What is Bluetooth?

Bluetooth is a method of connecting devices so that they can communicate with each other wirelessly and, often, automatically. The most common form of Bluetooth is the earpiece people use to talk on their cell phones. Bluetooth can be used with many other technologies, such as computers, entertainment systems or telephones, and other electronic devices.

In general, Bluetooth technology can be used to send and receive things like phonebook/address book contacts, pictures & videos to other Bluetooth enabled devices wirelessly over a short range.

How Does It Work?

When two Bluetooth enabled devices are paired, information travels along a radio wave to transfer data. For a more technical explanation of how it works, go here: http://www.bluetooth.com/Bluetooth/Technology/Works/

How Do You Pair a Device?

Pairing means that two Bluetooth devices are partnered so that each time they are both turned on and in range, they know to trust each other and work together. To pair the devices, a pass code must be shared by both Bluetooth devices, which proves that both users have agreed to pair with each other. On some devices, the code can be anything you like as long as it is the same for both Bluetooth wireless devices. On other devices, such as Bluetooth headsets, the pass code is pre-set. Refer to the product's manual for the default pass code.

- Jill's Bluetooth phone is set to "discoverable mode" and looks for other Bluetooth devices in the area

- Jill's Bluetooth phone finds Brad's Bluetooth Device Usually the discoverable device will indicate what type of device it is (Such as a printer, cell phone, headset, etc.) and its Bluetooth device name.

- Both Bluetooth Devices prompt their users to enter a pass code. Both users must agree on the pass code and enter it into their device. In general, devices only need to be paired once.

- The devices are now paired and able to exchange data. So, Jill can now use their Bluetooth connection to send Brad a copy of the new game she downloaded, sync her calendar with Brad's calendar, or send photos. When sending things via Bluetooth, no extra charges are incurred (as they might be when you send photos via text message or email).

Web: nnedv.org/safetynet • Email: SafetyNet [at] nnedv.org • Phone: 202-543-5566

Bluetooth: Security Risks

What are the Bluetooth Security Risks?
Bluetooth allows users to share contacts (business cards or address book entries), images, or videos. However, since Bluetooth is wireless it is vulnerable to hacking, spying, and remote access.

Bluejacking: usually involves sending a random message to a stranger's phone without needing to know their phone number. For example, Julie uses her Bluetooth enabled phone to search for other Bluetooth devices. She sees another Bluetooth phone and decides to have a little fun and send a message saying "You've been bluejacked." The message isn't harmful to the phone and data on the victim's device doesn't get changed or stolen. For some people, a random message popping up on the screen would just be a weird annoyance. But if an abuser is sitting outside the victims workplace and starts to send messages that say "I know what you did last night" it can quickly become a vehicle for stalking. The sender must be within 30 feet.

Bluesnarfing: allows illegitimate access to a calendar, contact list, emails and text messages, and on some phones users can steal pictures and private videos. A bluesnarfer can:

- Read and delete phonebook entries
- Read and delete SIM card entries
- Make phone calls from target phone

Generally, the hacker must be within a 30 feet range unless s/he has advanced equipment and expertise. According to Bluetooth Special Interest Group (SIG), only specific older Bluetooth enabled phones are susceptible to bluesnarfing.

Bluebugging is similar to bluesnarfing. Hackers can make phone calls, send and receive text messages, read/write phone contacts, eavesdrop on phone conversations and connect to the Internet.

Car Whisperer is software that uses the Bluetooth hands-free car kit to send or receive audio from the inside of a car. The software takes advantage of the fact that many of these hands-free systems use the same default access code. For hackers to pair their phone or PDA with your car's hands free, the hands free kit must be on and in "pairing" mode and NOT be connected to a phone. As with other hacking risks, the hacker must be within 30 feet of the Bluetooth, unless s/he has special equipment. To minimize your car's Bluetooth being compromised by the Car Whisperer, ensure that the hands free kit is not in continuously paired mode and change the passcode from the factory default.

In addition to using Bluetooth to access your phone/PDA, a stalker can also use it to detect when you're within (the range) 30 feet or so. The stalker can set up a program on his/her own cell phone or computer that will automatically alert him/her when your Bluetooth comes into range.

Bluetooth: Safety Tips

How Can I Minimize Security Risks?

- ✓ If an abuser has access to your device without your knowledge (for ex: while you're in the shower) the abuser can set your device to pair with the abuser's device. Some phones will show a pop up message or an icon every time they connect to another device while others will not. If you feel your phone is acting strangely, turn your Bluetooth setting to "off."

- ✓ Users can set their Bluetooth to be "discoverable" or "non-discoverable." If the Bluetooth option is set to discoverable, it is very easy to discover your device and download your information. Setting the Bluetooth to **non-discoverable** or **off** will decrease the risk of your data being hacked.

- ✓ Pick a pass code that is harder to guess. When you first pair your devices, it asks for a pass code. Don't use your birth date or the last 4 digits of your SSN or phone number. Only share that PIN with trusted individuals or trusted pairing devices.

- ✓ Don't pair your device with unknown devices. Also avoid pairing devices in public, since a hacker can compromise the pass code during pairing.

What Devices might have Bluetooth?

- Cell phones (particularly smart phones, like a BlackBerry or a Treo)
- Personal digital assistants (PDAs)
- Hands-free headset (including Bluetooth hands free car-kit)
- Computers (laptops)
- Keyboards, mouse, and printers
- Nintendo Wii and Sony PlayStation 3

For more information about Bluetooth, go to:
http://bluetooth.com/Bluetooth/Fast_Facts.htm
http://bluetooth.com/Bluetooth/Technology/Works/Security/Protecting.htm

Did You Know…

Bluetooth was named for a late tenth century king, Harald Bluetooth, King of Denmark and Norway. King Bluetooth was known for uniting warring factions of what is now Norway, Sweden, and Denmark. According to Bluetooth SIG, Bluetooth technology is designed to unite different types of technologies, such as computers, cell phones, keyboards, etc.

Web: nnedv.org/safetynet • Email: SafetyNet [at] nnedv.org • Phone: 202-543-5566