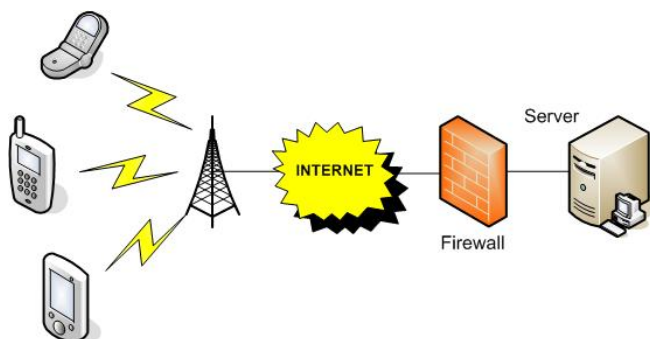




## Handheld Communications

### Introduction

Cell phones, Personal Digital Assistant (PDAs) and Smartphones are all considered "Handheld devices". They may incorporate voice and data communications and may also possess independent processing capability.



### Overview

**Cell phone devices** utilize the cell phone network maintained by the company that issued the cell phone. A cell phone can provide voice, text and e-mail communications as well as internet browsing.

**PDAs** (Personal Digital Assistant) are handheld computers that include cell phone capabilities as well as office productivity tools such as calendars, task manager, address book and note pads. PDAs are also referred to as "Smartphones".

### Features

Powerful handheld devices have become the targets of cyber-threats and should be protected to a level commensurate with the sensitivity of the data it contains or has networked access to. A determined attacker can intercept the devices' wireless transmissions; therefore the employee should consider the following aspects of security:

**Authentication:** employees should be required to authenticate their 'system access credentials' to both the handheld device and to any networked application server.

**Availability:** The handheld device should have unrestricted access to the 911 emergency system. The employee's ability to answer incoming calls should not be disabled or require user authentication.

**Malware:** Handheld devices are vulnerable to malware through internet browsing and the inadvertent downloading of malicious files.

**Confidentiality:** Privacy issues or breaches of the organizations security policy may be caused by improper disposal or theft of the device.

**Bluetooth:** Publicly known vulnerabilities render Bluetooth insecure. If it is not specifically required disable this functionality. Otherwise the Bluetooth functionality should be configured so that other Bluetooth enabled devices cannot sense it nor initiate communications with it; synchronize the handheld device with a PC manually.

**Encryption:** The employee should assume that the handheld devices' wireless communications can be intercepted; this requires that all transmissions be encrypted. Data privacy requires that all stored data be encrypted for its protection in the event that the device is lost or stolen.