

# YOUR GET CYBER SAFE GIFT GUIDE 2022



Cyber security is the gift everyone needs. Whether you give or receive a new gadget, **BE CYBER SAFE!**

## BEFORE BUYING ANYTHING:

- > Check security features
- > Read the privacy policy
- > Secure your home Wi-Fi



## ENTERTAINMENT

### SMART TV



- > Your camera and microphone could be monitored by **hackers**

**TIP:** Install a security shutter on the camera and mute the microphones when not in use

### SMART HOME ASSISTANT



- > An unsecured smart speaker may not protect **your data**

**TIP:** Never allow the device to remember your passwords or credit card number

### GAMING SYSTEM

- > Oversharing could put your **privacy at risk**

**TIP:** Create usernames that do not contain personal info



## PERSONAL DEVICES

### SMARTWATCH



- > Smartwatches may collect data about you, such as your **location** and **sleep patterns**

**TIP:** Read and understand the privacy policies of the apps and services you use

### TABLET



- > Apps downloaded from untrustworthy sources may contain malware to **steal your info**

**TIP:** Only install apps from trusted sources such as your tablet's official app store

### SMARTPHONE



- > Jailbreaking or removing the manufacturer's software controls may make your phone more vulnerable to **malware**

**TIP:** Never "jailbreak," "root" or otherwise bypass security measures

### LAPTOP



- > You might download malware that steals your **data**

**TIP:** Install anti-virus and anti-spyware software

## AROUND THE HOME

### SMART LIGHTING



- > Your daily routine could be exposed to a **hacker**

**TIP:** Keep your device secure by installing software updates as they become available

### VIDEO DOORBELL



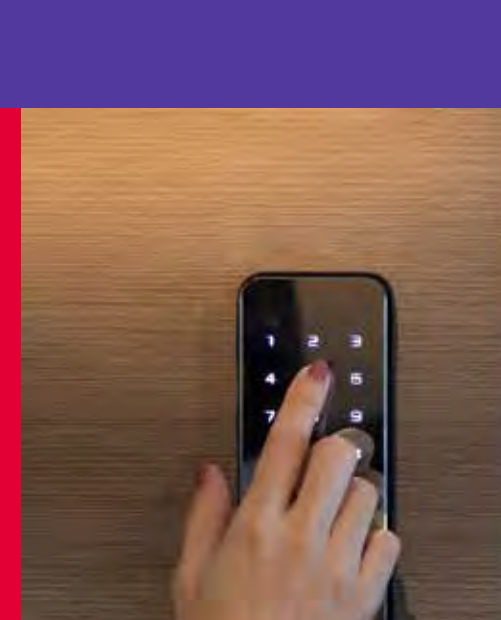
- > An unsecured video doorbell could be hacked, giving cyber criminals access to your doorbell's camera or your **home network**

**TIP:** Make sure you can set your own strong and unique password or passphrase for the device

### KEYLESS LOCK

- > An unsecured smart lock could let intruders into your home

**TIP:** Choose a lock that requires more than one authentication factor to open



## ON THE GO

### SMART CHARGERS



- > Plugging in a foreign device to your network-connected smart charger could **expose your data**

**TIP:** Only use smart chargers with your own devices and turn chargers off when not in use

### WIRELESS HEADPHONES AND EARPHONES



- > Unsecured wireless signals can be **hacked** to access your sensitive information

**TIP:** Disable connections and turn off device when not in use

## HEALTH AND FITNESS

### WEARABLE FITNESS TRACKER



- > A wearable fitness tracker could capture and **transmit information** you don't intend it to

**TIP:** Read and understand the privacy policy of any wearable fitness tracker or fitness tracking app

### SMART FITNESS EQUIPMENT



- > Smart fitness equipment or exercise machines could be hacked and **expose your data**

**TIP:** Be careful connecting any of your social media accounts to your smart fitness equipment

Protect your devices, and yourself, and enjoy  
**#CyberSafeHolidays!**

GET MORE TIPS TO SECURE YOUR ACCOUNTS AND DEVICES AT

[GETCYBERSAFE.CA/cybersafeholidays](https://getcybersafe.ca/cybersafeholidays)

 Communications Security Establishment Centre de la sécurité des télécommunications

