24 July 2020

WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

West Midlands | Regional Cyber Crime Unit

Bluetooth

In the 10th Century, the Danish Viking leader Harald Denmark, also known as Harald Bluetooth (Harald Blåtand), became the king of Denmark. In recognition of the important role Nordic countries have contributed to the world of cell phones - the technology for wirelessly transferring information from one device to another - it was named after him.

What Bluetooth Offers

- **Pair devices:** Allows individuals to connect various devices such as wireless speakers or make hands-free calls with mobile.
- **Share files:** Photos, videos and music can be sent between different devices. It is common for fitness trackers and smart watches to share data so individuals can monitor their daily activity and health.
- **Set up tethering:** If a computer does not have internet access and a phone does (due to its mobile network), it is possible to share this internet connectivity.

Security Concerns

The more dangerous Bluetooth attacks require a degree of technical knowledge that make them very uncommon. Further, Bluetooth attacks require the victim to be in close proximity to the attacker for a sustained period of time. This further decreases the risk of compromise.

- **Bluejacking** involves sending a `business card' to another nearby user via text. The card can contain unsolicited messages, this is a nuisance rather than a security concern.
- **Bluesnarfing** is when the same business card is used to request a Bluetooth connection. If an individual unwittingly gives a hacker permission to the device, they can send malicious files or steal information leading to identity theft, social engineering or worse.
- **Bluebugging** allows skilled hackers to take control of a mobile in order to make phone calls, send and read SMS, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.
- **Blueborne** are the more recent attacks that compromise a range of electronic devices such as laptops, smart cars, smartphones and wearable tech. The hacker can assert control over each device or use them as a spring board to attack other devices.

Security Solutions

- **Update devices:** Updates fix security weaknesses. Google and Amazon have already released patches that address serious vulnerabilities such as Blueborne attacks.
- **Secure Bluetooth connections:** Set up the device to only connect with trusted devices and to require a pin code before establishing a new connection. These can be done in the Bluetooth settings.
- **Turn your Bluetooth off:** When not in use, in crowded locations or whilst working with sensitive data.
- **Configure App permissions:** Limit your apps that utilise Bluetooth through the `settings' menu. Turning off Airdrop, for example prevents your phone unwittingly sharing or receiving sensitive. Alternatively, if it is an app you use more frequently, configure settings to `contacts only' mode.

WM ROCU REGIONAL CYBER CRIME UNIT