2727 COWORKING / RESEARCH & PRACTICAL GUIDANCE

Remote Work Security Checklist for Small Businesses in Canada

> Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Published by 2727 Coworking · 2026-10-01 · remote work security checklist · small business cybersecurity · canada · public wifi security · coworking cybersecurity · home office security · byod · multifactor authentication · client data

Original article: https://2727coworking.com/articles/canadian-remote-work-security-checklist

In this article

1. Executive Summary
2. Introduction and Background
3. Home Office
4. Café and Public Space
5. Coworking Space
6. Client Site
7. Feature Comparison
8. Performance and Benchmarks
9. Data Analysis and Evidence
10. Implications and Future Directions
11. Frequently Asked Questions (FAQs)
12. Conclusion

Executive Summary

A Canadian remote work security checklist begins with the **task**, then the **device**, **connection**, **surroundings**, and **response contact**. A home office can support confidential work when the household network and physical space are controlled; a café is usually best limited to public or low sensitivity tasks; a coworking desk is conditional on the worker's controls and the venue's answers; a client site requires the client's access rules. This is an editorial decision framework, not a certification of any location. The Canadian Centre for Cyber Security recommends organization owned devices where possible, automatic updates, backups, and access limited to job needs. (www.cyber.gc.ca) (www.cyber.gc.ca) (www.cyber.gc.ca) (www.cyber.gc.ca)

Public Wi-Fi is a conditional risk, not a blanket claim that every session is unsafe. The US Federal Trade Commission notes that widespread website encryption improves safety for ordinary web browsing, while the Canadian Cyber Centre advises avoiding public Wi-Fi for business when possible. A cellular connection or known network can reduce exposure; a virtual private network (VPN) helps only with traffic routed through it and cannot stop a user from opening a malicious link. Check a venue's network name with staff, and keep confidential screens and calls out of open sight and hearing. (consumer.ftc.gov) (www.cyber.gc.ca) (www.cyber.gc.ca) (www.ncsc.gov.uk) (www.cyber.gc.ca) (www.getcybersafe.gc.ca)

The minimum operating set is named accounts, multifactor authentication (MFA), supported and updated devices, full-disk encryption on portable devices, restorable backups, a short screen lock, least privilege, and a known route for reporting a lost device or suspicious message. NIST recommends full-disk encryption on portable laptops and tablets. (tsapps.nist.gov) Get Cyber Safe addresses small businesses directly and recommends a plan covering personal devices; the RCMP's physical-security advice is written for Government of Canada personnel and is adapted here as practical guidance, not a private-sector legal duty. (www.getcybersafe.gc.ca) (www.getcybersafe.gc.ca) (www.nist.gov) (www.cyber.gc.ca) (rcmp.ca)

The quantitative evidence describes control uptake, not relative safety of venues. In Statistics Canada's **2023** survey of firms with **10 or more employees**, **16%** reported a cyber security incident; the final sample was **12,462 enterprises** with a **71% response rate**. Its scope excludes microbusinesses with fewer than ten

employees. Neither that survey nor the venue guidance provides a defensible probability that a particular café, home, or coworking space is secure. Use the printable matrix below to approve a specific task and record the compensating control and owner. (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca)

Introduction and Background

A freelancer drafting a public proposal in a café, a startup employee reviewing client records at home, and a consultant joining a private call at a client site face different exposures. The same laptop can be well configured in every setting yet show confidential material to a neighbour, leave papers on a printer, or join a lookalike hotspot. This report compares **home**, **café**, **coworking**, and **client site** work as operating environments. It answers whether a task should be done there and which conditions must be true first. The Cyber Centre identifies physical access and spoofed Wi-Fi among remote-work concerns, and the Australian Cyber Security Centre advises avoiding sensitive information in public locations. (www.cyber.gc.ca) (www.cyber.gov.au)

For this guide, **public** means material approved for anyone to see; **internal** means ordinary non-public business work; **confidential/client** means data subject to a customer commitment or meaningful commercial harm if exposed; **regulated/high sensitivity** means work whose contractual or sector requirements deserve a qualified security and privacy review. These are editorial decision categories, not statutory classifications. A small business should record its own classification and any customer restrictions before picking a workspace. The Canadian Cyber Centre's baseline addresses organizations with fewer than **500 employees**, but its advice does not replace a microbusiness's own judgment about higher-consequence information. (www.cyber.gc.ca)

The checklist separates **worker controls**, **business controls**, **platform controls**, and **workspace-provider controls**. A venue can supply a room and connectivity; it cannot decide which employee should access a client's file or whether a personal laptop may store it. Get Cyber Safe advises small businesses to set expectations for activity on personal devices, while the Cyber Centre advises limiting access to what each job needs. (www.getcybersafe.gc.ca) (www.cyber.gc.ca) Where personal information is involved, obtain appropriate privacy or legal advice for the business and client context; eligible businesses can seek an advisory consultation from the Office of the Privacy Commissioner of Canada. (www.priv.gc.ca)

Home Office

Capabilities

A home office usually gives a worker the most control over screen direction, doors, calls, and paper storage. It may be appropriate for confidential work if the business approves the device, the home network is maintained, and other household members cannot see or hear the material. **A room with a door** is a stronger physical control than merely moving a laptop to a quieter corner. The RCMP recommends positioning remote workspaces to limit outside viewing, and Australian government guidance favours a private location for confidential web meetings. Both sources are government guidance being adapted to a private workplace. (rcmp.ca) (www.cyber.gov.au)

For a secure remote work setup, make the home network a deliberate choice. Confirm that the router is supported and configured for current security, that the work device does not share files with household devices, and that guests use a separate network if the equipment allows. The Cyber Centre explains that guest access should not expose the main network and advises separating guest and normal traffic. (www.cyber.gc.ca) (www.cyber.gc.ca) A personal hotspot may be preferable when the home network is uncertain, but it still leaves device, account, and physical controls to manage.

Adoption

The practical home checklist is short enough for a sole operator to repeat: use an approved account, confirm MFA, allow system and application updates, verify backup status, close the door for a client call, and put papers away when the work ends. Get Cyber Safe recommends MFA where available; NIST recommends testing backups, not simply assuming that a backup exists. (www.getcybersafe.gc.ca) (www.nist.gov) (chamber.ca) If a shared household computer cannot meet the business's device and separation rules, use a managed device or move the task. The Cyber Centre prefers corporately owned devices because the organization can control their settings. (www.cyber.gc.ca)

Strengths and Limitations

Home's strength is **control over the room**. Its limits are uneven router maintenance, other people in the space, and the possibility that a lost or damaged device also holds the only local copy. The business should maintain a securely stored backup, ideally including an offline recovery copy for critical information, and should know how to reach its support contact. (www.cyber.gc.ca) A home office is therefore **conditionally approved** for confidential/client work when those controls are verified. High sensitivity work still needs an explicit client or specialist decision, rather than a generic home-work assumption.

Café and Public Space

Capabilities

A café is useful for work whose content can safely be seen or overheard. It is a poor default for client records, private financial information, sensitive calls, or printing. The Australian Cyber Security Centre specifically advises against accessing sensitive information in public locations. Get Cyber Safe warns about someone viewing a screen over the worker's shoulder. (www.cyber.gov.au) (www.getcybersafe.gc.ca) A privacy filter and careful seating reduce casual observation but do not make a live confidential conversation private.

Public Wi-Fi deserves a precise answer. The FTC says encryption on modern websites means public Wi-Fi is usually safe for ordinary web browsing, while the Cyber Centre recommends avoiding it for business where possible. These statements are compatible: transport encryption mitigates one network risk, but a business still has to assess spoofed networks, exposed devices, application security, and task sensitivity. (consumer.ftc.gov) (www.cyber.gc.ca) A malicious hotspot can imitate a café's network name, so ask staff for the exact network name and turn off automatic joining of unknown networks. (www.cyber.gc.ca) (www.getcybersafe.gc.ca)

Adoption

For public or low sensitivity work, use a supported device, MFA, a locked screen when stepping away, and a known encrypted service. If the business requires VPN access, connect it before using business resources and confirm it remains active. The Cyber Centre says VPN security depends on configuration and consistent use, and the UK National Cyber Security Centre notes that only traffic routed through the VPN gains its protection. (www.ncsc.gov.uk) When uncertain about a hotspot, switch to cellular data or defer the task.

Keep the device with the worker or lock it away when it cannot be supervised. A cable lock can add friction but is not permission to leave client data unattended. University of British Columbia guidance suggests a cable lock in shared or public spaces, while UK guidance recommends carrying or locking away an unsupervised device. (privacymatters.ubc.ca) (www.ncsc.gov.uk) Avoid speakerphone calls, sensitive printouts, and visible notes. A public-space session should have a clear end: close the application, collect belongings, and confirm the device reconnects only to an intended network.

Strengths and Limitations

A café's strength is convenience for **public or low sensitivity tasks**. Its limitation is lack of control over neighbouring people, network administration, and confidential conversations. The rule is **not approved for confidential/client or high sensitivity work** unless a specific exception has been reviewed and compensating controls genuinely address every exposure. A VPN cannot stop phishing or shoulder surfing. (www.getcybersafe.gc.ca) For most microbusinesses, deferring a sensitive task is cheaper and easier than trying to engineer a private room inside an open café.

Coworking Space

Capabilities

Coworking can offer desks, meeting rooms, and a support contact, but availability varies by site and membership. The security decision should distinguish an **open desk** from a **bookable private room**, and both from the business's own account and device controls. The RCMP's shared-space guidance recommends meeting or quiet rooms when a conversation needs privacy, separate Wi-Fi for visitors and shared-space users, and a central point of contact for security concerns. Its intended government setting should be disclosed when adapting those questions to a commercial venue. (rcmp.ca) (rcmp.ca) (rcmp.ca)

Ask a provider whether guest and member traffic are separated, whether devices on the same wireless network can communicate with one another, who handles network problems, and how a worker can report a physical concern. These are **questions**, not claims that a particular venue has those controls. The Cyber Centre recommends restricting guest devices from interacting with primary-network devices; that principle makes separation an appropriate provider question. Ask whether a private room is available for a confidential call and whether printing uses a release code or immediate pickup. Ontario's public-sector standard calls for prompt retrieval of printed documents, a useful practical control to adapt without presenting it as a duty for private coworking users. (www.ontario.ca)

Adoption

A member should verify the intended network name, apply the company's device and MFA rules, position the screen, and decide where papers will go at the end of the session. The worker, not the venue, decides whether a file may be downloaded to a personal device. The Cyber Centre recommends defining which data classes can be accessed or stored on bring-your-own-device (BYOD) equipment. (www.cyber.gc.ca) Before a sensitive meeting, use a room whose door and audio conditions have actually been checked. Do not assume that a phone booth, shared room, or alarm system controls network traffic.

Strengths and Limitations

A coworking space can be **conditionally approved** for internal work and, after specific verification, confidential work. The extra value is a possible private room and a place to ask operational questions; neither makes the venue automatically secure. For example, **2727 Coworking** advertises hot desks, dedicated desks, private offices, and gigabit internet in Montreal, with a hot desk listed from **$300 per month** as of October 2026. Its published pages do not establish network segmentation, device isolation, or an incident contact for a customer's data; a user should ask the operator directly before approving confidential work. (2727coworking.com) (2727coworking.com) (2727coworking.com) The business still owns access permissions, backup, and incident response. (www.getcybersafe.gc.ca)

Client Site

Capabilities

At a client's premises, the client controls some physical and network conditions, but the visiting business remains responsible for its own device, accounts, and handling of its copies of information. A client may supply a desk, guest network, printer, or meeting room. Treat each as **unverified until the client explains permitted use**. The Cyber Centre's baseline says visitor Wi-Fi should be separate from internal resources, and the RCMP's shared-space advice supports a clear reporting contact and private conversation space. (rcmp.ca) (rcmp.ca)

The initial question is which party's rules govern the task. A visiting consultant should get the client's approved connection method and confirm whether local downloading, personal devices, or printing is permitted. The Cyber Centre's BYOD guidance recommends specifying what data may be accessed, developed, or stored on personal devices. (www.cyber.gc.ca) If the client provides a workstation, do not assume it can be used for the visitor's other customers. Use distinct accounts and only the permissions required for the assignment, consistent with NIST's account guidance. (www.nist.gov)

Adoption

Before beginning, confirm the host contact, authorized network, meeting room, file transfer method, and paper disposal route. Keep devices and documents in sight during travel; RCMP guidance says sensitive information or assets should not be left unattended in transit. (rcmp.ca) For video calls, share the needed application

rather than the entire desktop when possible, as the Australian Cyber Security Centre advises. (www.cyber.gov.au) At departure, collect printed pages and notes, sign out of a borrowed station, and record any unresolved access or document issue.

Strengths and Limitations

The client's site may be the only approved environment for some **regulated or high sensitivity** work, but being on site does not automatically authorize every workflow. The client may forbid a personal laptop, require its own isolated environment, or restrict what can leave the premises. The business should seek explicit project instructions and qualified security review when the information category is high consequence. A visiting worker should never infer a legal permission from the presence of a network port or printer. The practical decision is **conditional on client authorization** and documented controls.

Feature Comparison

Table 1 is a printable task-to-location matrix. “Conditional” means the listed control must be checked for the specific task; it is not a risk score. Each row assumes an approved account, MFA, a supported device, backup, and a reporting contact. The assessments are this report's operational synthesis of Canadian cyber guidance, physical-security guidance, and the public-Wi-Fi distinction above. (www.getcybersafe.gc.ca) (rcmp.ca) (consumer.ftc.gov)

Location and task	Work sensitivity	Network control	Device ownership	Screen and audio	Paper and printing	Storage	Decision	Compensating control	Owner
Home office	Public, internal, or confidential/ client	Household router checked; separate guest use where possible (www.cyber.gc.ca)	Managed preferred; BYOD by written rule (www.getcybersafe.gc.ca)	Door, screen position, private calls (rcmp.ca)	Lock paper away; avoid shared printer trays (mednet.med.ubc.ca)	Approved cloud or encrypted local storage, with backup	**Conditional approval** for confidential work; high sensitivity requires review	Cellular fallback, private room, managed device	Business and worker
Café or public space	Public or low sensitivity internal work	Verify network name; use cellular if uncertain (www.getcybersafe.gc.ca)	Managed device preferred	Assume bystanders can see and hear (www.cyber.gov.au)	No sensitive printing or loose notes	Avoid local confidential copies	**Approved only for low sensitivity**; confidential work normally **not approved**	Defer task or move to private room	Business and worker

Location and task	Work sensitivity	Network control	Device ownership	Screen and audio	Paper and printing	Storage	Decision	Compensating control	Owner
Generic coworking open desk or private room	Internal; confidential only after checks	Ask about member, guest, and device separation (rcmp.ca)	Business approves device	Open desk exposes screens; private room for calls (rcmp.ca)	Ask about release printing and disposal (www.ontario.ca)	Business-managed storage and backup	**Conditional approval**, based on task and verified room/network	Private room, cellular, no local download	Business, worker, provider
2727 Coworking, Montreal	Same task rules as coworking	Gigabit internet advertised; network security details must be confirmed (2727coworking.com)	Business approves device	Hot desks and private offices advertised (2727coworking.com)	Confirm printing and disposal on site	Business-managed storage and backup	**Conditional approval**, not a security endorsement	Ask operator about separation and response contact	Business, worker, 2727 for venue facts
Client site	Client-approved tasks only	Use client's authorized method	Follow client and employer device rules	Confirm room and call permissions	Confirm client's print, collection, and disposal rules	Follow project data-location instructions	**Conditional on client authorization**	Written task instructions and host contact	Client, business, worker

The matrix should be filled in for a **specific task**, not used as a one-time badge for a venue. A confidential call may be acceptable in a private coworking room while the same information should not appear on an open desk. The table's “not approved” designation is a conservative editorial default for microbusinesses, not a statement that a provider's facility has failed a test. If the client imposes tighter instructions, those instructions govern the work.

Table 2 allocates control ownership. A venue's physical amenities cannot replace decisions about account permissions, backups, or data classification. Get Cyber Safe calls for a business cyber plan, and the Cyber Centre says employees should know whom to contact when a device is lost. (www.getcybersafe.gc.ca)

Control	Worker	Business or employer	Platform or service	Workspace provider or client host
Task classification and allowed location	Follow instruction	Set decision and exceptions	Enforce data permissions where configured	State site and client restrictions
Accounts and MFA	Use own account and challenge	Provision, review, remove access (www.getcybersafe.gc.ca)	Supply MFA and logs	Manage only venue accounts, if any

Control	Worker	Business or employer	Platform or service	Workspace provider or client host
Device and updates	Keep device locked and report loss	Approve ownership, updates, encryption	Offer device controls where contracted	State equipment rules
Connection	Verify network name and VPN status	Set connection policy	Protect routed traffic, as configured (www.ncsc.gov.uk)	Explain guest/member separation
Screens, calls, and paper	Position screen, use room, collect pages	Specify allowed handling	Offer sharing and storage controls	Supply room and print process, if available
Backup and response	Report promptly	Test recovery and lead incident response (www.nist.gov)	Retain or restore data under contract	Give a venue support contact (rcmp.ca)

The business owns the final approval decision because it understands the data and customer obligations. The platform controls only the service it supplies, and the workspace provider controls only its facilities and network. A sole proprietor may fill both worker and business columns, but should still make each decision explicitly.

Table 3 is a provider-question sheet. Record the answer, date, and name of the person who gave it before relying on the venue for sensitive work. The questions follow the Cyber Centre's guest-network guidance and the RCMP's shared-space recommendations, adapted to a commercial workspace. (rcmp.ca) (rcmp.ca)

Ask the workspace or client host	What a useful answer identifies	If unanswered
Which network is for members, guests, and staff?	Exact network names and who may use each	Use approved cellular access or defer
Can devices on the member or guest network reach one another?	Isolation or separation policy, and support contact	Do not infer isolation from a Wi-Fi password
Who handles a network or physical security concern?	Named role and reachable channel	Obtain a contact before sensitive work
Is a private room available for a client call?	Room access and audio privacy conditions	Move or reschedule the call
How are print jobs released, collected, and disposed of?	Pickup method and confidential disposal route	Do not print client material
What are the access and equipment rules?	Hours, visitor rules, approved devices, storage	Bring no sensitive equipment or paper

A **yes** is meaningful only if the answer addresses the actual workflow. “We have Wi-Fi” does not explain network separation; “we have meeting rooms” does not confirm that a room is available for a particular call. Record uncertainty as a reason to use a simpler task or a different location.

Performance and Benchmarks

There is no credible, comparable public benchmark in the fetched sources that assigns a probability of compromise to a home office, café, coworking desk, or client site. The available guidance identifies controls and exposures, so this report uses **decision gates**, not a fabricated location score. A VPN can protect traffic routed through it, but the Cyber Centre says it does not protect against clicking malicious links. (www.ncsc.gov.uk) A private office improves the audio and screen situation only if the worker actually uses it, while a properly isolated network addresses a different pathway. (rcmp.ca)

The nearest measurable benchmarks concern **program readiness**. The Cyber Centre prioritizes four starting areas for small and medium organizations: incident response planning, patching, strong authentication, and backup with encryption. (www.cyber.gc.ca) The federal CyberSecure Canada information sheet describes a voluntary program based on **13 controls**. (ised-isde.canada.ca) Neither measure certifies that a particular café or coworking venue is suitable for client records. A small team can use the categories as a checklist and then test its own operational capability: can a device be locked or recovered, can a backup be restored, and can an account be disabled promptly? NIST expressly recommends testing backups. (www.nist.gov)

This distinction matters when comparing **home versus coworking security**. A home office may offer better control over bystanders but weaker provider support; a coworking site may offer a private room yet require extra checks about shared network and printing. The answer changes with the task and the controls in place. The report's matrix therefore records **approval, compensating control, and owner**, rather than a universal winner.

Data Analysis and Evidence

The available Canadian data describe business cyber practices, not venue safety. Statistics Canada's **2023** Canadian Survey of Cyber Security and Cybercrime covered enterprises with **10 or more employees**, so it does not directly measure freelancers or the smallest Montreal startups. Its final sample was **12,462** with a **71%** response rate. About **16%** of surveyed businesses reported being impacted by a cyber security incident; **26%** reported written cyber policies, and **22%** reported formal training for non-IT employees. These figures are useful context for why a short documented plan matters, but they cannot rank a café against a home office. (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca)

CIRA's **2022** cybersecurity survey gathered **500** online responses from Canadian cyber decision makers. **55%** characterized their organization as more vulnerable because employees worked remotely. That is a perception among respondents, not a measured venue-specific incident rate. CIRA's **2025** survey, also based on **500** decision makers, reported **98%** of respondents' organizations providing cyber training. The CIRA series and Statistics Canada survey use different populations and question wording, so their training figures are not a trend line or a contradiction. (www.cira.ca) (www.cira.ca) (www.cira.ca)

A **2024** Business Development Bank of Canada poll reported that **11%** of responding small businesses had a formal cyber incident response plan, while others described an informal plan or none. The poll is a directional indicator, not a probability for any one firm. (www.bdc.ca) The Office of the Privacy Commissioner of Canada's **2025 to 2026** business survey reported **65%** using MFA and **55%** using encryption for customer personal

information. These survey measures show uneven reported control adoption, but the populations and methods differ. They support asking whether a specific organization has implemented a control rather than assuming it has. (www.priv.gc.ca)

For an individual microbusiness, the most actionable quantitative measure is **completion of the local checklist**, not a borrowed national percentage. Record whether each required control is present, when it was last checked, and who owns the gap. If a high sensitivity task fails even one required gate, move it or seek specialist review. The Cyber Centre's backup guidance describes multiple copies, including an offline copy, and NIST recommends a restore test. These are concrete checks a small business can perform without inventing a risk score. (www.cyber.gc.ca) (www.nist.gov)

Implications and Future Directions

A ten-minute pre-work check

The following is a **yes/no** checklist for a session. A “no” means resolve the item, lower the task sensitivity, or change location. Ten minutes is a practical target for reviewing a prepared setup, not a claim that a new security program can be installed in ten minutes.

- **Task:** Is the information classified as public, internal, confidential/client, or high sensitivity, and is this location allowed?
- **Client rule:** Have any contract or project instructions about device, network, room, or printing been checked?
- **Account:** Is the worker using an individual approved account with MFA where available? (www.cisa.gov)
- **Permissions:** Is access limited to the files needed for this task?
- **Device:** Is the device approved, supported, updated, set for full-disk encryption, and set to lock when unattended? (www.cyber.gc.ca) (tsapps.nist.gov)
- **BYOD:** If it is personal, are the allowed data classes and removal method written down? (www.cyber.gc.ca) (www.priv.gc.ca)
- **Network:** Is the actual network name verified, and is a cellular or other approved fallback available? (www.getcybersafe.gc.ca)
- **VPN:** If required, is it active for the intended traffic, with its limitations understood? (www.ncsc.gov.uk)
- **Screen:** Can someone nearby see the display, whiteboard, notes, or notifications? (www.getcybersafe.gc.ca)
- **Audio:** Is a private room available for a confidential call? (www.cyber.gov.au)
- **Paper:** Will printouts be collected immediately and stored or disposed of properly? (www.ontario.ca)
- **Storage:** Is the approved file location available, with a recent recoverable backup? (www.nist.gov)
- **Response:** Does the worker know whom to contact about loss, phishing, or a venue problem? (rcmp.ca)

Lost device or suspected phishing response card

Keep this card with the work instructions, separate from the device. It assigns **immediate actions**, not a complete forensic procedure.

- **Lost device:** Report the loss to the business contact immediately; give the last known location, device identity, and whether it held local client files. UK guidance calls for immediate helpdesk contact. (www.ncsc.gov.uk)
- **Protect access:** Ask the account administrator to revoke sessions, rotate relevant credentials, and consider a preconfigured remote wipe or business-data container. The Privacy Commissioner describes a container that an organization can erase after a personal device is lost or stolen; it does not promise wiping will work while a device is offline. (www.priv.gc.ca)
- **Suspicious request:** Do not follow the message's call-back details. Verify with a known number or previously trusted channel. (www.ftc.gov)
- **Possible click or credential entry:** Contact the business lead; change compromised passwords and isolate a device suspected of malware according to the business procedure. (www.ftc.gov)
- **Preserve context:** Keep the suspicious email or text and relevant timestamps for the responder; the Canadian Anti-Fraud Centre advises preserving message copies and offers online reporting for fraud or cybercrime. (antifraudcentre-centreantifraude.ca) (antifraudcentre-centreantifraude.ca)

A small business should rehearse who receives the call and who can disable accounts. The Cyber Centre's remote-work guidance explicitly says workers should know whom to contact after a security issue or device loss. If personal information may be involved, seek appropriate privacy or legal advice for the facts and jurisdiction; the Privacy Commissioner has an advisory service for eligible businesses. (www.priv.gc.ca)

Frequently Asked Questions (FAQs)

Is it safe to work from a café on public Wi-Fi?

For **public or low sensitivity browsing**, often yes when the website connection is encrypted and the device is maintained; the FTC specifically cautions against treating all public Wi-Fi as automatically unsafe. For confidential business work, the Cyber Centre advises avoiding public Wi-Fi where possible, and the open room adds screen and audio exposure. Verify the hotspot name, use a business-approved connection, and move sensitive calls and records to a private setting. (consumer.ftc.gov) (www.getcybersafe.gc.ca) (www.cyber.gov.au)

What should a Canadian microbusiness put in its remote work cybersecurity checklist?

At minimum: task classification; approved account and MFA; supported and updated device; clear BYOD rules; known network; private screen and calls; controlled paper; restorable backup; limited permissions; and a reporting contact. This sequence combines Get Cyber Safe's small-business planning advice with the Cyber Centre's technical and response controls. (www.getcybersafe.gc.ca) (www.getcybersafe.gc.ca)

Is a coworking space more secure than a home office?

Neither setting wins automatically. The home worker may control the room and household network, while a coworking provider may offer a private room and a support contact. Ask about the actual network separation and room conditions, then approve the **specific task** in the matrix. RCMP shared-space guidance makes network separation and privacy rooms sensible questions; it is government guidance adapted to this commercial decision. (rcmp.ca) (rcmp.ca) (rcmp.ca)

Can a VPN make client work safe anywhere?

No. A VPN covers only traffic routed through it and does not stop a malicious link, someone viewing a screen, or an audible conversation. Use it when the business requires it, alongside MFA, device security, and a suitable room. (www.ncsc.gov.uk) (www.cyber.gov.au)

Conclusion

The useful unit of approval is **a task at a particular location under verified controls**. Home can support confidential work when the room, network, device, backup, and response route are controlled. A café usually suits public or low sensitivity work. Coworking can be suitable for more sensitive tasks after questions about network separation, private rooms, paper handling, and support receive usable answers. A client site requires the client's own authorization and workflow rules.

For a small Canadian business, the starting point is an approved device, individual account, MFA, updates, least privilege, backup that can be restored, and a named response contact. The worker then checks network identity and physical exposure before each session. A venue supplies part of the setting; the business supplies the decision about information and access. Use the matrix and yes/no card as living operating documents, and escalate high sensitivity or personal-information questions for qualified review. The aim is a repeatable approval process that a freelancer or small team can actually carry out.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.cyber.gc.ca/en/guidance/telework-security-issues-itsap10016
2. https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know
3. https://www.cyber.gc.ca/en/guidance/protecting-your-organization-while-using-wi-fi-itsap80009
4. https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
5. https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks
6. https://www.cyber.gc.ca/en/guidance/virtual-private-networks-itsap80101
7. https://www.getcybersafe.gc.ca/en/secure-your-connections/public-wi-fi
8. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957322
9. https://www.getcybersafe.gc.ca/en/blogs/staying-cyber-safe-when-your-employees-work-remotely
10. https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-businesses
11. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics

12. https://rcmp.ca/en/lead-security-agency-physical-security/guidance-and-publications/gcpsg-008-2022-physical-security-considerations-remote-and-telework-environments
13. https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm
14. https://www.cyber.gov.au/protect-yourself/staying-secure-online/security-tips-remote-working
15. https://www.priv.gc.ca/en/about-the-opc/what-we-do/advisory-services-businesses/
16. https://www.cyber.gov.au/business-government/protecting-devices-systems/remote-working-secure-mobility/remote-working/web-conferencing-security
17. https://www.cyber.gc.ca/en/guidance/guest-wi-fi-itsap80023?wbdisable=true
18. https://chamber.ca/canadian-small-business-cyber-security-survival-guide/
19. https://www.cyber.gc.ca/en/guidance/security-considerations-mobile-device-deployments-itsap70002
20. https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002
21. https://privacymatters.ubc.ca/news/your-laptops-quiet-vulnerabilities
22. https://www.ncsc.gov.uk/guidance/end-user-devices-advice-end-users
23. https://rcmp.ca/en/lead-security-agency-physical-security/guidance-and-publications/gcpsg-023-2025-physical-security-considerations-shared-space
24. https://www.ontario.ca/page/go-its-250-general-security-requirements?redirect_id=document%2Fgo-its-250-general-security-requirements&redirect_year=2021
25. https://www.cyber.gc.ca/en/guidance/end-user-device-security-bring-your-own-device-byod-deployment-models-itsm70003
26. https://2727coworking.com/
27. https://2727coworking.com/virtual-tour/
28. https://www.nist.gov/cyberframework/csf-11-quick-start-guide
29. https://mednet.med.ubc.ca/resources/facilities/hybrid-work-sharing-space/additional-resources-frequently-asked-questions-faqs/
30. https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035?UTMmessage=2024-05-30+-+Bulletin+CPA+-+Contacts
31. https://ised-isde.canada.ca/site/cybersecure-canada/en/cybersecure-canada-information-sheet
32. https://www.cira.ca/en/resources/documents/cybersecurity/2022-cira-cybersecurity-survey/
33. https://www.cira.ca/en/resources/documents/cybersecurity/2025-cybersecurity-survey/
34. https://www.bdc.ca/en/articles-tools/blog/cyberattacks-small-businesses-remain-denial
35. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2026/por_bus_2025-26/?wbdisable=true
36. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication
37. https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/gd_byod_201508/?wbdisable=true
38. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
39. https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm?t=tools&wbdisable=true

THE PUBLISHER

About 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore private offices, day passes and desks, the conference room, business addresses and virtual mailboxes. Book a visit or contact the team to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Website: https://2727coworking.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.