Overview of the Internet of Things and Connected Devices

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

What Is The Internet of Things?

The Internet of Things (IoT) refers to devices connected to each other and to a device or app that can control them. These devices may be connected through the Internet, Bluetooth, or other means. Unfortunately, these devices and systems can provide yet another, highly invasive way that technology can be misused to monitor, harass, threaten, or harm. At the same time, they are also potential tools people can use to strategically increase their safety.

Most Common Iot Devices

Home Automation and Personal Assistants

Our homes are rapidly being filled with “smart” and “connected” devices that promise to increase convenience, improve energy savings, and strengthen personal security, such as smart lights, thermostats, and security cameras. Home automation IoT allows remote control and surveillance through Internet-connected devices in the home.

Smart Toys and Location Trackers

“Smart” and “connected” toys promise to entertain, increase safety, and connect us to our kids and pets while we’re away from home.

Smart Cars and Driverless Vehicles

While driverless vehicles get all the headlines, many newer cars come off the lot already “connected,” allowing parents to monitor and control teen drivers and employers to monitor employee driving habits. In addition, small gadgets can be attached to a car to allow for remote monitoring and, in some cases, remote control of some features.

Connected Health and Medical Devices

Many health and medical devices are now connected to the Internet, offering to help you track information about your healt or even send that information to your doctor.

Steps to Increase Safety and Privacy

Be aware of the risks when you use a smart device and learn what you can do to increase privacy and security. Although each smart device will be different, here are some general tips.

1. Know How Your Smart Device Works

The first step to staying on top of your privacy, security, and safety when using a smart device is to understand how it works. When you set up a smart device, you will either create an account for that device, attach an email to that device, or connect that device to a network (usually your home Wi-Fi network) – or perhaps all of the above. Having a general idea of how your smart device works and what it’s connected to will help you determine what information is shared and how it is accessed, which will help you identify and minimize potential risks.

2. Limit Connections to Your Smart Device

Review how and what it is connected to. If it’s connected via Wi-Fi, turn it off when you’re not using it. If you can’t turn it off, disconnect it from the Internet. If it has other types of access, such as Bluetooth, turn off the connection access. If it’s turned off or not connected, it will not be possible for someone to access the device remotely.

3. Limit Personal Information Shared from Your Smart Device

Information about you is stored either on the device, in an account, or with the company. If you are worried about someone gaining access to your information, determine whether you can limit personal information stored or shared via the device. This can include turning off the device when not in use, turning off cameras or microphones, or reviewing the device’s settings and limiting how much information the company can gather about you. Read the company’s privacy policy to learn about how they share your personal data.

4. Secure the Account Associated with Your Device

Some devices require you to set it up with an account, prompting you to create a username and password. Create a username and password that someone else (including the perpetrator) can’t guess. Some accounts may offer 2-step verification so that if someone tried to access your account from a different device or location, they will require an additional verification code (generally in the form of an SMS code).

If the device doesn't require a username/password to access, know how it connects and whether someone else could connect to it.

5. Increase the Security of Your Home Network Router

Because smart devices are mostly connected to a home Wi-Fi network, make sure that your home router is secure. There are many things you can do to increase your home router's security, including the following:

- Put a passcode on your home Wi-Fi network
- Change the router's username/password from the default
- Use WPA2 encryption
- Turn off remote management on the router

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from WESNET's Tech Safety project, based on their resource Smart Devices and Internet of Things.

© Copyright 2023 Women's Shelters Canada | All Rights Reserved

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.