



# Voyager USB Bluetooth security

## How secure is my Plantronics headset and can the USB device be used to copy files to or from my PC?

Plantronics takes customer's security concerns seriously and despite widespread press reports of Bluetooth security vulnerabilities in Bluetooth devices such as phones and PDAs, the audio connection between a PC or phone and a Plantronics Bluetooth headset remains highly secure.

The Plantronics Voyager USB system comes with a USB "dongle" that allows a PC to communicate with the Voyager headset. The USB dongle only supports the Bluetooth standard Headset profile and therefore only allows the PC to send and receive audio data. It cannot be used to transfer files, contact information or other data. For security, none of the other standard Bluetooth profiles are available. Furthermore, the PC will detect and install the Plantronics dongle as a standard Windows™ compatible HID audio device, not a Bluetooth device. Even if standard Bluetooth software was installed on the PC, it cannot recognize or use the Plantronics USB device to transfer data.

Bluetooth headsets take advantage of Bluetooth security features such as authentication and encryption to ensure that a headset conversation remains private.

Headsets need only be "discoverable", or visible to other devices when they are newly introduced to a mobile phone. This mode enables the devices to exchange a unique Bluetooth address – similar to a long serial number. When headsets are not in discoverable mode, they will not appear in a search performed by another Bluetooth device. However, the headset is still available to those devices that have already discovered its' unique address during an earlier exchange.

Plantronics headsets are always in non-discoverable mode unless they are explicitly put into "Pairing mode", when they will be discoverable for only a short time, so that a user can set up a connection from a mobile phone.

When pairing is initiated, the devices exchange their Bluetooth addresses and the user will be asked to enter a PIN number. The Bluetooth address, PIN number and a unique time-related code generated from the mobile phone are exchanged to generate a 128-bit security key which is used by the headset for future connections to the phone. The time-related code is extremely difficult to guess at a later date, even if the address and PIN are already known to a potential eavesdropper.



For optimal security, care should be taken during pairing to ensure that a potential eavesdropper is not within range of the phone and headset and that none of the three elements required are accessible to them – the Bluetooth addresses, PIN code and time-related information.

## How secure is my Plantronics headset?

The Plantronics headset subsequently uses the generated 128-bit security key to digitally encrypt audio streams between the headset and phone, just as the GSM radio signals between the mobile phone and base station are encrypted. This system ensures that telephone conversations never appear as unencrypted speech across the air.

Because of the low power of Bluetooth transmissions, the audio conversation is broadcast over a short range, typically 10 metres radius, making it even more difficult for a potential eavesdropper to attempt to listen in as they must be in very close proximity during any conversation, or use a large antenna.

Many widely publicised Bluetooth vulnerabilities do not apply specifically to headsets, but there are some things that can be done to improve security on the phone:-

For instance,

“Bluesnarfing” is a method by which telephone contact details can be stolen from a Bluetooth phone or PDA. No data is stored in the headset, so the only vulnerability remains in the phone. To make the phone more secure, “discoverable” mode can be disabled as it is not necessary when pairing or using a Bluetooth headset.

Making the phone “non-discoverable” also eliminates many other possible Bluetooth security exploits such as “Bluejacking”.

[www.plantronics.com](http://www.plantronics.com)

© 2005 Plantronics, Inc. All rights reserved. Plantronics, the logo design and Sound Innovation are trademarks or registered trademarks of Plantronics, Inc. The Bluetooth name and the Bluetooth trademarks are owned by Bluetooth SIG, Inc., and are used by Plantronics, Inc. under license. All other trademarks are the property of their respective owners.