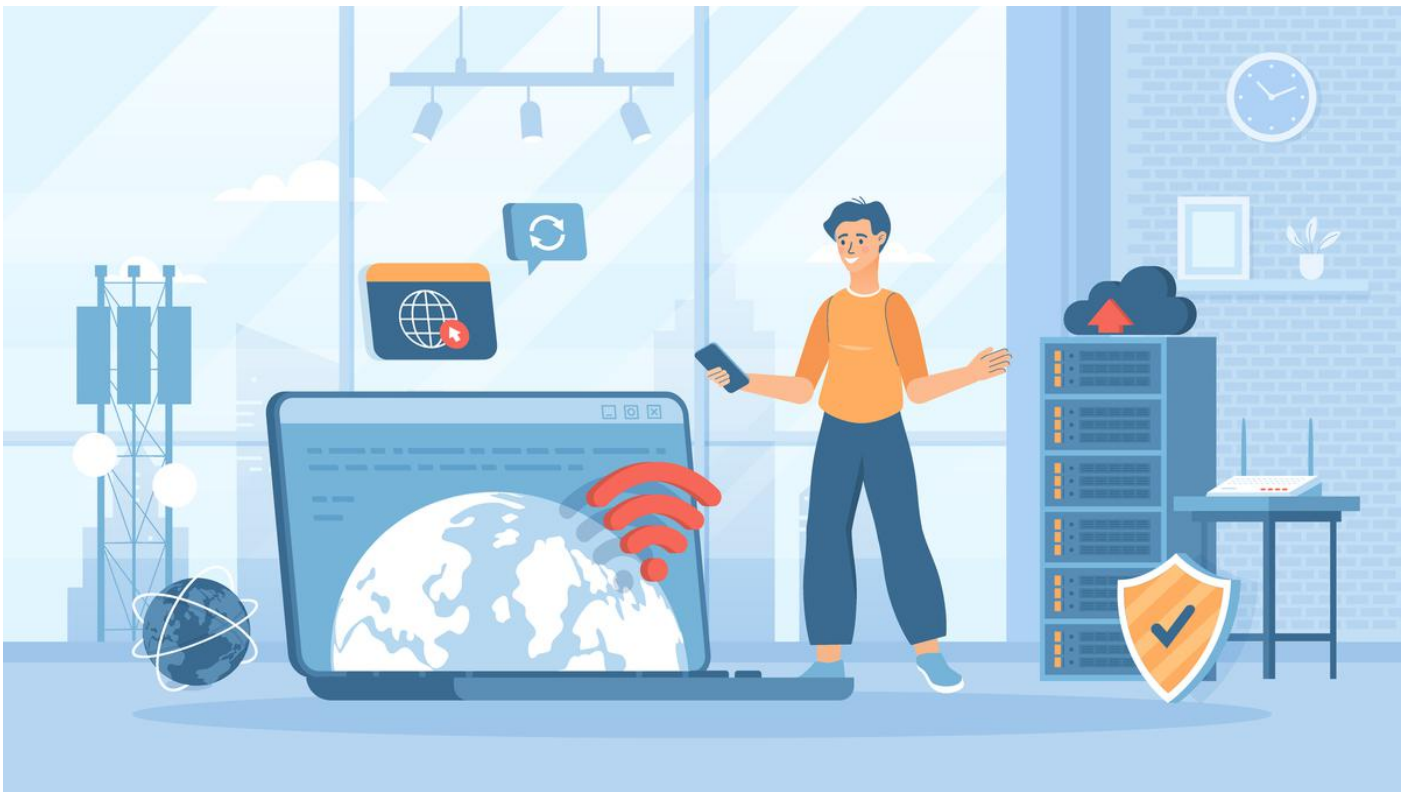
devices?

Several smartphones have their Bluetooth settings on discovery mode as it is a default setting, making it easy for hackers to access the phones when they are within 10 metres from the device

November 28, 2022 10:30 am | Updated 10:30 am IST

ABHISHEK CHATTERJEE

COMMENTS SHARE READ LATER



The story so far:

Cybersecurity experts note that apps that let users connect smartphones or laptops to wireless earplugs can record conversations, and are vulnerable to hacks. Even the most secure smartphones like iPhones are vulnerable to such attacks. Any app with access to Bluetooth can record users' conversations with Siri and audio from the iOS keyboard dictation feature when using AirPods or Beats headsets, some app developers say. Through a process called bluebugging, a hacker can gain unauthorised access to these apps and devices and control them as per their wish.

What is bluebugging?

It is a form of hacking that lets attackers access a device through its discoverable Bluetooth connection. Once a device or phone is bluebugged, a hacker can listen to the calls, read and send messages and steal and modify contacts. It started out as a threat for laptops with Bluetooth capability. Later hackers used the technique to target mobile phones and other devices.

Independent security researcher Martin Herfurt blogged about the threat of bluebugging as early as 2004. He noted that the bug exploited a loophole in Bluetooth protocol, enabling it to download phone books and call lists from the attacked user's phone.

How does bluebugging hack devices?

Bluebugging attacks work by exploiting Bluetooth-enabled devices. The device's Bluetooth must be in discoverable mode, which is the default setting on most devices. The hacker then tries to pair with the device via Bluetooth. Once a connection is established, hackers can use brute force attacks to bypass authentication. They can install malware in the compromised device to gain unauthorised access to it. Bluebugging can happen whenever a Bluetooth enabled device is within a 10-metre radius of the hacker. However, according to a blog by VPN service provider NordVPN, hackers can use booster antennas to widen the attack range.

How can one prevent bluebugging ?

Turning off Bluetooth and disconnecting paired Bluetooth devices when not in use, updating the device's system software to the latest version, limited use of public Wi-Fi and using VPN as an additional security measure are some of the ways to prevent bluebugging, Shubho Pramanik, senior vice president, Applied Cloud Computing, a Thane based cloud service provider, said to *The Hindu*.

Most devices make Bluetooth discoverable by default, leaving your devices susceptible to unsolicited connections. So, the first step would be to make your Bluetooth devices undiscoverable from Bluetooth settings. This will keep them invisible to hackers, thereby not letting them pair with the device, NordVPN said in the blog.

Users must also watch out for suspicious activities on their devices, NordVPN suggested. “If your phone is suddenly disconnecting and reconnecting calls, or if you notice messages that haven’t been sent by you, it could indicate that someone is controlling your device. Reset the device to its factory settings or uninstall any apps you don’t recognise.” One should also monitor sudden spikes in data usage. If the amount of data used suddenly spikes beyond reason, someone could be controlling the device as part of a botnet that eats up data, NordVPN said.

Modern anti-virus softwares can also help thwart such attacks. The new-age antivirus softwares are helping users to detect strange and spam-like content by filtering, blocking and consistently reminding people to be alert, Manoj Kumar Shastrula, CEO and Founder, SOCLY.io, a cybersecurity company told *The Hindu*.

Which devices are most susceptible to such attacks?

Any Bluetooth-enabled device can be bluebugged. Wireless earbuds are susceptible to such hacks. Apps that enable users to connect to their TWS (True Wireless Stereo) devices or earbuds can record conversations. The apps of these TWS devices can record conversations. Once hacked, the attacker can make and listen to calls, read and send messages, and modify or steal your contacts, Mr. Pramanik said.

Apple also acknowledged earlier that wireless earbuds can record conversations. “An app may be able to record audio using a pair of connected AirPods,” Apple said on its support page while releasing the fixes to the issue. However, smartphones are more vulnerable to this type of hacking as most of the users leave their Bluetooth on in public places, where hackers may be lurking.

Today, several smartphones have their Bluetooth settings on discovery mode, making it easy for hackers to access the phones when they are within 10 metres from the device. Some earlier models of Bluetooth phones were vulnerable to bluebugging, but have since been corrected,