

We think we have been hacked: the first hour

A one-page plan for the moment something looks wrong. Print it and keep it somewhere that does not depend on your email working.

Free to use and adapt.

Before you do anything

Do not turn the computer off. Powering down can destroy evidence and, with some ransomware, makes recovery harder. Disconnect it from the network instead: unplug the cable, turn off Wi-Fi.

Do not delete anything. Not the suspicious email, not the strange file. You will need them.

Write down the time. Start a simple log now and keep adding to it. What you saw, when, and what you did. This matters later for your insurer and possibly your regulator.

The first fifteen minutes

- ☐ Disconnect affected devices from the network, but leave them powered on
- ☐ Tell one person who is coordinating. One channel, no rumour mill.
- ☐ Call your IT provider. Write their number in the table at the end of this page now, while things are calm.
- ☐ No IT provider, or cannot reach them? Brevity.Tech is on 778-321-2372 during business hours. If it is out of hours and serious, call your cyber insurer's incident line first. They run around the clock and you are already paying for it.
- ☐ Do not use the possibly-compromised email account to discuss it. Use phone or text.

The first hour

Order matters here. Remove the attacker's foothold **before** you reset the password, or they simply sign back in.

- ☐ **First:** check for multi-factor methods, phone numbers, or devices you do not recognise on the affected account, and remove them. An attacker who registered their own method can get straight back in after a password reset.
- ☐ Check for app passwords and OAuth app consents granted to apps you did not approve. These survive a password change.
- ☐ Now reset the password, from a device you trust
- ☐ Revoke all active sessions and tokens. A password change alone leaves signed-in phones working.
- ☐ Look for mail forwarding rules, inbox rules, and mailbox delegates you did not create. Forwarding rules are the single most common sign of a compromised mailbox.
- ☐ Check whether any payment details were changed or any payment was requested

- ☐ Export the sign-in and audit logs for the affected account now, before they age out of your retention window. You will want them later and they do not keep forever.
- ☐ Confirm your backups are intact and, critically, not reachable from the affected network

Then

- ☐ Contact your cyber insurer. Most policies require prompt notification, and many provide an incident response team as part of the cover.
- ☐ Decide, with advice, whether personal information was involved. What you must do next depends on which law reaches you. Most BC businesses fall under BC's PIPA, which requires reasonable security arrangements but does not require you to report a breach. The BC Privacy Commissioner recommends reporting voluntarily and has asked government to make it mandatory. PIPEDA is different. Where it applies, which is federally regulated businesses and personal information crossing provincial or national borders, a breach creating a real risk of significant harm must be reported to the Privacy Commissioner of Canada and to the people affected.
- ☐ Check what your professional body, your insurer, and your client contracts require. For a law firm or a clinic these usually ask for more than either statute, and they are the obligations most often missed.
- ☐ Keep a record of the breach either way. PIPEDA requires a two-year record where it applies. Even where nothing requires it, that record is the only way to reconstruct what happened for your insurer.

If it is ransomware

- ☐ Disconnect everything affected from the network immediately
- ☐ Do not pay anything before taking advice. Paying can be unlawful in some cases, because the recipient may be under sanctions. Your insurer's incident team runs that check. Paying also does not reliably get you back faster, and it does not undo the fact that data left.
- ☐ Call your insurer before making decisions. They usually have a panel who do this daily.

If it is a fraudulent payment

- ☐ Call your bank immediately. Speed is the only thing that matters.
- ☐ Report it to the Canadian Anti-Fraud Centre
- ☐ Preserve the emails. Do not delete or forward them around.

Numbers to fill in now, while it is calm

Who	Number
IT provider	
Cyber insurer / policy number	
Bank fraud line	

Who	Number
Owner or decision maker	

About this template. Free to use, edit, and share, including commercially. No credit needed and no permission required. It is a starting point built from common practice. It is not legal advice, not a compliance certification, and not a substitute for advice about your situation. Your obligations depend on your industry, your regulator, your insurer, and your contracts. If you are in a regulated field, have someone qualified review this before you rely on it.

Last reviewed: August 2026 · Latest version: brevitytech.ca/templates

Made by **Brevity.Tech**, managed IT and automation for small businesses in Metro Vancouver. If you would rather not find out how good your plan is during an actual incident, a free 30-minute check will tell you where you stand. brevitytech.ca · 778-321-2372