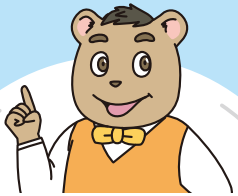


Be vigilant
about information
security and enjoy using
the internet

GOsafeonline.sg
Cyber Security Awareness Alliance

https://www.gosafeonline.sg/

ASEAN · JAPAN
Information Security Awareness

Be Aware, Secure, and Vigilant

Information Security

Use the Internet with Confidence

Smartphone Security

Smartphones have become more popular all over the world, and the percentage of smartphones in the mobile phone sales has been increasing.

Smartphones are highly sophisticated devices compared to traditional cellular phones. They enable us to view the websites designed for computers and various kinds of applications can be downloaded and used freely.

The updated version of OS*1 and applications*2 on smartphones are regularly provided. These updates*3 may provide more functionalities and hence increase the sophistication of the smartphones or enhance the security.

*1 - OS is an abbreviation of Operating system which is a software that controls computer or smartphone. For example in computers, OS manages various kinds of functions such as I/O(Input/Output) functions managing inputs from keyboards, or outputs to displays, or printers .

*2 - Application refers to software developed for specific purpose, such as word processing, or making spreadsheets. Users can choose applications they need, and use them after installation in the OS which has fundamental functions commonly used by every software.

*3 - Update means minor amendment of software to fix bugs, or to offer functional improvements.By applying them, users can keep their software up to date.It's also important to update security software for information security.

Risks and Threats

1 The number of malware targeting smartphones is increasing. If your device gets infected by malware, contents of the address book or other personal information might be sent to an external server or unauthorized charging of money might occur.

2 Besides being infected by malware, when downloading applications, the application may ask to use device information or request the contents in the address book to be sent to an external server. For example, there was a case of an application claiming to be designed to increase battery life, but actually it tries to send address book information irrelevant to the use of the application to an external party.

Countermeasures

- Keep the OS, applications and anti-virus software on the smartphones updated to the latest available versions. Since smartphones contain address book information and other sensitive information, much more caution is necessary .
- When downloading applications, make sure to check whether the site can be trusted and who provides the application. Also when downloading, make sure to check the consent agreement and/or terms of service for the information collected and how it will be used, prior to consenting or using the application.

Wireless LAN Security

In recent years, computers have become lighter in weight and smartphones have become more popular, which has accelerated the use of "Wireless LAN" enabling the access to the internet via wireless communications even outside of home or office.

In addition to paid services by providers, free public Wi-Fi services provided at airports, train stations and commercial buildings have also increased.

Risks and Threats

1 Since wireless LAN can be connected freely within the area covered by the radio waves, communications may be intercepted unless proper security measures are taken.

2 Also, unauthorized access to a wireless LAN network might lead to leakage of personal information or being used as a stepping stone for an attack on a server.

Countermeasures

- Use wireless LAN after setting data encryption (WPA2: Wi-Fi Protected Access 2, etc.) so that clear text communications cannot be intercepted and to prevent unauthorized access. Also limit the devices that can connect (using MAC address filtering) to the base unit (Access point, router, etc.) so that unauthorized third parties cannot connect.
- When accessing public wireless LAN services, users should only access SSL*4 encrypted websites (websites whose URL starts with "https") and disable file sharing on the computer prior to using the service.

*4 - SSL is an abbreviation of Secure Socket Layer which is a protocol to encrypt data sent on the web.

One-Click Fraud

One-click fraud refers to the defrauding of money by displaying a screen to bill for an enrollment fee or service usage fee after clicking an image or a video on a website.

Recently, there have been one-click frauds that use smartphone applications and social media services such as blogs*1/SNS*2.

Beside "one-click" cases, the billing screen may be displayed after a few clicks such as age verification, etc. In some other cases the techniques used are becoming more devious and sophisticated, such as the billing screen not disappearing even after the power has been shut down on the device.

*1 - Blog is a shortened form of Weblog with which users can write their opinion or impression like journal, and visitors can freely give their comments on their posts.

*2 - SNS is an abbreviation of Social Networking Service which provides web site that has many functions such as opening our diary or photo album to the public, or making community in which users can exchange their opinion freely.

Risks and Threats

1 Clicking free images or videos that are interesting to a user may lead to an unauthorized billing or to a fraudulent site.

2 There are some cases where the IP address*3 and/or the provider information is listed on the billing screen to arouse fear by making it look like that the individual has been identified.

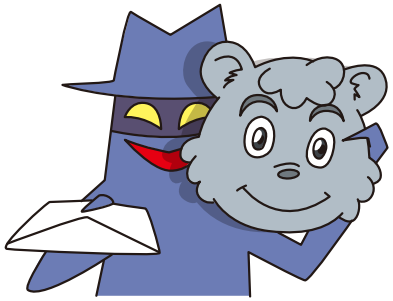
*3 - IP address is an identification number automatically assigned to the instruments or computers when they are connected to the internet.

Countermeasures

- Block attempts to connect to malicious sites by using filtering software or other latest security software. Also be sure to download smartphone applications only from trusted sites.
- Be aware that when using a computer, a single click will not identify you, so do not respond to requests for payments. For smartphones, be cautious that depending on the application, information stored on the device such as your own contact information or other information in the address book might be disclosed.
- If you happen to access one of these sites and received unauthorized billing or a court order, consult an authority (administrative counseling or free attorney consultation, etc.) for advice.

Targeted Email Attacks aka Spear Phishing Attack

A targeted email attack is an attack where an email is sent disguised as if sent from an acquaintance of the user. The email will likely contain a malicious attachment which when accessed will infect the system with a virus or trojan.



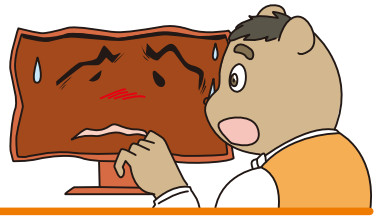
A typical example is that the target is a specific organization or an individual user. An email with a virus-infected attachment is sent from an attacker pretending as a related party or a colleague of the organization.

Cases have been reported of passwords being stolen or virus infections, etc. caused by targeted email attacks.

Risks and Threats

1 In recent attacks, the methods used to disguise as a trusted email have become increasingly sophisticated and advanced. The name of departments and/or individuals that actually exist are used, in addition to using contents or information that only the concerned parties would know.

2 If a virus is attached, opening the attachment will result in an automatic connection to an external server and information within the computer will be leaked.



Countermeasures

- Do not open any suspicious e-mail attachments or URL.
- If you happen to open a suspicious email, do not panic and do not shut down the device. Disconnect the network cable and ask for assistance from a system administrator.
- Install antivirus software and make sure that it is always up to date.
- Periodically update applications in addition to the OS.

DDoS Attacks

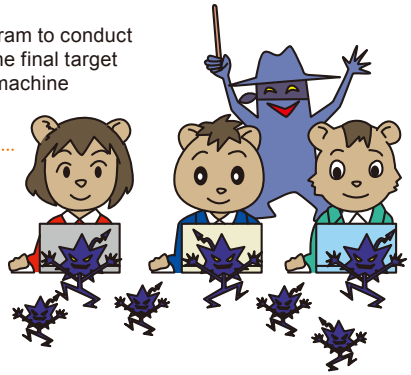
A DDoS attack is an attack that a specific server is bombarded with packets from a large number of compromised computers across multiple networks, until communication line is overflowed and the server ceases to function.

DDoS: Distributed Denial of Service

Risks and Threats

1 An attacker will covertly install a malicious program to conduct the attack to computers that are not related to the final target (server). Therefore, a user may attack another machine without knowing.

2 Compromised computer may conduct attacks other than DDoS attacks such as infecting other computers with a virus, sending spam emails or defacing websites on behalf of the attacker.



Countermeasures

- Keep the OS on the computer, smartphone or any other device that will connect to the internet updated to the most recent version.
- Install antivirus software and make sure that it is up to date.
- Periodically update applications in addition to the OS.

Etiquette When Using the Internet

Due to the increased use of SNS (social networking service), issues on the internet that were not previously thought of have surfaced.

There have been cases that individuals post contents on the internet where the slandered individual may be identified or where companies have had to issue public apologies.

Risks and Threats

1 There is a possibility where a casual posting on an SNS may lead to personal information to be disclosed or defamation of the others or a violation of privacy.

2 A casual posting on the internet may result in a demand of payment for damages, reprimand by law or even an arrest.

Countermeasures

- Be careful not to disclose unnecessary personal information on the internet through an SNS, blog or miniblog, etc. Posting images may reveal location information so you should be cautious.
- Even on the internet, be sure to consider other people's privacy and dignity and check the contents prior to posting information.

Proper Setting and Management of ID and Password

In order to use email, internet shopping, internet banking and other services on the internet safely, there are many types of authentication schemes, while the most popular one is ID/password combination.

There has been an increase in cyber-attacks that target user account information such as ID and password.

Risks and Threats

1 A malicious third party may impersonate a user and disclose information or cause monetary damages if the ID/password is a very simple combination (such as a 4 digit birthdate, or "9999", etc.) or if it is carelessly managed. (for example, password left on a post-it note on the monitor, etc.)

2 If using the same ID/password for multiple sites and the information is leaked from one of the sites, the possibility of becoming a victim of a cyber-attack at another site will increase.

If personal or important information is entered into the computers open to the public, such information might be stolen.

Countermeasures

- Set the passwords with an unpredictable string that is at least 8 characters long containing numbers, upper and lower case characters and symbols. Also change the password regularly.
- Do not share passwords with other people or use the same password for multiple services.
- When entering personal information into the computers open to the public at such place as internet cafes and other places, be cautious about your personal information not to be stolen.

Spam E-mails 1

Email is quite a convenient communication tool by which sending and receiving can be performed without considering where the recipients are or how far they are. However, from the recipient point of view there may be a lot of unnecessary email, spam messages, that are sent and received.

Due to a large number of spam email messages being sent, there have been issues where the equipment at the providers facilities may become overloaded which may lead to delays in getting other messages sent/received.

Risks and Threats

1 There are cases that a computer will randomly generate a large number of email addresses and send email messages. Therefore, the use of short email addresses and popular names in the address may result in an increased possibility of receiving spam emails.

2 Some of the valid email addresses to send spam email are collected through the registration of a free fake service or through fictitious unsubscribe procedures.

Additionally, opening a file attached to an email or accessing a link within the email may lead to visiting an unauthorized website or lead to a virus infection.

Countermeasures

- Email addresses should contain a large number of characters and include numbers randomly to make it hard to guess.
- Do not carelessly enter your e-mail address into the website or show your e-mail address on the website, if it's not necessary.
- If it is necessary to use a site that may not be entirely trustworthy, it may be effective to use a freely available email address as opposed to using the provider supplied address.

Spam E-mails 2

Spam emails may not only cause displeasure to the recipient or interrupt work, the methods used has also become increasingly malicious and ingenious, which may lead a user to an unauthorized site where money might be stolen, or go through spam email filter setting.

Smartphones may be infected by virus within the spam emails, and manipulated from distant place to send large amount of spam emails without user's knowing.

Risks and Threats

1 There are cases that a computer will randomly generate a large number of email addresses and send email messages. Therefore, the use of short email addresses and popular names in the address may result in an increased possibility of receiving spam emails.

2 Some of the valid email addresses to send spam email are collected through the registration of a free fake service or through fictitious unsubscribe procedures.

Additionally, opening a file attached to an email or accessing a link within the email may lead to visiting an unauthorized website or lead to a virus infection.

Countermeasures

- Try to block spam emails by using the spam email countermeasure services such as the rejection function or anti-spoofing functions by internet service providers or filtering software.
- If you receive a spam email, delete it without opening it. Also, do not open attachments or access links from suspicious emails. It may also be effective to forward the spam email to your provider or a public agency.
- Take countermeasures on smartphones as well as computer.

Protect your own smartphone and computer.

Smartphones and computers are useful tools, But on the other hand they face many dangers such as becoming infected with computer viruses. Remember to obey the three top tips of information security to ensure safety and security when using computers and smartphones.

Three top tips of information security

Handle important personal information with care.

Protect your computer with the latest security updates.

Don't access suspicious websites or unfamiliar emails.

Information security measures can be likened to fastening our seatbelts when we ride in a car, and it's something we must not forget when we use a computer or a smartphone.