Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

USING BLUETOOTH TECHNOLOGY

MAY 2021 **ITSAP.00.011**

Many business and personal devices use Bluetooth technology. Bluetooth is a wireless technology used to transfer and synchronize data between devices without the use of physical cables (e.g. a laptop and headphones, a fitness tracker and an app). Bluetooth is also used by exposure notification applications with signal distribution to perform effectively (e.g. COVID Alert). As Bluetooth technology evolves, newer versions of Bluetooth can transfer data between devices at increased speed and range. Overall, it is a low-cost and effective way to connect your devices. However, threat actors can exploit vulnerabilities in this technology to gain access to your devices and steal sensitive information.

SECURITY CONSIDERATIONS WHEN USING BLUETOOTH

USE UPDATED VERSIONS OF BLUETOOTH

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. Although newer versions of Bluetooth have improved security measures, you should still use Bluetooth with caution.

PROTECT SENSITIVE INFORMATION

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.

DISABLE DISCOVERY MODE

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

USE DEVICES WITH APPROPRIATE SECURITY MEASURES

Choose Bluetooth devices that use security mechanisms, such as changeable passwords. Some Bluetooth products do not use PINs or passwords, or they use fixed passwords (e.g. 0000 pin). With a changeable passwords, you can make it more difficult for a threat actor to connect to and access your devices.

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 device.

AWARENESS SERIES

THREATS TO BE AWARE OF

Bluetooth-enabled devices are susceptible to general cyber threats. Threat actors use different attack methods to connect to your devices, eavesdrop, and steal information. Some of these attack methods are included in the following:

Protocol attacks: A threat actor broadcasts packets (e.g. small pieces of data) or impersonates a device to bypass authentication and encryption.

Denial-of-Service (DoS) attacks: A threat actor jams the signal to prevent your device from connecting to another device. DoS attacks are often used with protocol attacks to deny access to intended devices and redirect you to connect with a spoofed device.

Once a threat actor connects to your device, they can carry out additional attacks, such as the following examples:

Eavesdropping attacks: A threat actor captures and decodes sensitive information in your Bluetooth transmissions (e.g. password typed into a Bluetooth keyboard).

Impersonation attacks: A threat actor uses direct spoofing or person-in-the-middle attacks to access your device contents and services to download contents and change settings. Internet of Things devices are often vulnerable to these types of attacks.

In addition to these methods, threat actors can take advantage of device, software, and application vulnerabilities to access and gain control of your Bluetooth devices. Once your device is compromised, threat actors can steal information, track locations, and change device settings without your knowledge.

Keeping your devices, software, and applications updated can address vulnerabilities and protect you from cyber threats. Be sure to run updates and patches regularly.

Be sure to check out ***ITSAP.00.001 Using Your Mobile Device Securely*** for more tips on keeping your devices safe.

SUMMARY OF SECURITY TIPS

Bluetooth technology continues to evolve, but you can continue to protect your data and devices with a few simple actions:

- Keep all Bluetooth devices up to date (e.g. phones, headphones, keyboards, gaming equipment)
- 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

***Note:** Exposure notification applications (e.g. COVID Alert) need Bluetooth to be continuously enabled. In this case, you should consider removing any paired devices that are not in use and restrict your device permissions.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**