

## **Protecting your Bluetooth Device**

- Always upgrade. Make sure the software and firmware on your Bluetooth devices, especially cell phones, are the latest versions.
- Disappear. Place all Bluetooth-enabled devices in a nondiscoverable mode. You can make this setting through a software menu on your handheld.
- Scramble your data. Encrypt everything stored on your device so that in the event of a hack, the information is protected.
- Don't jot things down. Avoid storing usernames, passwords or other sensitive information on a Bluetooth-enabled device.
- Be smart. Avoid pairing with unknown devices.
- Change your PIN. A personal identification number is normally needed for pairing. Make yours at least eight characters long and alphanumeric. Hackers have demonstrated ways of intercepting simple PINs.
- Be discrete. In theory, device-to-device connections could be monitored by a third person. For maximum security, don't pair in public or in a crowded area.
- Location, location, location. Bluetooth attackers need to be close (within 10 meters) so if you're getting attacked, move to another area and note who's following you.
- Power down. For maximum security, turn off your Bluetooth features when not using them.