

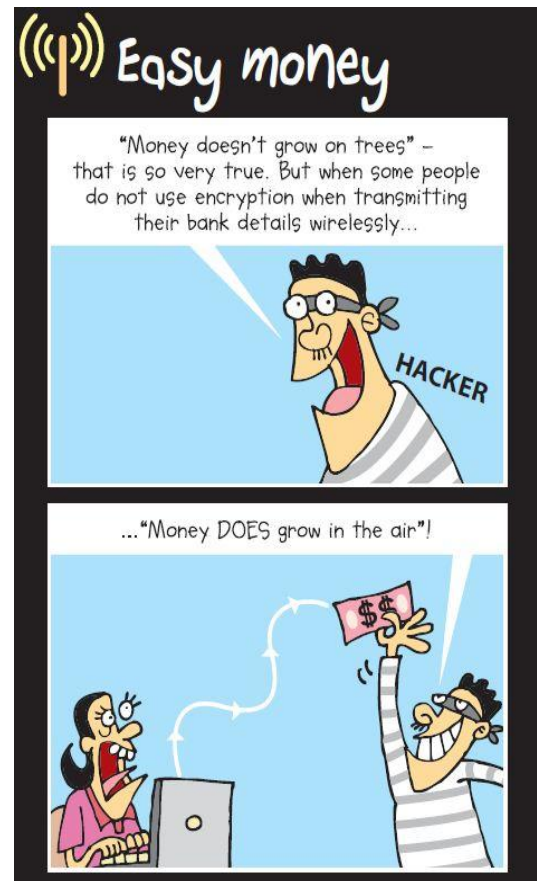


## The Bluetooth Security Issues

In the past, the only way to connect devices was via cables, which can be cumbersome and messy. With the introduction of Bluetooth technology, devices could be connected using short range radio frequency (RF) with low power, to share information and resources over a distance of up to 10 metres. Bluetooth is mainly used to establish a Wireless Personal Area Network (WPAN) by allowing users to form adhoc networks between various Bluetooth enabled devices including mobile phones, laptops, automobiles, medical devices, printers, keyboards, mice, and headsets.

## What Are The Bluetooth Security Issues?

**Bluetooth** offers several benefits and advantages, but the benefits are not provided without risk. Bluetooth security includes authorisation, authentication and optional encryption. Authentication is the proving of identity of one Bluetooth-enabled device to another. Authorisation is the granting or denying of Bluetooth connection access to resources or services from the requesting device. Encryption is the translating of data into secret code so that eavesdroppers cannot read its content.








Despite all the defence mechanisms in place, usage of Bluetooth might result in exploits and data loss from the device through the following methods:

<p><b>Bluejacking</b></p>	<p>This is the process where an attacker sends unsolicited messages or business cards to a Bluetooth-enabled device, mostly for advertising purposes. Bluejacking resembles spam and phishing attacks conducted against e-mail users.</p> <p>When a bluejacking message is sent with a harmful intent, it might entice users to respond with action to add the new contact to the device’s address book. Bluetooth device owners should be aware that this might cause a variety of social engineering attacks where it manipulates user into performing actions or divulging confidential information.</p> <p>Devices that are set in non-discoverable mode are not susceptible to bluejacking and in order for bluejacking to work; the sending and receiving devices must be within 10 meters distance.</p>
---------------------------	--

<b>Bluesnarfing</b>	<p>This is a method to force a connection with a Bluetooth-enabled device to gain access to data such as contact list, calendar, emails, text messages, pictures, videos and the international mobile equipment identity (IMEI) stored in the memory. IMEI is a unique identifier for devices, and can be exploited by an attacker to divert all incoming calls from the user's device to the attacker's device.</p> <p>As sensitive information may be stolen from devices through bluesnarfing, it is much more malicious compared to bluejacking, even though both exploit devices' Bluetooth connections without the owners' knowledge. By setting a device's Bluetooth to non-discoverable mode, the device becomes less susceptible to bluesnarfing although it may still be bluesnarf-able via brute force attack.</p>
<b>Bluebugging</b>	<p>This method was developed after the onset of bluejacking and bluesnarfing where it allows attackers to remotely access a Bluetooth-enabled device and use its features, such as read phonebooks, examine calendar, connect to the Internet, place phone calls, eavesdrop on phone calls through call forwarding and send messages without the user's knowledge. As with all the attacks, the attacker must be within a 10 meters distance from the device.</p>
<b>Bluesmack</b>	<p>This is a Bluetooth Denial Of Service (DOS) attack where the Bluetooth-enabled device is overwhelmed by malicious requests from an attacker, causing it to be inoperable by its owner and draining the device's battery, affecting the continued operation of the device after the attack. Due to the proximity required for Bluetooth connection, users can move the device to a new location to prevent the attack from happening.</p>

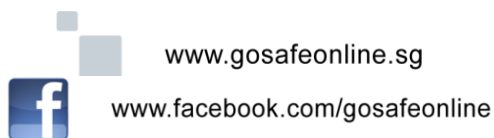
## Tips On Safe Bluetooth Usage

You may already be using Bluetooth technology to communicate to a mobile phone headset or connect your computer to an optical mouse, as with all the good technology, attackers are finding ways to exploit the capabilities. Use the following tips to help keep your Bluetooth-enabled device secure.

- 
  - ✓ The 'discoverable' mode on your device is only meant to be used to "pair" two Bluetooth-enabled devices. When the pairing process is done, the 'discoverable' mode can be turned off as the devices should remember each other.
- 
  - ✓ Refrain from communicating or transmitting sensitive and personal information using the Bluetooth-enabled device as it might be sniffed.
- 
  - ✓ Use strong passkey that is randomly generated when pairing Bluetooth devices and never enter passkeys when unexpectedly prompted for them.
- 
  - ✓ Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- 
  - ✓ Avoid accepting attachments or applications received on your phone or device if you were not expecting it no matter how legitimate it may be. If your device asks to pair and you didn't initiate the pairing, deny it and check that your 'discoverable' setting is set to 'off' or 'hidden'.

## Interesting Reads

- Bluetooth:  
<http://en.wikipedia.org/wiki/Bluetooth>
- How Bluetooth works:  
<http://www.techrepublic.com/article/secure-your-bluetooth-wireless-networks-and-protect-your-data/6139987>
- Bluetooth vulnerabilities and risk :  
[http://www.infosecwriters.com/text\\_resources/pdf/Bluetooth\\_CRhodes.pdf](http://www.infosecwriters.com/text_resources/pdf/Bluetooth_CRhodes.pdf)
- Bluetooth precautions :  
[http://www.nsa.gov/ia\\_files/factsheets/1732-016R-07.pdf](http://www.nsa.gov/ia_files/factsheets/1732-016R-07.pdf)



Published by:

A member of:



## In the next issue...

Learn about the different types of hacking .

Let us know what you like about this newsletter and what we can do to better serve your infocomm security awareness needs.

If you have any enquiries or feedback for our newsletter, do write to us at [contact\\_us@gosafeonline.sg](mailto:contact_us@gosafeonline.sg).



**BE AWARE, RESPONSIBLE  
AND SECURE!**

Copyright © 2013 - Infocomm Development Authority of Singapore.  
All rights reserved. Reproduction without permission is prohibited.