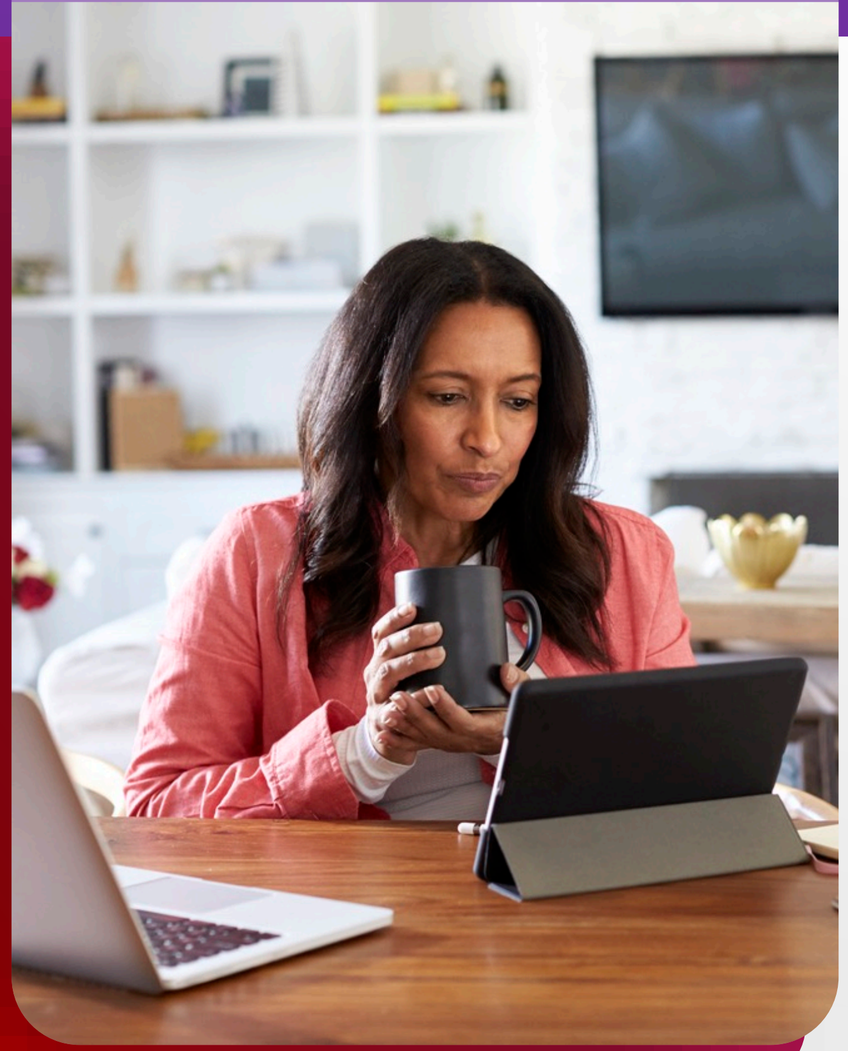
Cybersecurity for Remote Workers

HOW TO STAY SECURE ONLINE

WHEN WORKING FROM HOME

cira



Cybersecurity when working from home

Working from home is the new normal. Even before a global crisis, roughly half of Canadians were working from home a couple days per week.

Now, pretty much everyone who is able to is either working or studying from home for the foreseeable future.

Most offices and schools have some level of IT and cybersecurity protection for people on their networks. Unfortunately, most people do not have those same protections at home.

Just because you're cozy on the couch doing your work, it doesn't mean you're suddenly less vulnerable to cyber-attacks.

Whether you're working or studying from home, you're still using work devices, email addresses and systems. Getting attacked or compromised at home means other people in your organization are at risk as well.

This is why cybersecurity at home is extremely important.

Fortunately, you can do a lot to protect yourself when working from home with some simple tips and practices.

We're going to cover those in this course so you can protect yourself and your organization.

Six topics covered in this course

- **Secure** your home **Wi-Fi**
- Protect **confidential** information
- Use **strong passwords** and **multi-factor authentication**
- **Be careful** with personal devices
- Use a **VPN**
- Watch out for **phishing**

Protect your Wi-Fi

The most important part of your work-from-home setup is your Wi-Fi network.

Your network is the bridge that connects your devices with each other and the internet. If a bad actor were to gain access to your network, they can use this information to take over your devices and hold them for ransom, or steal your personal and financial information. They could also use this information to steal from your organization.

The first (and easiest!) step is to make sure your default administrative password and login for your router are changed. Many brands use common default credentials like “admin” and “password”, which make it easy for anyone to hijack their way in.

Other ways you can protect your home Wi-Fi

Enable WPA2 encryption

Encryption scrambles the information that your router exchanges with a device on your network, so only the device can see it.

This way, if someone is trying to sniff this data from outside your network, the data they get won't make any sense.

Create a guest network

You should turn on your guest network and use that for all of your personal devices, like IoT (internet of things) devices, smart speakers, game consoles, children's devices, and for anyone visiting.

Then, use your normal non-guest network only for work devices.

Replace old routers

Like all technology, older devices are less likely to get security updates from their manufacturer, and are more likely to have security vulnerabilities.

Replace routers every several years to take advantage of the latest security features and updates. You'll also likely get improved Wi-Fi coverage!

Watch out for public Wi-Fi

The café might make a great latté but they aren't cybersecurity experts (unless they took this course as well!) You have to assume that any shared, public, open Wi-Fi can put you at risk.

You should not use networks at cafés, hotels, and airports to access work documents or systems without additional protection, like a virtual private network (VPN).

If you do not have a VPN, but you do have a work phone, you can consider using it as a Wi-Fi hotspot to tether your laptop through a secure connection.

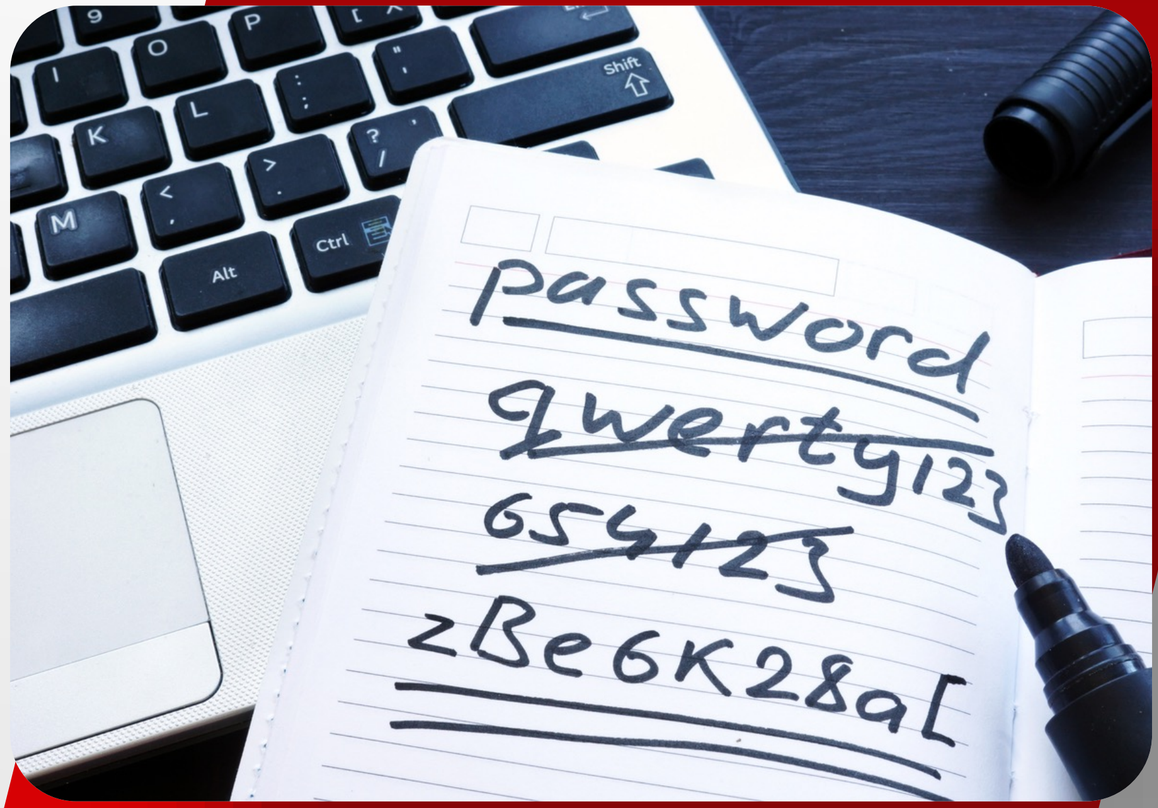
These can use a lot of data that your company has to pay for, so check with them first to see if your device allows it.

Create strong passwords

Strong, unique passwords are your most important form of protection from cyber-attacks.

Never, ever re-use passwords—especially between your personal and work accounts. Every account should have its own unique password.

It is very easy to identify which accounts are linked together, especially through email. If one of your accounts gets compromised, and that password is shared with another account, it won't be long before you lose both accounts.



What makes a password strong?

PRO TIP:

Remembering so many long, unique passwords is super tough, especially when people have so many accounts these days. This is where password managers come in, like LastPass or 1Password. They can generate strong passwords for you, and auto-populate them when you try to login to a website or app.

Make it long

Longer passwords are harder to crack. Make your password as long as possible. We recommend passwords that are at least 15 characters.

Use special characters

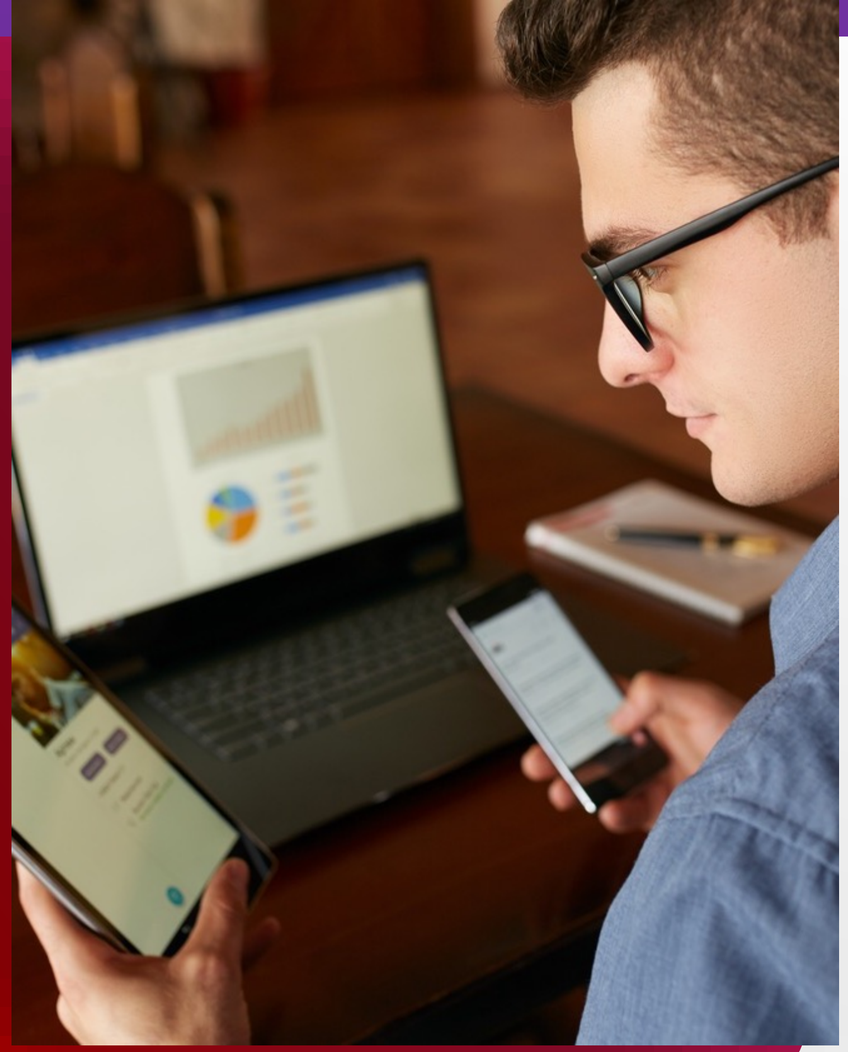
Include numbers, symbols and spaces in your password whenever possible.

Avoid patterns and personal words

Do not include personal information like birthdates and pet names in your passwords. These clues are usually posted on social media!

Avoid substitutions

Do not replace letters with numbers (like E and 3) on already short, weak passwords.



Use multi-factor authentication

Multi-factor (or two-factor) authentication is a way of confirming your identify using multiple factors beyond just a password.

These factors are usually something:

- You **know** (like a password)
- You **have** (like a token or SMS code)
- You **are** (like a fingerprint or face scan)

This is why some apps ask to send you a text code before you can login or verify an account. That's multi-factor authentication! If you have the option to set it up for a device or account, do it.

The best form of authentication is "token-based", which creates a single-use login code right when you need it. Popular apps for this include Google and Microsoft Authenticator.

Use a VPN

A VPN is a way to create a secure tunnel to another network over the internet. It's a powerful and simple way to protect the information you're sending and receiving when on your home network.

Many employers provide a VPN option that allows an employee's home computer to securely connect to their work network. Sometimes this is the only way to access certain files or systems.

If you're interested in getting a VPN, speak with your IT team. They can help you set up their preferred VPN correctly.

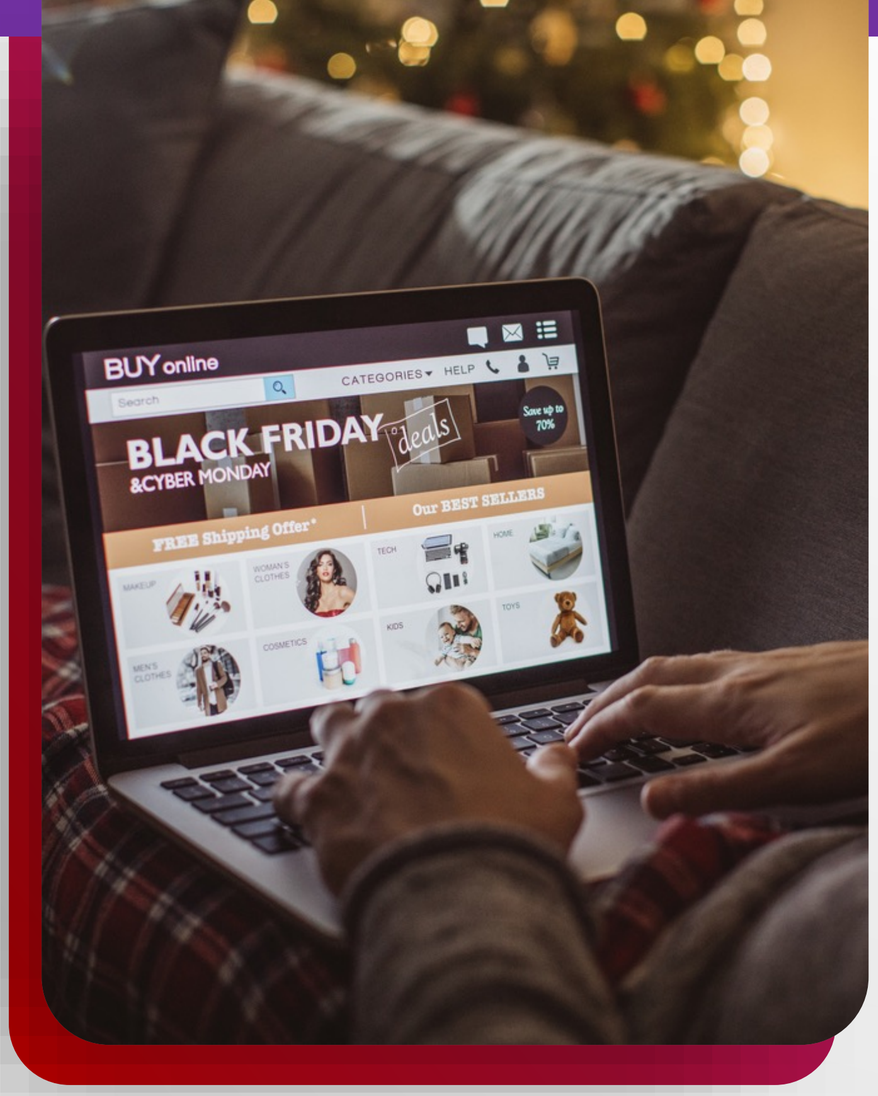
If you work in a smaller team, or you just want one for yourself, there are many cloud-based options that are easy to setup. With VPNs, you get what you pay for, so spend a little bit of money from a reputable vendor.

Protect confidential information

When you're working from home, you need to treat documents and information with the same level of privacy and confidentiality that you would if you were in an office.

At work, you usually have a clean-desk policy, where you can't leave documents or devices open for anyone to access. This is especially important in a household where family members or roommates could see confidential information.

Do not store files onto your personal device if you're using it for work. If you have to print documents, or save files to a USB drive, double check with your employer to see what your shredding, destruction, and file security policies are.



Protect personal devices

Before using a personal device for work, check with your employer about your Bring Your Own Device policies. You may need special security software or permissions added before you can use your personal devices to access work files or systems.

If you've logged in to a work system from a personal device, and your personal device gets compromised, your work systems can also become compromised.

Good digital hygiene for personal devices includes:

- Updating software and operating systems when prompted
- Only download verified apps from approved App stores
- Use anti-virus software

Device hygiene is extremely important when sharing your device with family members—you might not know what they're downloading!

Always update your devices

It's important to update all of your work and personal devices when prompted because updates might include important security and bug fixes.

If you're able to, turn on automatic updates so you never forget.

You can schedule automatic updates for the end of your workday, or overnight, so you're not tempted to hit snooze on your update when it happens.

Don't work near smart speakers

We don't want to spook you, but smart speakers listen to a lot of stuff, and those audio recordings are often saved somewhere that you don't have access to.

Some employers may have policies preventing you from working near them, because they may pick up audio from confidential calls and video conferences.

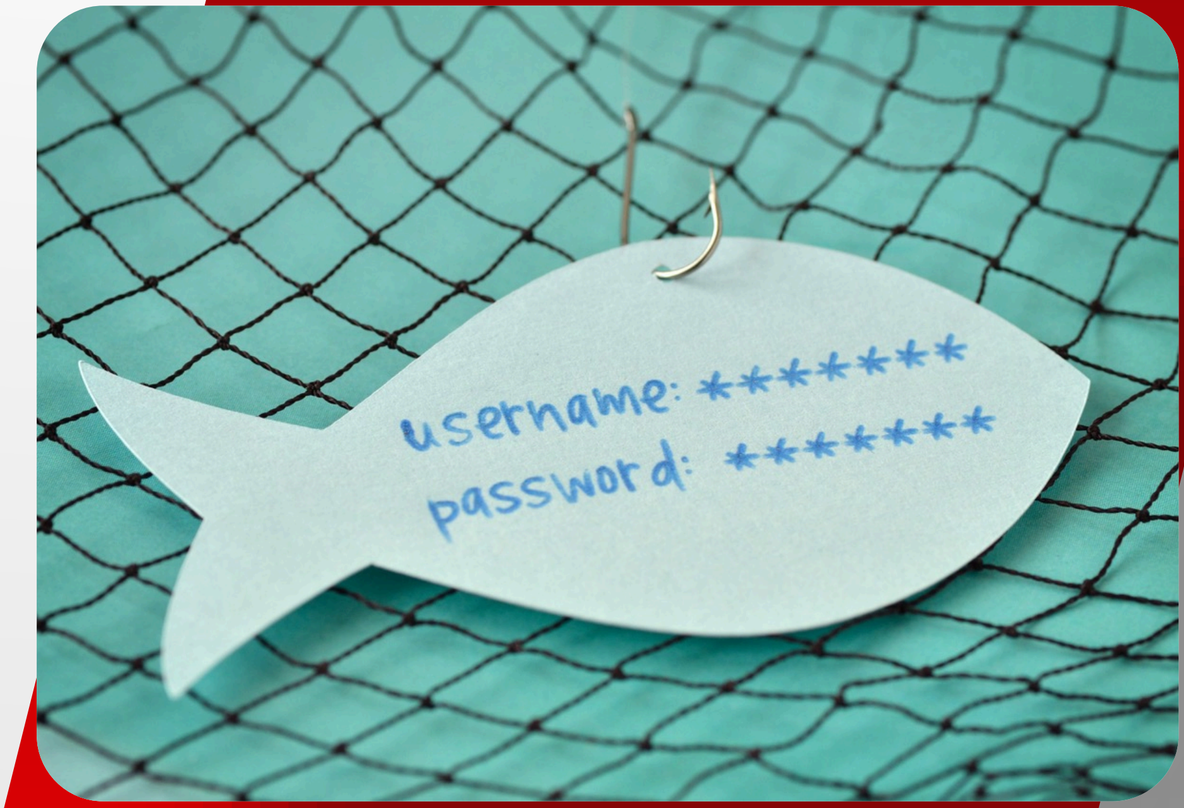
IoT devices are notorious for having poor security patching support, so in general it's a best practice to put them on a separate network and avoid working near them.

Keep an eye out for phishing scams

Phishing scams are where cyber criminals try to extract information, login credentials and even money from you by impersonating real people and companies through email, phone calls, text messages, and social media.

We're all familiar with the CRA phone scams, or fake text messages from Netflix or Apple asking to update your billing information.

These may seem silly and obvious, but the fact is, they work. Over 93% of all malicious data breaches in an organization come from scams that target people.



Financial scams

One common—and costly—phishing scam is the umbrella of scams trying to extract money from you by pretending to be your boss, payroll department, or a supplier of yours.

These types of scams can happen more easily when everyone is working remotely.

If someone in your organization is asking to transfer money, don't rely on just email, even if it's your boss.

Set up additional ways to verify financial transactions, like a phone or video call. A simple double-check can save you and your team a ton of money.

How to identify a phishing email

Check the domain name

Double-check the domain name and sender name for all emails.

Phishing emails usually have typos or extra characters that make it look close to a real name (like Facebok.com).

The email is poorly written

Phishing emails generally have typos and grammatical errors.

They'll also omit common personal information, like your name or your company's name.

There are suspicious links or attachments

Always check every link before you click it by hovering over it first.

Phishing emails try to take you to websites that are also fake, and are used to trick you into giving login information or downloading viruses.

There's a sense of urgency

Phishing emails try to compromise your thinking with fear or urgency. This is why you see so many emails about lost accounts, or saying you're going to be arrested.

Stay calm and verify the email is real or fake before acting.

Summary

Remote work can offer a host of benefits to workers and organizations. The simple steps and tips provided in this course can help you and your organization to be both productive and secure.

When in doubt, ask your IT team about policies and tools to follow so you can work from home safely.

Your home Wi-Fi holds a lot of information. There are several simple steps you can take to lock down your network.

Make all of your passwords strong and unique. Store them in a password manager. Turn on multi-factor authentication whenever possible.

Secure your personal devices, especially if you use them for work. Always keep them up-to-date, and make sure smart devices are on a separate network.

Phishing emails are a constant threat, especially during a crisis. Look for typos in the sender's email address, and always double-check links before you click them.

Course Quiz

Question #1

Your organization is immune to cyber attacks when you're working from home.

A True.

B False.

Question #2

What is the best way to secure your home Wi-Fi?

A Change the router's default password.

B Turn on encryption.

C Make sure the router is up to date.

D All of the above.

Question #3

When is it ok to reuse your passwords for multiple accounts?

A Always. Having one password makes it easier to remember.

B It's okay to reuse my personal passwords, but I should use a different password for work.

C Never. Every account should have a unique password.

Question #4

When should you install updates for your computer or apps?

A Immediately.

B The next morning.

C Before going on vacation.

Question #5

What are the types of factors in multi-factor authentication?

A Something you **know**, **have**, and **are.**

B Something you **have**, **are**, and **feel.**

C Something you **know**, **pay for**, and **suspect.**

Question #6

What does VPN stand for?

A Very Personal Network.

B Virtual Private Network.

C Virtualized Personal iNformation.

D Variable Private Network.

Question #7

What is the best way to protect your personal devices?

A Install updates immediately.

B Use a password manager.

C Only download apps from approved app stores.

D All of the above.

Question #8

When at home, is it ok to leave work documents and devices unlocked?

A Yes.

B No.

Question #9

If your boss emails you asking to e-transfer money to them, what should you do?

A Do it right away, because they're my boss.

B Email them back and ask if this is a real request.

C Use a second form of communication, like a phone call, to verify the request.

Quiz answer key

Question	Answer	Explanation
1	B	Your personal devices can be used to gain access to your work network and systems.
2	D	All three tips are extremely important when securing your home Wi-Fi.
3	C	All accounts, whether personal or for work, should have unique passwords.
4	A	You should install all updates immediately because there may be security updates.
5	A	Multi-factor includes **know** (ex: password), **have** (ex: token or SMS), and **are** (ex: fingerprint).
6	B	VPN stands for **V**irtual **P**rivate **N**etwork.
7	D	All three tips are extremely important when protecting your personal devices.
8	B	Work information and devices are confidential, even to your family or roommates. It should always be protected when you are not using them.
9	C	You should always confirm financial transactions with a second form of communication, like calling the person or visiting them in-person.

Learn more about **CIRA** at **www.cira.ca**