Securing Mobile Devices

Module 13

Simplifying Security.

Certified Secure Computer User

Module 13: Securing Mobile Devices

Exam 112-12

Module Objective

Wireless networks, as the name suggests, allow users to connect their devices to the Internet without relying on wires. Attackers may **intercept** an **unsecured** wireless network to steal the information present on the **wireless device**. This module talks about security measures that users need to follow to secure their wireless devices.

This module will familiarize you with:

- Mobile Device Security
- Mobile Phone Services
- Mobile Device Security Risks
- Mobile Malware
- Threats to Bluetooth Devices
- Mobile Security Procedures
- Mobile Phone Anti-Virus Tools
- Secure Bluetooth Connectivity
- Securing iPhone and iPad
- Securing Blackberry and Windows Phone 7 Mobiles
- Mobile Security Tools
- Mobile Phone Security Checklist

Module Flow

Introduction to Mobile Security

Mobile Security Threats

Mobile Security Procedures

Securing iPhone, and iPad

Security Blackberry and Windows Phone 7 Mobiles

Mobile Security Tools

Mobile Device Security

Source: http://www.gartner.com

- The rate of mobile device **adoption** and **sophistication** is increasing rapidly.
- Mobile devices such as smartphones, PDAs, and laptops facilitate **seamless communication** and information storage and have been an incalculable productivity boon for today's enterprises.
- Mobile devices offer flexibility and convenience, while at the same time; mobility presents **significant security challenges** for IT security administrators and other users.

Mobile Phone Services

Mobile phone services include:

- Emails & Messaging
- Mobile commerce
- Gaming
- Web browsing
- GPS maps and tracking
- General purpose applications such as calculator, planners, etc.

IMEI Number

International Mobile Equipment Identity (IMEI) is a number unique to every mobile phone. A user should always use a mobile containing an IMEI number, which helps the user track the phone and gives the device an identity.

IMEI is usually found printed inside the battery compartment of the phone. In some mobile devices, it can also be displayed on the phone's screen by entering ***#06#.**

IMEI number identifies the subscriber with the number's transmission. It has no permanent or temporary relation with the customer or the subscriber. IMEI is used to **deactivate** the phone if it is stolen or lost.

Mobile Device Security Risks

Mobile devices have many uses. However, as the number of mobile devices increases day by day, access to the corporate information also increases with **increased security risks**.

Security risks associated with mobile devices include:

- **Mobile malware:**

  Mobile malware is a fast growing threat that is difficult to detect. Among all other malware, mobile malware can **spread more quickly**. It is expected that the growth of mobile malware will increase the growth of Internet malware. Most individuals and organizations now depend on mobile communication. A pandemic-level attack can **harm millions of mobile users**.

- **Application vulnerabilities:**

  Mobile devices running on Symbian, PalmOS, and Windows mobile operating systems consist of many open application programming interfaces (APIs), which are **vulnerable to attack**. The OS has a number of connectivity methods through which malware can be spread.

- **Lost or stolen devices:**

  When a user loses a mobile device, he/she is not only losing the hardware but also valuable **confidential personal data**. So, securing mobile devices keeps a user free from worry that personal data that is lost.

- **Unauthorized access:**

  Unauthorized access is used by attackers to access a mobile device and **gain confidential data** or contacts of the user. A user can prevent unauthorized attacks by securing the device with updated security programs and techniques.

Mobile Malware

Mobile malware may be transmitted to mobile devices from infected computers or other infected mobile devices. Mobile malware may spread through:

- **Emails, IMs, Bluetooth, memory cards, and Wi-Fi:** A malware-infected smartphone spreads malware to another smartphone via wireless LAN. The mobile malware can infect many mobiles through Multi Messaging Service (MMS), and then the infected device can spread malware to another mobile device by using General Radio Packet Service (GPRS)
- **Rouge software:** Rogue software often contains malware and spreads onto the mobile device when the user tries to install the software on the device.
- **Infected computers:** Malware can be transmitted onto mobile devices through Bluetooth or infrared technologies when the mobile device is within range of an infected computer.

Mobile malware can:

- **Monitor** and record all the actions on a mobile phone

  Malware allows attackers to access critical and often confidential information stored on the device and on the network those devices connect to.

- **Capture** emails, text, and multimedia messages

  Malware can steal contact information, address lists, and message and call logs.

- Allow the attacker to silently turn the phone on to **listen** to a user's conversation

  It is difficult to the user to detect the secret listener.

- Make a user's mobile work slowly or **crash**

  In some cases, the malware can also be used to issue commands from the device, so the attacker can have total control of a smartphone or mobile phone to make calls and send messages.

- **Wipe out** contact books and other **information** on the phone

  Malware will spread faster across a mobile network and it is difficult to detect because of complicated virus-writing techniques.

Mobile Application Vulnerabilities

The latest mobile devices provide openness platform functionality. This gives the user the flexibility to operate and program any type of mobile applications that are supported by and compatible with their smartphones. Openness also leads to **unrestricted access** to mobile resources and applications. Vulnerabilities in applications can be used by attackers to access the device. They can also access a user's contact book, read messages and mail using various mobile spywares, and gain access to a user's call to listen the personal conversations.

Mobile Operating System

Advanced mobile phones usually work on any of the following operating systems:

- **Symbian**

  The Symbian operating system is an open mobile operating system founded in 1998. This OS supports a wide range of devices that are categorized with different user interfaces.

- **Windows Phone 7**

  Windows Phone 7 is a mobile operating system developed by Microsoft, and is the successor to its Windows Mobile platform. It offers a new user interface with its design language named Metro, integrates the operating system with third party and other Microsoft services, and controls the hardware it runs on.

- **Windows Mobile**

The Windows Mobile operating system was developed by Microsoft Corporation. It is a non-component based operating system used in mobile devices and smartphones. It acts as a standard platform for PDAs and cell phones to provide common user interfaces.

- **Pocket PC**

  Pocket PC is the freeware operating system developed by Windows. Some of its features are remote control, weather reports, mapping and GPS navigation flexibility, and an organizer.

- **Linux**

  This is another important operating system that provides integrated software environment to run Java and Linux applications.

- **Palm OS**

  Palm OS is one of the most popular handheld compact operating systems designed in 1996. It is also called Garnet OS. This embedded OS was first developed by U.S. Robotics, which was later owned by Palm Computing, Inc. for personal digital assistants (PDAs). Palm OS provided a touch screen based graphical user interface. It also created a collection of basic applications for personal information management.

Applications

A user can choose from various applications available in the features of the mobile device. Some of the applications include:

- **Web browser**

  A Web browser connects the user to the Internet just like a browser in a PC. It helps the user retrieve and send information by connecting to the World Wide Web.

- **Mobile Banking Application**

  Mobile banking helps the user perform transactions and banking options such as fund transfer, bill payments, and net banking.

- **Mobile Gaming**

  Mobile gaming is similar to video games. It is played on mobile phones, portable media player, smartphones, PDAs, etc.

Threats to Bluetooth Devices

Bluetooth is an open standard wireless technology for exchanging data over **short-range radio frequencies** from fixed to mobile devices by creating **Wireless Personal Area Networks (WPANs).** Threats to Bluetooth device include:

- **Bluejacking**

Bluejacking refers to anonymously sending an electronic business card or photo to another Bluetooth user.

- **Bluesnarfing**

  A Bluesnarfing attack is launched using the Bluejacking technique. It allows an attacker to access the address book, contact information, email, and text messages of another user's mobile phone.

- **Bluesniping**

  Bluesniping uses a highly directional antenna and a laptop to establish connections with Bluetooth-enabled devices from more than half a mile away.

- **War Nibbling**

  War nibbling refers to finding unsecured or unpatched Bluetooth connections and cruising for open 802.11 networks.

Mobile Security Procedures

The security procedures for mobile devices include:

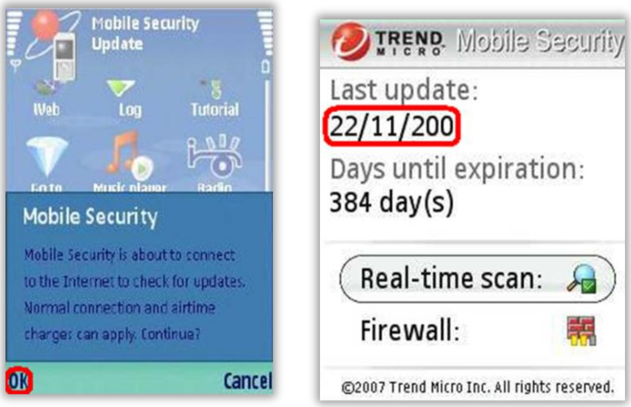
- Patch mobile platforms and applications
- Avoid mobile device theft
- Use power-on authentication
- Regularly back up important data
- Use encryption to secure data in mobile device
- Enable the auto-lock feature
- Install only signed applications
- Install mobile phone anti-virus
- Secure Bluetooth connectivity

Patching Mobile Platforms and Applications

All mobile platforms and applications should be **updated regularly** with the patches released by the vendor. Patching enhances the performance of a mobile device, updates the operating system, fixes security holes and bugs, etc. To patch your mobile operating system and applications:

- Download the update to your mobile device to install the patch.
- Back up all data and files on your mobile device.
- Install the patch file to your mobile device.

- Turn off your mobile device for 5 to 10 minutes before you start using it.



Mobile Security is about to connect to the Internet to check for updates. Normal connection and airtime charges can apply. Continue?

Last update:
22/11/200

Days until expiration:
384 day(s)

Updating **Updated**

Figure 13-01: Patching of Mobile Platforms and Applications with Latest Update

Avoid Mobile Device Theft

Mobile phone thefts are increasing day by day and thousands of people lose their mobile handsets everyday around the world. The loss of a mobile phone results in the **loss of important data**, contacts, messages, images, and videos stored in the mobile phone.

- **Avoid lending** mobile phone to strangers.
- Do not talk/text while walking or driving and do not leave the handset in the vehicle.
- Do not leave the phone unattended in any place.
- **Use PIN** codes to lock the phone.
- Turn off the ringer.
- **Record** the unique 15- or 17-digit code **IMEI** (International Mobile Equipment Identity) of the mobile and keep it in a secure place.
- **Report** doubtful calls to the service provider.
- **Review** phone bills at the end of every month.
- Avoid using the cell phone at the public spots or lonely areas; this can prevent the cell phone thefts.
- Only use the phones with an IMEI number so it can be tracked if the phone is lost.
- Always choose to use a **security code** or password on the mobile device.

What to DO if Your Mobile is Lost or Stolen

Attackers use unauthorized access to gain confidential data or contacts from a user's mobile device. Most users do not protect their mobile phones and devices with a **password**.

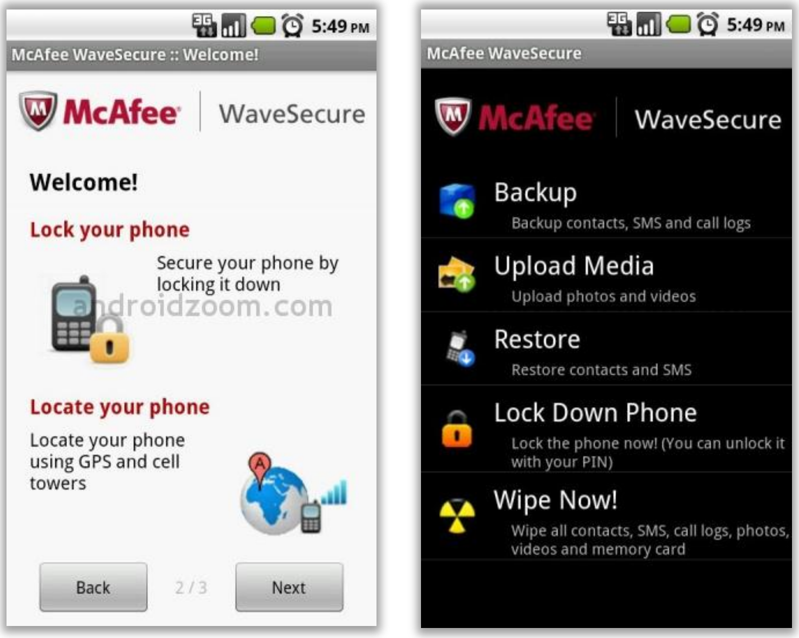
They can download addresses and other personal information from the users' mobile device without their knowledge. Attacker may use those mobiles for **illegal activities**. Some attackers not only extract the users' information but also change all of the contact numbers. Some of the best practices to secure mobile phones include:

- Use **anti-theft software** to remotely wipe the data and make the device unusable
- Inform local police and file first information report (**FIR**)
- Contact the service provider and **cancel the SIM** card
- Claim the mobile **phone insurance** to replace the cost of the handset

Use Power-On Authentication

Provide a **power-on password** or PIN, so that the device cannot be powered by an unauthorized user. This keeps the personal information of the user untouched. This configuration setting also secures the data and contacts of the user.

- Set power-on authentication in your phone to ensure maximum security and so that no other unauthorized user can use it.
- Power-on authentication helps protect valuable information from malicious users who can gain access to a user's mobile phone.
- You can use the **WaveSecure tool** to lock your mobile phone.



McAfee WaveSecure :: Welcome!

Welcome!

Lock your phone

Secure your phone by locking it down

Locate your phone

Locate your phone using GPS and cell towers

McAfee WaveSecure

Backup

Backup contacts, SMS and call logs

Upload Media

Upload photos and videos

Restore

Restore contacts and SMS

Lock Down Phone

Lock the phone now! (You can unlock it with your PIN)

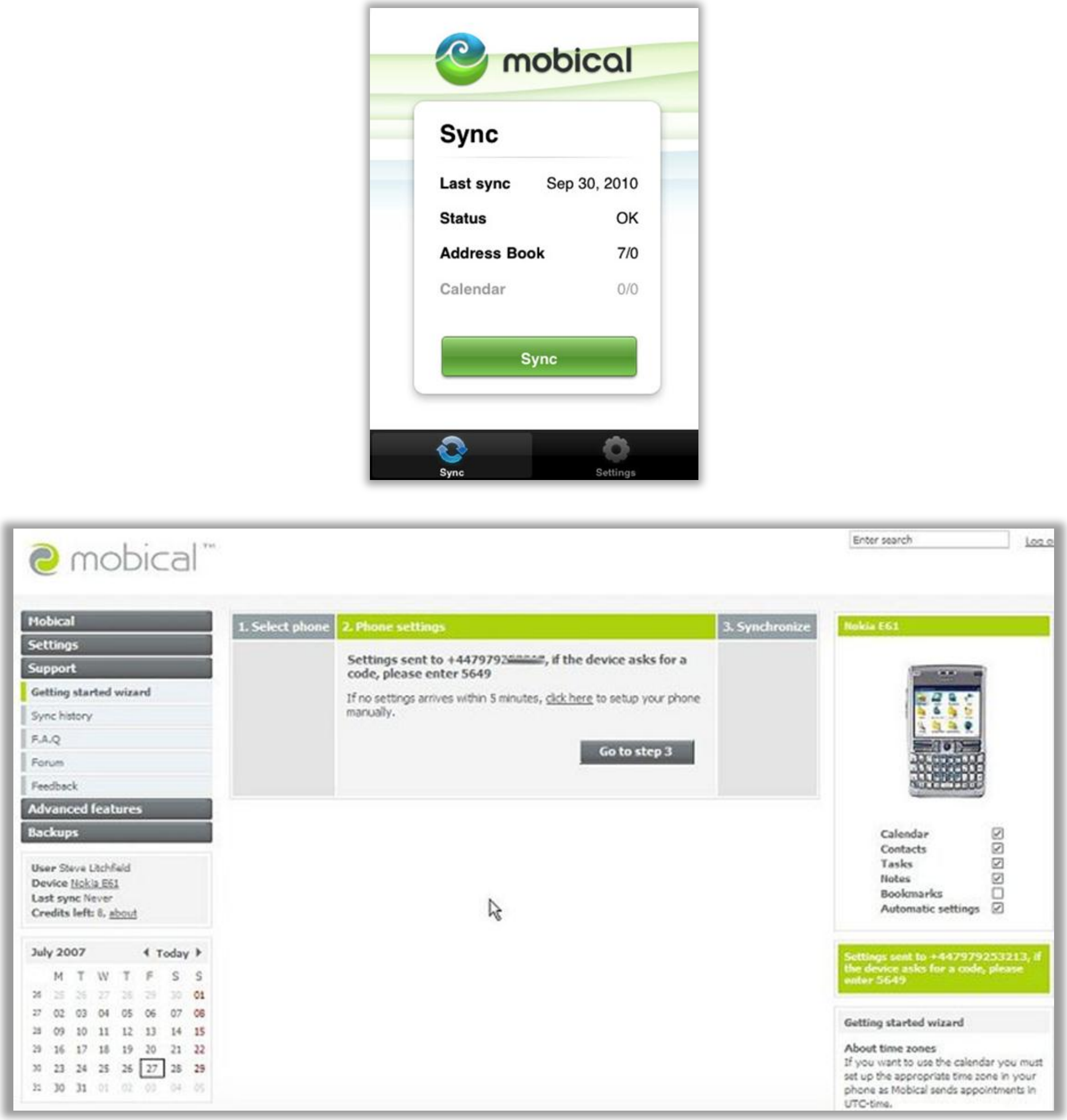
Wipe Now!

Wipe all contacts, SMS, call logs, photos, videos and memory card

Figure 13-02: Using Power-On Authentication

Regularly Back Up Important Data

Most phones today come with suites and applications that allow a user to easily manage and back up important data. To prevent losing important data such as contact details, calendar entries, messages, etc., **regularly back up** your phone data. A user can use third-party tools and services like mobical.net to back up their mobile data**.**



Sync

Last sync	Sep 30, 2010
Status	OK
Address Book	7/0
Calendar	0/0

Settings sent to +447979[redacted], if the device asks for a code, please enter 5649

If no settings arrives within 5 minutes, click here to setup your phone manually.

User Steve Litchfield
Device Nokia E61
Last sync Never
Credits left: 8, about

July 2007 ◀ Today ▶

	M	T	W	T	F	S	S
26	25	26	27	28	29	30	01
27	02	03	04	05	06	07	08
28	09	10	11	12	13	14	15
29	16	17	18	19	20	21	22
30	23	24	25	26	27	28	29
31	30	31	01	02	03	04	05

Calendar	☑
Contacts	☑
Tasks	☑
Notes	☑
Bookmarks	□
Automatic settings	☑

Settings sent to +447979253213, if the device asks for a code, please enter 5649

About time zones
If you want to use the calendar you must set up the appropriate time zone in your phone as Mobical sends appointments in UTC-time.

Figure 13-03: Data Backup in Mobile Devices

Use Encryption to Secure Data in Mobile Device

Encrypt the data stored in mobile phones such as telephone numbers, important messages, voice calls, and emails **to keep them safe** from prying eyes.

It ensures that, even if the mobile phone is lost, the **data cannot be accessed** once it is encrypted.

Mobile phones such as Blackberry can encrypt data as **standard**, whereas other mobile phones require special applications to encrypt data.

To encrypt internal Blackberry files:

- Turn on the **Content Protection** option (**Options** → **Security Options** → **General Settings**).

To encrypt external Blackberry files:

- Turn on **Media Card Support** (**Options** → **Media Card** or **Options** → **Memory** → **Media Card Support**).
- Set the encryption mode for the external file system. The BlackBerry smartphone encrypts files stored on the media card.
- Choose whether to encrypt media files in external memory on the BlackBerry smartphone.

Enable the Auto-Lock Feature

The auto-lock security feature allows only authorized viewing of mobile phone data. An unauthorized user cannot view or even use the phone once the auto-lock option is enabled as, in most cases; a valid pin number needs to be entered.

General steps to enable the auto-lock option on mobile phones:

- Navigate to your cell phone's main menu screen and select the icon labeled **Settings.**
- Press the **OK** or **Home** buttons on the keypad to select the settings menu.
- Locate the **Security** option and press **OK** or **Home** to select it.
- Scroll down to find the **Auto-Lock** feature on the list of security options.
- Press the **OK** or **Home** button on your keypad to begin setting the auto-lock feature**.**
- Choose a **PIN number** that you will remember to unlock your device once the auto-lock feature has been saved.
- Type your desired four- to eight-digit **PIN code** on the keypad. Press the **Save** button to save your pin, and initiate the auto-lock feature.
- Press the **End** button to return to the main menu.

Note: These steps vary slightly for different mobile devices.

Install Only Signed Applications

Smartphones today provide open platform functionality and deliver the ability to install, remove, or update applications multiple times.

The openness gives unrestricted access to mobile resources and APIs. Unrestricted access to mobile resources presents challenges and risks, and **unsigned applications** may likely increase the complexity and security risks.

To reduce the risk of malware and installing unsigned applications, follow these guidelines:

- Identify the files created on the phone by the application during installation
- Always install the applications on external storage memory cards
- Do not download mobile software from any **untrusted third-party** vendors
- Ensure the quality and accountability of mobile applications by carefully investigating the vendor
- Always try to download applications from the market place provided by the mobile manufacturer

Install Mobile Phone Anti-Virus

People may unknowingly or knowingly install a virus (programs or .exe files) through direct or indirect transferring. Wi-Fi enabled handsets and Bluetooth may let malware in if anti-virus is not installed. The virus, once in the device, can **alter** or **delete** all of the contact details, crash, or permanently lock up your mobile phone applications. Anti-virus software prevents, detects, and removes malware including viruses, worms, and Trojan horses.

Mobile anti-virus software includes Norton mobile security, F-Secure mobile security, Kaspersky mobile antivirus, etc.

Mobile Phone Anti-Virus Tools

F-Secure Mobile Security

Source: http://www.f-secure.com

F-Secure Mobile Security provides complete security protection for smartphones. It mainly protects phone content, enables safe mobile web browsing, and assists you if your phone is stolen or lost.

McAfee VirusScan Mobile

Source: http://us.mcafee.com

VirusScan Mobile provides real-time protection against worms, spywares, viruses, Trojans, and battery-sapping malware. It protects from threats that are originated by instant messaging, Internet downloads, and emails.

Norton Smartphone Security

Source: http://us.norton.com

Norton Smartphone Security will protect your personal information and privacy on your mobile device. It prevents hackers from stealing your information or spying on your mobile when you are using public networks.

ESET Mobile Antivirus

Source: http://www.eset.com

ESET Mobile Security provides you with comprehensive protection for your Windows mobile and Symbian smartphones by protecting against the latest threats to keep your personal information safe.

Trend Micro Mobile Security

Source: http://us.trendmicro.com

Trend Micro Mobile Security protects against infections, data loss, and attacks from a central console that can also manage desktop protection. Remote wipe functionalities, authentication, and encryption defend data privacy and integrity on stolen or lost devices.

Symantec Antivirus for Handhelds

Source: http://www.symantec.com

Symantec Antivirus for Handhelds protects against virus definitions periodically. It allows users to check whether their protection is up to date.

Kaspersky Mobile Security

Source: http://www.kaspersky.com

Kaspersky Mobile Security locates your stolen or lost smartphone by using its inbuilt GPS find function as well as secures your contacts, images, and files from unauthorized access. It stores all your digital assets in an encrypted folder and remotely blocks or wipes your smartphone if it is stolen or lost.

BitDefender Mobile Security

Source: http://www.bitdefender.com

It provides you with complete anti-virus protection for mobile devices that are running Symbian or Microsoft windows mobile. It is easy to use and will keep your mobile devices safe from threats.

Avast! PDA Edition

Source: http://www.avast.com

Avast! PDA Edition is mobile anti-virus protection for Palm OS, Windows CE, smartphones, and Pocket PC-based devices. It generates a complete, detailed report of the scanning process and contains an integrated log viewer.

Avira AntiVir Mobile

Source: http://www.avira.com

Avira AntiVir Mobile offers complete protection for your devices. It provides you with real-time protection. The program is transmitted by coupling with the local PDA or through Bluetooth, GPRS, IrDA, or serial cable.

Secure Bluetooth Connectivity

Mobile phones are the most common and familiar devices that use Bluetooth connectivity. In Bluetooth connectivity, we have **less security**. A hacker will do the following to hack Bluetooth:

- An attacker or hacker breaks the connection between two paired devices by force
- An attacker or hacker steals the packets
- An attacker or hacker breaks the pin code

Bluetooth Security

Basic Bluetooth security refers to identifying whether a device is in **Visible/Discoverable** mode or **non-visible/non-discoverable** mode. Bluetooth security measures include:

- **Turn Off Bluetooth:**

  Turn off Bluetooth interfaces when not in use, and **disables Bluetooth's discovery feature.**

- **Use Strong PIN:**

  Choose a strong PIN for connecting the Bluetooth.

Securing iPhone, and iPad

Enable Passcode Protection

Enabling password protection helps the user to protect personal details in an iPhone when it is stolen. To enable passcode protection in iPhone:

- Click the iPhone's **Settings** app → **General** → **Passcode Lock** → **Turn Passcode On.**
- Enter a 4-digit passcode that you will remember; re-enter it to confirm.
- Press the **power** button to put the iPhone to sleep.
- Press it again and the iPhone will require the password to be unlocked.

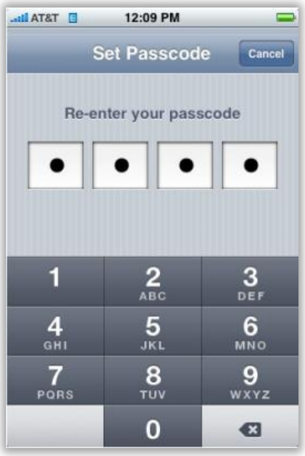


Figure 13-04: Enabling Passcode for iPhone

Enable SIM PIN Protection

To enable SIM PIN protection in iPhone:

- Click iPhone's **Settings** app → **Phone** → **SIM PIN** → **Change PIN.**
- Enter the current password (if it is for the first time, wait and find out the default SIM PIN code).
- Enter the new password, a four-digit passcode you can remember and re-enter it to confirm.

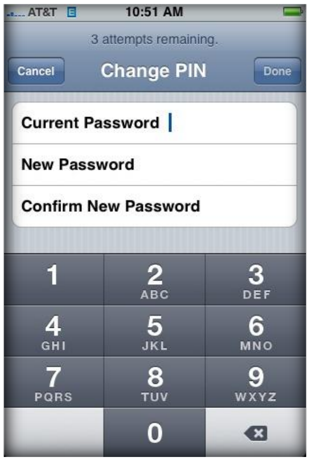


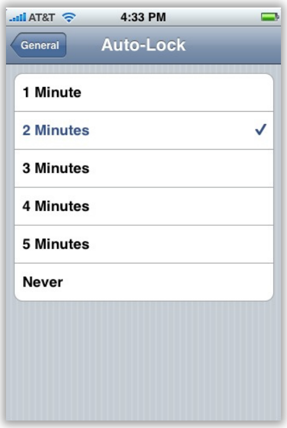
Figure 13-05: Enabling SIM PIN Protection for iPhone

Enable Auto-Lock and Re-map Button

Enable Auto-Lock

The auto-lock feature locks the touch screen when the phone is inactive. The user may turn off the auto-lock option, but it is recommended that he/she always has it enabled. The user can configure when the phone auto locks. This feature prevents the user from making any inadvertent calls or launching applications (such as Wi-Fi or Bluetooth). To configure the auto-lock settings:

- Tap iPhone's **Settings** app → **General** → **Auto-Lock**
- Select the amount of idle time you want the iPhone to wait before it goes to sleep



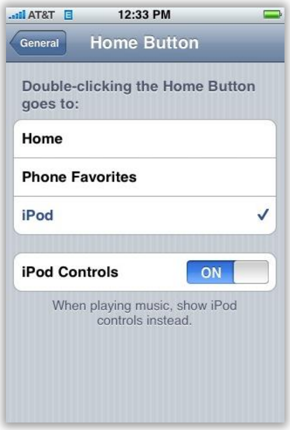
1 Minute
2 Minutes ✓
3 Minutes
4 Minutes
5 Minutes
Never

Figure 13-06: Auto-Lock Settings

Re-map Home Button

To remap the home button:

- Tap iPhone's **Settings** app → **General** → **Home** button
- Instead of **Phone Favorites,** select either **Home** or **iPod**



Double-clicking the Home Button goes to:

Home
Phone Favorites
iPod ✓

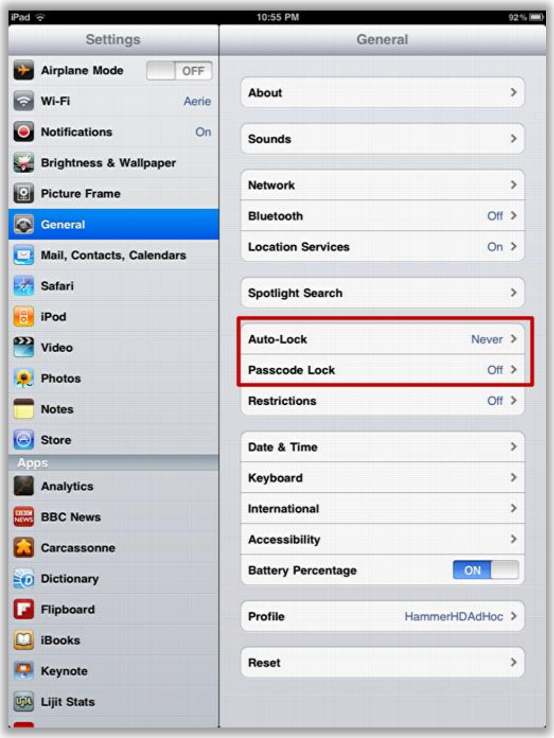
iPod Controls ON

When playing music, show iPod controls instead.

Figure 13-07: Re-map Home button

iPad Security

- **Auto-Lock Feature in iPad**
  - Set the **Auto-Lock** feature to turn off the display and prevent unintended operation of your iPad.
  - To set the amount of time before iPad locks, select **General → Auto-Lock** and specify the time.
- **Passcode Lock**
  - To set a passcode, tap **General → Passcode Lock → Turn Passcode On.**
  - Enter a **4-digit passcode** and then enter it again again to verify.
  - iPad then requires you to enter the passcode to unlock it or to display the passcode lock settings
- To set how long before your passcode is required, select **General → Passcode Lock** and enter the passcode.
- Tap **Require Passcode** and select how long iPad can be idle before you need to enter a passcode to unlock it.
- To turn off the passcode, select **General → Passcode Lock → Turn Passcode Off** and enter your passcode.



iPad 10:55 PM 92%

Settings

Airplane Mode OFF
Wi-Fi Aerie
Notifications On
Brightness & Wallpaper
Picture Frame
General
Mail, Contacts, Calendars
Safari
iPod
Video
Photos
Notes
Store
Apps
Analytics
BBC News
Carcassonne
Dictionary
Flipboard
iBooks
Keynote
Lijit Stats

General

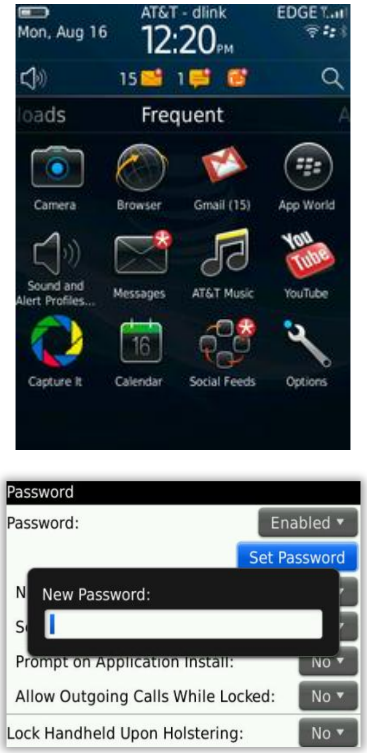
About
Sounds
Network
Bluetooth Off
Location Services On
Spotlight Search
Auto-Lock Never
Passcode Lock Off
Restrictions Off
Date & Time
Keyboard
International
Accessibility
Battery Percentage ON
Profile HammerHDAdHoc
Reset

Figure 13-08: Auto-Lock and Passcode Lock feature in iPad

Security Blackberry and Windows Phone 7 Mobiles

BlackBerry: Setting Device Password

- On the **Home** screen or in a folder, click **Options.**
- Click **Security → Password.**
- Click **→ Set Password.**
- Type a password.
- Press the ⊞ key and click **Save.**
- To turn off the BlackBerry device password, clear the **Enable** check box.



Password

Password: Enabled ▾

Set Password

New Password:

Prompt on Application Install: No ▾

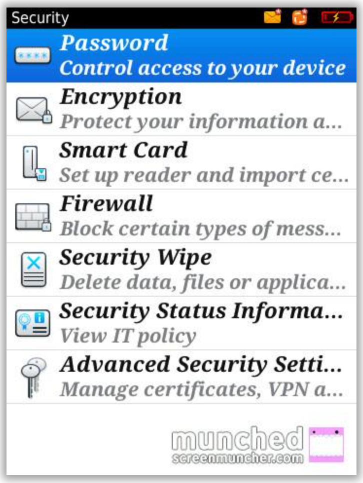
Allow Outgoing Calls While Locked: No ▾

Lock Handheld Upon Holstering: No ▾

Figure 13-09: Setting Password in BlackBerry Device

BlackBerry: Changing the Device Password

- On the **Home** screen or in a folder, click the **Options** icon.
- Click **Security → Password → Change Password.**



Security

Password
Control access to your device

Encryption
Protect your information a...

Smart Card
Set up reader and import ce...

Firewall
Block certain types of mess...

Security Wipe
Delete data, files or applica...

Security Status Informa...
View IT policy

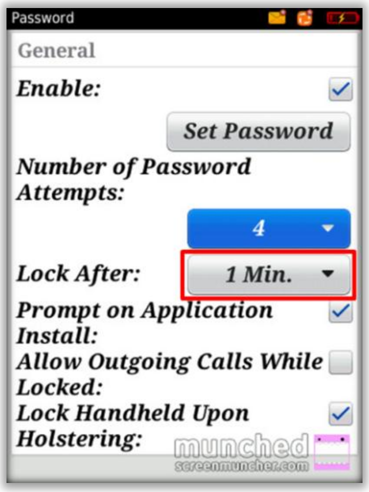
Advanced Security Setti...
Manage certificates, VPN a...

Figure 13-10: Changing the Device Password

BlackBerry: Lock Your Device

You can lock the screen to avoid pressing it accidentally. To lock your BlackBerry device, do one of the following:

- If you have set a device password, then on the **Home** screen or in a folder, click the **Password Lock** icon.
- To lock the screen, press the 🔒 key on the top left of your device.
- To unlock your device, type the device’s password and press **Enter.**
- To unlock the screen, press the 🔒 key again. If necessary, type your device password.



Password

General

Enable: ☑

Set Password

Number of Password Attempts: 4

Lock After: 1 Min.

Prompt on Application Install: ☑

Allow Outgoing Calls While Locked: □

Lock Handheld Upon Holstering: ☑

Figure 13-11: Locking the Device

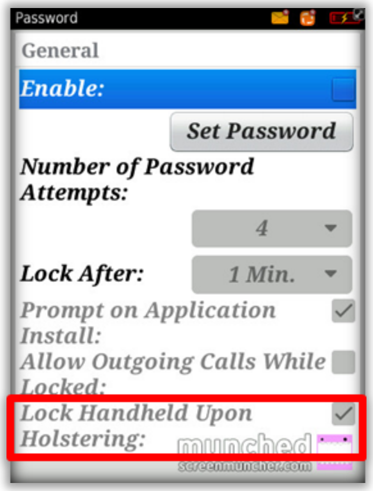
BlackBerry: Device Password

To lock the device when inserted in the holster:

- On the **Home** screen or in a folder, click **Options.**
- Click **Security** → **Password** and select the **Lock Handheld Upon Holstering** check box.
- Press the key click → **Save.**

To set a limit for password attempts:

- On the **Home** screen or in a folder, click **Options.**
- Click **Security** → **Password** and change the **Number of Password Attempts** field.
- Press the key and click → **Save.**



Password

General

Enable: □

Set Password

Number of Password Attempts: 4

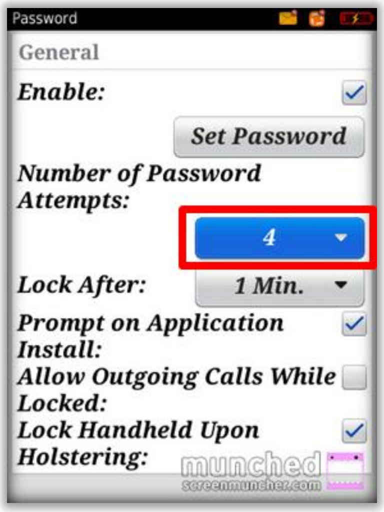
Lock After: 1 Min.

Prompt on Application Install: ☑

Allow Outgoing Calls While Locked: □

Lock Handheld Upon Holstering: ☑

Figure 13-12: Enabling the Lock Handheld Upon Holstering Option



Password

General

Enable: ☑

Set Password

Number of Password Attempts: 4

Lock After: 1 Min.

Prompt on Application Install: ☑

Allow Outgoing Calls While Locked: □

Lock Handheld Upon Holstering: ☑

Figure 13-13: Selecting the Number of Password Attempts

BlackBerry Password Keeper

Password keeper stores all the passwords in one place. It is designed to protect your passwords with its own password. When you type this password, password keeper decrypts your passwords. You can also use the password keeper to generate random passwords that contain numbers, letters, and symbols.

Changing the password in password keeper

1. On the **Home** screen or in the **Applications** folder, click **Password Keeper** and highlight a password.
2. Press the ⁘ key and click **Open.**
3. Change the password information.
4. Press the ⁘ key and click **Save.**

Add a password to password keeper

1. On the **Home** screen or in the **Applications** folder, click the **Password Keeper** icon.
2. Press the ⁘ key → **New** and type the password information.
3. Press the ⁘ key.

Prevent password copying

1. On the **Home** screen or in the **Applications** folder, click the **Password Keeper** icon.
2. Press the ⁘ key and click **Options.**
3. Clear the **Allow Clipboard Copy** check box.
4. Press the ⁘ key and click **Save.**

Set a limit for password attempts in the password keeper

1. On the **Home** screen or in the **Applications** folder, click the **Password Keeper** icon.
2. Press the ⁘ key and click **Options.**
3. Set the **Password Attempts** field.
4. Press the ⁘ key and click **Save.**

Hide passwords in the password keeper

1. On the **Home** screen or in the **Applications** folder, click the **Password Keeper** icon.
2. Press the ⁘ key and click **Options.**
3. Clear the **Show Password** check box.
4. Press the ⁘ key and click **Save.**

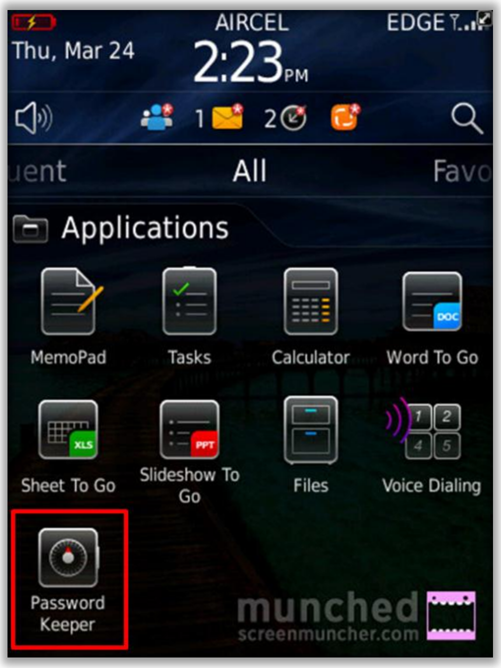


Figure 13-14: BlackBerry Password Keeper

Encrypting Data on your BlackBerry Device

When the user turns on the encryption option in a BlackBerry phone, the phone uses a private key to encrypt data. A user can encrypt files on the device and on a media card using an encryption key generated by the device.

Turn on Encryption:

- To encrypt data on your BlackBerry device, first set a password for your device.
- On the **Home** screen or in a folder, click **Options.**
- Click **Security** → **Encryption.**
- Select the **Encrypt** check box to encrypt data on your device in the **Device Memory** section.
- Select the **Media Card** check box to encrypt the media card files and do one of the following:
- Change the **Mode** field to **Device Key.**
- Change the **Mode** field to **Device Password.**
- Change the **Mode** field to **Device Password & Device Key.**
  - Select the **Include Media Files** check box to encrypt media files such as pictures, songs, and videos.
  - Press the ⁝⁝ key and click **Save.**

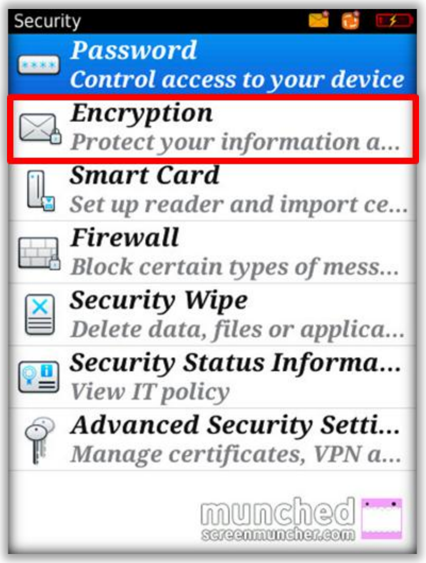

Security
Password
Control access to your device
Encryption
Protect your information a...
Smart Card
Set up reader and import ce...
Firewall
Block certain types of mess...
Security Wipe
Delete data, files or applica...
Security Status Informa...
View IT policy
Advanced Security Setti...
Manage certificates, VPN a...
munched
screenmuncher.com

Figure 13-15: Encrypting Data on BlackBerry Device

Windows Phone 7 Mobiles: Use of PIN to Lock SIM Card

You can use a PIN for the subscriber identity module (SIM) card in your phone to prevent people from making unauthorized phone calls. After turning on SIM security, you will be prompted to enter your SIM PIN each time you start your phone.

Steps to turn on SIM security

- On **Start,** click/tap **Phone** → **More** → **Call Settings** and turn on **SIM Security.**
- It prompts you to **Enter SIM PIN** and then enter the **PIN** for your SIM card by doing one of the following:
  - If you are setting the PIN for the first time, try typing **1234** → tap **Enter.**
  - If you have already set a PIN for the SIM card, then type your **PIN** → tap **Enter.**

Windows Phone 7 Mobiles: Changing the Password of the Phone

- On **Start,** flick left to the App list and tap **Settings.**
- In **Settings**, tap **Lock & wallpaper.**
- To set up a password for the first time, turn **ON Password**. Enter a new password in the **New password** field. Reenter it in the **Confirm password** field.

- If the phone already has a password and if you want to change it, tap **Change password.** Enter the phone's current password in the **Current password** field before entering the new password.
- Tap **Done** to save your changes.

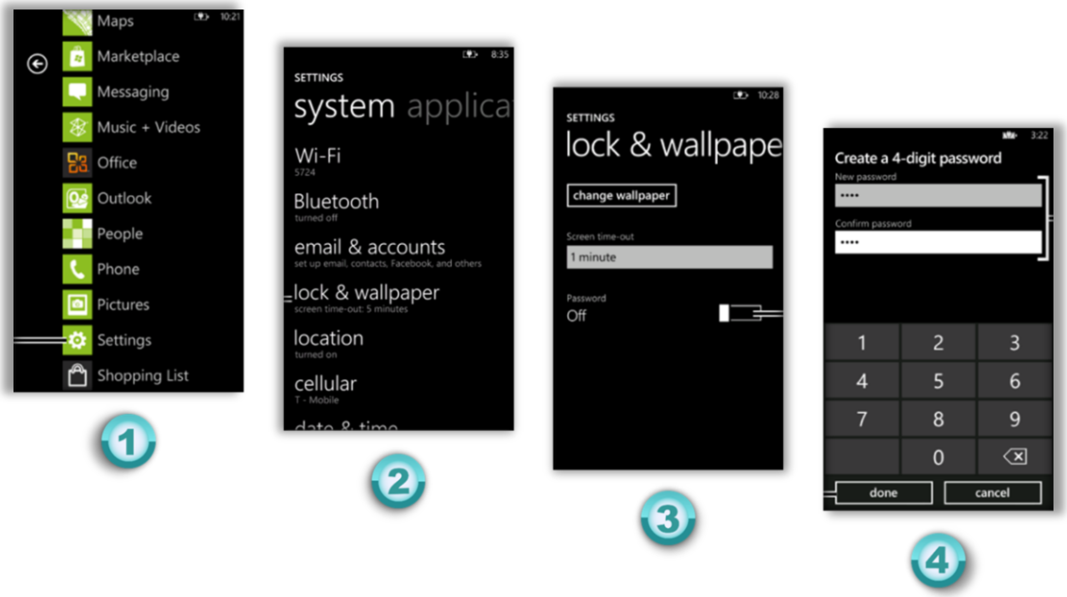


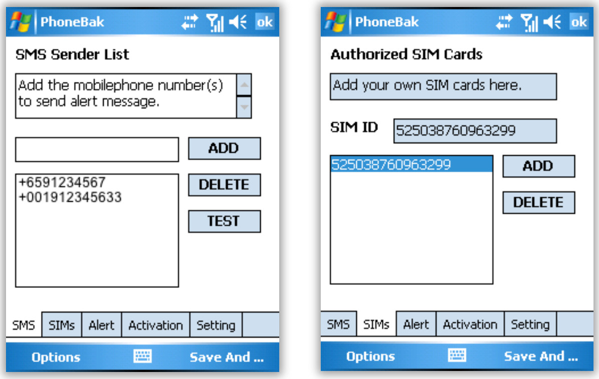
Figure 13-16: Changing Password in Windows Phone 7 Mobile

Mobile Security Tools: PhoneBAK Anti-theft

Source: http://www.bak2u.com

PhoneBAK protects a PDA phone from theft and risk of unauthorized access to sensitive information. If the PDA is stolen, it tracks down the person via his mobile phone number.

PhoneBAK checks any SIM card inserted into the PDA phone, and if it is unauthorized, it sends SMS text alerts to notify the person who lost the phone of the theft and wipes out all video, photos, and documents!


SMS Sender List

Add the mobilephone number(s) to send alert message.

+6591234567
+001912345633

Authorized SIM Cards

Add your own SIM cards here.

SIM ID 525038760963299

525038760963299

Figure 13-17: PhoneBAK Screenshots

Mobile Security Tools

WaveSecure

Source: https://www.wavesecure.com

Wave Secure locks down your mobile device remotely. It wipes out the important data stored on your mobile to protect your privacy. It plots the location of your lost phone on a map and tracks phone calls on the inserted SIM. You can access your data online from anywhere as well as easily restore your data on a new phone.

Sprite Terminator

Source: http://www.spritesoftware.com

Sprite Terminator can locate your mobile devices using GPS and track it via Google maps or virtual earth by sending an SMS to initiate the wipe operation in all external storage cards by using Remote Delete feature.

Airscanner Mobile Encrypter

Source: http://www.airscanner.com

Airscanner Mobile Encrypter provides a simple interface, creating volumes to hold your sensitive data, and maintains control over the encryption or decryption at files or folder levels.

btCrawler

Source: http://www.silentservices.de

btCrawler provides you with the following features:

- Runs on Windows mobile devices
- Blue Snarfing of detected devices
- Service queries if Bluetooth devices are detected
- Searches a list of Bluetooth devices

Resco Backup for Pocket PC

Source: http://www.resco.net

Resco Backup for Pocket PC provides fast incremental backup, custom and full backup, FTP backup, in addition to tracking registry changes and many more features to protect your pocket PCs. It creates reserve copies of your PDA on the storage card.

SecuBox

Source: http://www.aikosolutions.com

SecuBox is a convenient and powerful disk encryption solution for Windows CE and Windows phones. It features automatic encryption, automatic data lock if the user becomes inactive, encryption key backup, and many other advanced features.

eWallet

Source: http://www.iliumsoft.com

eWallet protects your mobile devices from identity theft. It uses high-end security for your important and private information. You can store your passwords, PINs, credit cards, bank accounts, and other information. It is simple to use and safe.

Kaspersky Mobile Security

Source: http://usa.kaspersky.com

Kaspersky Mobile Security locates your stolen or lost smartphone by using its inbuilt GPS find function, as well as secures your contacts, images, and files from unauthorized access. It stores all your digital assets in an encrypted folder and remotely blocks or wipes your smartphone if it's stolen or lost.

Module Summary

Mobile phones are becoming the new tools for checking email and browsing the Internet.

Mobile malware comes through emails, IMs, Bluetooth, memory cards, and Wi-Fi.

Bluetooth is an open standard wireless technology for exchanging data over short-range radio frequencies from fixed to mobile devices by creating wireless personal area networks (WPANs).

All applications should be updated regularly with patches released by the vendor.

Anti-virus software prevents, detects, and removes malware including viruses, worms, and Trojan horses.

Bluetooth devices should be configured—and should remain—undiscoverable, except as needed for pairing.

Bluetooth Security Checklist

□ Change the default settings of the Bluetooth device.

□ Choose PIN codes that are sufficiently random and long.

□ Bluetooth devices should be configured by default and remain undiscoverable except as needed for pairing.

□ Ensure that Bluetooth devices are turned off when they are not in use.

□ Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.

□ Install anti-virus software on Bluetooth-enabled hosts that are frequently targeted by malware.

□ Install Bluetooth software patches and upgrades regularly.

□ Ensure that link keys are based on combination keys rather than unit keys.

□ Users should not accept transmissions of any kind from unknown or suspicious devices.

□ Set Bluetooth devices to the lowest possible power level.

□ Unnecessary Bluetooth services, user controls, and applications should be removed from the host device.

□ Devices should support only a single headset connection between one headset and one handheld device.

□ In the event a Bluetooth device is lost or stolen, users should immediately unpair the missing device from all other Bluetooth devices with which it was previously paired.

□ The user should authorize all initial incoming connection requests, and both the handheld device and the Bluetooth headset should indicate an active Bluetooth link.

Mobile Phone Security Checklist

□ Encrypt sensitive data on the device.

□ Regularly back up PDA data to a PC.

□ Use anti-virus and anti-spyware software for mobile devices.

□ Keep the mobile phone operating system and other applications up-to-date.

□ Give a password to access the device and change the default Bluetooth password.

□ When entering a crowded zone, make sure the Bluetooth is switched off.

□ Never follow links from unsolicited email or text messages.

□ Never transmit sensitive information when connected to the Internet at public places (shopping malls, cafes, etc.).

□ Immediately report the loss of device to the service provider.

□ Register the 15-digit IMEI (international mobile equipment identification) number of the GSM mobile phone handset, which makes it easier to deactivate the phone if it is stolen.

□ Wipe all the data before disposing wireless devices.

□ Properly read the device's user manuals to ensure appropriate protection.