|  |  |  |
| --- | --- | --- |
| logogreen | ASIA-PACIFIC TELECOMMUNITY | **Document No.:****ASTAP-31/TMP-51** |
| **31th APT Standardization Program Forum(ASTAP-30)** |
| 11–15 June 2019, Tokyo, Japan | 14 June 2019 |

Chairman, EG IS

**THe final text of the security guideline: GUidelines for Secure use of IT devices and services (Revision 1.0)**

This document includes the final text of the security guideline: Secure use of IT devices and services (Version 2.0) agreed by EG IS in ASTAP-31.

Highlights:

* Added Part C Security Threats
* Added new ICT technologies related contents

Attachment 1: The final text for the security guideline: Guidelines for secure use of IT devices and services (Version 2.0)

Attachment 1

*Guidelines for secure use of IT devices and services*

*– Security: Protect your data –*

**Version 2.0**

Revision History

|  |  |  |
| --- | --- | --- |
| 2017  | Version 1.0 | Approved at ASTAP-28 |
| 2019 | Version 2.0 | Approved at ASTAP-31Part C |
|  |  |  |
|  |  |  |

**Guidelines for secure use of IT devices and services**

--- Security: Protect your data ---

**Version 2.0**

**Contents**

Introduction

Guidance

Part A: IT devices

1. Smartphone
* Methods for protecting smartphone from intrusion and malicious code
1. PC/Tablet PC
* Methods for the choice and use of highly secured password and ID
* Minimal check points for security weakness of PC or notebook

Part B: IT Services

1. Wireless LAN
* Special attention for securing public wireless LAN
* Secure use of wireless LAN at home
1. Transaction services on the Internet
* Special attention required for secure bank electronic transaction
1. Social Network Services
2. E-mails
* Protecting smartphone from spam text messages or e-mail spam
* Protecting smartphone from spam (methods for reducing spam messages)
* Protecting from e-mail spam (methods for reducing spam messages)

Part C: Security Threats

1. Ransomware
* Guideline of personal level for preventing from the damage
* Guideline of company/organization level for prevention from the damage
* Guideline for the Recovery Process
1. One-Click Fraud

Appendix

Guideline of urgent response for hacking incident

# Introduction

Our life becomes more than ever convenient and people can enjoy various types of devices and services with the latest technologies, thanks to the development of information and communication technologies. Today, the Internet is an essential infrastructure and we accept its benefits at many aspects of our lives through wider range of devices such as PC, tablet computer and smartphone both cable connection and wireless access.

Particularly in Asian Pacific region, with development of information and communication infrastructure, the number of smartphone users and tablet computers has been dramatically increased in past 5 years and still has been growing. The number of online transaction services uses has been also growing and numerous people accept the new way of services such as online banking and money transfers.

That is obviously the positive aspects of new ICT development. However, today is also the time that we need to know to protect such devices by ourselves. ICT development has indeed brought serious security issues, which are often called one of the greatest challenges in the 21st century. It is therefore becoming essential knowledge to all ICT users to protect data, personal information, personal property, and even personal life.

This document is to guide minimum security points that have to be noticed by ICT users. It can be applied to general situation and all ICT users – it is worth understanding that users can protect their data with careful attention and basic knowledge.

The guidelines in this document are for all users of ICT devices such as smartphone, PC, tablet PC, and services such as electronic bank transfer and SNS.

.

**Part A: IT devices**

Smartphone

Methods for protecting smartphone from intrusion and malicious code

## Term

Multimedia Messaging Service: a kind of messaging service after short message service which can transfer various multimedia messages including texts, graphics, audio, video etc. through mobile network, wireless network or fixed network

## Abbreviation

 DDos: Distributed Denial of service

## Guideline

Security for Smartphone

Malicious code infection happened in PC tends to move to the damages in the smart phone. Malicious code infection in the smart phone has been increasing. Like malicious code infection in PC, smart phone can be used as DDoS attack tool accidentally when smart phone is infected by malicious code. Moreover leakage of private information, forgery or alteration of data, violation of privacy, money loss and equipment malfunction are the frequent candidate in this situation. Therefore we have to be accustomed to the following several safe rules to prevent smart phone from accidents by malicious code.

1. Don’t change the structure of smartphone platform at one’s discretion

If you modify a smart phone platform structure (e.g. Jailbreak), accidents can be happened by influencing basic security functions. Don’t alter smart phone platform structure by yourself.

1. Update the latest version for the operating system and vaccine program

Hackers disseminate malicious code using security weaknesses of a smart phone platform and use various attack methods to avoid detection of anti-virus software /vaccine program. Using the latest version updated operating system and anti-virus software /vaccine program should be fulfilled.

1. Use password set up function and change the password regularly

Password in the smart phone should be set up to prevent privacy from leakage when losing or being stolen the smartphone. Password set up is also important after regaining the lost smartphone because malicious code could be installed by someone with ill intentions. An initial password when using a smart phone for the first time (e.g. 0000) must be changed and easy password suck as ‘1111’ or ‘1234’ must not be used.

1. Turn on Bluetooth function only when you use

It is inspected that many smart phone malicious code happening abroad has been disseminated by Bluetooth which is one of wireless interfaces. Therefore turning off Bluetooth or wireless function is necessary when not using Bluetooth or wireless LAN. This action is not only decreasing probability of malicious code infection but also preventing unnecessary battery consumption of a smart phone.

1. Install anti-virus software / vaccine program on your smartphone and check the virus regularly

Data backup, copy, music file transfers or operating system patches can be executed between smart phone and PC by using synchronization program. In this procedure, malicious code hidden in PC can be transferred to smart phone, too. Therefore vaccine program installation and regular checking is inevitable.

1. Use downloaded file after checking the virus infection

Malignant program for a smart phone can be disseminated through the Internet by hiding in specific programs or files. Therefore when you want to execute program or file after downloading, it is better checking the presence of virus using anti-virus software / vaccine program for the smart phone.

1. Don’t download suspicious smartphone application(s)

There is a possibility that malicious code for a smart phone can be disseminated by forged or altered application. Therefore we have to check ourselves once again when downloading suspicious application(s). Your data in the smartphone including personal information and other data could be easily stolen by such malicious application.

1. Don’t visit untrustworthy site

Malignant program disguised in normal program can be secretly installed when visiting suspicious or unknown site. It is better not to visit untrustworthy sites to prevent smart phone from infection by malicious code. Your smartphone could be easily taken over by malignant program.

1. Check the malicious code infection if abnormal symptom continues

When smart phone malfunction or abnormal symptom such as background alteration of the phone or deletion of private information happen after connecting web site or running application, we have to take follow-up measures by smart phone manual. After appropriate measures, if abnormal symptom continues, anti-virus software / vaccine program should be run to diagnose and cure because it is highly probable that smart phone is infected by malicious code. It is also necessary that we notify malicious code infection to related government organization, mobile vendors, smart phone manufacturers or vaccine companies to prevent dissemination of malicious code.

1. Delete messages and mails immediately if the sender is uncertain

Message Service and e-mail are used as a good method to disseminate a smart phone malicious code because they provide the attachment function. Hackers disseminate malicious code by delivering exciting or interesting contents such as game, free gift or privacy of celebrity. It is desirable that we immediately delete uncertain or suspicious message and e-mail.

PC/Tablet PC

Methods for the choice and use of highly secured password

## Guideline

Secured password is the password that can’t be guessed easily by others, can’t be found by using user information which is stored in the system and by hacking the information through the Internet, and needs much time to be known.

1. Set a password using combined characters such as uppercase and lowercase English characters, numbers and special characters.
2. Use a password as 8 or more characters as possible.
3. Don’t use following passwords;
* 7 or less characters
* Having regular or special patterns such as
	+ - Repetition of same characters such as ‘aaabbb’, ‘123123’
		- Characters which are placed adjacent on keyboard such as ‘qwerty’, ‘asdfgh’
		- Password in which number is placed in the first or the last such as ‘security1’, ‘1security’
* Characters which is related to user’s personal information so that others can guess easily such as
	+ - Family member’s name, birth date, home address, cell phone number etc.
* Password using user ID
* Password which is a word in the dictionary
* Password containing special person’s name or well-known words such as
	+ - Computer terminologies, site name, company’s name, famous person’s name etc.
* Password which is initially set in the system or suggested as an example
1. Methods for using password securely are the followings:
* Users set the password by referring above.
* If initial password is set by the system, user should change into new password as soon as possible.
* User should change password regularly.
* When user wants to change password, brand-new password should be used and new password should not be related to the previous password.
* User shouldn’t expose the password by others.
* If exposed, user should change the password immediately.

Minimum check points for security weaknesses of PC
(including notebook and tablet PC)

## Abbreviations

USB: Universal Serial Bus

## Guideline

Minimum check points for protecting general personal computers including notebook and tablet PC from malicious code attack or hacker’s attack are the followings and these points should be checked at all times.

1. Check the installing and running anti-virus software /vaccine program

To protect PC from malicious code, virus vaccine should be installed and run at all times in PC or notebook.

1. Check the latest security patch of virus vaccine

Running anti-virus engine should be always updated with the newest vaccine function provided by service providers.

1. Check the latest security patch of operating system

Security weaknesses are often found in most of operating systems. Therefore latest security patch should be installed for using operating system.

1. Check the safety of login password

After checking if login password is being used in PC or notebook and it is properly used, if security is weak, password should be changed.

1. Check the period of login password change

Although user uses login password in PC or notebook, it should be changed regularly. Period of login password change should be checked by the policy like forcing user to change login password every three months.

1. Check the use of screen saver

Screen saver should be set so that it is operated if PC or notebook is unused for certain amount of time to protect various information in PC or notebook. Moreover user should check if time setting for screen saver to activate properly and password should be used to deactivate the screen saver.

1. Check the setting of user sharing folder

User sharing folder function to easily share the information stored in PC or notebook should be immediately deactivated after its use. Moreover when sharing folder, login password should be set

1. Check whether or not automatic USB running is permitted

When automatic USB running is permitted in PC or notebook, malicious code can be spread easily through USB. Therefore automatic USB running shouldn’t be permitted.

**Part B: IT services**

Wireless LAN

Special attention for securing public wireless LAN

## Terms

AP(Access Point): IEEE 802.11 wireless hub, a special kind of station(STA) operating as an access point

## Abbreviations

SSID: Service Set Identifier

## Guideline

Public wireless LAN is the service that connects to the Internet via wireless LAN in public places. Public wireless LAN provides wireless Internet service using notebook, tablet, and smartphone, etc. around hotel, airport, bus terminal, hospital, department store, school and train station, etc.

Malicious user can make various threats such as personal information leakage by connecting to wireless LAN because this wireless LAN can connect to the Internet without wire freely.

Therefore matters that demand special attention for users to use public wireless LAN securely are the followings. For public wireless LAN constructors and managers, there exist more and various matters that need special attention above the followings.

1. Be careful for public wireless LAN which providers are unclear.
(Recommend not to use it.)

Data on devices can be easily leaked when we use wireless AP which is installed with bad will. Since wireless AP provider can collect all the traffic which go through wireless AP, wireless AP provider with bad will can take personal information out of the traffic. If one needs to use public wireless LAN, one should use well-known or identifiable public wireless LAN.

1. Don’t use sensitive service using wireless LAN without security setting

User’s connecting behavior or personal information can be leaked in wireless LAN circumstances without security setting. User rather not to use sensitive services like bank transaction, enterprise business, service which needs login or service which needs personal information even though user needs to use wireless LAN.

Especially AP without security setting or AP which unknown provider provides is highly probably rogue AP which is installed for taking sensitive personal information like ID/Password out of user. Sensitive personal information can be leaked for reckless Internet user using Rogue AP by the leak of the key for encrypted communication from the initial security setting message for security connection even though security connection between server and terminal is used with SSL security setting.

1. Be careful for wireless LAN automatic connecting function.

Wireless terminal has a function that automatically connects to the once connected wireless LAN. Since the name of the wireless LAN can be freely changed by the manager, personal information can be leaked when hacker lure the user out to connect using automatic connection function by pretending Rogue AP as a AP with well-known wireless SSID. Therefore, turn off the automatic connection function of the wireless LAN and regularly delete the wireless LAN list which has the name of AP connected in the past.

Secure use of wireless LAN at home

## Guideline

Wireless LAN can be installed and used these days quite often. Although wireless LAN is easy to access and convenient to use, it has a weakness. Because anyone can connect to the network freely without wire, various security threats can happen by malicious users. Therefore several special attentions are needed to use wireless LAN securely.

Anyone can construct and manage wireless LAN by buying and installing AP easily at home. But, because everyone can freely connect wireless LAN without wired connection, many security threats such as leakage of personal information can happen by malicious users. Therefore users who want to install and utilize wireless LAN at home need to oblige the following several special attentions.

1. Initial setting of AP should be changed.

In case one person installs wireless LAN for himself or herself, the very user of wireless LAN at home is a manager of the AP as a whole. Moreover, ID or password of AP is not set or is set commonly the same. Therefore users who installed AP at home should manage wireless AP by setting secure password.

Moreover, wireless LAN management page should be set which can be accessed by not wireless but wired.

1. SSID and password should be changed regularly if possible.

SSID and connection password should be changed as regularly as possible. Moreover, password of high security level should be used.

Transaction services on the Internet

Special attention to securing electronic bank transactions

## Guideline

Electronic bank transaction is quite frequently used on the Internet. Users are using PC, notebook /tablet PC and mobile devices including smartphone for their purposes of using electronic bank system. In proportion to increment of users, users are unaware of using those services properly and safely.

Various passwords should be changed frequently to prevent from loss, guess or exposure in order to use the Internet banking securely. It is safe to manage the password by making own special rule not to forget. Password management is very important, for example, if it is possible that authentication device is lost, stolen or copied, it should go along with you.

1. Users need special attentions for bank electronic transaction.. Security program provided by your bank should be installed.
2. Information for electronic transaction shouldn’t be stored or written in the devices

Devices can be easily exposed to others such as PC or notebook and shouldn’t let one know including bank workers.

1. Various passwords used in bank account should be set differently and changed regularly.
2. Mobile service, which notifies electronic bank transaction to the users should be used actively.
3. Bank transaction site should be inputted on the address window or used in bookmark.
4. Virus vaccine and spyware deletion program should be used and latest window security patch should be applied.
5. Suspicious e-mail or article on the Internet bulletin board shouldn’t be opened and attached file should be inspected by programs like anti-virus software or vaccine before opening or installing.

If someone asks prior deposit, balance maintenance with pleading loan or suggests exceptional loan condition which is much above average, we should suspect the case as fraud and should check the situation by calling call center of your bank directly.

Social Network Services

## Guideline

Social Network services (SNS) are widely used for communications among people including sharing interests, activities and backgrounds. They are also often used as messaging tools. However, communications on SNS have security concerns such as unrespecting information spreading or unintended information leakage and it also brings privacy concerns. Although SNS can be used as an convenient communication tools, serious issues happened on the services which seems to be in virtual world, it may cause further serious incidents in the real world.

For safer use of SNS, it is recommended to pay following attentions;

1. Check policy setting for disclosure, particular in your profile including personal data such as physical address and telephone number.
2. Change policy setting, ideally to minimum access/disclosure. In many cases, default setting on SNS is for ‘Disclosure’ based on the open policy.
3. Be mind that there are many ways to be seen your behavior/actions on SNS such as “tag”, check-in function and geolocation (GPS).
4. Be careful to connect or communicate unknown people

Connecting fraud accounts may bring you to real crimes, e.g. Thefts of your personal data and incidents by malicious hacking.

1. Do not click advertisement or URL in unknown messages

 They often include malware and your click will expand such malware to all of your friends and the others who connects to your friends.

E-mails

Protecting smartphone from spam text messages or e-mail spam

## Terms

Spam messages : unsolicited electronic bulk communications over e-mail or mobile messaging/SMS for the purpose of marketing commercial products or services

Electronic spamming: use of electronic messaging systems to send unsolicited messages (spam), especially advertising, as well as sending messages repeatedly on the same site.

Email spam(junk email, unsolicited bulk email(UBE)): a subset of [electronic spam](https://en.wikipedia.org/wiki/Spam_%28electronic%29) involving nearly identical messages sent to numerous recipients by [email](https://en.wikipedia.org/wiki/Email).

## Guideline

This document provides the methods for normal users not to receive unnecessary spam messages or spam advertisement when using smartphone or private e-mail. Other methods from manager of web or mail server can be thought other than normal users’ methods. But since it is not our goal, we focus on the methods for normal users.

Protecting smartphone from spam
(methods for reducing spam messages)

1. Actively use the function for blocking spam which is built in smartphone

Almost all types of smartphone have the function for blocking spam and users use the function actively.

1. Do not agree to receive unnecessary commercial.
2. Do not agree on receiving unnecessary phone commercial in normal life or online.

Complete management is needed private phone number not to be leaked or unnecessarily published. Users manage private phone number thoroughly not to be leaked or unnecessarily published in real life or online.

1. Do not reply if it is in doubt.
2. Do not use the service or purchase merchandise through spam messages.

Use the service or purchase merchandise through the secure channel such as surfing the Internet with the contents known from the spam messages, not to use the service or purchase merchandise directly from the spam messages.

1. Use the spam blocking service (if user’s phone company provides the service).

Protecting from e-mail spam(methods for reducing spam messages)

1. Actively use the spam blocking function inside the e-mail platform you’re using

(for example, google gmail service, etc.).Most of the e-mail platform contains spam blocking function and users actively use this function.

1. Do not agree on receiving unnecessary spam commercial e-mail.

Do not agree on receiving unnecessary commercial e-mail spam in real life or online.

1. Complete management is needed private e-mail address not to be leaked or unnecessarily published.

Users manage private e-mail address thoroughly not to be leaked or unnecessarily published in real life or online. For example, do not unnecessarily leave private e-mail address on such as web site bulletin board.

1. Immediate deletion is needed if user thinks it as a spam.
2. Do not use the service or purchase merchandise through commercial e-mail spam.

Use the service or purchase merchandise through the secure channel such as surfing the Internet with the contents known from the e-mail spam, not to use the service or purchase merchandise directly from the e-mail spam.

**Part C: Security Threats**

**Ransomware**

**Guideline for the prevention from ransomware infection and damage**

Recently ransomware attack damages many area worldwide. Ransomware asks money with electronic file as hostage, thus named ransomware which is a compounded word from ransom and software. These ransomware is generally distributed by untrusted site, spam mail, content sharing site, flash advertisement or network(Internet).

Criminal usually asks electronic money like bitcoin which cannot be easily traced(of course, he/she can ask the cash) for letting the victim know the replaceable key value after making the victim helpless by asking password for booting of the device or after preventing using file by encrypting document/picture file.

Because the final goal of the ransomware is getting money from the victim, prevention not being infected by the ransomware should be completely needed to avoid the monetary loss. In this section we presented the guideline to protect the people and enterprise/organization from ransomware.

1. **Guideline of personal level for preventing from the damage**

Best way of personal level to prevent a person form the ransomware is of course not to be infected by the ransomware. In other words, it is normally the same as the way to respond the general malicious code. Difference lies in backup which is not emphasized in normal malicious code prevention. To achieve this several methods for prevention are as follows.

* Update the operating system and various application programs to the newest version

Recent ransomware is frequently distributed through the weakness of OS or various application programs. Therefore maintaining the newest version of security patch of using OS and various programs(various web browsers, JAVA, Flash, Acrobat, Microsoft Silverlight, etc.) is very important. This is the basic requirement for countermeasure against various malicious code(including ransomware).

All the application programs are recommended setting to ‘automatic update’ to be updated in latest version.

* Maintain the latest version for vaccine program

Maintaining latest version is very important for anti-virus program to secure own system from malicious code(including ransomware).

But be cautious that although vaccine program prevents various malicious code infection and sometimes cures the infected system, it can’t automatically decrypt the encrypted document by malicious code like ransomware.

Vaccine program is also recommended setting to ‘automatic update’ for latest version.

* Use the anti-ransomware program

Anti-ransomware program which is a defense program specialized in ransomware can be used. This kind of program is even stronger countermeasure than usual vaccine program because it prevents from infection by focusing on ransomware other than general malicious code. It should be checked if it can be used with pre-existing anti-virus vaccine program without collision.

* Do not execute attached file of spam

It is better not to open attached file of an e-mail or URL link from unknown sender or unbelievable sender. Do not open e-mail although its title is interesting if sender is not certain. Sometimes criminal sends e-mail attaching malicious code(including ransomware) by other person’s malicious code infected e-mail account. Therefore be cautious to open the link or attached file even from the acquaintance.

High level of caution is needed downloading or executing the file from untrustworthy site or file sharing site if it is necessary.

* Backup the important data regularly is essential

It is almost impossible for restoring encrypted file which is infected by ransomware without decryption key. Therefore regular backup to physically separated storage for important user documents or data can minimize the damage.

In other words, backup for important data is a core countermeasure for preventing unexpected accident like ransomware infection. But backup to exterior memory or USB memory connected to PC is ineffective. Because it is also encrypted when PC is infected by ransomware.

Recommended method in reality is using exterior memory for regular backup or using CLOUD service. Possible measure for a user is using free CLOUD service since backup costs.

1. **Guideline of company/organization level for prevention from the damage**

Company/organization level measure to prevent user from ransomware is almost similar to that from the general malicious code. Multi-level defense strategy can be applied for company/organization distinctively from a user because of the expense problem. For doing these, several methods are as follows.

* Establishment of multi-level defense strategy and activation

Intrusion path of the ransomware is web and e-mail system which are the same as the one of malicious code like work, virus, etc. But damage is totally different problem between ransomware and work or virus infection. Damage by ransomware is much more fatal. Therefore it is very important establishing the multi-level defense strategy and activating by company/organization. Furthermore measures minimizing the damage should be established when ransomware infection is not effectively defended.

For example, multi-level defense strategy should be established referring strategies like Gartner’s ‘end-to-end kill chain’ concept.(establish the strategies for pre-attack state, attacking state, post-attack state, respectively)

* Establishment of regular and consistent backup system and management

Company/organization level establishment and management of regular and consistent backup system(backup equipment, network construction, backup procedure, restoration procedure, access control, etc.) is very important for effective defense against ransomware attack.

* Establishment of patch management security solution about OS and application program and management

Recently distributed various ransomware frequently uses the weakness of OS or various application program. Therefore one way to defend against various malicious code including ransomware is that company/organization establishes and manages centralized patch management solution.

* Establishment of security solution like spam mail response and management

Since normal intrusion path of ransomware is Web and e-mail system, separate establishment and management of special security solution(spam mail block system, etc.) could be effective countermeasures.

* Executing regular security education

It could be very effective educating people regularly about general cyber security including ransomware prevention for company/organization. Many problems in cyber security are frequently caused by careless system users. Therefore regular education is the right solution to awaken the people about cyber security to resolve the above problems.

etc.

Other than the above, we have to consider various countermeasures such as making and managing a whitelist about various application programs used in company/organization, regular education to IT security specialist who manage the principal system, giving disadvantag to people inducing serious cyber security violation, etc.

After infection of ransomware, guidance for using various ransomware recovery program would be needed.(ransomware recovery program provided by international NMR(No More Ransom), ransomware recovery program supported by many security companies, etc.) It is an important point that one should try with copied one.

For the references, since separate responses according to operating system don’t exist, each operating system should manage the various responses as above. Above all, responses to ransomware are the same as the one of existing malicious code and the distinction of the responses for ransomware is that preparing periodic backup system for data is important.

**3) Guideline for the Recovery Process**

In spite of the preparation of responses, danger for being infected to ransomware always exists. General symptoms when infected to ransomware are that one can’t open files such as document files or picture files which were open well, extension or the name of files are altered, or specific extensions are added. Sometimes operating system which user used can’t boot and screen which says the infection of ransomware appears and asks money.

When infected by ransomware like the above, recovery process for the data is the following.

o Firstly, take immediate measures to minimize the damage.

If infected by ransomware, files stored in shared folders, USB, or external hardware can be infected. Therefore one should cancel shared folders and connection to the external storages physically. Furthermore network system should be disconnected not to spread of ransomware through the network.

But power supply of infected computer needs to be maintained if possible. It is because booting of the infected computer is often impossible after being turned off.

o Secondly, check if immediate recovery is possible after understanding the type of ransomware and then proceed the procedure for the recovery.

One can try to format the operating system of the computer and reinstall or to recover by vaccine program.

If one has backup data, one can recover the system using backup data after curing the ransomware. In this case, reinstallation of the operating system will be a better option for any possibility.

One other way for that is asking to data recovery company which specialized data recovery.

It is NOT recommended recovering by paying money to attacker. By the statistics, data recovery didn’t work well and economic damage occurred frequently even if one pay the money for recovery.

These recovery processes can be executed in private level or in organization level such as network management team or security team of the organization if one works for the organization.

o Thirdly, execute data recovery referring the following methods.

First step is that the computer data which is infected by ransomware should be backed up in normal storage. After that, formatting the infected computer and installing the operating system should be done before latest security update of the software. The reason why we backup files infected by ransomware is that recovery tool can be developed later or encryption/decryption key can be revealed by attacker or someone else.

If existing backed up data, recover the data with backed up files. Otherwise, try infected data recovery with ransomware recovery tool or vaccine program.

Trying recovery after paying money to attacker is not recommended. It is because there is no guarantee for getting decryption key after paying money and even if we get the decryption key, we can’t make sure if it works well. Moreover, this kind of deal with attacker is unlawful in most of the countries and therefore we can’t get any support by the law.

o Fourthly, report ransomware damage.

Reporting ransomware damage to related organization can be executed. Forensic procedures can be done for the damage.

**One click Fraud**

Guideline for the response of the users from one click fraud

## Terms

Phishing: Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.(https://en. wikipedia.org/wiki/Phishing)

SMS Phishing(Smishing): In computing, SMS phishing or smishing is a form of criminal activity using social engineering techniques. Phishing is the act of attempting to acquire personal information such as passwords and details by masquerading as a trustworthy entity in an electronic communication. SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information.(https://en.wikipedia.org/wiki/SMS\_phishin g)

Pharming: Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.(<https://en.wikipedia.org/wiki/Pharming>)

## Guideline

Click fraud is a type of fraud that occurs on the Internet in pay-per-click (PPC) online advertising when a person, automated script or computer program imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.(<https://en.wikipedia.org/wiki/Click_fraud>)

1. Minimize the exposure of personal information

Exposure of the personal information in the public area should be minimized to protect the personal information from the danger of being exposed by voice phishing or smishing.

1. Be cautious clicking internet address included in SMS

Users should be very cautious being clicking internet address included in SMS because sending internet address including vicious code using disclosed personal information is frequent in smishing.

1. Manage the mobile phone safely;
* Do not change the authority of smartphone arbitrarily
* Be cautious installing the application which shows the sentences ‘unknown resources(not authorized)’
* Install the smishing blocking application
* Install mobile vaccine application
* Update the operating system of the smartphone with the newest version
* Refrain the smartphone from using unsecured wireless WIFI. But if you have to use it, do not send any personal information because data transaction can not be protected by such wireless WIFI.

* Pay attention to the malicious code infection of PC

Main reason for PC connecting pharming site is because PC is infected to malicious code. In this case even though normal address is input on the internet address window, it is connected to pharming site. Therefore users should be careful for PC not being infected by malicious code. For example, maintain computer anti-virus program updated, check security of the PC regularly and carryout security update for important application program regularly.

**New ICT Technologies**

Security considerations on using new ICT technologies

Recently new ICT technologies such as block chain technology, AI related technology, IoT technology and etc. often appear and related new services for general users also tends to be appeared rapidly. Security threats immediately follow thereafter appearing these new technologies.

## Example

Eexisting security threats related to block chain are

* key management threats: if attacker robs private key, encrypted data can be decrypted without permission
* cryptographic threats: using random numbers which are intentionally restricted or using keys with low encryption level is dangerous
* privacy threats: since implementation for ‘rights for being forgotten’ by deleting data is difficult, unauthorized access to existing block chain data is possible
* DDoS attack threats: DDoS attack is possible which generates expired enormous spam transactions on the network

 Possible security threats can exist which are not known except known security threats such as the above.

Provisions for security threats are increasing along with the appearance of new ICT technologies and countermeasures on the security threats for general users using these new technologies should be added to the provisions.

## Guideline

The general users who want to use new ICT technologies should consider the following security threats at least.

 - security threats such as encryption related key theft and key loss

 - security threats such as authentication related authority abuse and misuse

 - privacy related security threats

 - malicious code related security threats

 - existing security threats such as DDoS attack

 - security threats for interoperability related to existing technologies

**Appendix**

Guideline of urgent response for hacking incident

This guideline provides urgent response actions for system manager or general users for arresting criminals or minimizing the loss when hacking is happened. Additional damage can be preventable according as how efficiently one can use the given time after recognizing the first attack.

## Guideline

Guideline of urgent response for hacking incident (General contents)

1. In case of first recognition of incidents (system manager or employee, etc.), situation related to the damage should be grasped as well as teamwork among related teams in the organization should be activated.

In general teamwork among related teams in the organization is needed to minimize the loss or to catch the criminals when hacking is occurred. For example, threat response team, forensic analysis team, network management team, incident prevention team and incident response team(these names can be different depending on the organization, therefore names in this contribution is just for reference) should be quickly cooperated.

1. Cooperation from outside in addition to the one inside the organization is also needed. Especially, quick help from the special organization should be obtained about law or regulations. If it’s needed, proper lawyer should be assigned for the incident and then efficient solution will come out through swift and smooth communication between organization inside and lawyer.
2. Public investigator such as police in the region should be asked for the incident. Distinction on cyber space should be considered that it is more difficult to find proofs for arresting criminals as time passes on.
3. Communication with outside should be concerned. Proper information related to the incident should be quickly transferred to the related customer, staff and organization inside. This is also related to law and regulations.
4. Related insurance company should be quickly notified. For example, when incident happens such as private information leaks, it is more efficient to discuss about the insurance coverage and cost than to try back to the past.
5. Strategy for the proper public relations should be arranged to prevent unnecessary turbulence or damage by distributing inaccurate rumor to outsiders, especially normal persons. Timely response should be activated by thorough monitoring with control of all information about incident
6. Incident response team should completely eliminate attacker on the network as soon as possible after first attack is recognized. By removing all the tools of attackers, reattack can be prevented by completely deleting related attack host and risk on the revenge attack can be minimized
7. All the tasks for the response above should be simultaneously progressed instead of progressing separately. Therefore, although first notification is done by system manager, all the related departments within organization should be simultaneously cooperated afterwards.

Guideline of urgent response for hacking incident (Depending on the time)

1. Manager who firstly recognized incident should be figure out the attack/intrusion situation quickly and clearly. (to collect quickly as much information as possible)
2. Taking measures should be performed to minimize the loss. (organization strategy or guideline such as whether setting all network or system offline or stopping the only some applications which make troubles should be established before the incident.)
3. Teamwork among related teams in organization should be quickly activated. Opening of the incident and the level of opening of the incident should be strategically decided. Especially organization strategy for how to react to the situation by law and regulations should be established before the incident.
4. Investigation request to the police and cooperation with insurance company should be decided.
5. Complete recovery of the system which is influenced by hacking should be done.
6. Security level should be intensified and patched the vulnerability at the same time.