10 security essentials for your TELUS journey

1. Set strong passwords

Strong passwords are critical, but remembering complex character sequences can be a challenge. To make it easier:

- Use a passphrase. This is a sequence of unlikely words, like 'PurpleFlyingElephant'. You can make your passphrases stronger by swapping a few letters for numbers (e.g. 'Purp1eFlying3lephant').
- Get KeePass, TELUS' approved password manager, to help you generate passwords and you keep track. KeePass is available through go/ICR.

Avoid the temptation to use the same password across multiple accounts. If you are impacted by a data breach, hackers will try out your password to see if you have used it elsewhere.

Watch this short video to learn more.

2. Watch out for phishing

Phishing scams are on the rise and getting more sophisticated. Stay alert for suspicious emails or text messages, and carefully assess links or attachments to ensure they are legitimate before you click.

Your TELUS email features a "Report phishing" button that you should use to notify the security team about suspected phishing attempts. If you don't see it in Outlook, reach out to go/SPOC to have it installed.

Learn more about identifying suspicious email and text messages at go/security, or check out our email security training courses for team members and contractors by searching for "TELUS_Security" in the Learning Hub.

Did you know? TELUS team members score above industry average at identifying phishing

3. Wear your TELUS ID badge

Imposters find creative ways to gain unauthorized building access, and one of their most common tricks is to sneak in behind you as you walk through the door.

If everybody wears their ID badge, it is easier to identify people who should not be in the office, so you can stop them from entering and take steps to protect our team.

All visitors are required to sign in, wear a visitor's badge and be accompanied by a TELUS team member at all times while at TELUS locations.

4. Connect wisely

Open-access Wi-Fi is not secure, even if you are required to use a password to sign in. Hackers often tamper with public Wi-Fi networks to snoop or expose users to malicious software (malware).

Turn off Wi-Fi on your phone when not in use to control access. Always sign on to the Virtual Private Network (VPN) when you work online remotely or are not directly connected to the TELUS network.

5. Encrypt external drives

Your TELUS laptop comes with a Windows encryption feature called BitLocker-to-go. Avoid storing data in external drives or USB keys unless it's absolutely essential, and don't ever save files to one without encryption.

If you find a USB key or external drive, turn it in to the security team, so that it can be opened in a protected environment. Hackers sometimes deliberately infect USB keys or external drives with malicious software and leave them where they can be found and plugged in to computers by unsuspecting users.

6. Protect cellphones and tablets

Fraudsters have lots of innovative ways to syphon off data and install malicious software on mobile devices. To protect yourself and TELUS:

- Only work from cellphones and tablets that have been enrolled in TELUS' mobile device management platform
- Password protect your device and ensure auto lock kicks in after no more than 15 minutes of inactivity
- Install updates regularly to stay ahead of the latest security threats
- Only download trusted apps and consider the implications of clicking "allow" before giving them access to features (e.g. camera, contacts)
- When you upgrade to a new device, remember to un-pair any peripherals (e.g. FitBit, Apple Watch) and wipe your phone before recycling it

Learn more about protecting cellphones and tablets at go/security or check out our mobile device security training for team members and contractors by searching for "TELUS_Security" the Learning Hub.

7. Keep devices secure when you're on the move

If you work on the road, enjoy Workstyles benefits or need to travel for business purposes, there are special precautions you need to take to protect TELUS equipment and information.

- Always keep devices on your person or securely locked away when not in use
- When flying, carry your devices with you and do not transport them in checked-in luggage
- Never allow family members or friends to use your work devices
- Manage data wisely. Only keep the data you need on your devices and, if you are travelling internationally, limit the data you bring with you to information you need during the trip

Questions? Contact us at:
security.awareness@telus.com

8. Be careful where you discuss TELUS business

You never know who is listening when you discuss work in a public place. Be mindful about your conversations and consider using a privacy screen on your computer when working in a public setting.

Talking near a smart speaker, like Google Home, is similar to having a conversation in public. If you work from home and keep a smart speaker in your home office, make sure the mic is switched off when you discuss business information, and review recordings weekly to check that confidential details have not been inadvertently captured.

9. Be mindful on the Cloud

Only use TELUS-approved Cloud services and get to know which types of data you can store on Cloud-based systems and tools. If you identify a Cloud-based solution you would like to use for work, reach out to the Data and Trust Office (go/privacy) and Secure by Design (go/sbd) teams before you sign up, so they can check to see if it meets TELUS' security requirements.

Remember not to store or transmit Personal Health Information (PHI) or data about customers on the Do Not Touch List (go/DNTL) via G Suite.

10. Familiarize yourself with TELUS' Acceptable Use Policy

Get to know TELUS' Acceptable Use Policy. It is regularly updated to keep pace with the latest cyber threats and security procedures, and will help guide you towards security best practices throughout your TELUS journey.