Security for Electronic Devices

When you think about security, remember that electronics such as cell phones and PDAs are also vulnerable to attack. Take appropriate precautions to limit your risk.

Why does security extend beyond computers?

Actually, the issue is not that security extends beyond computers — it's that computers extend beyond traditional laptops and desktops. Many electronic devices are computer — from cell phones and PDAs to video games and car navigation systems. While computers provide increased features and functionality, they also introduce new risks. Attackers may be able to take advantage of these technological advancements to target devices previously considered "safe."

For example, an attacker may be able to infect your cell phone with a virus, steal your phone or wireless service, or access the data on your PDA. Not only do these activities have implications for your personal information, but they could also have serious consequences if you store City information on the device.

What types of electronics are vulnerable?

Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the internet or a network that an attacker may be able to access. This includes wireless networks. The outside connection provides a way for an attacker to send information to or extract information from your device.

How can you protect yourself?

- Remember physical security — Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas.
- Keep software up to date — If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- Use strong passwords — Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different

passwords for different programs and devices. Do not choose options that allow your device to remember your passwords.

- Disable remote connectivity — Some PDAs and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when you're not actively using them.

Reference: Information in this document was provided by US-CERT, www.us-cert.gov.