Understanding Bluetooth Technology

Many electronic devices are now incorporating Bluetooth technology to allow wireless communication with other Bluetooth devices. Before using Bluetooth, it is important to understand what it is, what security risks it presents, and how to protect yourself.

What is Bluetooth?

Bluetooth is a technology that allows devices to communicate with each other without cables or wires. It is an electronics "standard," which means that manufacturers that want to include this feature have to incorporate specific requirements into their electronic devices. These specifications ensure that the devices can recognize and interact with other devices that use the Bluetooth technology.

Many popular manufacturers are making devices that use Bluetooth technology. These devices include mobile phones, computers, and personal digital assistants (PDAs). The Bluetooth technology relies on short-range radio frequency, and any device that incorporates the technology can communicate as long as it is within the required distance. The technology is often used to allow two different types of devices to communicate with each other. For example, you may be able to operate your computer with a wireless keyboard, use a wireless headset to talk on your mobile phone, or add an appointment to your friend's PDA calendar from your own PDA.

What are some security concerns?

Depending upon how it is configured, Bluetooth technology can be fairly secure. You can take advantage of its use of key authentication (see Understanding Digital Signatures for more information) and encryption (see Understanding Encryptionfor more information). Unfortunately, many Bluetooth devices rely on short numeric PIN numbers instead of more secure passwords or passphrases (see Choosing and Protecting Passwords for more information).

If someone can "discover" your Bluetooth device, he or she may be able to send you unsolicited messages or abuse your Bluetooth service, which could cause you to be charged extra fees. Worse, an attacker may be able to find a way to access or corrupt your data. One example of this type of activity is "bluesnarfing," which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost. You should also be aware of

attempts to convince you to send information to someone you do not trust over a Bluetooth connection (see Avoiding Social Engineering and Phishing Attacks for more information).

How can you protect yourself?

- **Disable Bluetooth when you are not using it** - Unless you are actively transferring information from one device to another, disable the technology to prevent unauthorized people from accessing it.
- **Use Bluetooth in "hidden" mode** - When you do have Bluetooth enabled, make sure it is "hidden," not "discoverable." The hidden mode prevents other Bluetooth devices from recognizing your device. This does not prevent you from using your Bluetooth devices together. You can "pair" devices so that they can find each other even if they are in hidden mode. Although the devices (for example, a mobile phone and a headset) will need to be in discoverable mode to initially locate each other, once they are "paired" they will always recognize each other without needing to rediscover the connection.
- **Be careful where you use Bluetooth** - Be aware of your environment when pairing devices or operating in discoverable mode. For example, if you are in a public wireless "hotspot," there is a greater risk that someone else may be able to intercept the connection (see Securing Wireless Networks for more information) than if you are in your home or your car.
- **Evaluate your security settings** - Most devices offer a variety of features that you can tailor to meet your needs and requirements. However, enabling certain features may leave you more vulnerable to being attacked, so disable any unnecessary features or Bluetooth connections. Examine your settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. Make sure that all of your Bluetooth connections are configured to require a secure connection.
- **Take advantage of security options** - Learn what security options your Bluetooth device offers, and take advantage of features like authentication and encryption.

Authors: Mindi McDowell, Matt Lytle

Produced 2010 by US-CERT, a government organization.
