[Brandmark of TELUS Wise]

[TELUS Wise online basics]

[12. Managing your digital footprint]

[A laptop and a mobile phone appear on the screen.]

[Voice of a woman]: When you visit a website or use an app on your tablet or smartphone,…

[Footprints appear on the computer and mobile phone screen.]

… you leave behind traces of your activity or what's called a digital footprint.

[Close-up of a mobile phone, displaying a photograph and comments.]

Sometimes we know when we leave these footprints, like when you share a photo or comment on someone's Social Media post.

[A question mark appears above the mobile phone.]

Sometimes, though, it may not be clear what a website or app knows about you once you use it.

[Footprints appear again on the screen, leaving a trail that goes by signs that read "Search Engine", "Social Networks" and "Websites".]

When it comes to the internet, once something is out there, it's permanent. It's like stepping in wet cement. The footprints you leave behind, last forever. Because of that, it's important to be careful what you share online.

[Never share online:
- Credit card number
- Bank information
- Passwords]

For example, you should never share personal information like credit card numbers, bank information or passwords anywhere online…

[Two images of a bank's website and a trusted website appear on the screen. Each of the two websites has a padlock symbol.]

… except if you are logging into your bank account or using a shopping site you trust and that you know it's secure.

[Screen capture of the TELUS website. Close-up of "https" and the padlock in the address bar.]

You'll know a site is secure if the web address reads "https" not just "http", and there's a padlock icon in the address bar.

[The image of a generic website appears on the screen. One finger taps on the User drop-down menu and then on "Log out". The message "Are you sure you want to log out?" appears. The finger taps on "Yes". The screen returns to the identification page.]

It's also important to make sure that you log out of online accounts when you are done using them, especially on shared devices, like computers at a library.

[A laptop appears on the screen. An email page is displayed. The window is closed without the user logging out. The window is opened again, and the email home page is displayed again.]

Just closing the tab or window isn't enough. If someone else uses the same device and goes to a page you haven't logged out of, they'll be able to access your account.

[Close-up of the laptop camera.]

You can also cover the cameras on laptops and other devices when you are not using them, to reduce the impact of potential unauthorised access to your camera.

[A sticky note covers the camera.]

You can do this with a sticky note or something similar that's easy to remove when you want to use the camera.

[Microphones appear above the laptop and below the mobile phone.]

Most computers and mobile devices also have microphones built-in. You can't just cover them like you can with the camera, but there are a few things you can do to keep them secure.

[A Mac appears on the screen. The finger taps on the System Preferences link of the Mac. The preferences window opens. The finger taps on the Sound icon and then changes the volume setting to zero.]

On a desktop or laptop computer, go to Settings on a Windows device, or System Preferences on a Mac, then find the Sound settings and turn the microphone volume all the way down to zero.

[The finger turns the volume level up for a videocall.]

Just remember you will have to turn it up again if you want to use the microphone for something like a video chat.

[An Android mobile phone appears on the screen, displaying the Settings menu. The finger taps Apps, then the three small dots on the right, on the Permission Manager menu, and then on Microphone. The finger taps on the Bonjoro app and changes the permission from "Allow only when the app is in use" to "Deny".]

On a mobile device, go to Settings, on an Android device tap apps, then tap the three dots on the right and tap Permission Manager. Now tap microphone to see which apps have permission to use the microphone. If there is an app that you don't think should be listening, select it and adjust its permission setting.

[An iPhone appears on the screen, displaying the Settings menu. The finger taps on "Privacy", then on Microphone. The finger deselects several apps.]

On an iPhone or iPad, tap Privacy, and then Microphone, and turn off access to any apps you don't think should be able to use the microphone.

[The same process is presented for the camera.]

You can do the same thing with the camera, too, and turn off access to the camera for apps that don’t require it to work.

[Google's homepage appears on the screen. The finger taps the File menu, and then taps the New Incognito Window link. A black window appears on the screen, displaying the message "You have gone incognito".]

You can also control how much your browser remembers about the sites you visit and what you do on them, by using Incognito or private browsing mode.

[The same process is presented for Mac. The finger taps on the File menu, then on the "New private window" link.]

When you do this, your browser will not track which sites you visit and also won’t remember any account information or passwords that you enter.

[Amazon's homepage appears. A list of recently viewed products is displayed.]

Just remember that these settings usually don’t stop the websites themselves from recording what you do there.

[An online profile, with a photo and information appears on the screen, then a social network page with personalized advertising messages is displayed.]

This matters, because websites and advertisers use what they know about your online activities to make a profile of you. They then use your profile to choose which advertisements to show you.

[Banknotes and a contract appear on the screen, to the right of the online profile.]

Your online profile may also be used to influence everything, from how much you pay for products and services to whether or not you can get insurance.

[Limit what apps and websites know about you.]

There are ways that you can limit how much apps and websites and the companies that own them know about you.

[Browser choice:
Firefox
Brave]

To start, you can use a browser that’s designed to give you more privacy, like Firefox or Brave.

[Google's homepage in the Firefox browser appears on the screen. The finger taps on the "Tools" menu and then on the "Add-ons and themes" link. The screen unfolds. The finger taps on "Find more Add-ons ". The Firefox Add-Ons page opens.]

You can also use extensions that protect your privacy. Extensions are mini-apps that work within your browser. To find extensions on Firefox, click Add-ons and then search for the extension you want.

[The same process is presented for Chrome. The finger taps on the "Window" menu and then on the "Extensions" link.]

On Chrome and Edge, click on Extensions.

[The Safari home page opens. The finger taps on the "Safari" menu and then on the "Safari Extensions" link.]

On Safari, click Safari Extensions.

[A results page for add-ons for "tracker protection" appears on the screen. Close-up of The Disconnect Premium and Ghostery Lite extensions.]

Privacy badger, Ghostery and Disconnect are all extensions that will block most websites from tracking you online.

[A mobile phone appears on the screen. The Disconnect and Ghostery mobile version apps are displayed.]

There are also mobile app versions of Disconnect, Ghostery and others that you can get for iOS or Android devices.

[A laptop and a desktop computer appear on the screen. The words "Friend's computer" and "Public computer" appear above the computers.]

If you are using a computer that isn't yours, like a friend's or a public computer at the library, always use private browsing if you can.

[The home page of a library website appears on the screen. The finger taps on the "New private window" link. A message reading "Do you want this computer to save your password for next time?" is displayed. The finger clicks on "No".]

If you can't, make sure to click "No" anytime the browser asks for permission to remember your account or password for next time.

[Brandmark of TELUS Wise]

For more information on Online basics checkout the other videos in the series.

[telus.com/WiseOnlineBasics].