Information Security Handbook

for Network Beginners

National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
The Government of JAPAN

NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

Ver 2.11e

September 29, 2017


INTERNET
OUR INTERNET
OUR SECURITY
NISC

Table of Contents

***Caution**

This handbook is intended to help beginners understand the problems related to cybersecurity, and simplifies actual cases for easier understanding. Some related information may be omitted so as to make the content easier to understand.

For those who want to deepen their understanding of cybersecurity by reading this handbook, we would appreciate it if you go a step further and try reading different specialty magazines and latest articles.

The persons and organizations that appear here are fictitious and any similarity to any actual persons or organizations is purely coincidental.

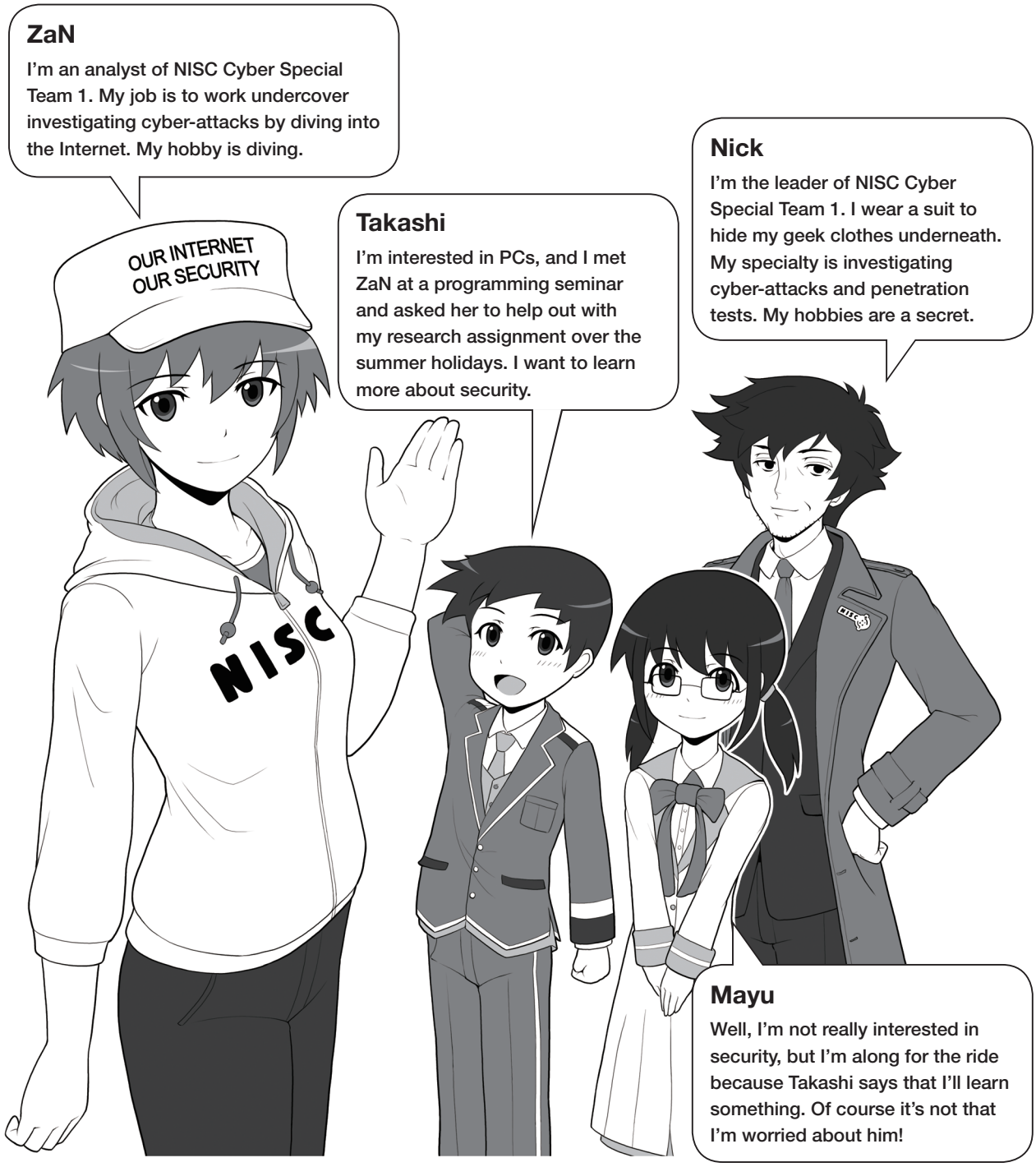
Foreword —Be your home CSIRT—

Hi, I'm ZaN, an analyst of NISC, the National Center of Incident Readiness and Strategy for Cybersecurity, and this is my boss, Nick, who is a bit tired from working so hard.

In this book, we will introduce knowledge about cyber-security from familiar topics, and Takashi and Mayu will join in to learn with us.

Various cyber-attacks happen on the Internet every day. Government agencies and the private sector are doing all they can against these cyber-attacks, but the attacks show no sign of slowing down and are steadily increasing.

What we need to do in these circumstances is to improve the security of computers and smartphones in the hands of each citizen that are at risk of a cyber-attack, and make it difficult for an attack to be carried out.



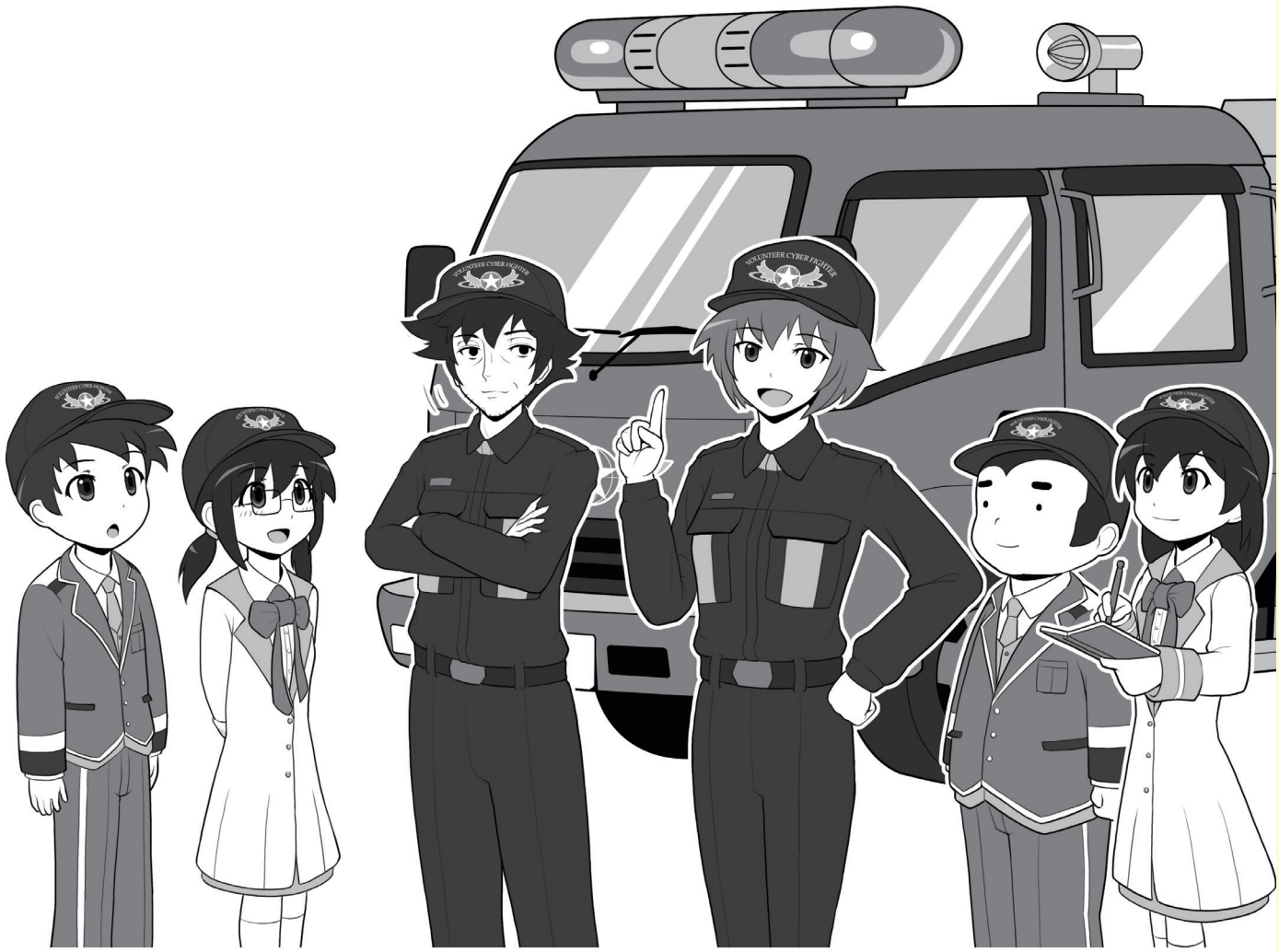
*NISC Special Team 1 is a fictitious group.

As seen in recent things like bank transfer scams, we have to prevent it as they skillfully prey on psychological security holes and can control victims at will.

So, just as the safety of the city is not only supported by professionals such as police officers and firefighters but also various volunteers, the safety of the Internet is supported by everyone sharing the Internet. We all need to be involved in raising security awareness and crime prevention activities related to the Internet as your home CSIRT.

When we say, “your home CSIRT,” the CSIRT stands for Computer Security Incident Response Team, which is a special organization in a company that deals with cyber-security incidents when they occur. Similarly, whether it is in your own home, a circle or group of friends, or in a small company which cannot set up a special CSIRT, if you have an interest in cybersecurity, we hope that you will take on the role of being your home CSIRT, your circle’s CSIRT, or a small company CSIRT.

We need your help in order to realize an Internet society that everyone can use securely.



We can create a safe Internet society when everyone is responsible for cybersecurity.

People with malicious intent on the Internet are targeting the smartphones in your hands and the computers in your homes. However, there is no easy way to protect all the smartphones and PCs in the world. Help us protect the Internet together just as crime prevention activities protect where you live through increased crime awareness, and develop an attitude of helping one another when something happens.

Black Hat the Cracker

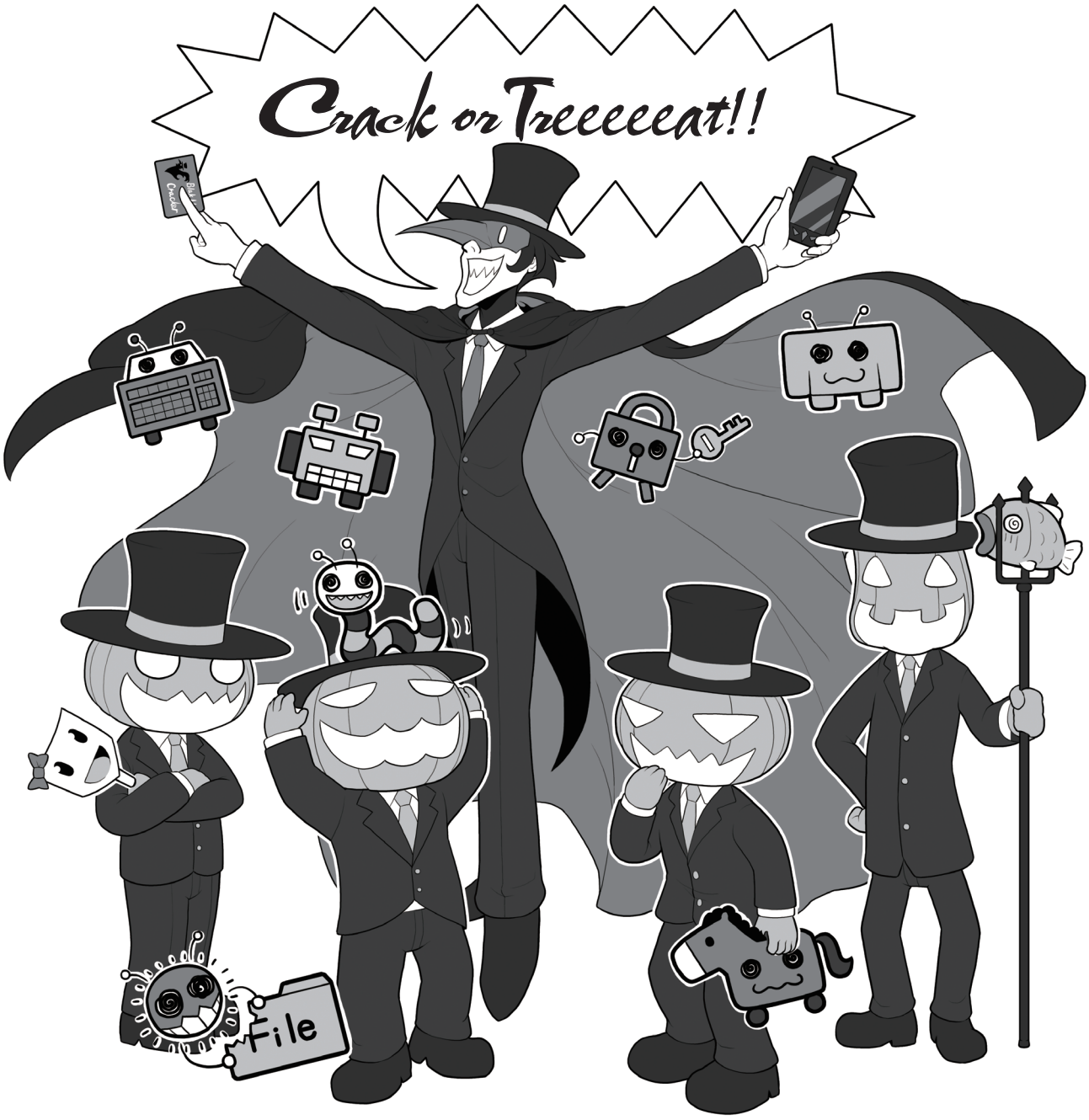
There are people who maliciously use cyberspace (the Internet) for their own benefit to rob others, and carry out cyber-attacks to demonstrate their ability.

In this book, those people appear as Black Hat The Cracker and his minions, the Black Pumpkins, and various malware.

Sometimes, they also put on masks of ordinary people, or ordinary people may wear their masks and do bad things.

I want to talk about these things in the illustrated explanations, so please be sure to read them carefully.

The origin of his (her?) official name, Black Hat The Cracker, will be explained in the column “Attackers, Hackers and Crackers.”



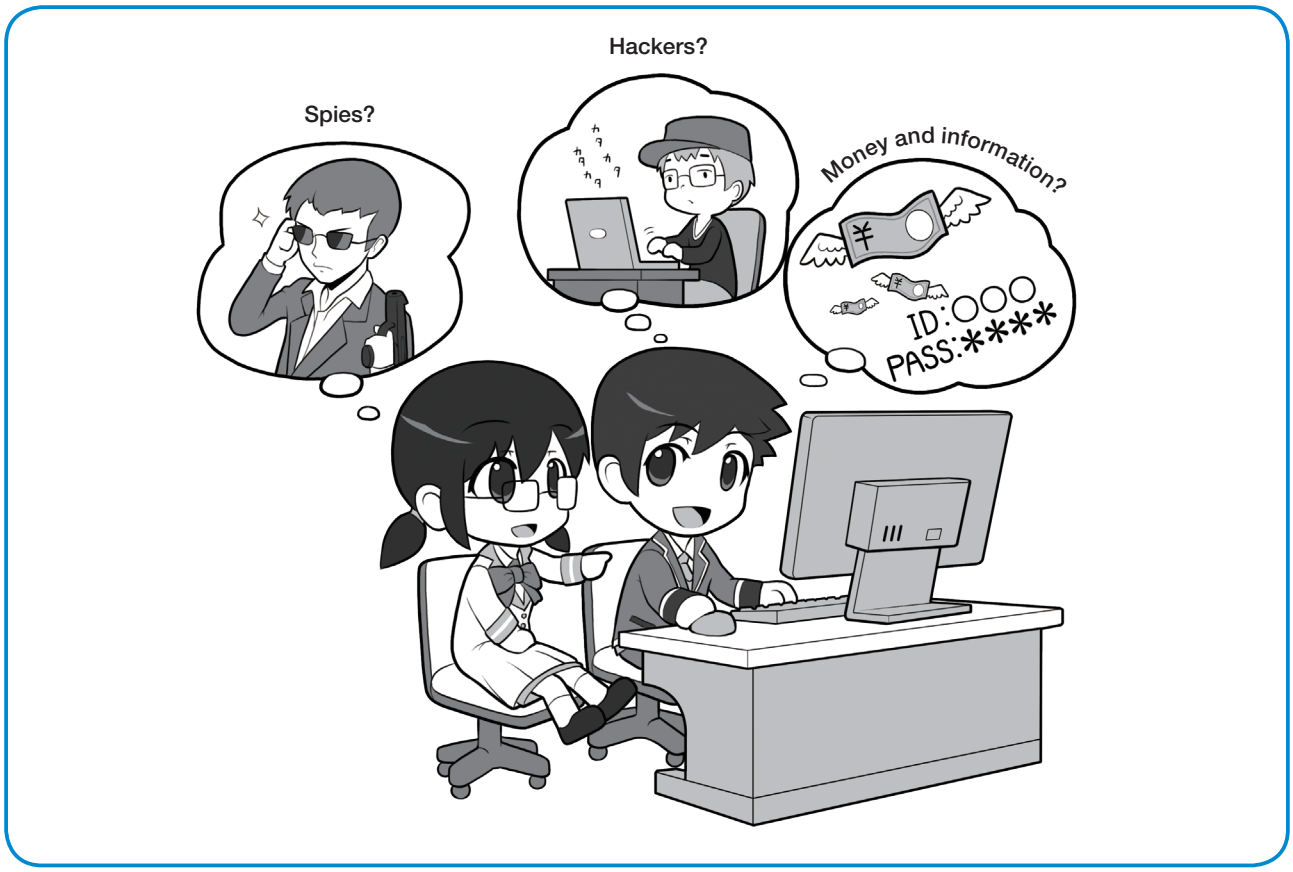
Prologue

What Is a Cyber-Attack?

What do you think of when you hear the word “cyber-attack?
What happens? Who does it?
But first, let’s learn about what a cyber-attack is.

1 What a Cyber-Attack Looks Like

1 Who carries out cyber-attacks? How do they do it?



Who carries out cyber-attacks and for what purpose?

Is it military or industrial spies? Or is it hackers?

Spies seek to obtain useful information for their own countries and companies, such as military secrets and information on advanced research. On the other hand, the cyber-attacks we normally encounter are aimed at something that will benefit the attacker, such as personal information or money.

Since spies must accomplish their objective, they will attack with any and all means, and try to intrude no matter how strong security is. They are a problem and there is no way to completely stop them for now.

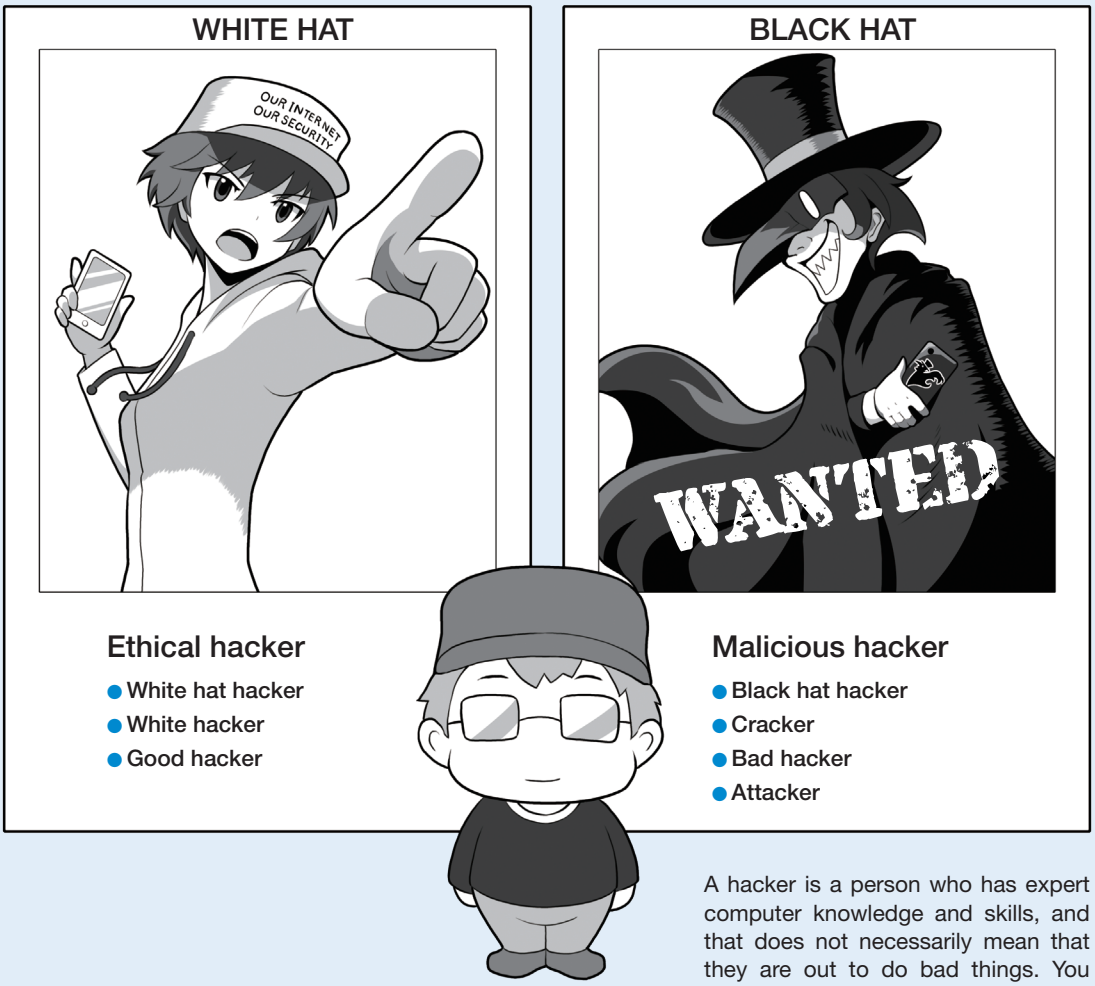
Meanwhile, cyber-attacks for profit are a business for attackers. For example, given that they will avoid something with strong security because it takes time and effort (≈ the cost is too high) and attack things that take little effort (≈ cheap), attackers will tend to go after easy targets, so if we increase the security level of our devices, we are less susceptible to attack to some extent. Think of it as you making an effort to reduce the probability of being victimized, even though it is difficult to completely prevent an attack.

Dealing with cyber-attacks is not like in cartoons where the hero appears to stop the bad guy, nor can they be tightly defended digitally. First of all, we need to steadily build up the way to secure safety.

Please keep this in mind as we continue to explain the story about cybersecurity.

Column: Attackers, Hackers, and Crackers

Hackers



A hacker is a person who has expert computer knowledge and skills, and that does not necessarily mean that they are out to do bad things. You need to be careful of the meaning of hacker when you use the word yourself or when you see it in the media.

Newspapers, magazines, and TV, often refer those who carry out cyber-attacks as “hackers.” The truth is, however, this way of putting it is not quite correct.

A hacker is a sort of honorific name for someone with expert computer knowledge and skills, but it does not mean that they are attackers who seek to do harm. The work they do using their skills is called “hacking” or simply a “hack,” and likewise this does not necessarily mean that they intend to do bad things.

However, because there are people who use their knowledge and skills with malice, to distinguish them from those with good intentions, they are called “black hat hackers” or “black hats,” while those who seek to penetrate defenses are called “crackers,” and those who carry out attacks, “attackers.”

And in Japan, they are also called “bad hackers” or “malicious hackers”. Conversely, people who use their expert knowledge and skills with good intent are called “white hat hackers,” “white hats,” or “white hackers,” and in Japan they are also called “good hackers” or “ethical hackers.”

In this book we will use these terms based on their original meaning, so please remember them and try and use the correct name so that it will become widely used in everyday life.

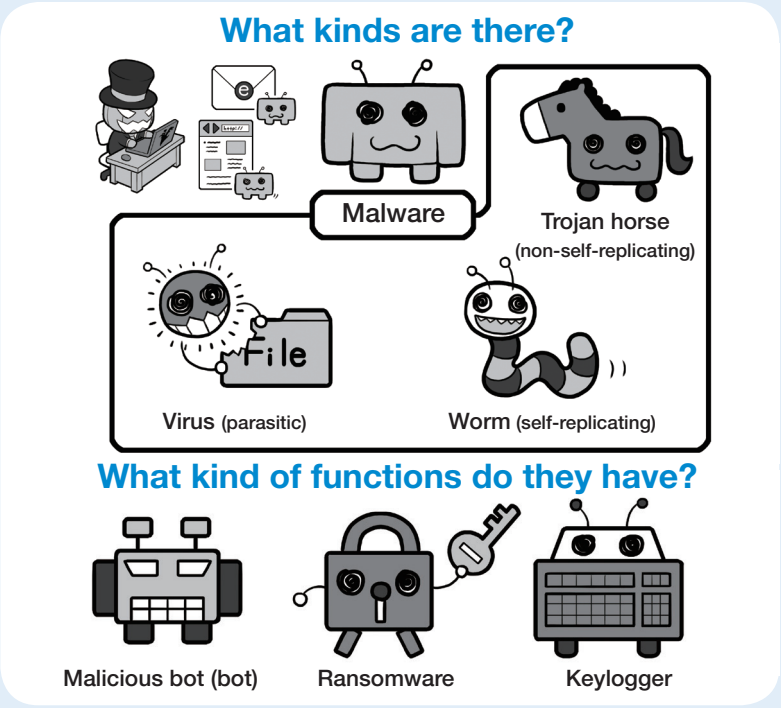
Column: Malware - The weapon of an attacker

What kinds are there?

As with the earlier examples of hackers and crackers, the term “computer virus” or simply “virus” is also not used properly.

When an attacker carries out a cyber-attack, they often use the method of infecting a target’s computer with a malicious program and gaining control of it. The programs used for this attack tend to be collectively called “viruses.”

However, the programs used for attacks should correctly be called “malware” or “malicious programs.” A virus is one type of malware limited to referring only to the type that infects files on a computer and acts like a parasite on the infected files.



To give a real-life example, malware is the generic term for a pathogen that causes a disease. It is similar to what we call a virus, a kind of pathogen, which cannot grow unless it infects cells.

Besides viruses, there are bacteria, protozoa, and parasites that can exist alone as pathogens. Similarly, with malware, there are independent and non-self-replicating types called “Trojan horses” and independent and self-replicating types called “worms.”

There are also “bots,” “ransomware,” and “keyloggers” that are defined by their functions. These are like the names of the symptom that represent the behavior of the pathogen.

However, the word virus is broadly used to mean the same as malware in general, so they are viruses in a broad sense for consistency.

It is important for everyone to remember this and spread the correct usage. When you see the word “virus” being used in newspapers, magazines, or on TV, it is important that you correctly understand from the context whether it means “a virus in a broad sense, such as malware,” or “a virus in a narrow sense, such as an intrusive program infecting files.”

What kind of functions do they have?

If you divide malware by function, they look something like this.

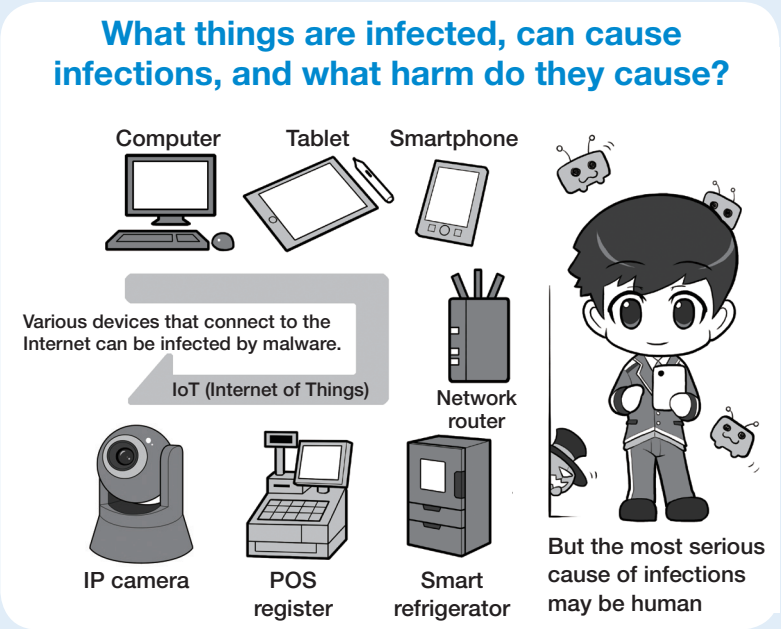
- **Malicious bot (bot)**
  Bot is short for robot. A malicious bot is one that infects a computer and allows an attacker to use it to attack another computer.

- **Ransomware**
  When a computer is infected by ransomware, the files on the computer are encrypted and a ransom is demanded for their return.

- **Keylogger**
  A comparatively older type of malware that records keystrokes and sends them to the attacker. The attacker can analyze the recorded keystrokes to steal passwords and other things.

For example, a Trojan horse first pretends to be harmless when intruding a computer, but once inside, it reveals itself as malware, invoking bots and ransomware from the outside, and starts causing harm. It gets its name from the Greek story of the Trojan Horse.

What things are infected, can cause infections, and what harm do they cause?



When it comes to malware infections, personal computers, smartphones, and tablets probably come to mind.

It is no mistake to say that malware is a malicious program that infects a computer. However, the wireless LAN router in your home, a printer connected to a network, a surveillance camera or IP camera, a smart TV, a smart refrigerator, and even a POS register can all be infected. If they don't look like computers, how can they be infected?

The key to solving this question is that modern electronic equipment, even if they don't look like computers, actually contain built-in computers.

Since these devices connect to a network and exchange data, they too can easily be infected by malware.

In particular, in the era of IoT (the Internet of things), the devices around us have become computerized and connected to the Internet, paving the way for even more devices to be potentially infected.

However, there is a problem even more serious than a malware infection from a malicious attack. That is a cyber-attack on humans' psychological security holes.

In order for malware to easily infect a device, a computer has to have a weak point in a program called a security hole. A security hole is like a broken window lock of a house. However, frequent security updates repair these problems and take care of most security holes.

Despite this, if an attacker can trick an owner into installing malware himself, they are free to do all the harm they want without having to intrude. This is a type of attack on psychological security holes, such as a targeted e-mail attack, which will be explained later. The problem is that a psychological security hole cannot be easily patched like a security hole on a computer. Security awareness does not improve unless the person himself recognizes that it is necessary.

No matter how hard you defend against cyber-attacks, there are numerous attack techniques to trick humans that are not easily prevented. This is important to know.

The victims can spread infections one after another to friends and colleagues in the workplace, and various devices may join the cyber-attack as part of a botnet, all without their owners knowing.

You may be a victim and may unwittingly be part of an attack, and may even be the assailant in some instances.

Let's first gain the knowledge to prevent these things, and then take action.

2 Examples of cyber-attacks

Let's look at a couple of examples of how the cyber-attacks we introduced earlier are actually carried out.

An attacker first attaches malware to an e-mail, sends it to you, or guides you to a website containing malware, and infects your computer with it. After that, your IDs and passwords are stolen, and the attacker can have your computer send images and important information in the background without you noticing. Your IDs and passwords can be used to make purchases without your permission and then later converted into money.

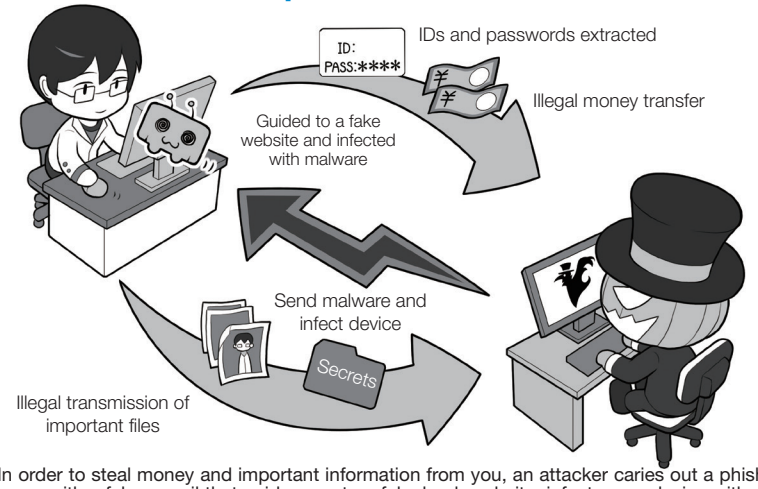
E-mail can be used to conduct "phishing scams" by leading you to fake bank websites that steal your ID and password, and then make illegal money transfers.

More directly, they may demand money from the target. Ransomware encrypts data on your PC or smartphone without your permission and demands that a ransom be paid to decrypt the files if you want them back.

A "DDoS attack[1]" forces infected PCs and devices to participate in an illegal scheme called a botnet without the owner's permission, and the botnet causes massive requests to target a website to prevent people from browsing the website. The owner is an unwitting accomplice to the attack.

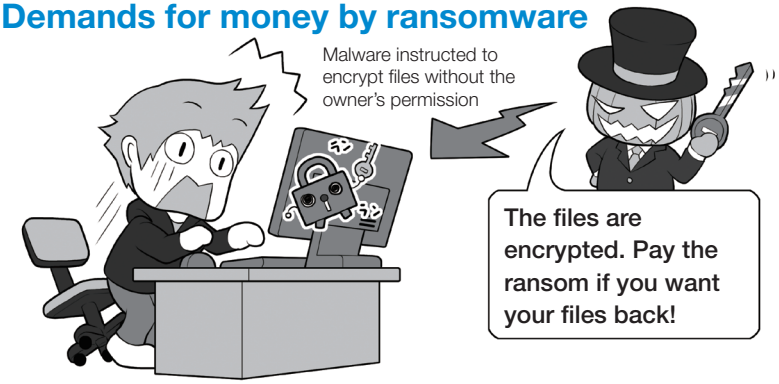
An attacker may rent out this illegal botnet mechanism on a time basis to make money.

Phishing scam with a fake website and illegal transmission of important information



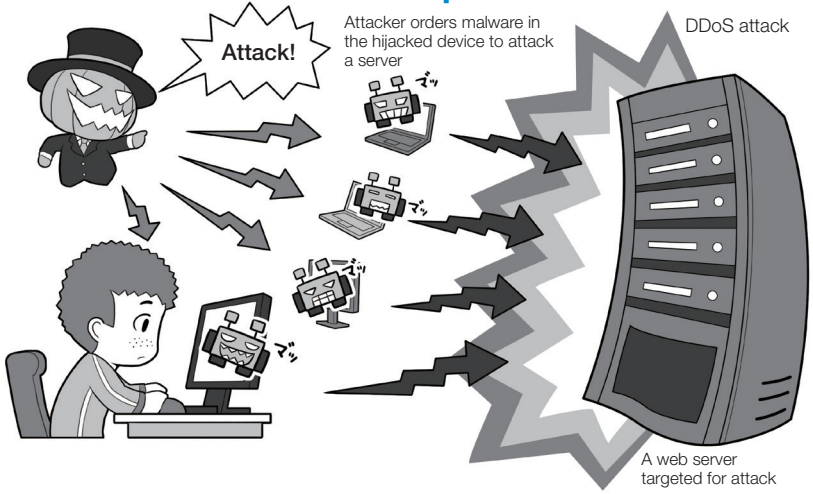
In order to steal money and important information from you, an attacker caries out a phishing scam with a fake e-mail that guides you to a fake bank website, infects your device with malware, and illegally transmits important files. Let's look at how you can be fooled.

Demands for money by ransomware



When infected with ransomware, files on computers and other devices are encrypted, and a ransom is demanded in order to decrypt the files. However, paying the ransom does not mean the files will be decrypted. Prepare for this situation by making backups of your system and data so you can restore your computer to its original state. Let's learn how intrusions happen by looking for examples in columns.

Devices that have become part of botnets



When infected with a malicious bot, the bot is connected to a botnet, which is an attack mechanism controlled by an attacker, and uses your computer or device in a cyber-attack without your knowledge. Without you knowing it, you may be the assailant.

1 DDoS attack: Distributed Denial of Service attack. Multiple devices attack a server or other device to overwhelm its communication capabilities and render it unavailable.

3 Crimes and problems in cyber-attacks

Besides cyber-attacks, various crimes and troubles happen on the Internet.

Impersonation and abduction/kidnapping are an example. There are instances where a person uses social networking service to impersonate the same age and gender of a minor to become friends with them, lures them into meeting, and then abducts or kidnaps them. There are also cases where an assailant finds the posts of a minor on social networking service who has run away from home and takes the minor to his or her own home.

Likewise, there are cases where a person can impersonate a minor on the Internet, gain their trust, request nude photos be sent saying that the person will reciprocate, and then use the nude photos to threaten the minor.

Children are casual about exchanging nude photos, called “sexting,” but once the photos are stored on their smartphone or other device, they are at risk of being leaked even if they do not intentionally give them to someone. Once you give a photo to someone, you have to think about the possibility that it will end up spreading on the Internet and cause you a lot of anguish for a long time.

This is not limited to minors, and is a problem for adults as the crime of “revenge porn” in which nude photos are posted on the Internet to get back at partners who have broken up.

There is also cyberbullying in which social networking service and underground websites spread bad things about someone, but even if it is done in jest, it can sometimes cross the line and result in tragedy, so just like bullying in the real world, cyberbullying is something you should never do.

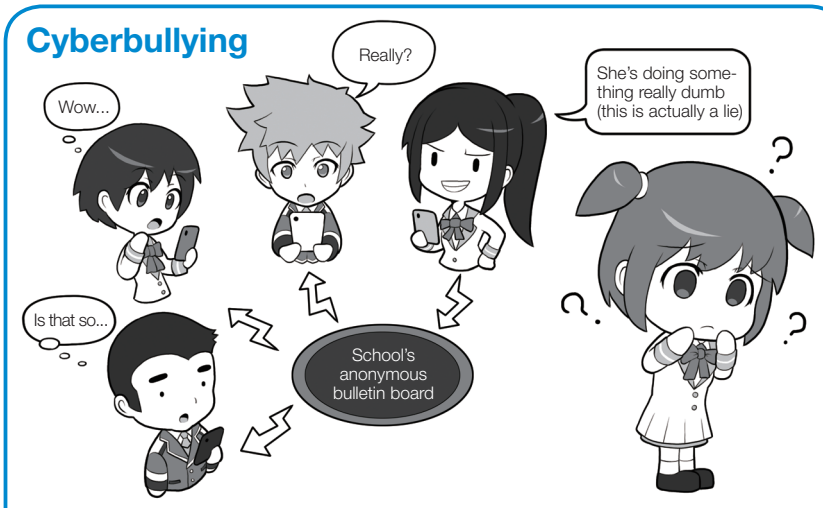
Impersonation and abduction/kidnapping

There are people who fake their age and gender to approach you through social networking service. They impersonate the same age and gender in order to become friends with you, then lure you into meeting, which could lead to your abduction or kidnaping. Be careful when people approach you on social networking service who you have never met as they may not be who they appear to be in their picture and personal information.

Sexting

Sexting is the casual sending of nude photos and explicit images which is popular among young people. But what if the photos online are sold or used to threaten you? Once a photo is released on the Internet, there is no way to completely erase it. Do not do this under any circumstances.

Cyberbullying



Just as bullying in real life is unacceptable, do not use the Internet to bully someone. The Internet should be a place where everyone can create their future, and it should not be used to cause suffering.

4 Social engineering attacks that exploit your psychological security hole

Putting cyber-attacks aside, what is a typical crime that you often hear of? Perhaps it's the grandparents scam that is a type of bank transfer fraud.

Although banks and other organizations are constantly calling attention to them, many people still fall victim.

To use a computer as an example, it would be as if you are desperately trying to fill security holes but you can't patch all of them, and the cyber-attacks keep happening one after the other right before your eyes.

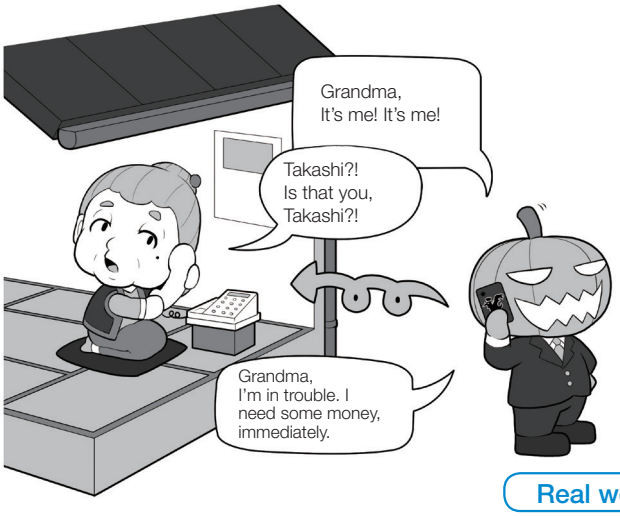
The reason is because these attacks target psychological security holes, and these attacks on psychological security holes are not easily prevented. There are many cyber-attacks targeting psychological security holes.

Take the "targeted e-mail" attack that was the beginning of the information breach at the Japan Pension Service in 2015 for example. An attacker is analyzing the target individual, and an e-mail is sent that is addressed personally to him, with an attachment appearing to be related to work, but which in fact contains malware, with the aim of infecting their computer with the malware when the attachment is inadvertently opened.

In order to reduce the damage caused by these attacks, it is important that everyone becomes familiar with cybersecurity and that awareness of the dangers becomes common sense.

Attacks targeting psychological security holes are broadly called "social engineering." Be sure to remember this.

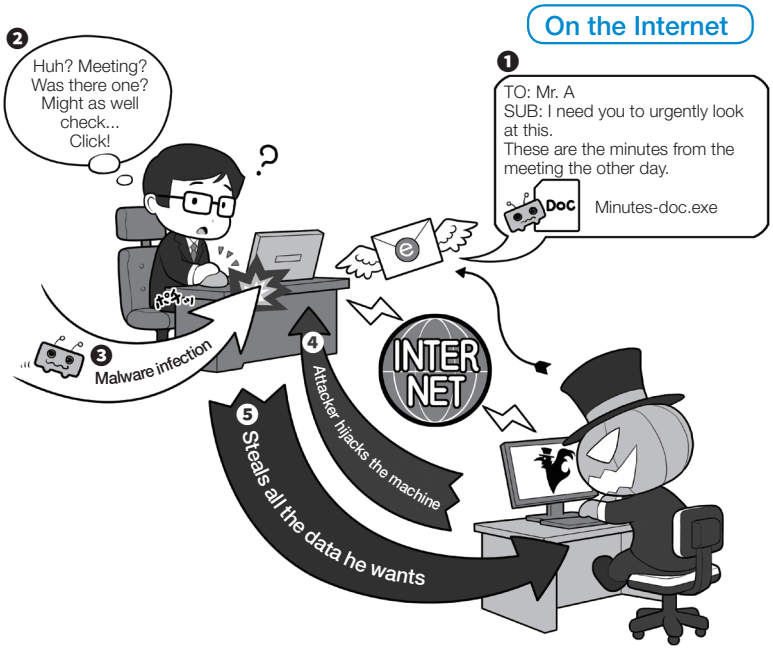
Social engineering exploits psychological security holes in real life and on the Internet



Real world

The nature of these two examples is that they prey on psychological security holes

On the Internet



With bank transfer scams, for example, the victim is led to believe that there was an accident or some kind of trouble with their relatives which deprives them of their ability to think clearly, such as confirming who is calling. Psychological manipulation, such as hurrying, impersonating a lawyer or police officer, and giving terms of negotiation like suggesting that paying money will solve the problem, are classic social engineering techniques along the lines of "hurry up," "name dropping," and "give and take."

Meanwhile, social engineering on the Internet uses the "friendship" method to send targeted e-mail as an acquaintance.

Whether in the real world or on the Internet, any security can be breached by exploiting psychological security holes. This technique of deception is called social engineering. Remember that this technique is out there.

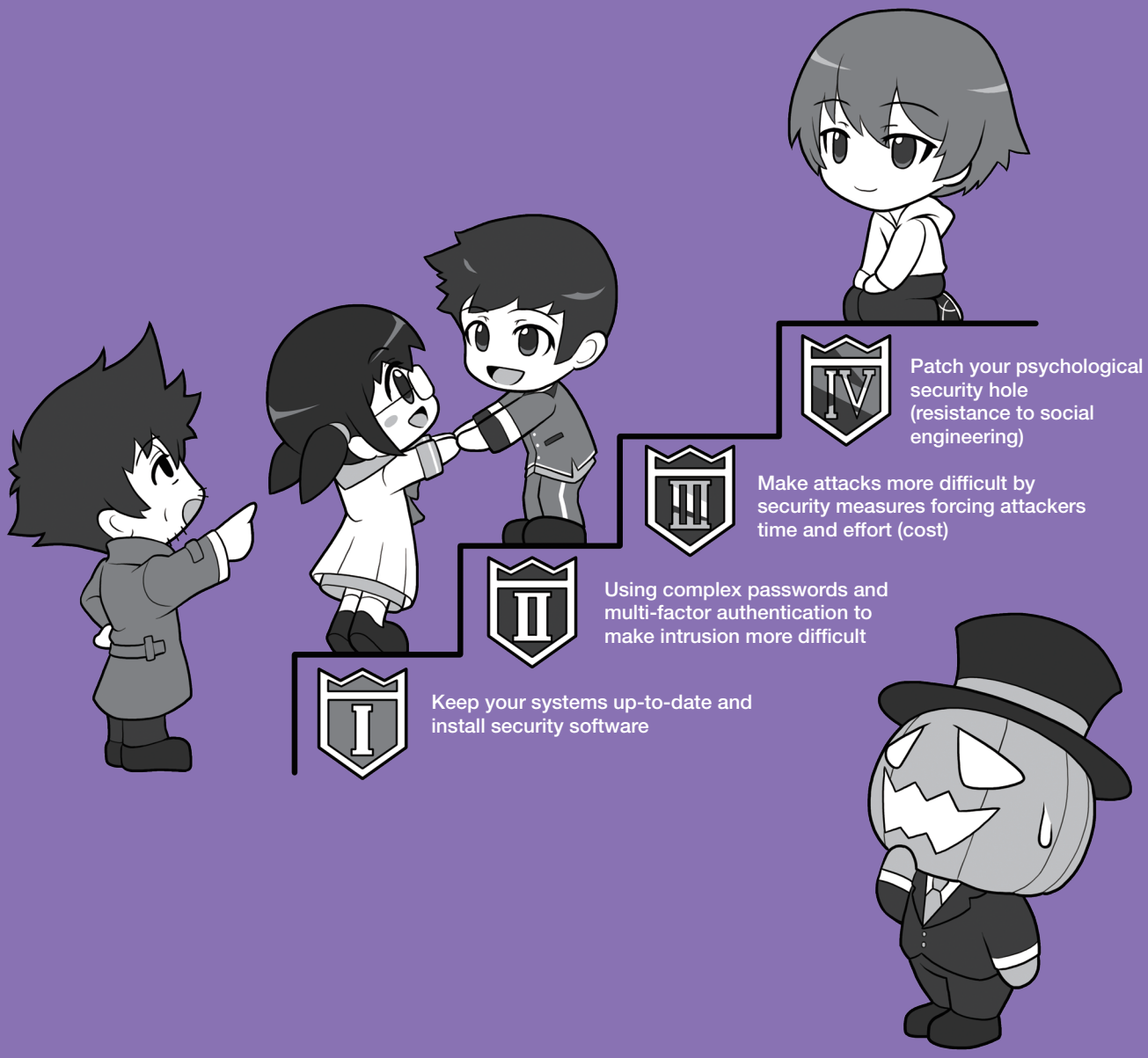
Chapter 1

Basic Security

—A Step-by-Step Guide to Strengthen Your Security—

In this chapter, we will explain step-by-step how to strengthen your devices' security against cyber-attacks.

We will also show you how to manage passwords and what you need to do so that an attacker will no longer want to attack you. We will also explain social engineering attacks that use psychological security holes.



1 4 Points to Maintain Security

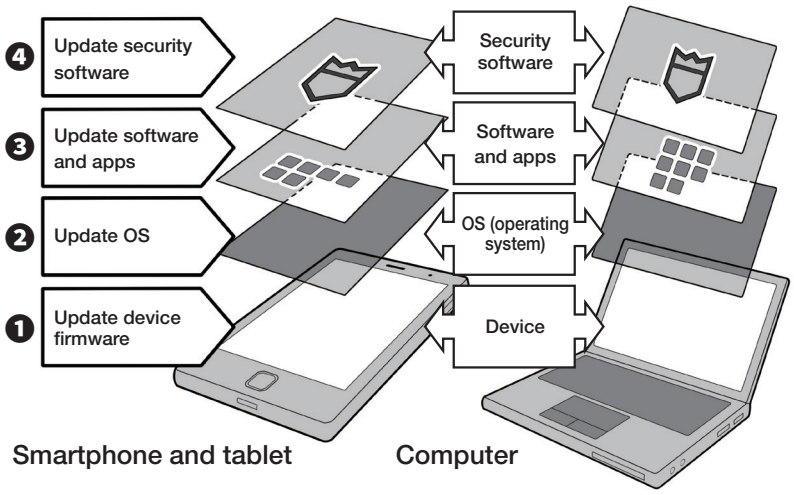
1 Keep systems always up-to-date and install security software for protection

The first step in protecting your property from cyber-attacks is to keep your system up-to-date.

The first thing to do is to update the firmware of your device. Next, is to update the operating system (OS) which is the interface that lets you control your device. After that, update your apps and software, which often contain security holes.

In the case of a computer, install and update your security software that detects malware, etc. In the case of a smartphone, please see p. 26, and install a security pack if necessary. You can patch the security holes by regularly updating these things.

Maintain security at various levels



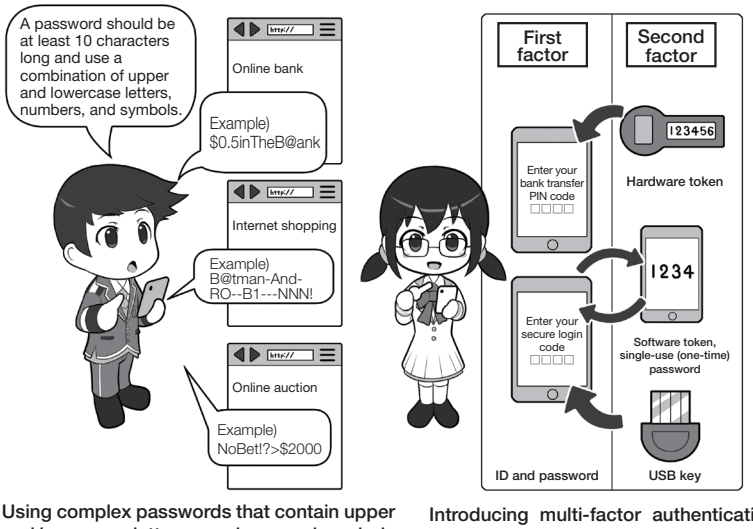
While there is free security software available, some detection functions are not as good as commercial software, and some are even act like a malware masquerading as security software. If you are unsure about which software to buy, consider software offered by your Internet service provider or from a trusted software company. The software costs money, but is an investment in improving your security.

2 Using complex passwords and multi-factor authentication to make intrusion more difficult

Another item vulnerable to cyber-attacks are passwords. Attackers will try to find or steal passwords. So first make sure to change your password when you purchase a device to make it more difficult to be find, and use a complex password for each web service or device. It is important to store your passwords securely not to be stolen.

Next, let's add an additional authentication measures with multi-factor authentication so that your device or service cannot be hijacked even if your password is stolen.

Maintain security with complex passwords and multi-factor authentication



Using complex passwords that contain upper and lowercase letters, numbers, and symbols that are not shared between different web services and devices.

Introducing multi-factor authentication and using physical device keys that cannot be leaked on the Internet.

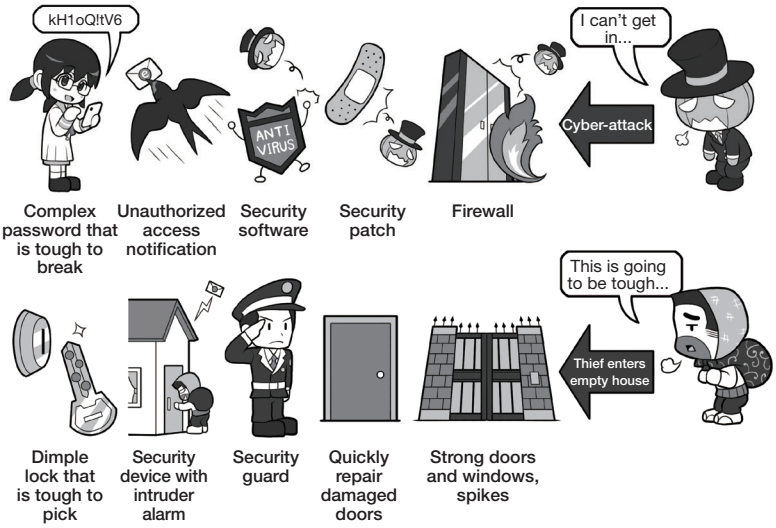
3 Make attacks more difficult by ensuring intrusion takes time and effort (cost)

With the exception of professional spies, efficiency is important for attackers to conduct cyber-attacks, so they tend to choose targets where intrusion is easier.

Imagine that a thief does not break into a place where there is a security guard and a locked door, but they will break into an unlocked house where nobody is home because of the low risk (cost) and ease to break in.

The story also happens on the Internet. If there are multiple defenses for your devices, the attacker need to take time and effort (cost) and even cannot penetrate in the first place.

Make intrusion even more difficult with multiple layers of defense



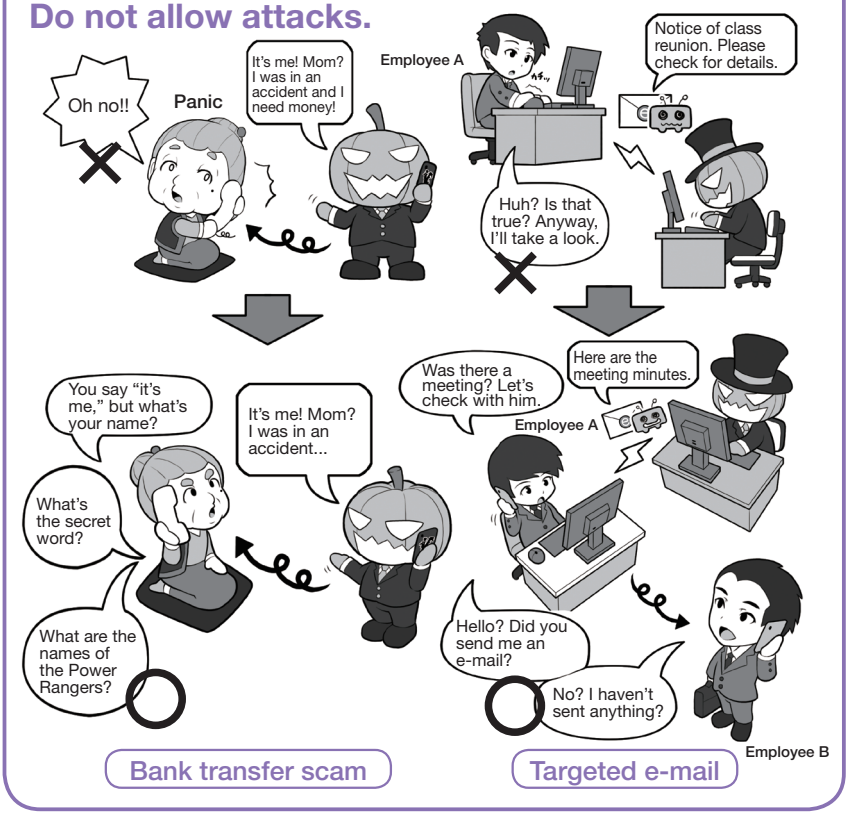
This is why it is necessary to keep your system up-to-date, patch security holes, use security software, as well as use complex passwords and multi-factor authentication.

4 Patch your psychological security hole (resistance to social engineering)

Even though taking security measures shown earlier, another form of attack such as social engineering which exploits psychological security holes to open the door from the inside may happen. If you don't defend against this, all effort of the system security itself will be meaningless. Increased system security and being conscious about psychological security holes go hand in hand.

Against bank transfer scam, you can protect yourself with a shared secret word over the phone. Against targeted e-mail and other cyber-attacks, you can protect yourself to confirm it with other communication means. These ways of protection, same as multi-factor authentication discussed earlier in the section above, are simple and effective.

Patch your psychological security hole. Do not allow attacks.



2 Keep Your Systems Up-to-Date And Install Security Software

1 Install security software to strengthen defenses

Basic virus detection and anti-virus software use a “wanted list” to detect malware.

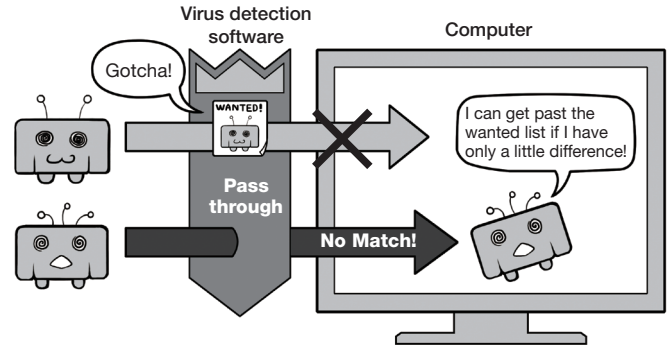
The wanted list contains the characteristics of known malware and is sent from the distributor to each device so that it can remove any malware that matches the list. The list contains information that identifies malware by file size, content, and other traits.

However, attackers are able to subtly change the malware made to each recipient and can even create tailor-made malware for their targets, so it is becoming difficult to use wanted lists to detect all malware.

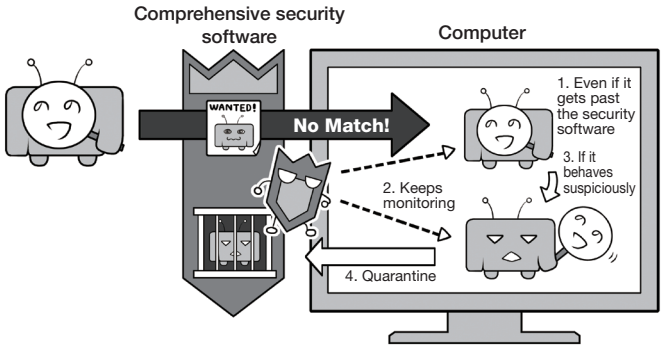
In addition to the wanted list method, recent comprehensive security software monitoring inside a PC continuously for detecting suspicious activity caused by unknown malware and removes it if detected. It is called “behavior detection.” There is also software that uses heuristic analysis to detect functions that are acting suspiciously. These methods can, to a certain extent, even detect unknown malware and counter it.

However, some types of malware cannot be detected. That is the malware that carries out so-called “Zero-Day attacks” which uses security holes and exploits them before its patch is released. Wanted lists cannot keep up with these attacks, and there is currently no definitive or effective way to defend against them. However, taking this into consideration, there are many merits to using comprehensive security software. Think about purchasing it to strengthen the defenses of your computer.

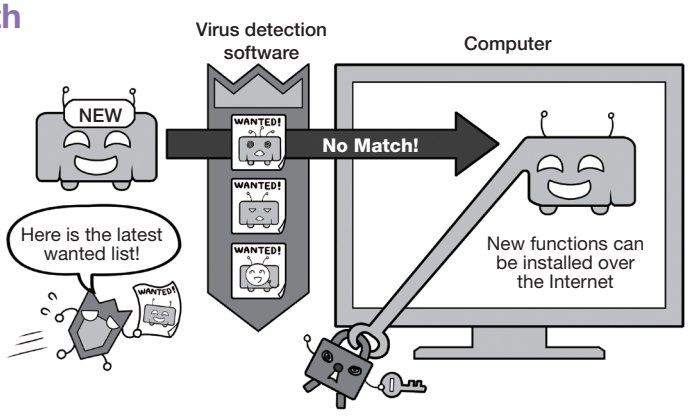
Basic virus detection software



Advanced security software (comprehensive security software). Behavior detection and heuristic analysis



Zero-Day attacks that wanted lists can’t keep up with



2 Keep your PC and security software up-to-date

Installing various updates is a must to keep the security of your PC up-to-date.

On recent devices, nearly all of the OS updates are installed automatically or an update alert is displayed prompting the user to install them. However, some OS updates only occur once a day, it is a good idea to regularly monitor security news websites and install updates by yourself. OS developers also update other important software they make, such as Office and other software suites, at the same time.

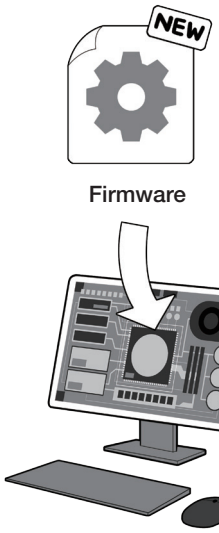
Furthermore, let's pay particular attention to updating software that is easily targeted by cyber-attacks. Adobe Flash Player, Adobe Acrobat Reader DC, Oracle Java, and various web browsers are generally used and are therefore easy targets for attack.

Also make sure to update the firmware of the device itself. Some devices do this update notification automatically while others do not, so be sure you know how to find out when your device has a firmware update and pay attention to the update releases.

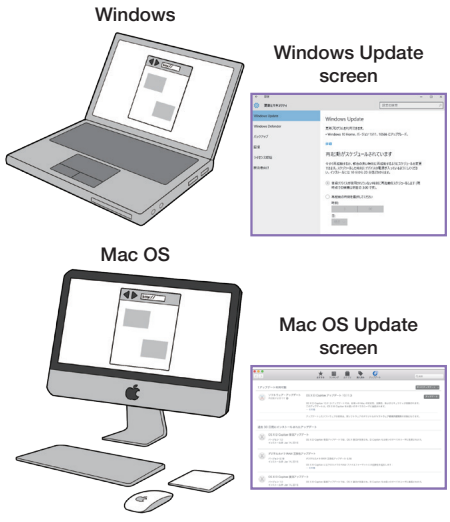
Security software normally automatically updates itself once installed, but try to make a habit of opening the security software and checking its security screen once a day. This is a way of checking the security condition of your device.

Update the device itself, the OS, security software, and any important software

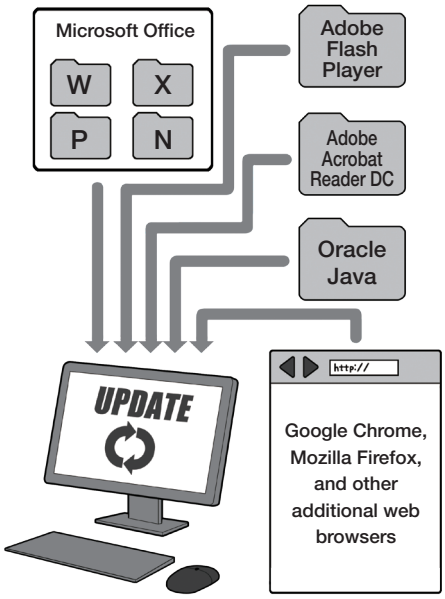
Update the device's firmware



Update the OS and basic software



Update important software



Update security software

The important software mentioned here is working like important public infrastructure such as railways, electricity, and gas services, and these softwares are used in most personal computers. Terrorists tend to target public infrastructure because of its high reward at a low cost, and the same reasoning applies to targeting important software. This is why you should update important software you use as soon as possible so as to prevent an attacker from making an attack. It is also a good idea to delete any important software that you are not using.

Botnets that appeared in an earlier section will not be established unless there is a machine that can be attacked and hijacked. Each person's behavior that does not leave a security hole creates a secure Internet.

3 Keep smartphone and network devices up-to-date

Similar to PCs, smartphones also require various updates.

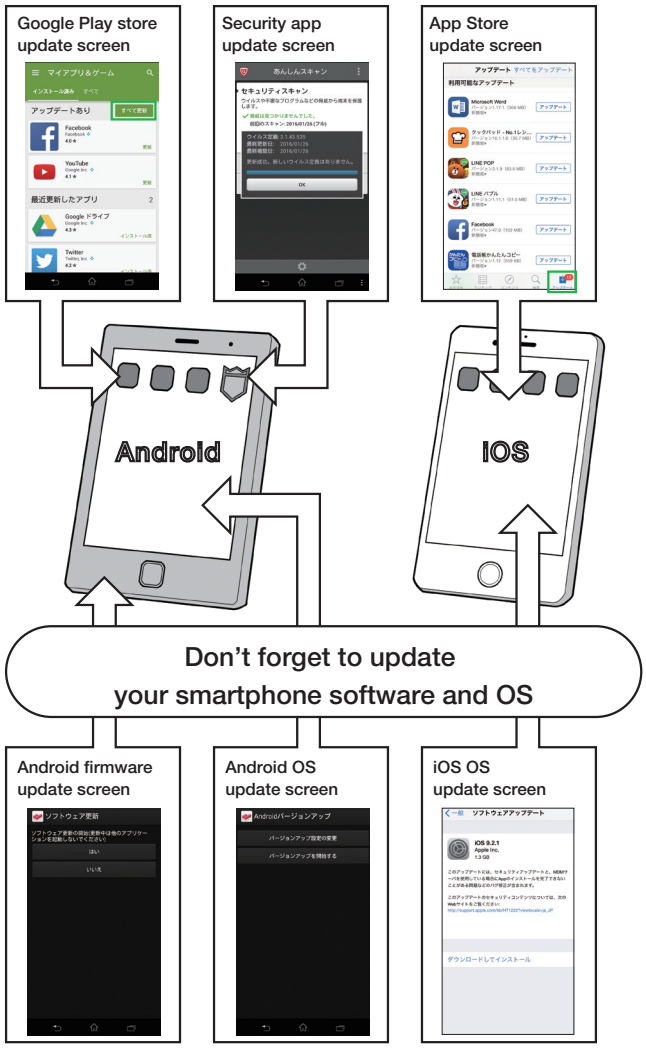
The update notifications on smartphones are relatively easy to understand, and the automatic update functions are also working well. Let's update devices, OS and apps for daily use anytime when update notifications appear on the screen.

To ensure this, let's check the update procedures of your device including the settings menu to update the device's firmware (software update and system update) and OS update. Also check that app updates are set to automatic.

Depending on the configuration, automatic updates for smartphone apps may run only on a wireless LAN connection, and even if you change the setting, the updates still may not be automatic due to permissions required to be confirmed on the update, thus, you may find a long list of apps needing to be updated. Be aware of this and frequently open the update screen and update all apps.

Although, smart home appliances and IoT devices connected to a network do not have these kinds of notifications, so even if the update file is published, you may not realize it and the security hole may remain open. Let's check once a week or even once a month for any new releases of update files. In particular, IP cameras and the similar devices may be controlled by attackers if it is not managed properly.

Updates for app and security software should be set to automatic and frequently checked



Let's also update the firmware of home appliances connected to the Internet
Let's change the setting page ID and password from the initial setting

Wi-Fi router | Network connected printer | IP camera

Updating the firmware of smart home appliances is normally done through a web browser. Be sure to change the ID and password from the default settings. Not doing so can result in unauthorized access or spying over IP cameras.

4 Download software and apps from trusted sources Pay attention to permissions

Even if the device itself and the system are kept up-to-date, some attacks are difficult to prevent. These are intrusions of malicious software that have yet to be identified as malware.

For security software to detect malware, past collected data is quite important. The more of this data there are, the more chance of detecting malware. It is the same as being able to find a reliable cure if there are many sick specimens.

But on the other hand, malware that the security software company does not yet know, or malware for which not enough specimens have been collected, is difficult to detect with security software.

When attackers try to distribute malware, they avoid official markets where management is strict; rather they use e-mail to guide targets to certain websites to keep malware hidden and undetected.

It is why it is recommended that software and apps be downloaded from trusted sources to avoid being infected.

In the case of iOS devices, apps can be installed only from the official app store, but in the case of Android devices, it is possible to install apps not only from the official store but also from unverified sources, so make sure to uncheck the "Unknown sources" item in the "Security" settings which allows installation of apps from unknown sources. This way, you can protect against downloading apps from unverified sources.

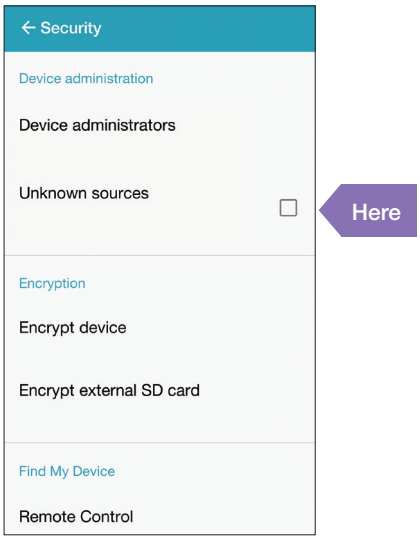
Also pay attention to permissions for accessing smartphone's functions when installing apps for the first time on Android and iOS. These permissions determine what kind of functions of smartphone you allow apps to use.

For example, simple camera apps which request permission to use your contacts, or other apps which request tens of permissions may be suspicious. Deny each permission which is not needed, and if you cannot deny each permission, then do not install that app. Also, be aware of additional request of permissions when updating the apps. There are some apps that initially appeared to be harmless when first installed and later attempt to get more control.

Additionally, there are apps that indirectly steal permissions by using link functions between apps or web services, so pay close attention to the word "link."

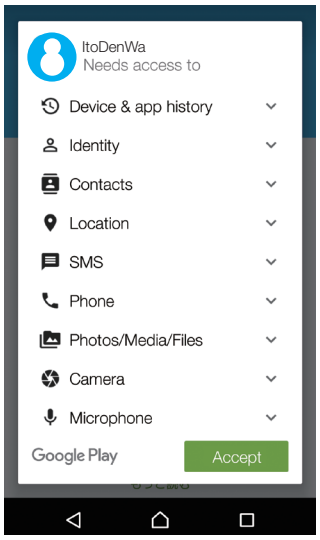
Do not install apps from unknown sources. Pay attention to permissions

Be aware the setting of unknown sources



• Android
The relevant items and detailed wordings may differ depending on the version and smartphone manufacturer, but it is important to always uncheck the "Unknown sources" item in the Security settings.
If you need to change this setting to install an app from a trusted market for some reason, you may check the item, but don't forget uncheck it once you have installed the app.

Pay attention to permissions when installing and starting apps



• Android, iOS (Android screen shown)
Many people have carelessly pushed the "approved" or "agreed" button in the grant permissions screen because they are casually displayed during installation or launch of the app, but this button is asking you for permission to let the app have free access to functions.
In some cases, permissions cannot be denied for each function separately, in which case do not install the app. Watch out for apps that ask for unnecessary permissions.

Column: Consider purchasing security packs for smartphones if necessary

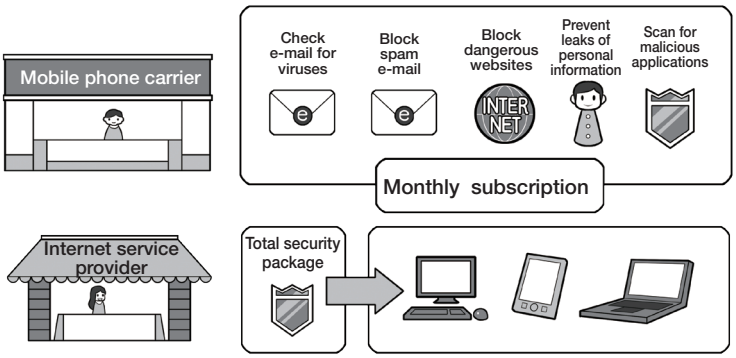
Since smartphones were developed relatively recently compared to PCs, the security functions are built into the basic design of their OS, so there is not much of a role to play for security apps in smartphones while PCs need security software.

However, you may want additional security apps that support checking the overall security, such as overlooking the points you must be careful about, detecting the installation of malicious applications, detecting suspicious e-mails, blocking dangerous sites, and checking for outflow of personal information. For meeting such needs, mobile phone carriers and Internet service providers offer total security packages that provide necessary security functions, including security apps. It may be good idea to sign up for such service after thoroughly reviewing their content.

In addition, remember that you never “root” an Android device or “jailbreak” an iOS device, as it makes the smartphones vulnerable to attack, because it is not prescribed usage defined by the manufacturer’s security design.

And, as smart home appliances become more sophisticated, even they may need some kind of security measures in the future. Please keep this in mind.

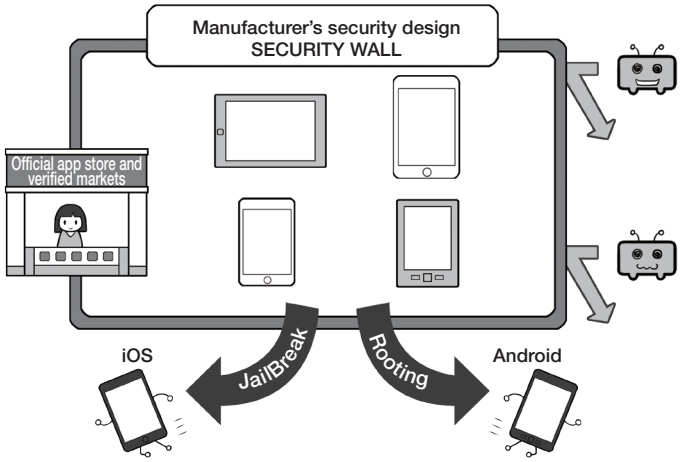
If you feel it necessary, consider installing a security pack on your smartphone.



Services as above are packaged for a monthly subscription and cover multiple devices.

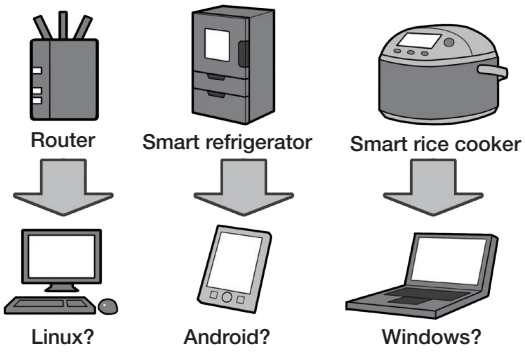
Mobile phone carriers and Internet service providers offer security-related services and products as packages. Check that the package has the functions you want and sign up it if you think it is necessary.

Do not tamper with your smartphone



It is assumed that users will use their smartphone in a way that adheres to the manufacturer’s security design concept. Tampering with a smartphone by rooting or jailbreaking it can be a breach of contract, and makes the security of your smartphone vulnerable. Do not modify your smartphone.

Do smart home appliances have computers or smartphones in them?



Smart home appliances may look like just a machine, but some have the Linux operating system built into them, and some use Android or Windows. As these appliances become more sophisticated in the future, they will likely require some sort of security measures.

Column: Even up-to-date PCs and smartphones are vulnerable to attack. The attack is called a Zero-Day attack!

In general, if a security hole in a system or software is widely exposed, attackers will quickly develop malware to attack it. When the manufacturer or developer finds out about the security hole, they develop and release an update security patch.

The attacker normally wins this competition. Attacks that exploit a security hole before it is patched by a manufacturer are called “Zero-Day attacks.”

Malware delivered by e-mail can be prevented to some extent if one is wary of it, but malware delivered by media such as video streaming, web pages, or web advertisements can infect a device just by accessing a certain website. So you cannot effectively protect against this type of Zero-Day attack without information about the malware.

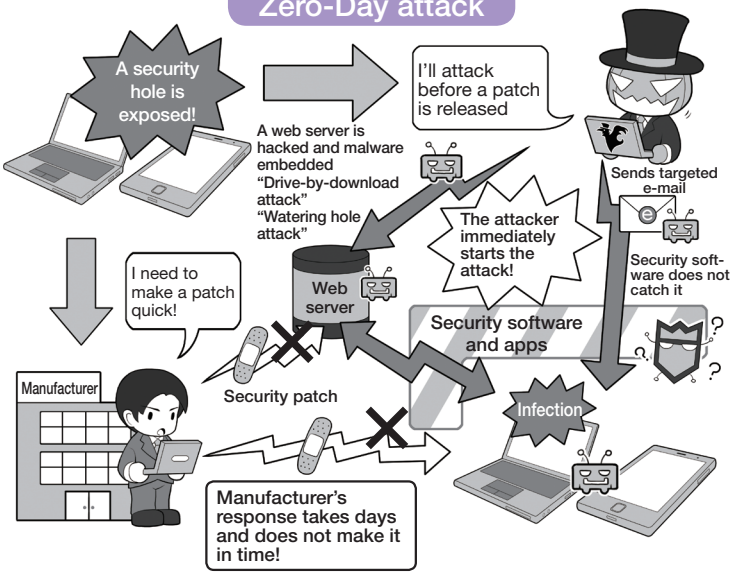
In recent years in particular, the scale of attacks has grown because attackers are paying money to deliver the malware through major commercial web video advertising networks so that it appears on major websites. That means that the attacker can gain greater benefits than the advertising cost.

In order to keep the damage at a minimum, make a habit of reading security websites daily, and, for example, turning off automatic playback for videos when video-based malware appears on the Internet, and uninstalling smartphone social networking service apps until a security hole is fixed.

Some services that are offered with apps are available in web browsers without having to use the apps, so it is a good idea to become familiar with the web browsers versions even on smartphones.

What is a Zero-Day attack? How to deal with it.

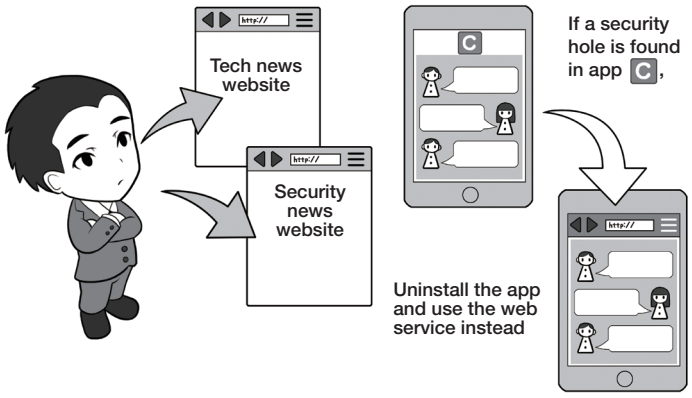
Zero-Day attack



How do I deal with a Zero-Day attack?

Be diligent in reading security websites and gathering information

Use other ways to avoid security holes



In the battle over Zero-Day attacks between the attacker and manufacturer, the attacker usually prevails. Attackers can acquire information that manufacturers are unaware of, and if attacks succeed with any one of the target devices, the attacker can initiate an attack, but a manufacturer has to acquire and review the information then take necessary and full countermeasures for all products affected by the vulnerability.

This is why users need to be prepared and take action. Doing so will allow you to protect yourself.

3 Make Intrusion into Your System More Difficult by Using Complex Passwords and Multi-Factor Authentication

1 Increase password security

In addition to infecting targeted devices with malware, cyber-attacks can also involve hijacking the target by stealing IDs and passwords in some way.

For example, an attacker can explore your passwords in the following way.

Using a device's initial password and attackers know it. The password is leaked in some way and attackers get it. The password stored by the web service has leaked, and attackers use it for a "list based attack." Using popular terms as passwords and attackers attempt a "dictionary attack" to find out. Attackers try all combinations of letters and numbers as a "brute force attack" to find out. The best defense against brute force attacks is to make the attack take a long time by increasing the types of characters or the number of characters in a password.

For example, if only numbers are used for a character, there are only 10 possible variations; but if you add a letter, there are now 36 possible variations; and if you use lowercase and uppercase letters, 62 possible variations; if you add the 26 symbols, 88 possible variations.

Login passwords should be at least 10 characters and use a combination of upper and lowercase letters, numbers, and symbols.

Why a password should be at least 10 characters and use a combination of upper and lowercase letters, numbers, and symbols.

Using numbers only → 10 billion possible variations
Using upper and lowercase letters, numbers, and symbols →
Approximately 27,850,097,601 billion possible variations

The difference between using a 10-character password with numbers only and a 10-character password with upper and lowercase letters, numbers, and symbols is night and day.
It is virtually impossible to search through such a large number of combinations.

Number of combinations with upper and lowercase letters, numbers, and symbols.

Example using uppercase letters + lowercase letters + numbers + symbols

26 + 26 + 10 + 26 = 88

Numbers	Uppercase letters	Lowercase letters	Symbols	Total		5	6	7	8	9	10
10				10	Number	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000
10	26			36	Numbers & letters	60,466,176	2,176,782,336	78,364,164,096	2,821,109,907,456	101,559,956,668,416	3,656,158,440,062,976
10	26	26		62	Numbers & uppercase & lowercase letters	916,132,832	56,800,235,584	3,521,614,606,208	218,340,105,584,896	13,537,086,546,263,552	839,299,365,868,340,224
10	26	26	26	88	Numbers & uppercase & lowercase letters & symbols	5,277,319,168	464,404,086,784	40,867,559,636,992	3,596,345,248,055,296	316,478,381,828,866,048	27,850,097,600,940,212,224

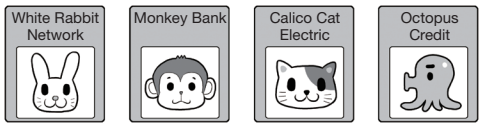
Increasing the length of a password increases the number of combinations exponentially.

Brute force attacks eventually succeed, but we can make them time consuming to be virtually impossible using complex passwords. A login password should be more than 10 characters and contain a mix of upper and lowercase letters, numbers, and symbols to be considered in the safe zone. The longer the password, the better the level of security.

2 Do not reuse passwords

Even if you use a complex password, using the same password with multiple web services is reckless. If you reuse a password that means that once the password is leaked, it can be used for attacks upon all other services. Also, using a complex password and then adding a number or regular pattern to the end of it for different web services. It is easy to guess if leaked. It is important to set complex passwords for each service and never reuse them.

Do not reuse the same password. Do not use similar passwords or guessable passwords.



	White Rabbit Network	Monkey Bank	Calico Cat Electric	Octopus Credit	
× Reuse	PASSWORD	PASSWORD	PASSWORD	PASSWORD	All the same
× Add number to end	PASSWORD1	PASSWORD2	PASSWORD3	PASSWORD4	Easy to guess
× Guessable regular pattern	PASS-RABBITS	PASS-MONKEYS	PASS-CATS	PASS-OCTOPUSES	If the regular pattern is guessed, passwords are compromised

3 Store passwords appropriately

Passwords with sufficient complexity and length that are not reused can withstand brute-force attacks, but if they have not been stored appropriately and stolen these measures do nothing to stop the attackers.

For example, if you stick a password on a PC or wall, someone seeing it will remember. And if you store it in PC as a plain text file it can be leaked when the PC is infected by malware, with the result that multiple accounts may be hijacked at once.

Also, be careful with the auto-complete functions of PC web browsers. While you are away from your desk, someone can use your browser and access your services or even steal your PC and all of the remembered passwords altogether.

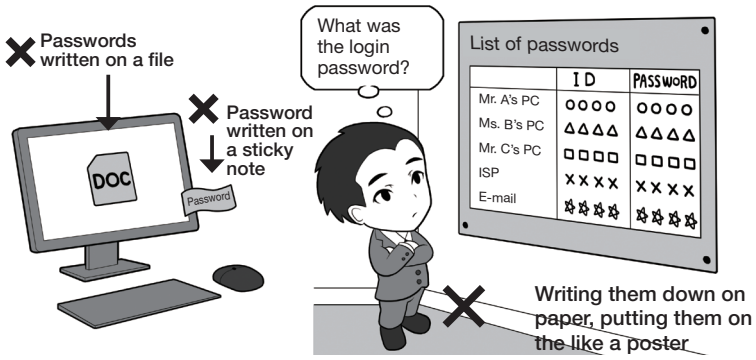
As a rule, you should never store passwords in the place where you use them. However, numerous complex passwords with different services can be difficult to remember. What should you do then?

One option is to manage your passwords in a notebook and store them in a separate location, or another option is to manage them with a smartphone password management app. With the latter, you should carefully consider whether to use a function of cloud-based data storage. And also it is recommended that you do not use such an app for which a security hole has been discovered. Because, this means to have someone manage your IDs and passwords, and also increases your risk of a breach.

If you are not supposed to store passwords where you use them, this may seem to apply to using a password management app on a smartphone. But smartphones and apps can be protected by PIN codes, biometric authentication, and encryption, which will be explained later. Even if your smartphone is stolen or lost, it cannot be easily used by others.

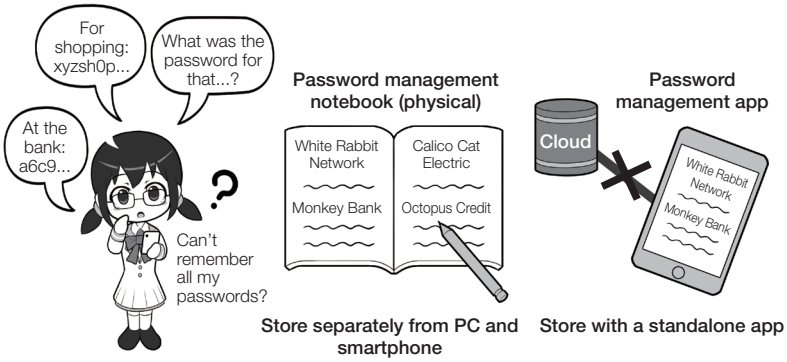
But remember to always back up passwords you manage. A lost smartphone will be not always returned to you.

Do not store passwords in the same place you use them. Never store them on a PC too



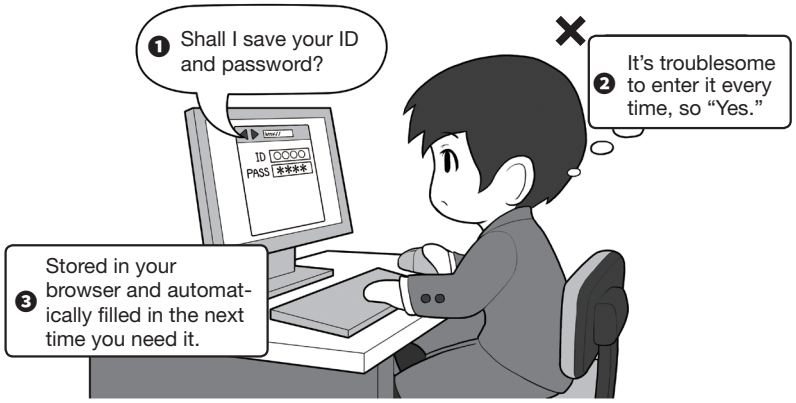
Do not think that people from outside the office cannot see your passwords. Contractors that come and go during the day could see them, and someone from the outside can even see your passwords using binoculars.

Manage passwords by writing them down in a notebook or use a password management app



Storing on the cloud is not always a bad thing but it should be balanced by its convenience. It is safer to manage the key yourself instead of depositing it with someone you do not know.

Do not allow your web browser to remember your password



It is convenient for your password to be automatically entered, but if you leave your desk without locking your PC, anyone can login to and use all of your web services.

4 Do not honestly answer security questions. Use multi-factor or biometric authentication

When web services need to verify the identity of a user who has forgotten their password or if there is a suspicious login, they use a “security question.” Users register in advance questions and answers that only they know and answer them like a shared secret word.

In some cases, you can make your own questions and answers, but others only offer limited options that are related to your life, such as “the city you were born in” or “the name of your pet dog.” Social networking service is now being used widely, so, such personal information can easily be found on the Internet and cannot be considered a reliable element for security.

So, it makes sense not to honestly answer security questions, but create a completely unrelated answer instead so that it cannot be guessed from social networking service.

Also, in order to log in securely to the web service, use two-step verification or multi-factor authentication, if available. With these methods, there are things that generate a disposable password with a hardware token or smartphone application, and some sent by e-mail. The user can log in by entering this second password together with the normal password.

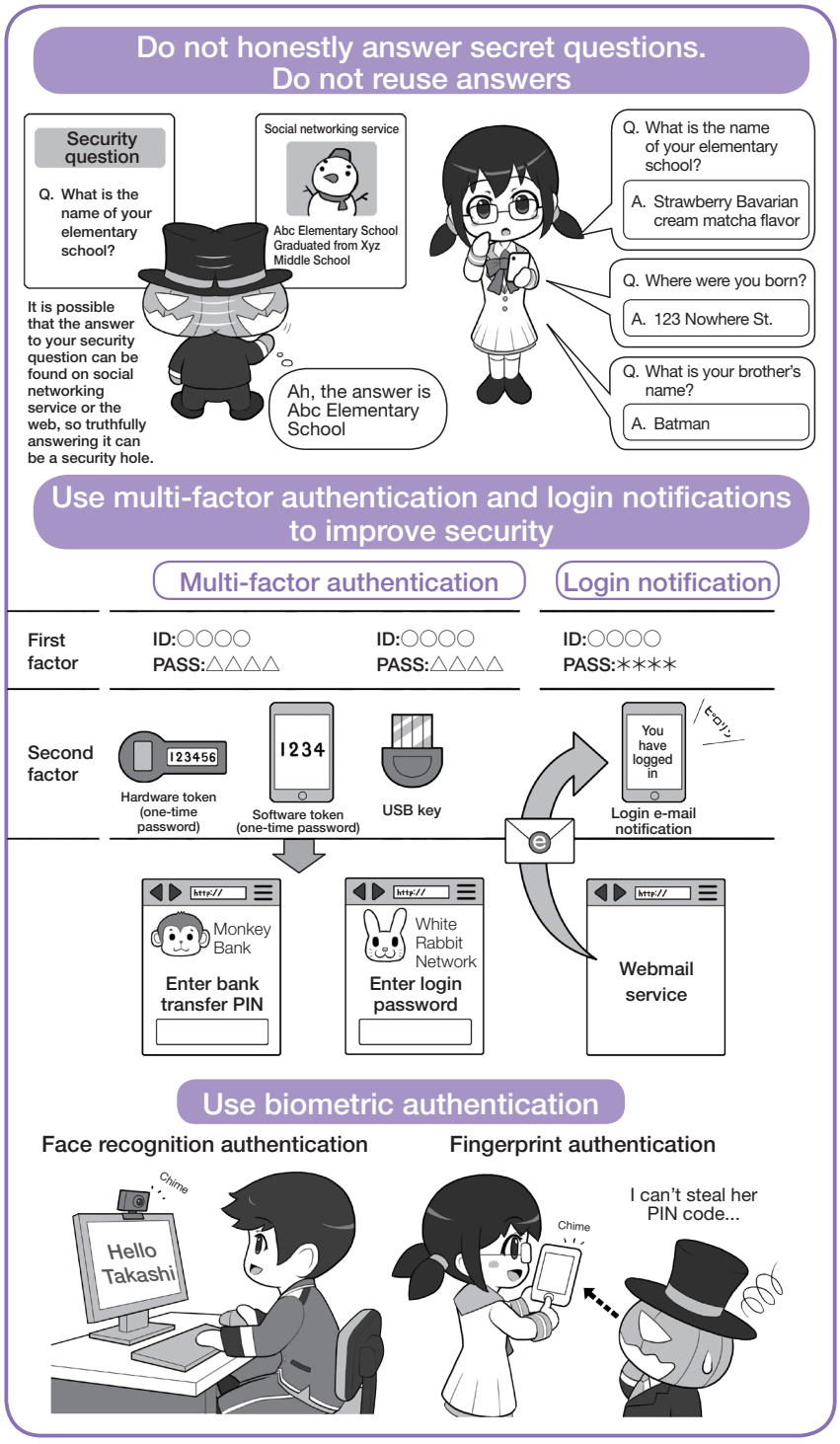
Furthermore, there are also methods for verifying users by using a USB key, or methods for detecting suspicious logins by sending a notification e-mail to a user when the service is logged in to.

Additionally, recent devices have biometric authentication functions, such as 3D face recognition, iris recognition, and fingerprint authentication, as ways to unlock devices.

Biometric authentication is a convenient function that allows only the owner to use the smartphone, but there are good and bad aspects.

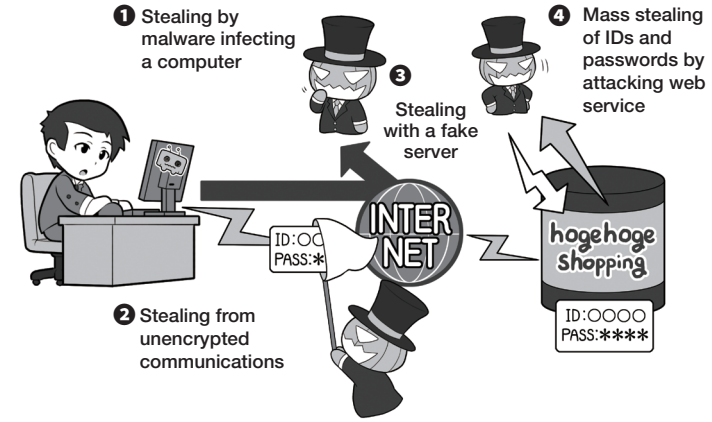
For example, fingerprint authentication can prevent shoulder hacking which is stealing a secret code (PIN code) over the shoulder like when you are riding on a train, but someone could use your fingers to unlock the smartphone while you are sleeping.

Note that biometric authentication usually skips the normal PIN code input, so if you fail authentication several times consecutively, you will return to the normal PIN code input. Let’s not use personal information for PIN codes, such as birthdays, so as not to be unlocked by searching for the PIN code when the smartphone is stolen.



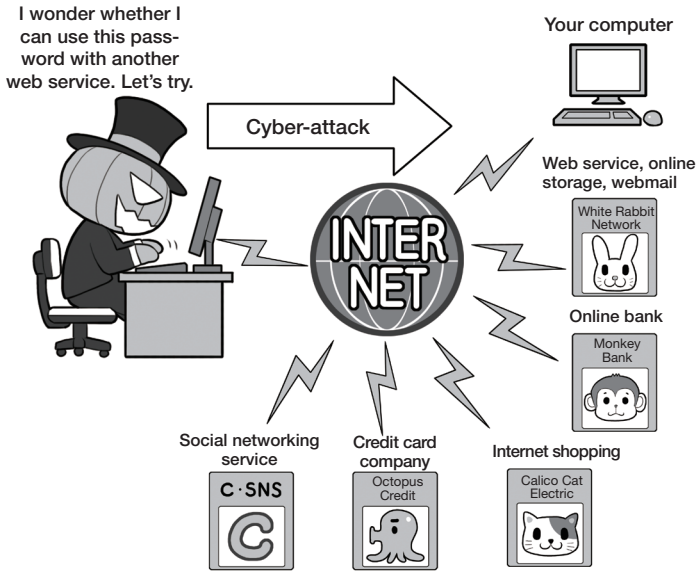
Column: How are passwords leaked? How are they used?

There are many ways to steal IDs and passwords



An ID and a password can be stolen through being infected by malware, being stolen from your own communications, or being leaked from a web service you use. Let's change it as soon as you find out your password has been leaked.

Stolen IDs and passwords are used to try and hijack other web services



An attacker who obtains IDs and passwords by some way tests them on various sites to see if they can be used at another service (list based attack). To prevent these attacks from succeeding, do not reuse passwords, use similar passwords, or use guessable passwords.

The IDs and passwords used on personal computers, smartphones, social networking service, or web services can cause a lot of harm if stolen in a cyber-attack. But how does it actually leak out?

One way is for malware to infect your computer or device where the malware steals your password and sends it to the attacker. Another is by having your password intercepted along the path from the device you are using to the web service you are logging into. Also, an attacker can steal IDs and passwords that a web service has stored for the authentication of the login.

What you need to know is that they can be leaked without your PC being infected by malware. Even if you normally do not use your ID and password, it does not mean that you are safe.

An attacker who steals IDs and passwords can try them on various sites (list based attack) to see if the service can be hijacked.

If you reuse or use a similar ID and password between multiple accounts, all of them can be hijacked in an instant. If that happens, your ID can be used to purchase things online without your permission, or money can be stolen by remitting it with some of remittance system even if actual cash cannot be sent. If you find your password has been leaked, change it immediately.

4 Make Attacks More Difficult by Ensuring Intrusion Takes Time and Effort (Cost)

Most cyber attackers carry out cyber-attacks with a profit motive, except for a military or industrial spy, or a malicious hacker who is out to make a name for himself.

It is a business for them, and business should be cost effective, namely, that it is important to make a large profit with little effort.

From the point of view of these attackers, it is clear that you need to create a difficult environment to attack.

In the real world, for example, a thief is more likely to break into a house that has open windows and no one home rather than a house protected by heavy security. That is because such a house is safe for them and requires no effort (cost).

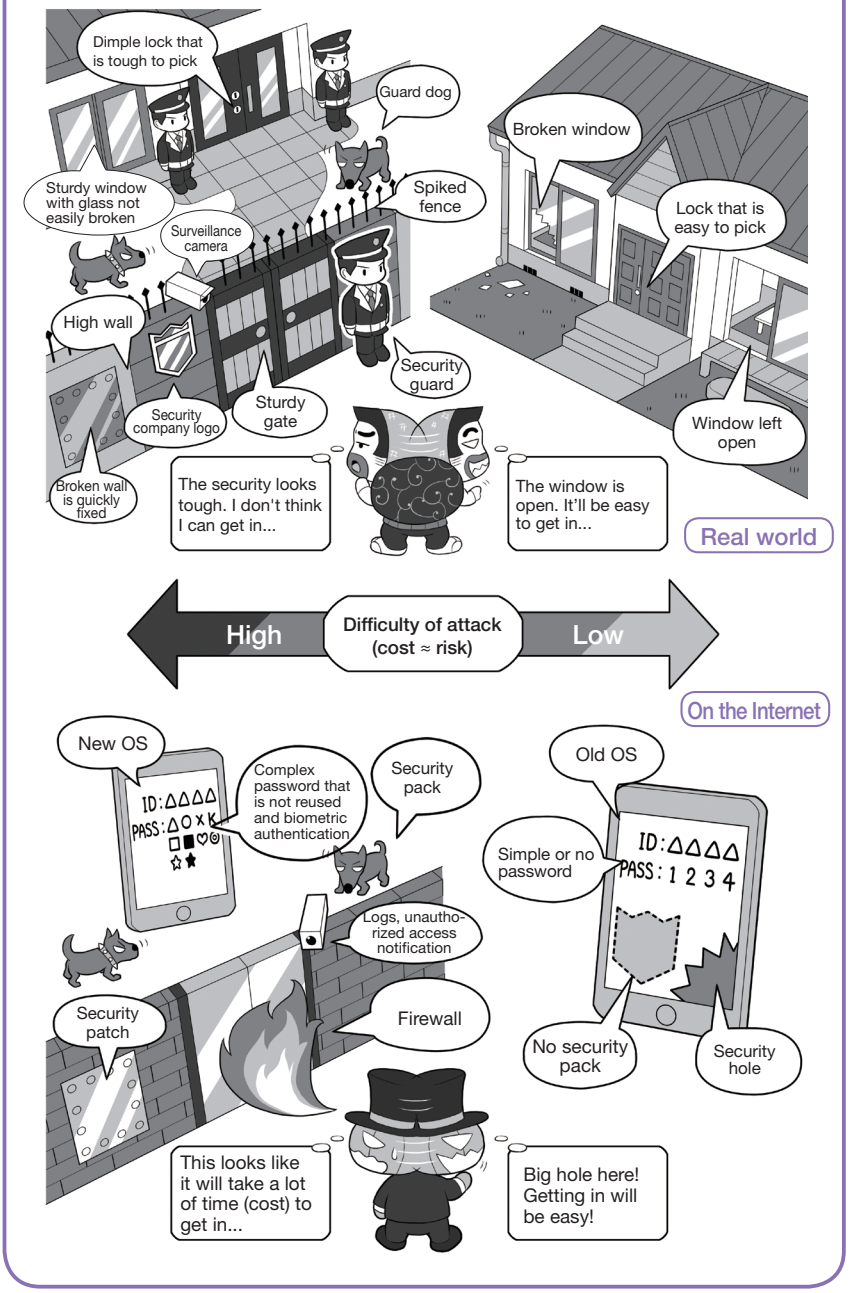
The same applies to the Internet. If there are many barriers to intrusion, such as break-in activities are recorded (in a log) and notifications may be sent to appropriate administrators, passwords are complicated and difficult to crack, the latest systems are used, where security holes cannot be found to attack, security software is also used, and even if files are stolen, they use complex encryption that would take hundreds of years to crack, rendering them unreadable. An ordinary attacker would avoid this.

But elsewhere, however, security holes are left unpatched, simple or no passwords are used, files are unencrypted, and the same passwords are used for multiple web services.

From a business perspective, these targets are clearly cost effective.

It is a good idea to look from the attacker's point of view and build an environment that makes it very troublesome to penetrate and protect from being attacked. But for attackers who are not motivated by profit, the countermeasures are a little different.

Make attacks more difficult by ensuring intrusion takes time and effort



For attacks that are not motivated by monetary gain, some aim for the targets themselves, that is, abducting minors or trying to obtain explicit photos.

On the street, most people would refuse and run away if asked to provide an explicit photo of themselves, but they would provide it on the Internet because an attacker pretends to be someone else who appears friendly to deceive the target.

When a person you do not know approaches you on social networking service or a bulletin board system, be careful and never give them your personal information. If you are invited to meet someone you do not know, do not meet them. If you need to do so, go with an adult or guardian.

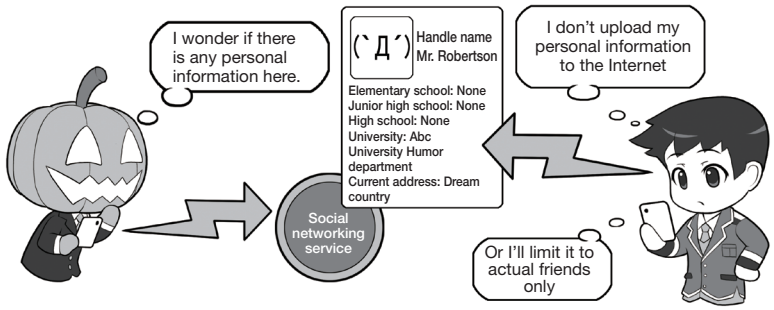
And if you feel something weird while talking, or the story is different from the conversation you previously had, it may be a psychological technique to trick you. Be alert and make the decision to leave and return home.

While you may not have heard about this kind of psychological technique to trick people (social engineering), they are systematized and kind of a manual is organized in the underworld.

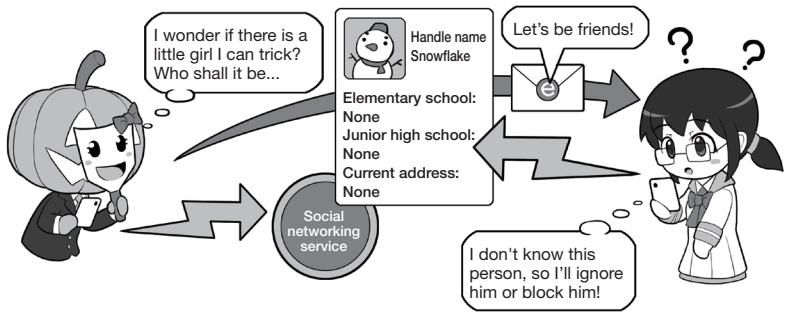
The techniques to deceive people are not limited to the above examples but happen in a variety of situations in daily life.

Bank transfer scams and targeted e-mail are two examples. No matter how tough your security measures, it is all meaningless if you are deceived and victimized by an attacker. Let's all be on the lookout.

Prepare for attacks that are not about money



Do not upload personal information to the Internet



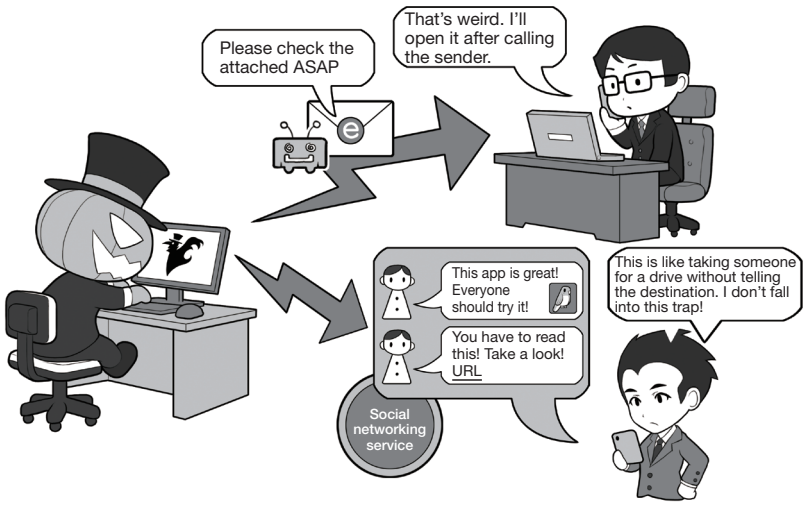
Do not become friends with anyone who is not someone you actually know

Minors who use social networking service should never make their photos and personal information public. Also, do not make your posts public; keep your social networking service post settings to friend only mode so just your friends can see them.

Never approve friend requests on social networking service from someone you do not know. Either ignore or reject them.

Without this, it is as dangerous as walking down the street with your personal information written on a name tag or going off with someone you just met and do not know their name.

Be alert so that an attacker cannot manipulate you to open the door to them from the inside



Be alert for suspicious e-mail and get in the habit of checking anything suspicious with the sender before opening it. If you watch security tech news every day, you will get skills to find out suspicious e-mail or social networking service posts. So let's train for it.

5 Patch Your Psychological Security Hole (Resistance to Social Engineering)

Social engineering attacks targeting psychological security holes include “trashing” (going through garbage cans), a technique that does not require direct contact with a target; “name dropping” (eliciting information by appearing to have authority), and “hurry up” (to get information by rushing a target) to control the situation where the target cannot think normally, elicit the necessary information or have the target perform a requested action.

For scams in general, including bank transfer scams, calling it “a commonly-used social engineering technique that targets psychological security holes” gives you an idea of its nature.

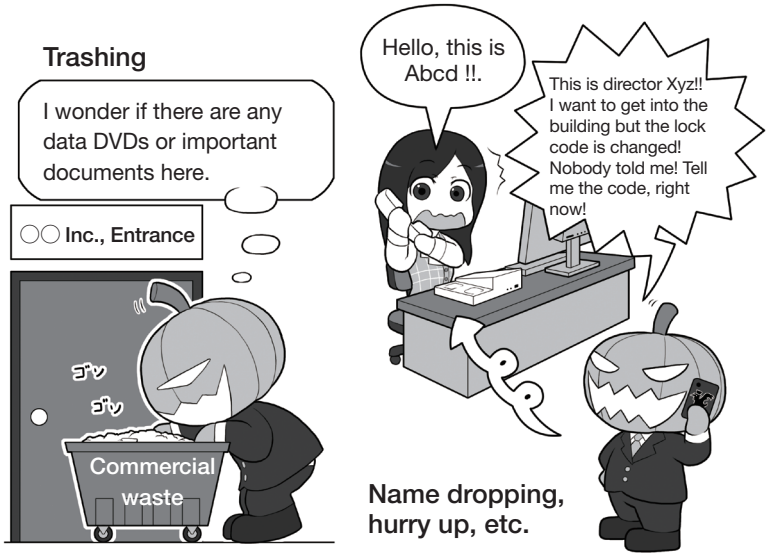
Social engineering in the digitalized generation also uses manipulation in the same way.

For example, as a way to obtain valuable information without direct contact with the target, the PIN code or pattern lock of someone using their smartphone on the train can be stolen using “shoulder hacking” while standing behind them. Or the pattern lock of a smartphone left on a table can be discovered by picking it up and looking at the finger traces on the screen. By identifying how to unlock the smartphone in advance, you can obtain all of their other personal data by stealing their smartphone later.

“Targeted e-mail” can also be used in attacks on psychological security holes. Just as a swindler investigates his target well, with targeted e-mail, attackers investigate the target’s name, affiliation, identity, and the pattern of e-mails exchanged at a similar company. By doing so, attackers can send scam targeted e-mails which cannot be distinguished from e-mail for everyday work.

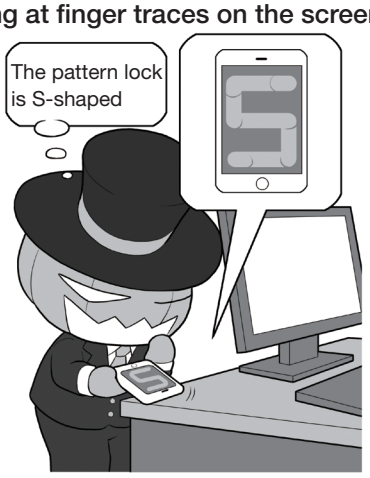
Patch your psychological security hole (resistance to social engineering)

Classic social engineering



Social engineering in the digitalized generation

When unlocking your smartphone in public place, be careful of people behind watching.



Never leave your smartphone unattended at your desk and never leave it on the table to reserve your space.

If this elaborate targeted e-mail is like a rifle that shoots only the target, then spam e-mail is a method for broad attacks.

While the success rate of spam attacks is low, its profitability is increased by targeting large numbers.

For example, the screen at the bottom left in the frame on the right is an example of spam texted to a smartphone that impersonates a bank.

There are many clues that tell you that this is a phishing e-mail. If the person receiving the e-mail does not have an account at the bank, they will not open the link. If you look closely at the link, the URL ends in gq instead of jp for Japanese websites. Despite these signs, a certain number of people will fall for this attack. If the link goes to a website embedded with Zero-Day attack malware instead of a fraudulent website, then the target will be infected.

What is more troublesome are people who are not attackers but spread malware in good faith. If the social networking service account on the screen on the right at the bottom right of the page is a friend's account, you probably would not be suspicious and think that the app is interesting and recommend it.

However, even if he doesn't know, the app may contain malware, and even if it causes no harm while being spread, it may later increase permissions and steal personal information.

Examples of targeted e-mail and spam e-mail

Example of Targeted e-mail

From: Nick Hide
To: ZaN

This week's schedule
Today

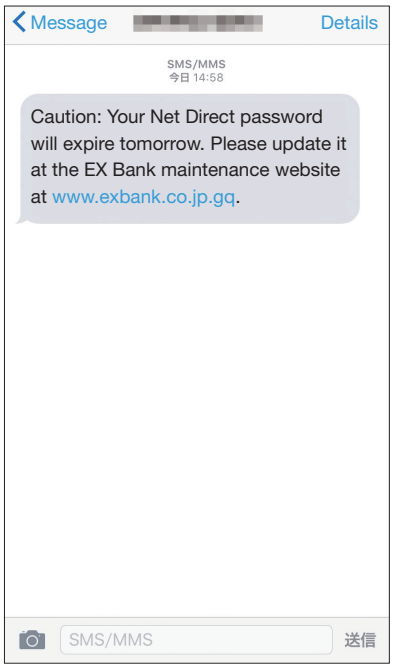
To all members of NISC Special Team 1

I've attached this month's schedule. Please review it and if you wish to take time off, please fill it in and keep it with you until further instructions.

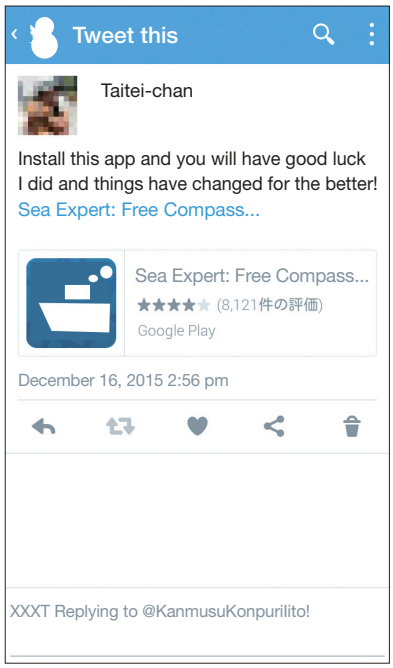
Nick, Leader, Special Team 1
Nick@nisc.govt.jp

kyukabo.exe

Example of Phishing e-mail (example using SMS Short Messages)



Example of proliferation without malicious intent



If it was from a stranger, you would be alarmed, but if it was from a close friend or family, would you be equally alarmed?

As a countermeasure to these kinds of recommendations, it is important to draw a line. You should be cautious of things that go beyond the information you see in the body of an e-mail. In addition to the interesting videos and schemes to make money, also be careful to avoid clicking links or installing unknown apps.

On the street, these would be the equivalent of "Come with me" or "Just get in the car."

Furthermore, even if you think that you can look it up with a search engine on the Internet instead of clicking the link, keep in mind that the attacker has thought of this and likely prepared a website containing malware to catch people doing searches.

Column: If you are targeted by military or industrial spies

Attackers who are not spies tend to choose targets in terms of cost effectiveness, but how do professional spies behave?

For military and industrial spies, their number one priority is to obtain the information, so even though something might be difficult to penetrate, they will not give up.

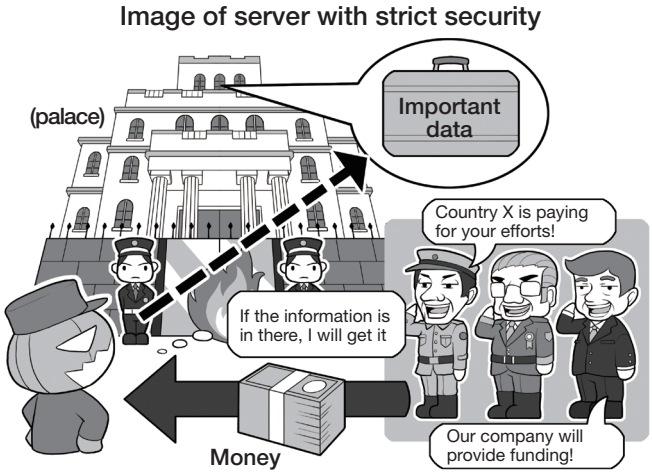
Second, these attackers do not cover the costs of their activities by themselves. Military spies are funded by the government and the military. Industrial spies that are not freelance but funded by a sponsor corporation carry out their attacks with little regard to cost effectiveness.

If you are interested, you can understand how unrelenting they can be in their purpose by reading a general book on spies. And once you understand this, you can substitute spies for cyberattacks on the Internet.

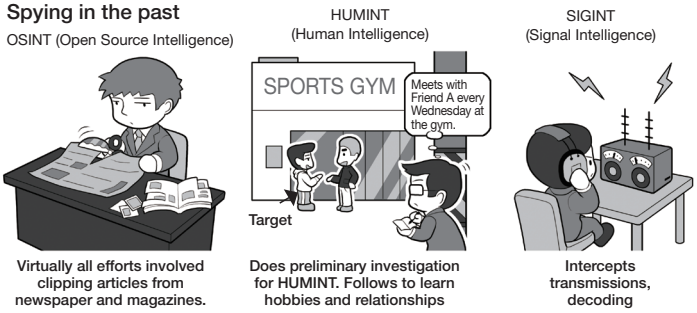
Before the Internet was developed, spies did their work using OSINT (Open Source Intelligence) by reading publicized information such as the newspapers and magazines of the target country, HUMINT (Human Intelligence) by investigating or following or questioning people, and SIGINT (Signal Intelligence) by intercepting or wiretapping communications.

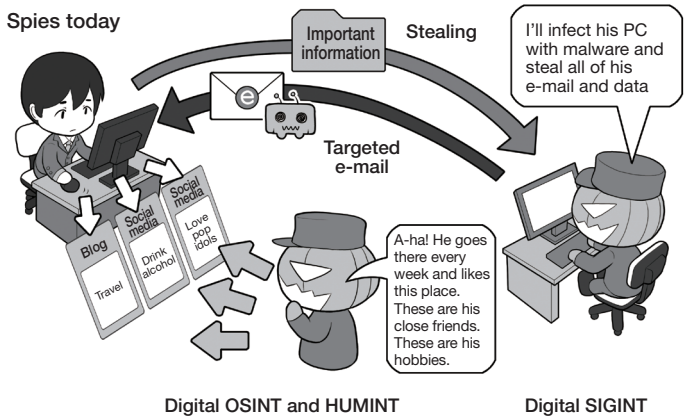
If you are targeted by military or industrial spies

Protection by spending is not effective against professional spies



Spying then and now





In modern society in the age of the Internet, all kinds of HUMINT can be obtained about a person's relationships just by looking at social networking service. Moreover, SIGINT can be collected by malware that steals e-mails and files, and can also eavesdrop on smartphone calls.

If the target is someone who likes social networking service, even an ordinary person can easily use HUMINT and OSINT in this age of cyber intelligence.

People in important positions should not disclose information carelessly on social networking service. Everything you do online is being monitored.

Column: Social engineering seen in the movie “Takedown”

Kevin Mitnick (left)

While driving around in his car, Kevin Mitnick deceives people by phone and obtains information.

Tsutomu Shimomura (right)

Shimomura is a physicist who, after initially falling behind, then catches up, and tracks down Mitnick.

“Takedown” was released in 1999 and is a film about the battle between two hackers that is based on a true story.

One of the characters in the movie, Tsutomu Shimomura, wrote the original book, “Takedown.”

His opponent, Kevin Mitnick, authored “The Art of Deception: Controlling the Human Element of Security,” and other books.

The story depicts Shimomura as a white hat hacker pitted against Mitnick the cracker, with an emphasis on the conflict between the pride of the two hackers and their techniques instead of the morality of their actions.

One thing to pay attention to in the movie are the hacking techniques and, in particular, the surprising point that elite hackers don’t restrict themselves to just the digital world for their goals. It is a movie that will change your view of hackers.

Mitnick uses social engineering in the movie to trick people to acquire information and then casually enters a computer center to perform cryptanalysis.

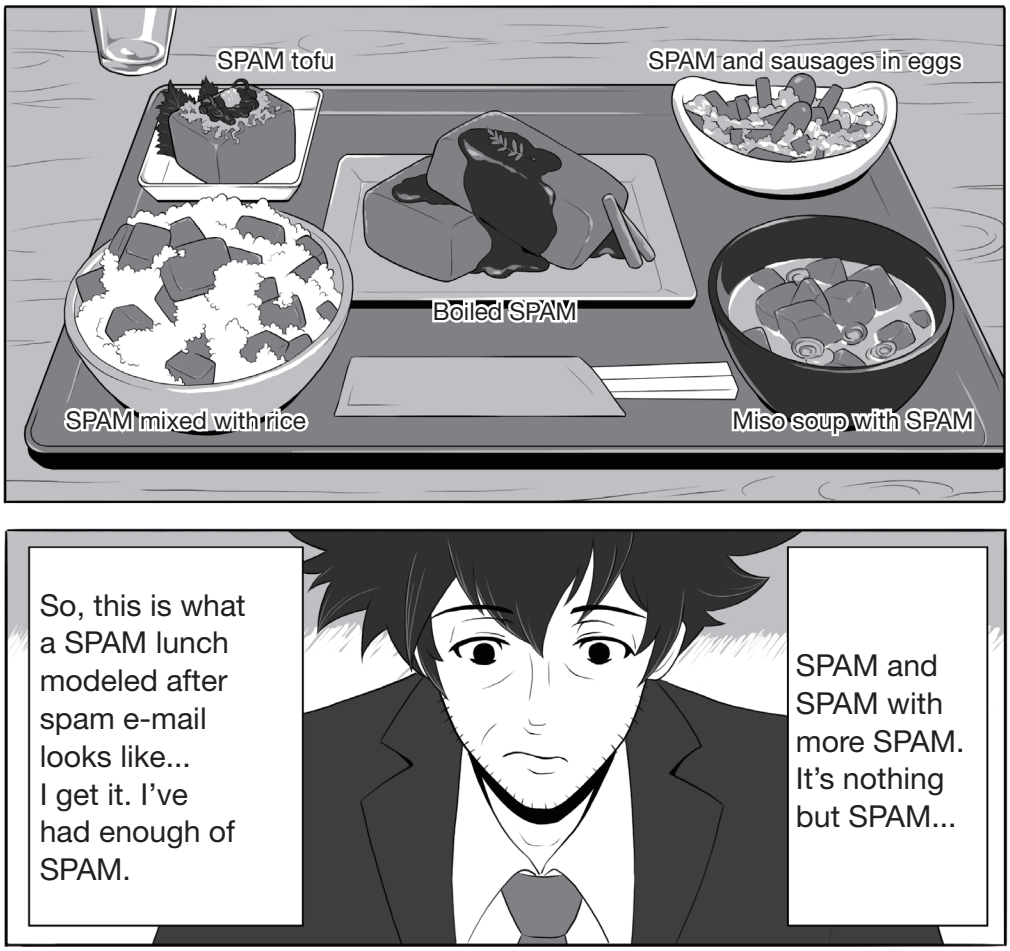
When we see on the news that the cause of the theft of a notable person’s e-mails and personal information was a phone, we think that that was because the information was poorly managed, but if you watch this movie, you will see how often people are easily deceived and how much information is leaked without much effort.

Most people who have seen the movie come away thinking that there would be no escape if they did the things in the movie.

If you can find a DVD or stream it online, it is worth watching. It is also recommended as security teaching materials with a focus on people.

Mitnick is currently a White hat hacker serving society. It is cool that he turned to justice to atone for his crimes.

Column: The origin of spam e-mail



So, there's SPAM rice balls, SPAM miso soup, sautéed SPAM, SPAM and pork omelets, but no such thing as whole boiled SPAM?! Well, there you are! (whole boiled SPAM is the dream of the writer)

In the past, there was a time when reading e-mail was depressing (sorry to be rude) as it was full of spam e-mails such as advertisements, solicitations, and phishing.

What is the origin of calling this disgusting mass e-mail "spam"? There are various opinions, but the most compelling is a sketch about the sausage-in-a-can SPAM by the British comedy troupe Monty Python.

Since the content of the actual sketch is nonsense that cannot be expressed in words, try searching for the video and experiencing it rather than imagining it.

The annoying use of SPAM in the sketch eventually became linked to the irritating spam e-mail of today.

Note that Hormel Foods Corporation, the manufacturer of SPAM, has accepted the usage of the word spam by naming the product with uppercase letters while spam with lowercase letters refers to the unsolicited e-mail called spam.

Although it is difficult to explain this irritating feeling, I tried to do it with an illustration in the style of a certain manga. Think of it as entering a restaurant called "E-mail Diner" and ordering the chef's special and this is what you get. Totally depressing, right?

By the way, SPAM is absolutely delicious! Apart from the boiled SPAM, you can find all of the other dishes in Okinawa prefecture. However, I have never encountered this complete SPAM set meal in Okinawa though.