IPA Countermeasure Guide Series (8)

Security Measures Guide For Smartphone <Avoidance of Risks>

For smartphone which is a convenient tool, risks can be avoided by implementing security measures for its safe and secure use!

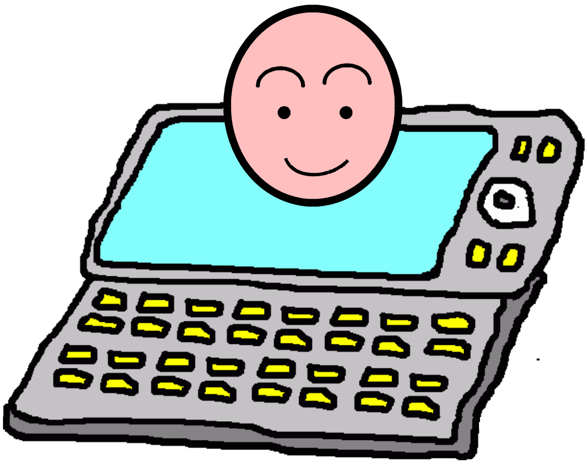
IPA

Information-technology Promotion Agency, Japan
IT Security Center

http://www.ipa.go.jp/security/ (in Japanese)

June 8, 2012 Second Edition

Table of Contents



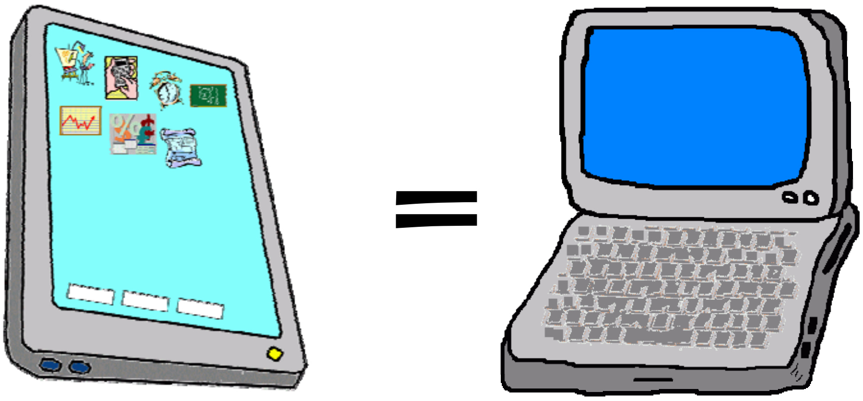
Introduction

Please look around. A handheld device called "smartphone" is spreading among people. Smartphone is casually used everywhere, including in trains, on platforms at train stations, in coffee shops, and on park benches.

By using smartphone, users can watch moving images or read novels on the Internet. They can also do shopping or keep pocket-money ledger.

Smartphone, which is referred to as a high-end mobile phone, allow users to access not only restricted websites dedicated to mobile phones, but also websites accessible from PCs, and to freely use private applications or applications used online by multiple users (NB: applications are programs that provide various types of functions).

That is to say, smartphone is equivalent to personal computer (PC).



You may not believe that smartphone is identical to PC that you are familiar with, but it is equivalent to mobile PC called "netbook" or "tablet PC (slate PC)", isn't it?.

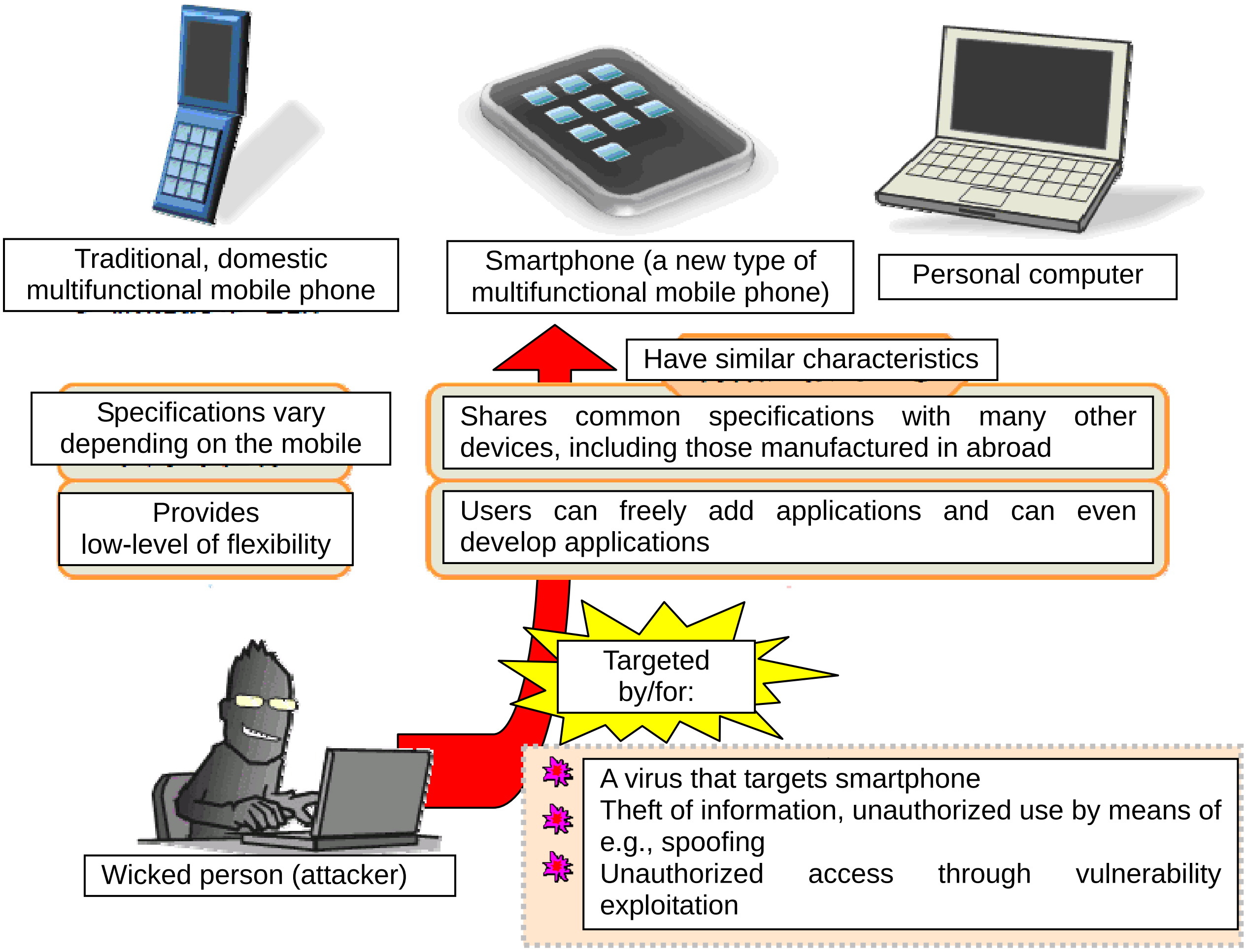
Being able to connect to many different networks via the Internet: this feature and mobility, along with the expansion of cloud computing*[1], is drawing attentions for its effectiveness in carrying out corporate activities. In fact, a smart phone equipped with a tablet-like large-screen display is becoming a new weapon (tool) for carrying out operating activities.

Above all, such smartphone has an impact in terms of visual effects and variation of movies/images it can display, so its effectiveness is outstanding. Furthermore, such smartphone is also used in lieu of textbooks at schools or as a portable information terminal in medical front, and further increase in the number of users is expected in the future.

However, the increase in the number of users brings another problem: an environment with a large number of users becomes an easy target for wicked people (i.e., attackers).

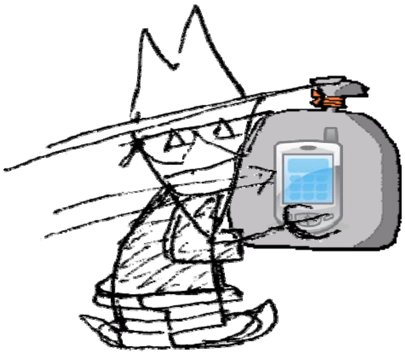
Since mobile phones' usage environment is closed in a sense (i.e., usage environment via their carriers; specifications vary depending on the models), they have hardly been targeted for attacks, but because smartphone can also work in the same usage environment as that of PCs, it is becoming the next target for attackers who would target PCs or networks for attacks.

That is to say, for reasons such as "having many users", "having similar (or the same) characteristics", "assets (resources) can be reused for that attack", smartphone has come to be fixed on by wicked people.


Traditional, domestic multifunctional mobile phone
Smartphone (a new type of multifunctional mobile phone)
Personal computer
Have similar characteristics
Specifications vary depending on the mobile
Provides low-level of flexibility
Shares common specifications with many other devices, including those manufactured in abroad
Users can freely add applications and can even develop applications
Targeted by/for:
Wicked person (attacker)
A virus that targets smartphone
Theft of information, unauthorized use by means of e.g., spoofing
Unauthorized access through vulnerability exploitation

By the way, what would be the most nagging concern (threat) for smartphone users? That is "**theft/loss**", as indicated by various research reports.

Smartphone is a convenient stuff, but if **lost**, like mobile phones, it would lead to a troublesome problem to its user. Smartphone is considered an electronic storage medium containing various information, such as information of one's own, prepaid money with the wallet capability, movies/image data taken with a camera, moving images/music/application data purchased by oneself, friends' information (e.g., registered in the address book), and even the information obtained through corporate activities (e.g., client information, sales & marketing information); so it is analogous to a USB stick that has many functions. As a matter of course, if lost, it might lead to information leakage.



Furthermore, unauthorized use due to theft/loss is also possible. It would be unacceptable for users to be charged for a service they have never used or a paid-application purchase they have never made. This sort of money-related trouble must be a threat to smartphone users.

In recent years, as far as information security is concerned, information leakage issues are making headlines, but it is important to not only implement countermeasures against theft/loss, but also **protect oneself against** the aforementioned **attacks by wicked people**.

In light of this situation, smartphone requires the same security measures as those for PCs and various electronic storage media.

Those security measures should be implemented proactively by smartphone users, having appropriate smartphone security awareness.

So now, let's think about three major categories of smartphone security measures.

Countermeasures against Theft /Loss of Smartphone
Countermeasures against Infection of Smartphone
Countermeasures against Leak of Information from Smartphone

*1) Cloud Computing
Cloud provides a means for enterprises/organizations to use IT services (hardware and software capability) without owning IT (operating environment: hardware).
Cloud computing allows users to enjoy services that help improve the efficiency of

clerical work as well as sales & marketing and business operation through simple operations like searching the Internet. Furthermore, it can be used from not only conventional PCs but also smartphones referred to as high-end mobile phones and other mobile phones and tablet computers, with sufficient performance. It also allows users to perform business processing from outside their office (e.g., in the field or at home), leading to more efficient sales & marketing and improved business operations.

1. Countermeasures against Theft/Loss of Smartphone

As in the case of mobile phones/electronic storage media/mobile PCs, smartphone requires security measures against theft/ loss.

First, please recall security measures for mobile phones/electronic storage media/PCs.

■ In the Case of Mobile Phones

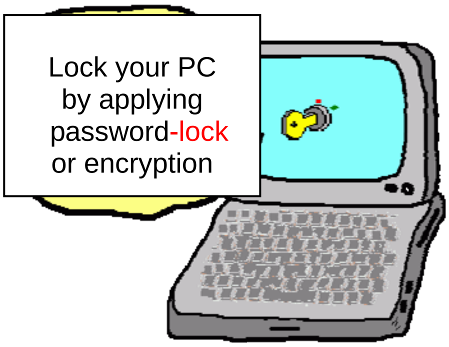
In the case of mobile phones, applying PIN-lock or password-lock against certain functions or forcibly locking phones from a remote site in the event of theft /loss (i.e., using such service provided by the carrier) is an effective security measure. Furthermore, to prevent SIM (UIM/USIM) cards[*2] from being abused (e.g., by means of spoofing), it is effective to lock them with your PIN code[*3]. Another important measure is, not to carelessly store critical data in expanded memories (e.g., SD memory)[*4].

■ In the case of Electronic Storage Medium

An effective countermeasure against theft/loss of electronic storage media is, of course, "encryption". Furthermore, there is also a function to forcibly delete data in case the user fails in authentication (i.e., enters a wrong password) at the specified number of times. There are also user-implemented security countermeasures, such as attaching a bell, a large tag, a strap dangling it from your neck, or not lending it to others.

■ In the case of Mobile PC

In the case of mobile PCs, there are various security measures available, including BIOS password-lock[*5], use of a hard-to-guess login password, and hard disk drive (HDD) encryption (so that information leakage is prevented even if the HDD is removed from your PC and then connected to another PC). Furthermore, additional security measures, function/service[*6] to forcibly delete HDD data by means of remote connection over the Internet or to identify users' location



from the connection environment, may also be implemented.

And now, what about smartphone?

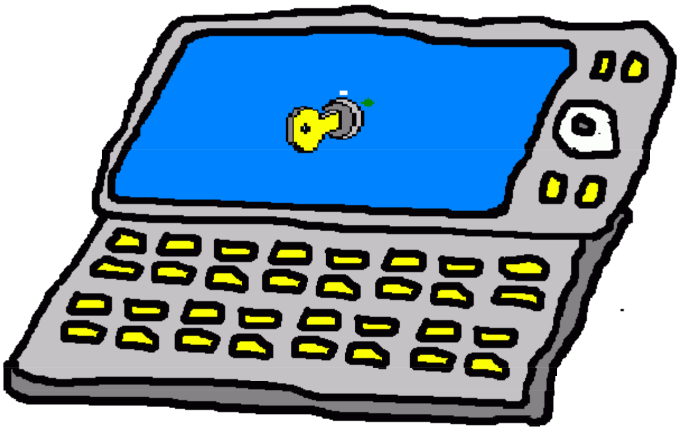
To counter theft/loss of smartphone, the same countermeasures as those for mobile phones/electronic storage media/mobile PCs can be applied.

- **It is effective to apply password-lock to your device (i.e., enabling user authentication);**
- **As in the case of mobile phones, PIN-lock should be applied to SIM (UIM/USIM) card (as a measure to prevent unauthorized use);**
- **If critical information is going to be stored/saved on that smartphone, data encryption measures(application) are required;**
- **As in the case of mobile phone/mobile PC, it is effective to use a service for forcibly locking smartphone or deleting its data from a remote site, a service for confirming the location information (in the event of misplacing or theft), or a dedicated application having those functions;**
- **If your smartphone has any expanded memory slot, do not carelessly store data in such memory (Flash memories such as SD card are electronic storage media which are difficult to completely delete data and therefore, supposed-to-be deleted data might be restored);**
- **For important data, back it up to a different storage than smartphone (e.g., an online storage or an external storage medium through your PC). Note, however, that such backup media also require security countermeasure against theft/loss.**

That's about it!!

As for the first two measures, setting method etc. vary depending on the model, so read carefully the instructions manual for your model.

According to a report[*7], surprisingly, "password-lock (user authentication)" is not being widely used. Not considering it cumbersome, just apply password-lock. And if you lose your smartphone in the unlocked state, recall the presence of the remote lock service provided by mobile carriers etc.



*2) SIM (UIM/USIM) card

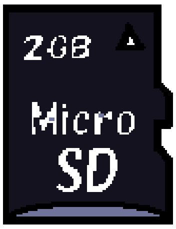
IC card on which a unique number assigned to the mobile phone or mobile device which phone number identification is stored. Phone charge etc. is charged to this number.

*3) PIN (Personal Identification Number) code

A secret number entered by mobile phone/device users to use its functions at the time of authentication. It is registered in the aforementioned SIM (UIM/USIM) card.

*4) Do not carelessly store critical data in expanded memories (e.g., SD memory)

In the case of flash memories such as SD card, even if you delete data stored or format them, the supposed-to-be deleted data might be restored. This is closely related to the life issue of flash memories. A flash memory is made up of a large number of small physical switches and each switch has lifespan in terms of how many times it can be opened and closed. In order to lengthen their lifespan, flash memories try not to use once-used switches. As a result, the parts on which data has been written once are less likely to be used. This means, supposed-to-be deleted data might not be overwritten with other data and therefore, such data might easily be restored.



Given such specifications, if you carelessly store critical data on flash memories, information might be leaked from those memories. For the same reason, it is safe not to lend your flash memories to others. What if your precious photos that you don't want to be seen by others and that you thought they had been deleted are restored? You don't want it, do you? …

*5) BIOS password-lock

BIOS (Basic I/O System) is a program that runs first when computers are booted, and password authentication feature might be applied to it. With this password authentication feature, you can prevent the unauthorized use of your computer. However, if any devices connected to your computer are removed and then connected to another computer, only your computer's main body is protected against unauthorized use. Furthermore, if you forget this password, you will fall into serious trouble (i.e., unless you change your computer's motherboard, nothing can be done with your computer), so be careful not to forget your password.

*6) A function or service to identify users' location

Depending on how your computer is connected to the Internet, anyone could, to some extent, identify the location of your computer from the access point(s), without even using Global Positioning System (GPS) which is used e.g., by car navigation system.

Various functions and services that utilize this capability to identify the location of computers are provided. Generally, this capability is used to provide users with information based on their usage environment (so called "marketing"), but it may also be used for searching for a stolen computer.

*7) Report

We found the following news item released in August, 2011

- 67 percent of mobile phone users are not protecting their phone with password (Sophos)
  http://www.sophos.co.jp/pressoffice/news/articles/2011/08/67-percent-not-password.html (in Japanese)

2. Countermeasures against Infection of Smartphone

Apart from the aforementioned security measures against theft/loss, there are other security measures that should be considered for smartphone.

As stated in "Introduction", users can freely install applications and use them for various purposes. For this reason, like PC users, smartphone users might suffer damages caused by computer viruses or unauthorized access. Furthermore, they might also be guided to an illicit site and fall for the phishing scam or one-click billing fraud.

On January 21, 2011, IPA released security alert*[8] on viruses that target smartphone. This was because a high-risk virus that might infect Android *[9]-based smartphone/tablet device had been detected and the possibility of domestic users suffering from the virus infection had increased.

Thereafter, viruses targeting Android terminals continued to increase, with their capabilities becoming more and more sophisticated. In that sense, the primary self-defense measure for smartphone is to counter the computer viruses that target smartphone.

*8) Security alert

🌎 Security alert on viruses targeting Android OS (IPA)
http://www.ipa.go.jp/security/topics/alert20110121.html (in Japanese)

*9) Android

Android is a Linux-based OS for mobile devices, which was released by Google, Inc in the U.S. OS stands for Operating System and is also called "base software". It is responsible for basic control over computers or other devices (hardware), including smartphone, and a base for running various applications software.

■ Countermeasures against Computer Virus

In order for your smartphone to self-defend against malware performing illegal operations (NB: malware, also known as “malicious-ware”, is collective term for harmful software and computer viruses) and/or unauthorized access, it must be able to prevent virus infection without user intervention. Once infected with a virus, it might allow for unauthorized access through the virus or the personal information stolen by the virus.

Main Causes of Virus infections are:

- A vulnerability that can be exploited by a virus exists in the smartphone's operating environment (operating system or browser)
- A virus is installed unintentionally by the user

The former case is addressed by eliminating vulnerabilities in that operating environment (operating system).

For the Operating System of Your Smartphone, Keep it Up-to-date

In the case of smartphone, basically, operating system upgrade and update is carried out at the initiative of their vendor (carrier or manufacturer). In the case of Android terminals, operating system versions vary depending on the model, and vendor-specific functions are often embedded, so version upgrade and update is not uniformly carried out.

Android terminals' operating system is a Linux-based operating system for mobile devices and constantly evolving, so for some models, there may be a delay in the provision of supports. Keep abreast of the model-specific information provided by its vendor and then take actions as needed.

The latter case is addressed by protecting against virus infection.

Install Applications from a Reliable Site

Generally, smartphone's virus infection is often caused by its users installing an application containing a virus (malicious code). Users can install applications from an application distribution channel called "application store" (such as "App Store" run by Apple, or "Android Market" for Android-based devices), or by giving in to application installation inducement through social networking service (SNS) or short message service (SMS).

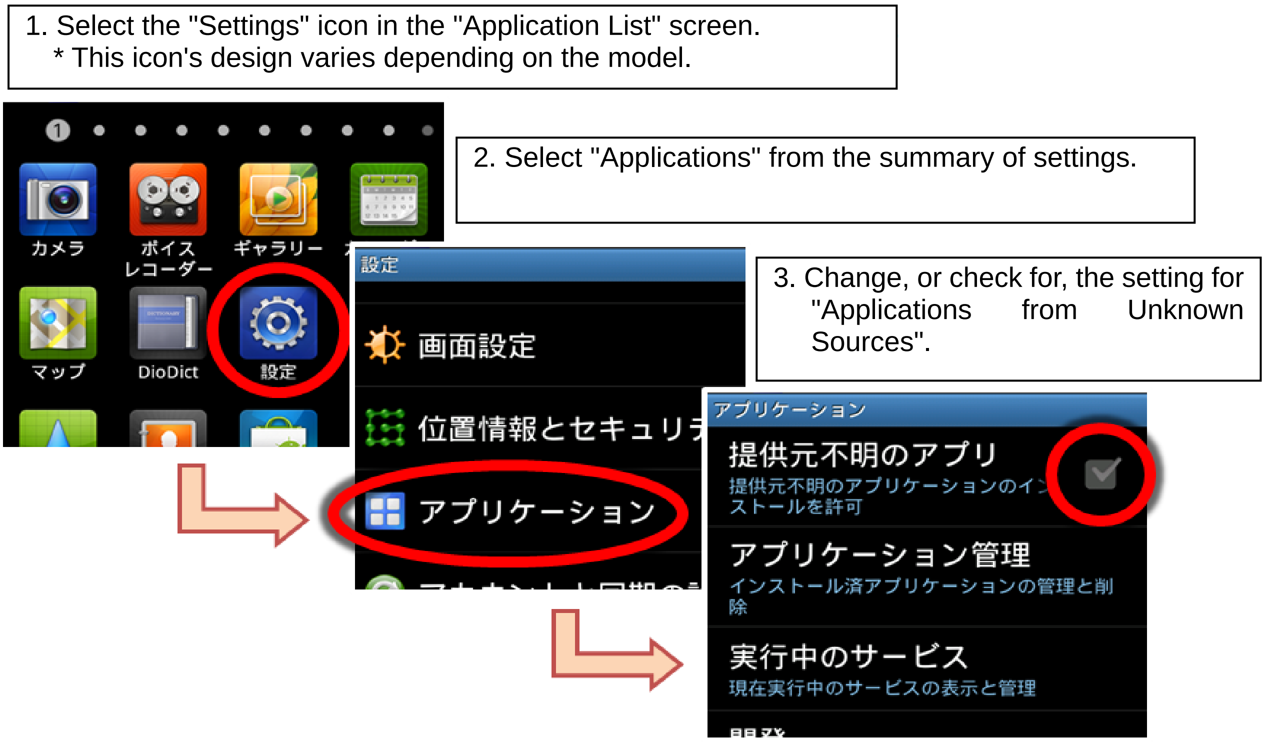
In the case of an application installed from non-legitimate application store, even though it may look like a legitimate application (i.e., pirated one), it may contain a virus.

So, when you install applications, be sure to install them from a reliable site.

In general, a reliable site refers to a legitimate application store provided by manufacturers or carriers. However, an application carrying a virus might enter into even such legitimate application store by getting around its scrutiny; so for Android-based smartphone (Android terminal), implement the following measures as well:

For Android Terminals, Disable the "Allow Installation of Applications from Unknown Sources"

The settings screen for Android terminals contains an item termed "Applications from Unknown Sources". If you uncheck this item, you can prevent any applications obtained from non-Android Market from being installed (NB: This item is unchecked by default). For procedures for changing, or checking for, the setting for "Application from Unknown Sources", see Figure 1.



1. Select the "Settings" icon in the "Application List" screen.
   * This icon's design varies depending on the model.

2. Select "Applications" from the summary of settings.

3. Change, or check for, the setting for "Applications from Unknown Sources".

Figure 1: How to Check or Change the Setting for "Applications from Unknown Sources"

So as not to install any malicious application by mistake, it is recommended to uncheck this checkbox except when absolutely necessary.

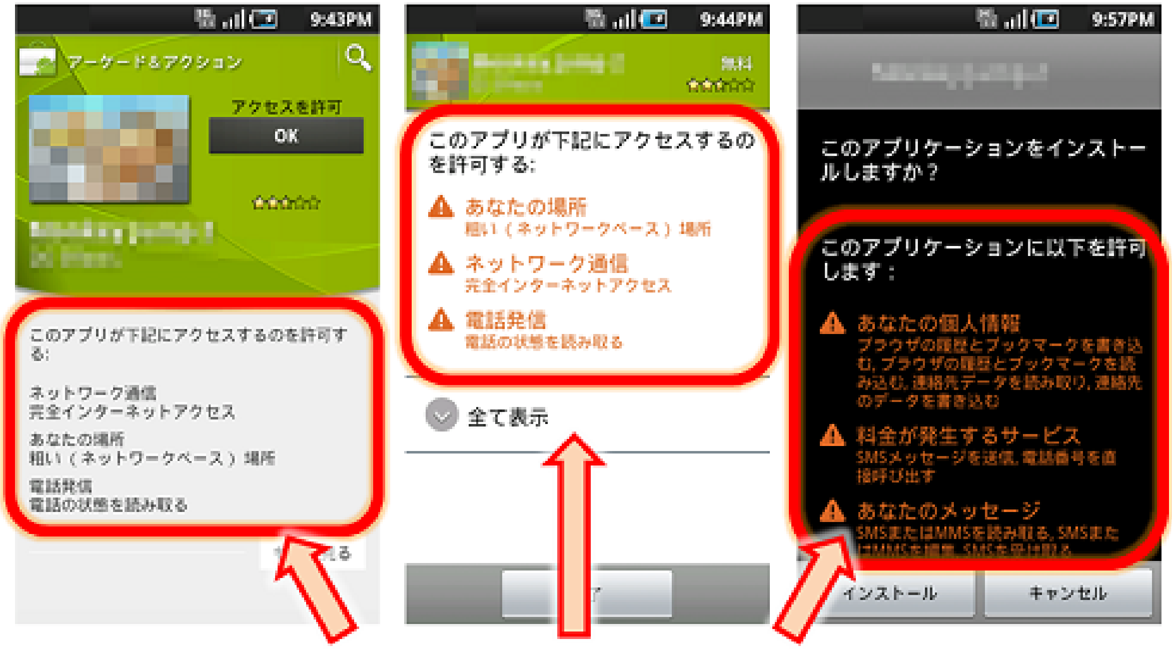
For application obtained from non-Android Market, you need to temporally change this setting (i.e., check it) to install them, even if they are from a reliable third-party application store. In such cases, be sure to uncheck it again after the installation is completed.

For Android terminals, confirm the access permissions requested, prior to installing that application

When you install an application on an android terminal, be sure to read through the "Access Permissions" list displayed (which shows which information/function(s) of that Android terminal will be accessed by the application) (See Figure 2).

Among the viruses targeting Android terminals and detected in the past, some request unnatural access permissions from users for the purpose of surreptitiously stealing personal information, etc. Examples include a wallpaper application asking for the permission "Read contact information", which is needed to access the contents of address book or call logs.

When you install an application on an Android terminal, if any unnatural/suspicious access permission is asked, cancel the installation of that application.



このアプリが下記にアクセスするのを許可する:

ネットワーク通信
完全インターネットアクセス

あなたの場所
粗い（ネットワークベース）場所

電話発信
電話の状態を読み取る

このアプリが下記にアクセスするのを許可する:

あなたの場所
粗い（ネットワークベース）場所

ネットワーク通信
完全インターネットアクセス

電話発信
電話の状態を読み取る

このアプリケーションをインストールしますか？

このアプリケーションに以下を許可します：

あなたの個人情報
ブラウザの履歴とブックマークを書き込む、ブラウザの履歴とブックマークを読み込む、連絡先データを読み取り、連絡先のデータを書き込む

料金が発生するサービス
SMSメッセージを送信、電話番号を直接呼び出す

あなたのメッセージ
SMSまたはMMSを読み取る、SMSまたはMMSを編集、SMSを受け取る

A list which shows which information/function(s) of that smartphone will be accessed by the application you are going to install.
* The screen's design varies depending on the model or the condition.

Figure 2: Display Screen Image for "Access Permissions" (Example)

Furthermore, some applications may request "access permissions" that seem irrelevant to their inherent functions, for such purposes as displaying advertisements. Table 1 shows typical examples of "access permissions", some of which are hard to make out.

Table 1: Description of "Access Permissions" (For some parts)

	Displayed Message	Description
1	Outgoing call -> Read the phone's status	This is thought to be used for stopping a played music depending on the phone's incoming-call status. The application which is given this permission is able to read the smartphone's **phone number** as well as **terminal identification number assigned to each phone**.
2	Your site -> Approximate Location (Network-Based)	"Approximate Location" refers to **that smartphone's approximate location** that is estimated from the distance from its base station or from wireless LAN facilities in the surround areas. The estimated location may have a margin of error of plus or minus dozen of meters to several kilometers**.** This positional information can also be used by an advertiser to determine the contents of advertisements to be displayed on the application's screen.
3	Network communication -> Full Internet access	Literally, this is a function that enables users to transmit/receive information over the Internet. This is also used for exchanging ad-related data.

* Displayed messages (expressions) for "access permissions" may differ slightly depending on the model

Most of smartphone applications become serviceable when the Internet connection is available. The problem is, if the access permissions as described in the above item 1 or 2, or item 3 plus for an access to "Your Personal Data" was requested by, and given to, a malicious entity, it might send the smartphone's telephone number and positional information somewhere over the Internet.

If you just look at the "Access Permissions" list, it may be difficult to determine whether the application is to be used for a legitimate purpose or malicious one. **So, based on the reliability of the application's source and developer as well as other users' remarks, grant "access permissions" within a scope deemed reasonable, just in case.**

Keep Your Applications Up-to-date (i.e., Enable "Automatic Update")

In the case of applications installed from application stores etc., users can generally apply automatic update.

If there are vulnerabilities in those applications, as in the case of vulnerabilities in operating system, those vulnerabilities might be exploited for virus infection or unauthorized access (e.g., to steal information).

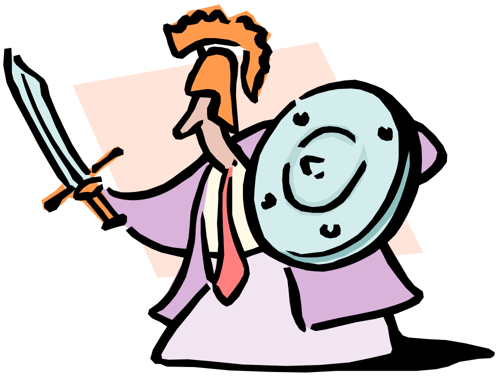
As a safeguard against vulnerabilities detected, you can configure your smartphone **so that automatic update is performed** and hence applications are kept up-to-date. This setting is highly recommended.

If for any reason you cannot apply automatic update, regularly check if any vulnerability has been detected for your applications and whether information on their update is available, and if any, manually update them.

There is another important measure to prevent virus infection and that is:

Use Security Software (Application)

As in the case of PCs, to prevent virus infection, it is recommended to use dedicated software (application).



When smartphone began to come up in the nation, no security application for smartphone was being provided by security software vendors. Though there were few viruses detected at that time …

Nowadays, however, viruses for smartphone are on the rise, and vendors have released security software for smartphone one another (For more details, refer to each vendor's product introduction).

These security software products utilize accumulated technology for PCs, so they are expected to provide sophisticated measures for smartphone as well. Furthermore, these security software products often provide not only antivirus measures but also other security functions, so it is recommended to check for the applicability of such products to your smartphone model and use them accordingly.

3. Countermeasures against the Leak of Information from Smartphone

Apart from the aforementioned security measures against theft/loss and self-defense measures for smartphone, there are other security measures that should be considered for smartphone. That is, measures to prevent information leakage from your smartphone.

Avoid the Shared Use by Multiple Users

If critical information such as personal information is stored on your smartphone, it is safe to avoid its shared use (though it is less likely in the case of a privately-owned smartphone). As separate management and operation for each user is not possible, one does not know what application will be used by the other users and it might lead to information leakage in some cases. This is as dangerous as lending your external storage media to others. For example, information leakage might occur due to supposed-to-be deleted data being restored or data being unintentionally left undeleted.

For the Communication of Critical Information, Use a Secured Line

Smartphone can be connected to the Internet or external networks in various ways. Examples include using a mobile phone line or a wireless LAN spot in the town (i.e., Wi-Fi environment). However, in the case of not using mobile phone lines, secure communication might not be ensured. When you transfer critical information, use a secured line. In the case of (charge-free) Wi-Fi environment that involves unspecified number of users, there is a risk of communications being tapped.

If You are Going to Use Smartphone for Your Business Operations at the Company, Follow the Company-Established Security Policy (Unauthorized Use Must be Strictly Prohibited)

If you are going to use smartphone for your business operations at the company, you need to be careful with applications other than those used for your business operations. Apart from viruses, you might accidentally leak the company's critical information while using SNS service or SMS service.

In order to prevent this sort of accidental information leakage, you would need to restrict applications other than those used for your business operations.

Furthermore, for being lost or stolen, you should always grasp what information is stored with appropriate management.

Given this situation, currently*[10], it is recommended not to use your privately-owned smartphone for your business operations without permission.

*10) Currently …

Recently, in the U.S., a business model called "Bring-Your-Own-PC" emerged, which states: "Even in the case of a privately-owned PC, if advanced virtualization technology is applied, employees may bring it to their office and connect it to their business system as security is ensured." Given this technical background, in the near future, we may see an environment where security is ensured even if privately-owned devices are used in workplaces. But currently, as stated above, it is dangerous to do so from the aspect of management and operation.

4. Other Countermeasures

Though this is not an antivirus measure …

When mobile phones began to be used actively, there were troubles such as minors being charged overly high price for accessing Dial Q2, online game users being charged overly high price for purchasing the game items using their PC or online terminal, personal information being leaked through one-click billing fraud or Phishing, all of which are beyond technical control even if he/she takes precaution. And these might also happen to smartphone. To address such problems, there is no alternative but to educate users to read the instruction carefully; not to proceed out with mere curiosity if they cannot understand; not to try to solve problems by themselves; and so forth. For underage users in particular, education to instill such sense would be required. The need to perform Web filtering, as implemented on mobile phones, may arise.

By lending their ears to many different troubles that occur in the world, users should learn the way of protecting themselves against such troubles.

<Reference Information>

Bits of Knowledge for Better Life (National Consumer Affairs Center of Japan)
http://www.kokusen.go.jp/book/data/mame.html (in Japanese)

5. Conclusion

Sophistications and deviousness of widely-prevalent PC-targeting viruses have been advancing over the years. And many different techniques that have emerged in that field are likely to be applied also to smartphones, putting smartphones users at risk.

For secure use, smartphones users, as in the case of PCs, should first be aware of what operating system is running on their phone model, and then implement required safeguard against viruses etc. while paying attention to security-related news.

- ☑ **As a countermeasure against theft/loss, it is effective to apply password-lock to your device; in case you cannot apply it, remember how to lock it from a remote site;**
- ☑ **If critical information is going to be stored on your smartphone, data encryption is required;**
- ☑ **For critical information, buck it up. Don't forget, however, to implement security measures for such backup media …;**
- ☑ **For the operating system of your smartphone, keep it up-to-date;**
- ☑ **Install applications from a reliable site;**
- ☑ **For Android terminals, disable the "Allow Installation of Applications from Unknown Sources";**
- ☑ **For Android terminals, confirm the access permissions requested, prior to installing that application;**
- ☑ **Keep your applications up-to-date (i.e., Enable "Automatic Update");**
- ☑ **Use security software (application);**
- ☑ **For the communication of critical information, use a secured line;**
- ☑ **If you are going to use smartphone for your business operations at the company, follow the company-established security policy (Unauthorized use must be strictly prohibited).**

6. Reference Information

<Security Vender Information>

NB: Since URLs contained here are Japanese only, we omitt this part.

In creating and publishing this guide, we gain cooperation from the following enterprises:

(In alphabetical order)

- Ahnlab
  http://www.ahnlab.co.jp/ (in Japanese)
- Kaspersky Labs Japan
  http://www.kaspersky.co.jp/ (in Japanese)
- Mcafee
  http://www.mcafee.com/us/
- Microsoft
  http://www.microsoft.com/
- Sourcenext
  http://www.sourcenext.com/ (in Japanese)
- Symantec
  http://www.symantec.com/
- Trendmicro
  http://us.trendmicro.com/us/home/

<IPA-Technical Watch>

- Report on Threats to Smartphones and How to Address Them
  - Looking at the Actual Status and Challenges of Android Device Vulnerability Countermeasures, Derived from IPA's inspection - (June 2011)
  http://www.ipa.go.jp/security/english/technicalwatch/pdf/110622report-eng.pdf

<Reminder for this Month: Computer Virus/Unauthorized Computer Access Incident Reports>

- Let's use your smart phone in a secure manner! (August 2011)
  http://www.ipa.go.jp/security/english/virus/press/201107/E_PR201107.html
- Watch out for smart-phone-targeting viruses (February 2011)
  http://www.ipa.go.jp/security/english/virus/press/201101/E_PR201101.html

<Rakuten Blog: IPA Information Security Blog>

- Emerged again, A virus that infects Android (February 2011)
  http://plaza.rakuten.co.jp/ipablog/diary/201102220000/ (in Japanese)
- Watch out for viruses that infect Android! (February 2011)
  http://plaza.rakuten.co.jp/ipablog/diary/201102220000/ (in Japanese)

<IPA Channel (YouTube)>

- Information Security News #1 Watch out for viruses that infect Android!
  http://www.youtube.com/watch?v=A-xIqfbZ_N0 (in Japanese)

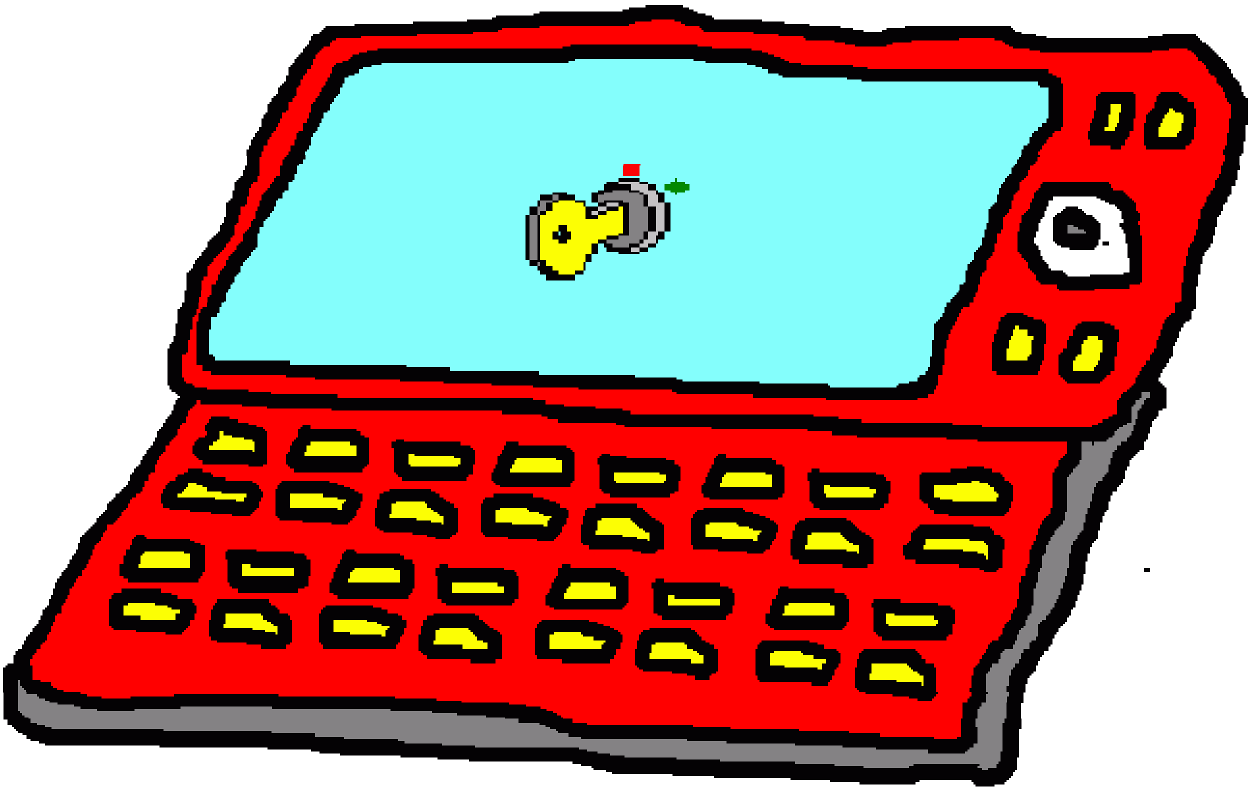
<IPA Security Alert>

- Security alert on viruses targeting at Android OS (January 2011)
  http://www.ipa.go.jp/security/topics/alert20110121.html (in Japanese)

IPA Countermeasures Guide Series

http://www.ipa.go.jp/security/english/virus/antivirus/shiori-e.html

- IPA Countermeasures Guide Series **(1) Countermeasures on Computer Virus**
- IPA Countermeasures Guide Series **(2) Countermeasures on Spyware**
- IPA Countermeasures Guide Series **(3) Countermeasures on Bots**
- IPA Countermeasures Guide Series **(4) Countermeasures on Unauthorized Access**
- IPA Countermeasures Guide Series **(5) Countermeasures on Information Leakage**



IPA

Information-technology Promotion Agency, Japan
IT Security Center

Bunkyo Green Court Center Office 16th Floors
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan 113-6591

URL **http://www.ipa.go.jp/security/ (in Japanese)**

[Worry-Free Information Security Consultation Service]

URL **http://www.ipa.go.jp/security/anshin/ (in Japanese)**
E-mail **anshin@ipa.go.jp**