 7. Backup and restore tips |
| 2. Multi-factor authentication | 8. Baseline security controls |
| 3. Recognize phishing | 9. Ransomware response |
| 4. Software updates | 10. Recover a hacked account |
| 5. Family and Wi-Fi security | 11. Contain and recover from malware |
| 6. Small-organization foundations | 12. Phishing-resistant authentication |

Source links open official Canadian guidance. DITC is an independent business; no government endorsement is implied.

General education, not a security guarantee. Follow your workplace policies and obtain help appropriate to your situation.