CANADIAN CENTRE FOR CYBER SECURITY

Using Bluetooth technology

April 2024 ITSAP.00.011

Bluetooth is a wireless technology that uses radio frequency to transfer and synchronize data between devices within a short distance, such as a laptop and wireless headphones. As Bluetooth technology evolves, newer versions of Bluetooth can transfer data between devices at increased speed and range. While it is a low-cost and effective way to connect your devices, threat actors can exploit vulnerabilities in Bluetooth technology to gain access to your devices and steal sensitive information.

Security considerations when using Bluetooth

The following are some security measures to consider before 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

When using Bluetooth technology, keep in mind that your computer is vulnerable to remote attacks. Avoid transferring sensitive information over Bluetooth connections. For example, avoid using Bluetooth enabled keyboards or enter sensitive information or passwords because this information can be intercepted.

Deactivate 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 only connect with devices you know and trust. Turn off discovery mode when you're not using it.

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. Use pairing codes and passkeys to authorize and verify Bluetooth connections. Be wary if you receive a pairing request you haven't initiated. Keep in mind that once paired, devices remain on your list of paired devices and will often connect automatically when within range and turned on.

Unpair old devices

Keep your list of Bluetooth pairings up to date. This list can be found in the Bluetooth settings on your device. Try to avoid temporary pairings, such as connecting to a speaker in a short-term rental to prevent unnecessary security risks. Remove lost or stolen devices from your pairing list as soon as possible.

Be wary of your surroundings

When pairing two devices for the first time, make sure to do so from a secure location to reduce the risk of your device being hijacked. Be careful of who you connect with and refuse all unknown connection requests. **You should turn off Bluetooth when it is not being used.**

AWARENESS SERIES

Cat. No. D97-1/00-011-2024E-PDF
ISBN 978-0-660-70858-4

Bluetooth threats

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 include the following examples:

Protocol attacks: A threat actor broadcasts packets, such as small pieces of data or impersonates a device to bypass authentication and encryption.

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.

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 you access to intended devices and redirect you to connect to a spoofed device. Once a threat actor connects to your device, they can carry out additional attacks, such as:

- **Eavesdropping attacks:** A threat actor captures and decodes sensitive information in your Bluetooth transmissions, such as a 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 apply patches regularly.

Learn more

- Using your mobile device securely (ITSAP.00.001)
- Security tips for peripheral devices (ITSAP.70.015)
- Mobile devices and business travellers (ITSAP.00.087)

Bluetooth-enabled cars

By connecting devices to Bluetooth-enabled cars, occupants can make hands-free calls, send texts, and stream music. When you pair your device with your car, your personal information (call logs, contacts, messages, etc.) is stored on the car's system. This might not seem like an issue if you own the car but is a concern if 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 speaker on your device or pair your phone with a personal Bluetooth device.