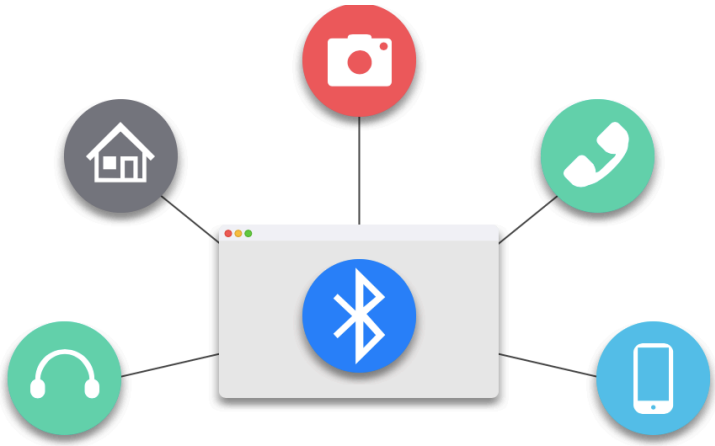
Volume #4 - Issue #150
March 9th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Securing Your Bluetooth Devices



Bluetooth is a wonderful technology. It allows you to connect to headsets, sync up with cars or computers, and much more. While Bluetooth connections have the advantage that they're automatic and wireless, they have the disadvantage of their data being vulnerable to interception along with any other data sent on low-power radio waves. In addition to the risk of other people being able to receive your

sensitive information, they're also able to send you files or viruses that you're absolutely not interested in. Plus, this is a very inexpensive hack. Anyone can buy the equipment needed to create a forced bluetooth pairing for less than $200.

Unfortunately, Bluetooth is one of the main security gaps by which hackers can get at your phone (or computer if you are using a bluetooth keyboard or mouse in a public setting).

Here are the three basic types of Bluetooth-based attacks:

Bluejacking

Bluejacking is a relatively harmless attack in which a hacker sends unsolicited messages to discoverable devices within the area. The attack is carried out by exploiting Bluetooth's electronic business card feature as a message carrier. The hacker cannot access any information or intercept messages. You can protect yourself from these unsolicited spam messages by putting your phone into "invisible" or "non-discoverable" mode.

Bluesnarfing

Bluesnarfing is much worse than bluejacking because it allows a hacker to get at some of your private info. In this type of attack, a hacker uses special software to request information from a device via the Bluetooth OBEX push profile. This attack can be carried out against devices in invisible mode, but this is less likely due to the time needed to figure out the device's name through guessing.

Bluebugging

When your phone is in discoverable mode, a hacker can use the same entry point as bluejacking and bluesnarfing to try and take over your phone. Most phones are not vulnerable to bluebugging, but some early models with outdated firmware could be hacked this way. The electronic business card transfer process can be used to add the hacker's device as a trusted device without the user's knowledge. This

trusted status can then be used to take control of the phone and the data within.
If an attacker uses a tool such as Super Bluetooth Hack, the hacker can pair with the device and perform some of the following malicious events:

- make the phone ring
- try to make calls.
- Steal or copy contacts
- Read SMS messages
- turn off the network / phone
- set or reset alarms
- change the date and time
- block the network operator
- start and delete java applications

There is no one way to completely protect your bluetooth from a hack, but the following measures can make it more difficult for the hacker to succeed.
1) Allow Bluetooth discovery only when absolutely required, then disable when finished.
How to turn off Bluetooth discovery mode:

- *Android:* Go to **Settings** > **Wireless and networks** > **Bluetooth settings** > **Discoverable**, and make sure it's not checked.
- *BlackBerry:* Go to **Options** > **Bluetooth**, then click the BlackBerry logo (Menu) button. Choose **Options**, set Discoverable to **No**, press the BlackBerry logo button again, and then choose **Save**.
- *iPhone:* You can't explicitly turn off the Bluetooth discovery, but the iPhone is only discoverable when you're on the Bluetooth settings page – **Settings** >**General** > **Bluetooth**.

- *Windows Phone:* As with the iPhone, Windows Phones are only discoverable when you're on the Bluetooth settings page at **Settings** > **Bluetooth**.

2) Pair devices using a secure long passkey.

3) Never enter passkeys or PINs when unexpectedly prompted to do so.

4) Regularly update and patch Bluetooth-enabled devices.

5) Purge trusted devices regularly and repair if necessary

6) Remove paired devices immediately after use.

These actions will help secure your bluetooth and let you take advantage of his amazing technology.

This Week's Cyber Alerts:

Alert Issued 3/7/18 **Locked Windows machines Can Be Compromised through Cortana**

Alert Issued 3/7/18 **Cyber Attacks Becoming No. 1 Business Risk**

Alert Issued 3/7/18 **Most Top US Higher Ed Institutions Fail to Protect Students from Phishing**

Alert Issued 3/5/18 **Android Phones Caught Selling with Pre-Installed Factory Malware**

Alert Issued 3/2/18 **US Carriers Testing Replacement for Two-Factor Authentication**

Alert Issued 3/1/18 **Popular Cache Utility Exploited for Massive DoS Attacks**

Alert Issued 2/27/18 **Mobile Banking Trojans Spread Confusion Worldwide**

Alert Issued 2/26/18 **IRS Warns of Spike in W-2 Phishing Emails**

Alert Issued 2/26/18 **Crooks Launder Money Using Real (and fake) Amazon Ebooks**

Thank you for subscribing to our email!