USING BLUETOOTH TECHNOLOGY

April 2019

ITSAP.00.011

Many business and personal devices (e.g. laptops, printers, GPS receivers, phones, fitness trackers, home appliances, and car audio systems) use Bluetooth technology. However, threat actors can use Bluetooth-specific vulnerabilities to exploit your devices to steal your information. Bluetooth technology is a low-cost and effective way to connect your devices, but should be used with caution.

BLUETOOTH TECHNOLOGY

Bluetooth is a wireless technology used to transfer and synchronize data between devices without the use of physical cables (e.g. laptop and headphones, fitness tracker and an app on your cellphone). As Bluetooth technology continues to evolve, newer versions of Bluetooth can transfer data between devices at increased speeds and range.

BLUETOOTH SECURITY CONSIDERATIONS

Although newer versions of Bluetooth have improved security measures, Bluetooth should still be used with caution. Devices that use earlier versions of Bluetooth don't have the same security features, making them vulnerable to interception and attacks. If you connect two devices and one of them uses an earlier version of Bluetooth, then the entire connection is vulnerable.

Avoid transferring sensitive information over Bluetooth connections. For example, avoid using Bluetooth-enabled keyboards to enter sensitive information or passwords, as this information can be intercepted (e.g. keystroke logging). When using Bluetooth technology, such as a wireless mouse, keep in mind that your computer is vulnerable to remote attacks if the wireless adaptor in the mouse, which enables the Bluetooth connection, is exploited and compromised.

DISCOVERY MODE

Discovery mode is a state within a Bluetooth-enabled device in which a device can search for and connect with other devices that are within range. Discovery mode should be turned off when you're not using it. If discovery mode is turned on so that you can connect devices, you should connect only with devices you know and trust.

AUTHENTICATE AND AUTHORIZE DEVICES

Protect your devices and information by authenticating and authorizing other devices. Always verify that a listed device is one that you know and trust before you pair it with your device. To authorize and verify connections, pairing codes and passkeys are used. Be wary if you receive a pairing request if you haven't initiated it. Keep in mind that once paired, devices remain on your list of paired devices. Always remove lost or stolen devices from your paired devices list.

BLUETOOTH-ENABLED CARS

By connecting devices to Bluetooth-enabled cars, drivers and passengers can make hands-free calls, send texts or emails, stream music, and connect to the Internet. When you pair your device with your car, your personal information is stored on the car's system. Your call logs, contacts, and messages, such as texts, emails, or any app-based messaging, can be accessed on the car screen through Bluetooth. This might not seem like an issue if you own the car, but it is a concern when you sell or rent a car. Make sure to delete stored data and devices when you are selling your car. It's best to avoid pairing your devices with rental cars altogether. If you need to use hands-free calling when using a rental car, use the built-in speakerphone on your device or pair your device with a personal Bluetooth headset.

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

BLUETOOTH-SPECIFIC VULNERABILITIES

Threat actors can use vulnerabilities to access your Bluetooth devices and steal your information. Certain vulnerabilities can be exploited to allow a threat actor to gain complete control of your devices. Some methods include:

Bluejacking—A threat actor sends unsolicited messages to your Bluetooth-enabled mobile devices. If you respond to the message or add the contact to your address book, you give the threat actor the opportunity to connect to your devices because you are establishing them as a known contact. Threat actors can then control your device remotely.

Bluebugging—A threat actor poses as a device you're looking to connect to (e.g. headphones). You may not even realize that you are connecting to a spoofed device. Once connected, your device and your data are accessible as long as the spoofed device is in your list of paired devices.

Car whisperer—Car Whisperer software allows a threat actor to send or receive audio from the car kit installed in your vehicle. If exploited, threat actors could eavesdrop on your conversations by receiving audio from the car microphone.

Crackle—A threat actor exploits flaws in the pairing process that allows key recovery so that your devices can be accessed.

GATTack—An attacker creates a man-in-the-middle attack (i.e. secretly relays and can alter communications between sender and recipient) to intercept, clone, block, or change messages.

SUMMARY OF TIPS FOR USING BLUETOOTH

Bluetooth technology is continuing to evolve. New versions of Bluetooth have increased ranges and speeds, making data transfers easier and more convenient. The technology is changing, but you can protect your data and devices with a few simple actions:

- Turn off Bluetooth when you're not using it
- Turn off discovery mode when you're not connecting devices
- Avoid pairing devices in public spaces
- Pair only with devices that you know and trust
- Never transfer sensitive information over Bluetooth
- Avoid using Bluetooth-enabled keyboards to enter sensitive information or passwords
- Remove lost or stolen devices from your list of paired devices
- Delete all stored data and devices from Bluetooth-enabled cars
- Avoid pairing devices with rental cars

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**