CENTER FOR
SECURITY STUDIES
& CYBER DEFENSE

How To Secure Bluetooth Devices

Written By: AUCSSCD Student Intern

Almost every device with a microchip nowadays has bluetooth functionalities, but not many people know how unsecure bluetooth is as a protocol. There are three main categories of attacks that take advantage of bluetooth devices and services. Bluejacking is an attack where using bluetooth contact sharing attackers can send unsolicited messages to nearby users' phones. Bluejacking attacks generally operate like phishing attacks where the message sent via Bluejacking attempts to manipulate the victim into giving up private information of their own free will believing that the attacker has already compromised them. Bluesnarfing involves looking for nearby bluetooth devices that are unprotected by a PIN code and pair with it in order to access all of its data. The final main attack is Bluebugging, Bluebugging starts just like Bluesnarfing but once the device has been compromised a backdoor is inserted in order to allow persistent access. Here are some steps to take to avoid these attacks.

First up is Bluejacking, there is good and bad news about protecting yourself from bluejacking. The bad news is that there is no real way to prevent a Bluejacking attack aside from just disabling bluetooth entirely from your device. The good news is that as with all bluetooth attacks it can only be carried out within close proximity to the victim so it is not a very common attack and even when it does happen it does not pose any actual danger to the victim. By knowing about Bluejacking and knowing that it is only a scare tactic you can avoid giving information to attackers in the future.

Next up is Bluesnarfing and Bluebugging, Bluesnarfing and Bluebugging is also limited by proximity in the same way as Bluejacking and Bluebugging and any bluetooth attack. Given that Bluebugging is a kind of Bluesnarfing attack, protecting yourself from Bluesnarfing necessarily protects you from Bluebugging as well. Bluesnarfing is also limited in how many devices are vulnerable to it. Most bluetooth devices have protections in place to prevent Bluesnarfing attacks such as pin numbers and encryption measures. If your device does have these measures make sure to enable them and you will most likely be protected from Bluesnarfing and Bluebugging attacks.