Smartphone Smart Card

Smartphone 082412_104242

Smart Phone -Do's and Don'ts

- Applications can track your location. Turn off location services to avoid unwanted location tracking.
- Malicious emails and text messages can infect your smartphone with malware. Run anti-virus software periodically on your device.
- The camera and microphone can be remotely activated on a smartphone. Do not take a smartphone near classified information, and you should remove the battery before discussing any sensitive information.
- Wireless networks may be insecure and subject to monitoring. Use VPN when accessing wireless networks, and do not access sensitive information over wireless networks.
- Malicious individuals may gain physical access to your smartphone. Protect your device with a password and run applications such as *lookout* and *find iPhone* to help you recover lost or stolen smartphones.
- Applications that you download may gain access to the data stored on your smartphone. Check to see if the application will access your location and other personal data. Read peer reviews of the application to see if other users experienced trouble after downloading.
- Hackers may be able to exploit your device using a Bluetooth connection. Turn off Bluetooth when you are not using it.

Application and Malware Threats

Your personal information may be compromised by applications that gain access to your data and malware that infects your smartphone

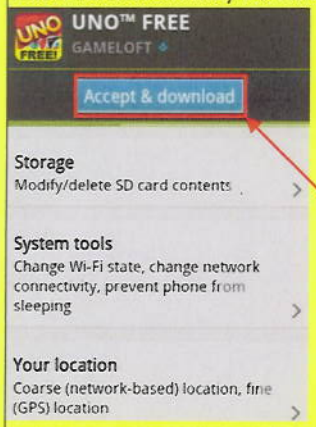
(1) Location threats - Your smartphone is vulnerable to applications that track your location. If you publish your location to smartphone applications it may be possible for other users to exploit your location information.

Applications can track your location

Beware of giving applications access to your location – Go to the settings menu and decide which applications to grant access to location data.

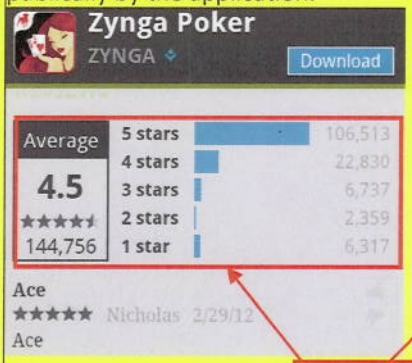
Disable location services to prevent third parties from learning your location

(2) Data-stealing applications - applications that you download may gain access to your personal information. This information may be visible to third parties.



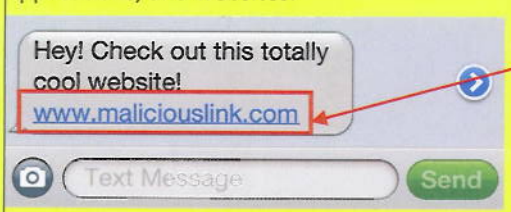
Applications that access your personal information can expose your personal information to third parties

Do not allow unfamiliar applications to access your data - Read ratings and reviews of applications before downloading them to see if other users have experienced problems with the application. See what information is published publically by the application.



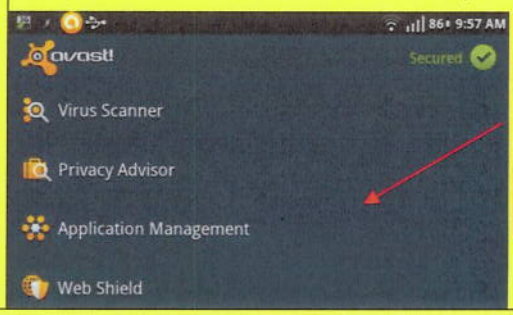
Read reviews of applications before downloading

(3) Malware - Like a computer, your smartphone is vulnerable to malware from emails, text messages, applications, and websites.



Be wary of clicking links in emails and text messages; these links may contain malware

Run anti-virus - Use anti-virus applications like *avast!* and *iVirusScan* to protect your phone from malware. Run anti-virus periodically to check for infection.



Run anti-virus periodically to protect your phone from malware

Smartphone Smart Card

Smartphone 082412_104242

Physical and Connection Threats

Malicious parties may compromise the security of your smartphone by gaining physical access to the device, remotely activating the camera or microphone, or by exploiting Bluetooth and wireless network connections.

(4) Microphone and Camera - Hackers may be able to remotely activate the camera and microphone of your smartphone.

Foreign governments and hackers may be able to record audio or video information remotely. Be careful what you say and do in the presence of your smartphone

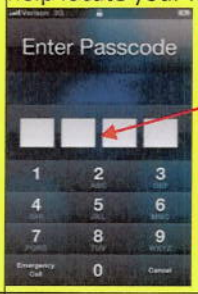
Do not discuss sensitive information near your smartphone, or remove the battery first - Avoid talking about classified information near your smartphone; do not bring your smartphone into secure areas. Remove the battery before discussing anything sensitive

Take out the battery before discussing anything sensitive

(5) Physical access threats - Your smartphone is vulnerable to malicious individuals who can attempt to physically gain access to your smartphone and the information inside of it.

When your smartphone is out of your physical control, your data may be stolen or lost. Third parties may install malware on your phone or copy your information

Password protect your device and **run applications to help recover lost devices -** Use a password to protect your smartphone. Do not let your device out of your physical control. Use the applications *lookout* and *Find iPhone* to help locate your lost smartphone.



Password protect your device to make it more difficult for third parties to access your information

Use applications like *lookout* and *find iPhone* to recover lost smartphones

(6) Wireless Networks – Wireless networks may be monitored or insecure. The information that you access over a wireless network my be intercepted by third parties.

Accessing the internet on insecure wireless networks may compromise your passwords, user names, and data

Use VPN on Wireless networks - Use VPN whenever your access the internet on your smartphone via wireless. Avoid accessing sensitive information on wireless networks; do not log into password protected sites and services via wireless networks.

Go to the settings menu of your smartphone and turn on VPN before using an insecure wireless network

(7) Bluetooth - Hackers may be able to access your contact information, calendars, emails, text messages, photos and videos by exploiting Bluetooth connections.

If you leave Bluetooth turned on, your phone is vulnerable to exploitation

Turn off bluetooth when you are not using it - If you are not connecting to another device, disable Bluetooth. Go to the settings menu of your smartphone and turn off Bluetooth.

Turn off Bluetooth when you are not using it to connect to another device

Smartphone Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Wired Kids	www.wiredkids.org/
Microsoft Safety & Security	www.microsoft.com/security/online-privacy/social-networking.aspx
OnGuard Online	www.onguardonline.gov/topics/social-networking-sites.aspx

ibg

www.ibgweb.com