



Hardware

Protect Yourself From Bluetooth Hackers

4:49 PM PDT • September 24, 2007

 Comment

I imagine most of our audience is quite familiar with Bluetooth security, but it doesn't hurt to have a refresher or, at the very least, pass this along to a colleague, friend or family n00bs. A recent study by InsightExpress revealed that 73 percent of mobile device users are unfamiliar with counter measures to prevent spam texts or even someone taking complete control of your phone.

The three most common instances of hijacking via Bluetooth are bluejacking, bluesnarfing and bluebugging. The first instance isn't much of a security threat, but getting spam texts can be annoying and cost you a pretty chunk of change depending on your data plan and the severity of the attack. A step up from bluejacking is a technique that allows hackers to access and copy data without your knowledge. The most severe threat is bluebugging and this is where things can turn out really bad. A clever hacker can take complete control of your phone to make calls, access data, send text messages and listen in on your phone calls. The tips offered by Symantec senior security consultant Ooi Szu-Khiam are no-

 **DISRUPT****Series A to B Startup? Join the ScaleUp Program At Disrupt 2024.**[LEARN MORE](#)

Stay invisible

If you are using the Bluetooth function and don't require your device ID to be visible to others, make sure the device's visibility setting is set to "hidden" so malicious hackers will not be able to scan and search for it.

Verify incoming transmission

Do not accept and run attachments from unknown sources unless you are expecting them. For example, if you receive a message to install an application and you don't know its origin, don't run it.

Use passwords

Ideally, use passwords with a large number of digits. A four-digit PIN or password can be broken in less than a second, and a six-digit PIN in about 10 seconds, while a 10-digit PIN is likely to take weeks to crack.



Disrupt 2024

Got Laid Off? Find Your Next Job At Disrupt.

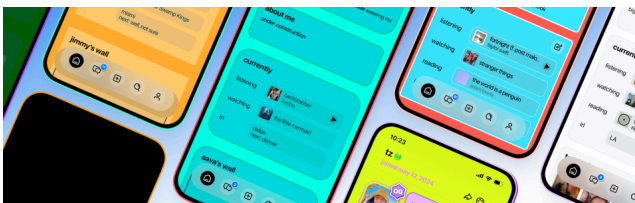
Get 50% Off The Disrupt Expo+ Pass San Francisco, October 28-30

[Book Now & Save](#)

[Users need refresher on Bluetooth security](#) [ZDNet Australia]



More TechCrunch



Series A to B Startup? Join the ScaleUp Program At Disrupt 2024.

[LEARN MORE](#)