

# Guide for First-Time Information Security Countermeasures

To All New Employees,  
Do You Know of "Information  
Security Countermeasures"?



Information-technology Promotion Agency, Japan  
IT Security Center

**IPA**

独立行政法人 情報処理推進機構  
セキュリティセンター

<http://www.ipa.go.jp/security/>

January 30, 2012 First Edition

# First-Time Information Security Countermeasures

There is the word "literacy". Literacy originally means "the ability to read/write in one's language", but nowadays, it refers to the ability to figure out and sort out events and leverage them by using knowledge and skills acquired.

In information-oriented society, whether or not one has computer-aided technique greatly affects individual potential and therefore, information literacy and computer literacy are said to be of importance.

This is why information security countermeasures are said to be implemented with such literacy.

However, before using the word "literacy", if one does not have security awareness, one will fail to implement information security countermeasures.



A decade ago, protecting one's own computer was said to be a security countermeasure. At that time, physical countermeasures were mainly taken, including computer virus countermeasures, elimination of vulnerabilities, encryption of information/data, making backup copies of information/data, plus for intra-company networks **(NB: you don't need to remember this)**, installation of firewall and IDS/IPS, and network monitoring and control on proxy servers.

However, after the legislation called "Private Information Protection Law" was enacted in April 2005, **issues concerning the leakage of personal information** began to be taken seriously.

Along with the emergence of this concept of "personal information", it has become increasingly important for enterprises to protect their corporate information and classified information as well. So, this was also regarded as a security countermeasure and the words such as information security countermeasures/management were brought to the fore.



Furthermore, in order to protect enterprise-handled information, enterprises need to implement not only physical security countermeasures (to protect their computers/networks managing that information), but also "security countermeasures by humans".

"Security countermeasures by humans" here refers to establishing security

countermeasure rules and systems and having employees follow them.

And now, let me explain about "security countermeasures by humans" by taking immediate problems as an example.

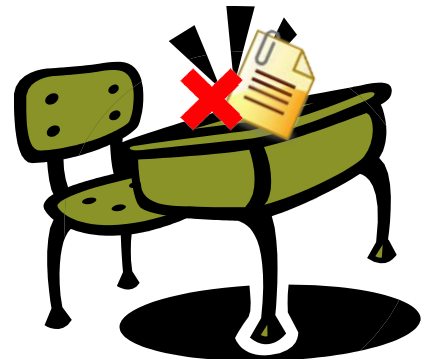
## Countermeasure (i): Critical Information for Enterprises is ...

For enterprises, critical (or needs-to-be-protected) information is the information which, if leaked to an outside party, **could cause a serious problem to their business operations**. Such information includes, for example, client's personal information entrusted to them by their clients; personal information of the employees who work at the enterprise; and classified (confidential) information such as corporate information and know-how for their business operation.

The first step for information security countermeasures is to understand which information is critical and protect it accordingly.

## Countermeasure (ii): On the Top of Your (Office) Desk in the Office ...

Information which is left unattended on your desk is at the risk of being carried away by someone else. To prevent critical information from being seen or accessed by people unconcerned, **do not leave such information unattended**, and manage and protect it in an appropriate manner.



In some cases, people unconcerned may enter your office. In such cases, if a critical document is left unattended on your desk, its content might be peeped or carried away by such people. To prevent this, you need to keep the top of your desk clean and be careful not to leave critical information unattended. Furthermore, if you stack documents in piles on your desk, you may not be able to locate critical documents when needed. Organizing and managing information is an important security countermeasure.

## Countermeasure (iii): If a Stranger Comes in Your Office ...

If the access to the company's premises is not restricted to authorized people, information held might be stolen by unauthorized people. In particular, for servers and book room/cashbox, do not let unauthorized people get close to or control them.

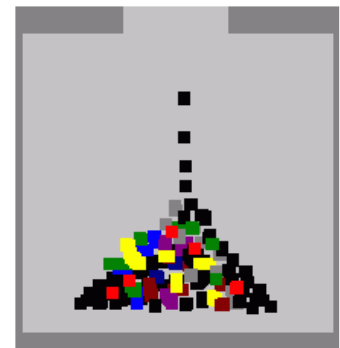
This countermeasure should be implemented in conjunction with countermeasure (ii).



## Countermeasure (iv): When Disposing of any Documents or Electronic Media that Contain Critical Information ...

When you dispose of critical documents, you need to shred them or take other actions to **make such critical information unreadable**. Similarly, when you dispose of a PC or a storage medium that contains critical information, you need to make its electronic data unreadable by using data erasure software or hiring a contractor for its erasure.

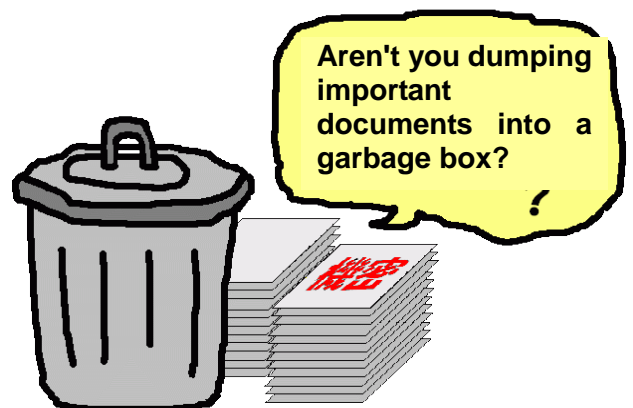
When you dispose of any documents or electronic media that contain critical information, if you just throw them into a dust bin and have a rag collector pick them up, it might result in a typical information leakage incident. Making critical information unreadable is an essential information security countermeasure.



There has been the following instance:

Instance: Household garbage?

A company worker who was unable to finish his work at the company took it home. After the work was done, he took the documents that contained critical information and dumped them to a household garbage, as he thought they were no longer needed. But because they contained a local government's resident



information, the garbage pickup contractor was surprised and reported it to the local government, which caused a big fuss.

Although it did not result in information leakage ...

The company to which the worker who caused this incident (accident) belonged was sued by the local government and was not offered any jobs for a period of time. The company had to spend a long time and a large amount of money in restoring its creditworthiness (including covering the expenditures for security countermeasures as well as the loss of profits due to the collapse of credit.)

## Countermeasure (v): Is it OK to Take Critical Information Out of the Enterprise's Premises? ...

When taking critical information out of the company's premises, employees should ask permission of their supervisor and then keep the record of take-out. Taking out a company's information without permission might constitute criminal act against that company.

Information which is taken out might be stolen unexpectedly or lost accidentally. For a cell-phone or a PC on which information is stored, if you set a password which is asked to enter at its startup or when opening a data file, you can prevent the information stored from being easily seen in the event of theft/loss.

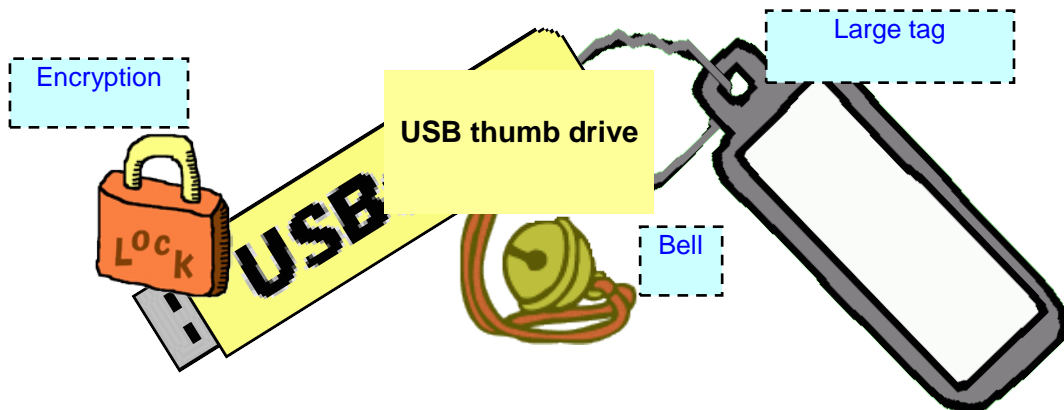
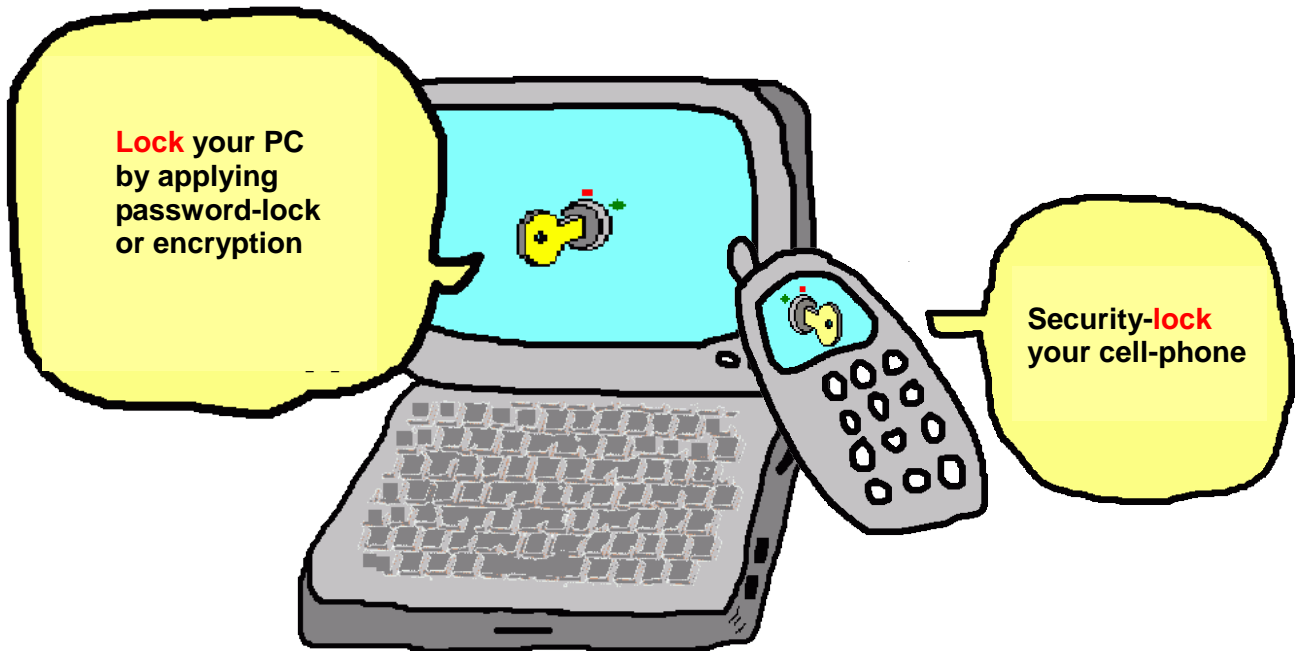


Before taking information out of the company's premise, one should make sure: **"Is it OK to take this information out?"** If the information is critical for your company and you need to take it out for business reasons, you should first ask permission of your supervisor and then keep the record of take-out so that in the event of theft/loss, the leaked information is easily identified. This kind of management for critical information is a fundamental information security countermeasure.

If we think about the taking out of information, we come up with not only PCs but also smartphones and other types of cell-phones, CD and DVD, as well as a variety of electronic memories. These storage media require solid physical security countermeasures in case of theft/loss.

For example,

**Preventive measures against information leakage in the event of loss of a PC or a cell-phone**



**Measures to prevent the loss of USB thumb drive**

Now that physical countermeasures have been touched upon, let's move on to the topic. Physical countermeasures should also be incorporated into organizational rules and observing such rules is "security countermeasures by humans".

## Countermeasure (vi): For Your PC ...

In the case of a PC that handles critical information, if a trouble occurs, business operation might be disrupted and it could even lead to information leakage in some cases. And if such PC is infected with a computer virus, or allow for unauthorized access by an outsider, or just breaks down, it might also result in the stagnation of business operation. So, daily maintenance and security countermeasures are of importance.

- ② Eliminate vulnerabilities
- ② Implement computer virus countermeasures
- ② Do not install (use) any applications that are irrelevant to your business operation
- ② Do not use any privately-owned PCs for your business operation
- ② Make backup copies of business data

### (1) Eliminate vulnerabilities

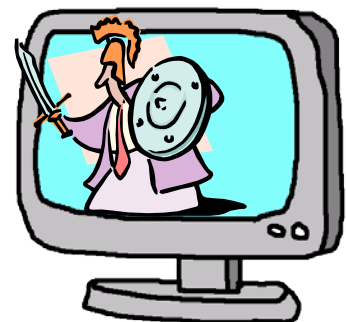
- In the case of Microsoft Windows
  - Perform Microsoft (Windows) Update (which is released each month)
- In the case of Apple's Macintosh
  - Apply security updates on a regular basis
- In the case of applications you use on your PC
  - Use the latest version at all times or apply security updates

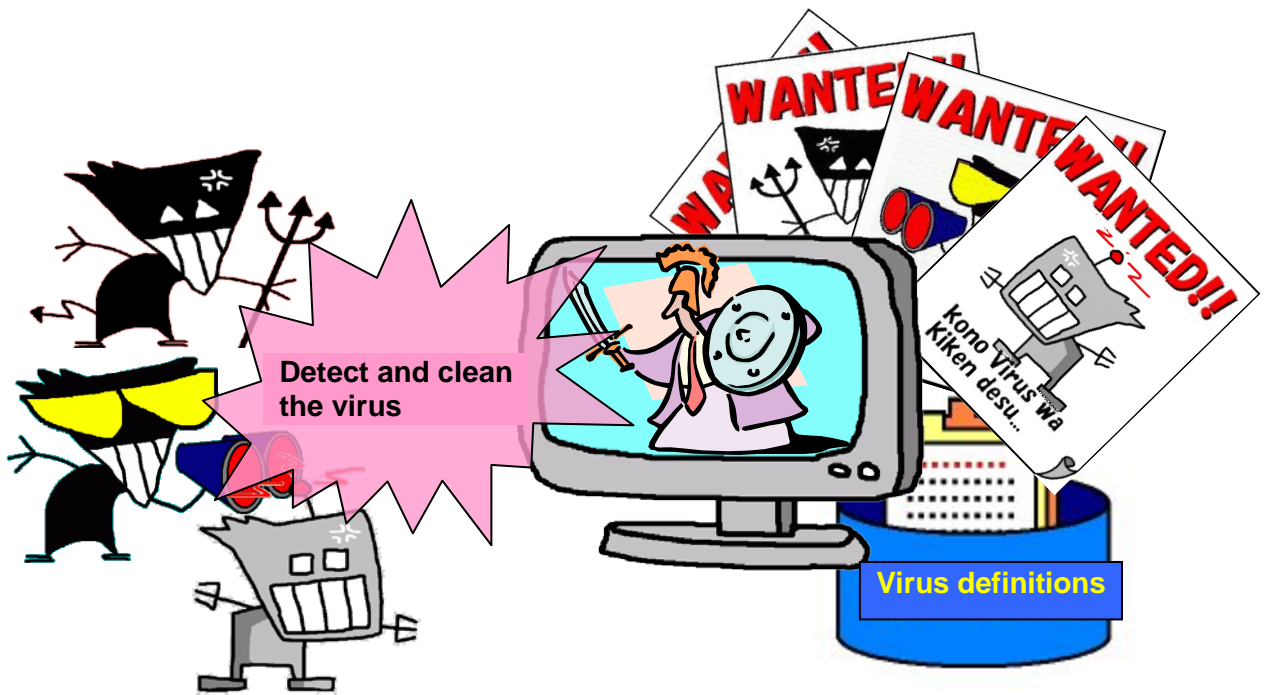


If you leave safety flaws (vulnerabilities) called "security hole" as they are, your PC might be infected with a virus exploiting them. For your operating system and software products, apply patches or use the latest version.

### (2) Implement computer virus countermeasures

- Use security (antivirus) software
- Keep its virus definition files (pattern files) updated (i.e., automatic update)
- Do not easily suspend security feature
- If you find any viruses, clean them and report it



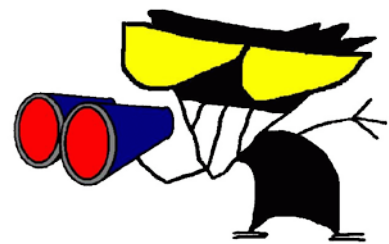


## Just For Reference: Introducing the Latest Computer Viruses

### Spyware

Spyware is a virus that covertly invades (infects) the victim's PC and records the information stored as well as operations performed by the user, and then transfer such information to an external party as needed. Among those that record users' operations is "keystroke logger" that records users' keyboard operation, which is a well-known tool. Internet reference record, which is also considered a history of users' operations, might be captured as well.

Spyware is thought to have been derived from so called adware which, for marketing over the Internet, displays information (such as commercial messages) or collects information (for the analysis of the user's preference). Spyware is said to be a radical version of adware in terms of activities.



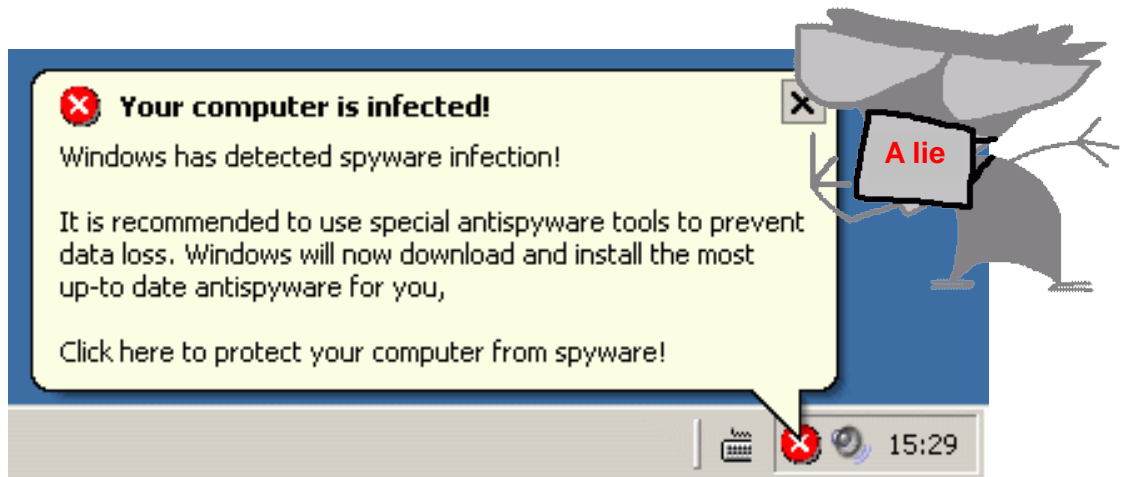
### Exposure Virus

A exposure virus causes information leakage via file-sharing software (e.g., Antinny virus) or covertly alters the victim's PC into an Internet website so that the information stored is exposed to the Internet (e.g., Yamada virus). These are also a type of spyware described above.



## Scareware

As indicated by its name, Scareware is a virus that scares the victims. It displays fake information such as "Your PC is infected with a virus" (i.e., self-produced virus hoax) and might also urge the PC user to purchase fake antivirus software.



## Ransomware

"Ransom" in "ransomware" refers to ransom money. Ransomware covertly encrypts specific files/folders on the target PC and demands a ransom by saying: "If you want to know the password to get them back, hand over your money!" In most cases, even if the user paid the money, the hostage (i.e., encrypted files/folders) would not be released (decrypted). The same things as real-world crimes are happening in the virtual world of the Internet.



## Bot

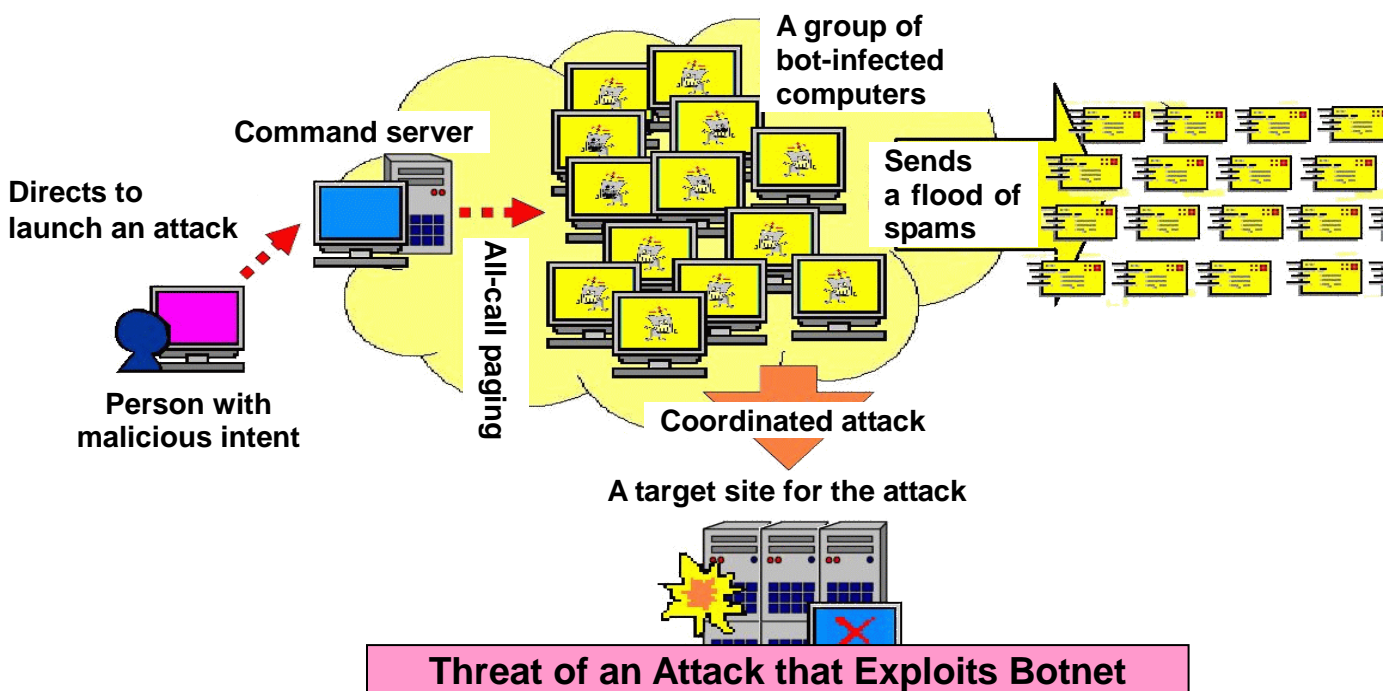
Bot is a program designed to infect PCs and then allow outsiders to remotely control them via a network (the Internet). Once it invaded the PC, it waits for commands from a command server (NB: communication with the command server is done at certain intervals) and executes any of the preprogrammed processes as instructed. Because this behavior is similar to that of a robot, it is called "bot". A bot virus that infects recently-popularized smartphone has also been confirmed, so smartphone users need to watch out.



Examples of preprogrammed process are:

- Spam delivery (sending a flood of spams)
- Attacks such as DoS attack (carrying out denial-of-service attack against a specific website)
- Network infection (gaining unauthorized access to a computer by exploiting its vulnerabilities and then infecting it)
- Network scan (collecting information on the target PCs for its infection or PCs having vulnerabilities)
- Version-upgrading of oneself or change of the command server
- Espionage activities (transferring the information stored in the infected PC to an external party)

A real threat of bots is: a group of bot-infected PCs might be under the control of a command server, forming a botnet. Botnet may consist of several hundred- to several hundred thousand-PCs, sending spams at the same time or carrying out a coordinated DDoS attack against a specific site. The larger the network, the greater the effectiveness of the attack.



## Trojan horse

Do you know of a Greek mythology "Trojan horse"? This is a story about dummy horses being sent by a troop to its opponent, claiming to be a gift; inside the dummy horses, however, are soldiers who are ordered to attack the opponent's castle once they get into it. As in this story, Trojan horse type virus is a virus that lurks in the victim's PC and does various bad things as needed. Generally, it belongs in a different category than those of spyware, scareware, ransomware and does the following bad things:

- **Installs a backdoor**  
It installs a backdoor on the victim's PC so that the PC can remotely be controlled by an outsider via the Internet (network). Through this backdoor, the outsider can break into that PC and perform various operations. It is a very dangerous situation.
- **Downloads malicious programs**  
It covertly downloads malicious programs from the Internet into the victim's and executes them.
- **Collects information from the victim's PC**  
It carries out so called spyware activities.
- **Uses that PC as a steppingstone for an attack (e.g., relaying an attack)**  
As with bots, it carries out an attack or works as a relay agent for an attack.

## Worm

Unlike the "virus" in general and narrow sense that infects (parasitizes) other programs or files, worm is a self-contained program that is installed and executed on the victim's PC. It creates copies of itself and places them on the victim's PC (i.e., self-propagation). To distinguish it from a traditional, narrowly-defined "virus", it was given a distinct name (type) "worm". Because it does bad things on the victim's PC such as destructive activities and infection (self-propagation) while wriggling like worms, it is termed "worm".

In fact, this type of virus is most-easily created; so many different types and subspecies have emerged. The foregoing spyware and scareware as well as ransomware and bots are also said to be of this sort. This means that traditional viruses are waning.

Anybody who can write a program can create worm. Generally, since it requires PC users to activate it, it is masqueraded as a useful program for them or exploits their PCs' vulnerabilities to get it activated.

### (3) Do Not Install (Use) any Applications that are Irrelevant to Your Business Operation

As typified by file-sharing software, applications whose use might lead to information leakage should not be used on corporate PCs. Employees should be banned from bringing game software from their home and installing it, as such software is not relevant to their business operation.

Big reasons for saying these things are: such applications may have vulnerabilities unremedied or there is a possibility that no support is available from their providers (i.e., there is no guarantee.) Furthermore, such applications might also lure malicious programs such as viruses. Is it not a problem to play with a business-purpose PC? ...

#### Information leakage via file-sharing software

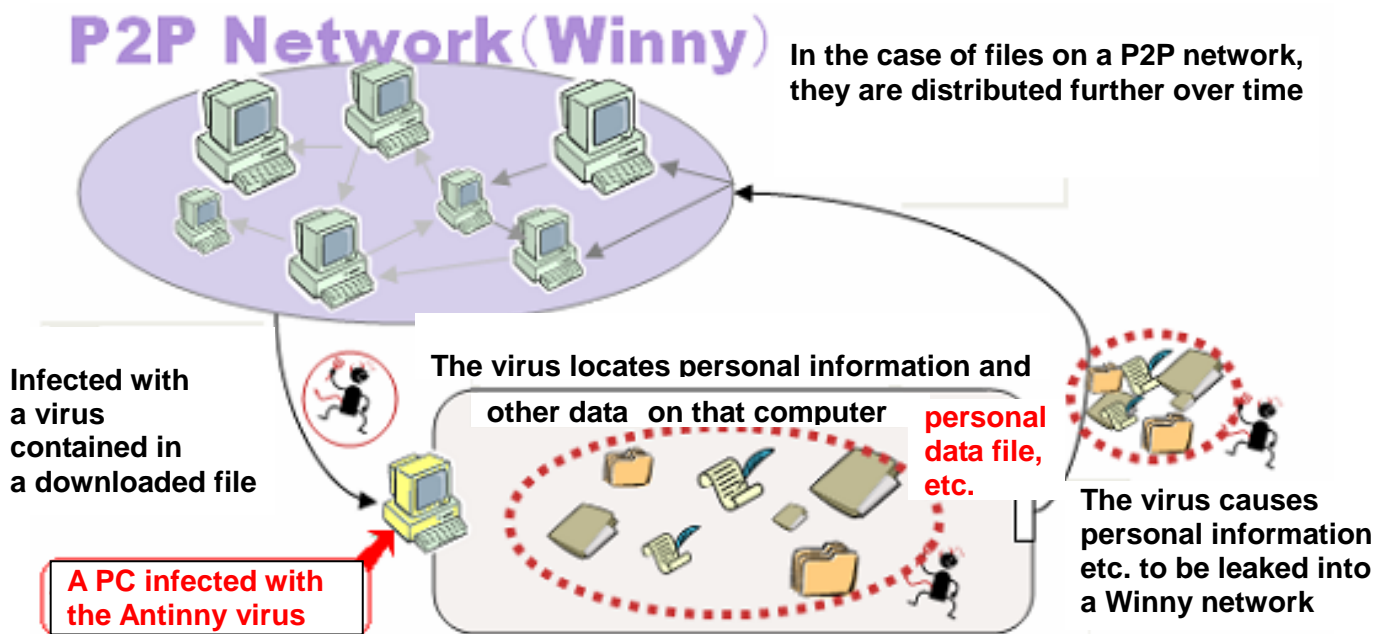


FIGURE: INFORMATION LEAKAGE ARISING FROM THE USE OF FILE-SHARING SOFTWARE

## Lamentable cases that have actually occurred

This figure shows the screen image of a sexually explicit site

- Visited a sexually explicit site while at work
- Fell for One-click Billing Fraud and ...
- A billing statement does not disappear from that PC's screen!!
- Is this also done by a virus? ...
- Too ashamed to continue your work?
- To avoid being discovered by his boss, a man reported to the boss that his PC has broken down!?
- Should this man's business be suspended?



### (4) Do Not Use any Privately-Owned PCs for Your Business Operation

For the same reasons as those for "Do Not Install (Use) any Applications that are Irrelevant to Your Business Operation", it is advisable not to use any privately-owned PCs for your business operation. When absolutely necessary, obtain permission from your supervisor and implement adequate security countermeasures before using such PCs. However, as a general rule, it is recommended not to use any privately-owned PCs as they cannot be adequately controlled by the company.

### (5) Make Backup Copies of Business Data

Data stored in a PC might be lost due to the breakdown or wrong operations of that PC. If you make backup copies of such data on a regular basis, you can prepare for contingency like this.

## Countermeasure (vii): Password ...

Password is important. Password is touched upon in Countermeasure (v) as well, and its usage ranges from a login password or PIN for PC/smartphone/cell-phone to many different passwords for various Internet services.

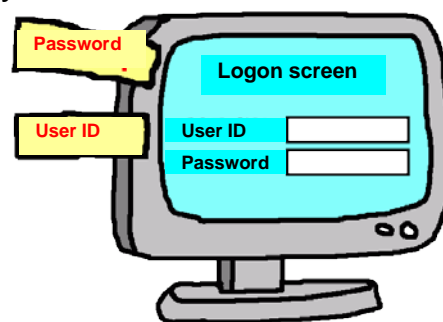
Everybody seems to understand the importance of password, but for various Internet services, people may use simple passwords or even the same password, which is a risk-taking attitude from the aspect of password operation and management. In fact, such cases are frequently seen.

There also has been a case where a user's password for an Internet service was guessed and abused by a third party. One of the causes was that the user was using a simple password (e.g., name or date of birth). If your password is guessed by a third party, it might be abused by means of spoofing. By using the combination of upper- and lower-case alphabetical characters, numeric characters, and symbols for your passwords and changing them on a regular basis, you can prevent such damages.

For the passwords to be used for your business operation, observe the following rules, while keeping them under a rigid control.

### Rules on Passwords

- Do not use any passwords that can easily be guessed by others (e.g., nickname or date of birth)
  - ☑ Use the combination of upper- and lower-case alphabetical characters, numeric characters, and symbols
  - ☑ Use a long password (preferably, eight or more digits)
  - ☑ Use a hard-to-guess, but easy-to-remember password
- Do not leave your password in a place where it can catch the eyes of others
- Change your passwords on a regular basis



If you are afraid of forgetting your passwords, you may write them down on a paper and keep it in a safe place (e.g., strong box) and then get it out only when needed. This is justifiable because if you forget your password, your business operation might be disrupted ...

## Countermeasure (viii): Electronic Mail ...

When you use electronic mails in your business operation, you should be careful not to make mistakes in transmission (e.g., misaddressing) as they may contain critical information.

To prevent wrong transmission, countermeasures such as those listed below are required.

- Prior to sending an electronic mail, check for its destination(s) and contents
- For critical information, do not include it in the main body of the mail but in an encrypted file attachment ...
- When you send an electronic mail to multiple destinations at the same time (i.e., broadcast mail), consider whether you should use "BCC", or simply "To" or "CC".

There has been a spate of incidents where a broadcast mail was sent in a misguided way, for which all the destination addresses specified (i.e., personal information) were disclosed to one another. Most of those incidents were caused by a person mixing up "CC" and "BCC".

## **Countermeasure (ix): What is the confidentiality obligation? ...**

In Countermeasure (i), it explains what kind of information is critical for enterprises. Employees must keep such information from outsiders. That is confidentiality obligation. In general, in order to have their employees protect corporate secret, companies let them know of the presence of this confidentiality obligation when hiring them and take other steps if needed.

There was the following incident (accident):

### **Instance:**

At a well-known hotel in Tokyo, a part-time worker at a restaurant in the hotel saw a couple of a famous sport athlete and a female TV personality who came privately to the restaurant. She then tweeted this matter on Twitter. This was not the first time she tweeted information of this sort, but this time, she came under an increasing criticism of Twitter users who read her tweet, as she revealed information on celebrities' personal life. It eventually led to so called "a flurry of festivity" and her personal information became searchable on other Internet bulletin boards as well.

According to the hotel, regardless of a full-time employee or part-time employee, every employee receives training in confidentiality obligation to protect clients information and is required to sign a confidentiality obligation pledge card.



## Summary

There must be many occasions for new employees to use the Internet in carrying out their tasks after joining their company. Nowadays, people are using the Internet more frequently than ever before in their daily life, but if employees are not aware of the fact that their company is handling important information, they might cause incidents such as information leakage anytime for any reason.

In using the Internet in a secure manner, you may face a situation where you find it difficult to make on your own decision. The number of cyber criminals having pecuniary motive is on the rise, including, for example, computer viruses whose purpose is to carry out phishing or steal information. Furthermore, there is also an attack called "targeted attack" that targets at a specific organization or company.





In order not to cause serious incidents from your own negligence or human error, it is important to have security awareness in daily life and to observe the security rules established by your company.

We hope that you will work as a member of society not just "protecting yourself on your own," but having the frame of mind: "I'll protect my company."



## Reference information

### <To Learn>

-  **Let's Do This at Least! Security Countermeasures**  
<http://www.ipa.go.jp/security/personal/base/>
-  **Points to Prevent Virus Infection**  
<http://www.ipa.go.jp/security/personal/know/virus.html>
-  **Points to Prevent Information Leakage**  
<http://www.ipa.go.jp/security/personal/know/leakage.html>
-  **Points to Prevent Invasion**  
<http://www.ipa.go.jp/security/personal/know/invasion.html>

### <To Protect>

-  **Virus Countermeasures**  
<http://www.ipa.go.jp/security/personal/protect/antivirus.html>
-  **Countermeasures against Information Leakage via File-Sharing Software**  
<http://www.ipa.go.jp/security/personal/protect/leakage.html>
-  **Five Clauses for Anti-Spyware Measures for PC Users**  
<http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html>
-  **Anti-Phishing Measures**  
<http://www.ipa.go.jp/security/personal/protect/phishing.html>
-  **About Mail-Related Troubles**  
<http://www.ipa.go.jp/security/ciadr/mailtrbl.html>
-  **To Protect from Being Charged for What You are Innocent of**  
<http://www.ipa.go.jp/security/personal/protect/oneclick.html>

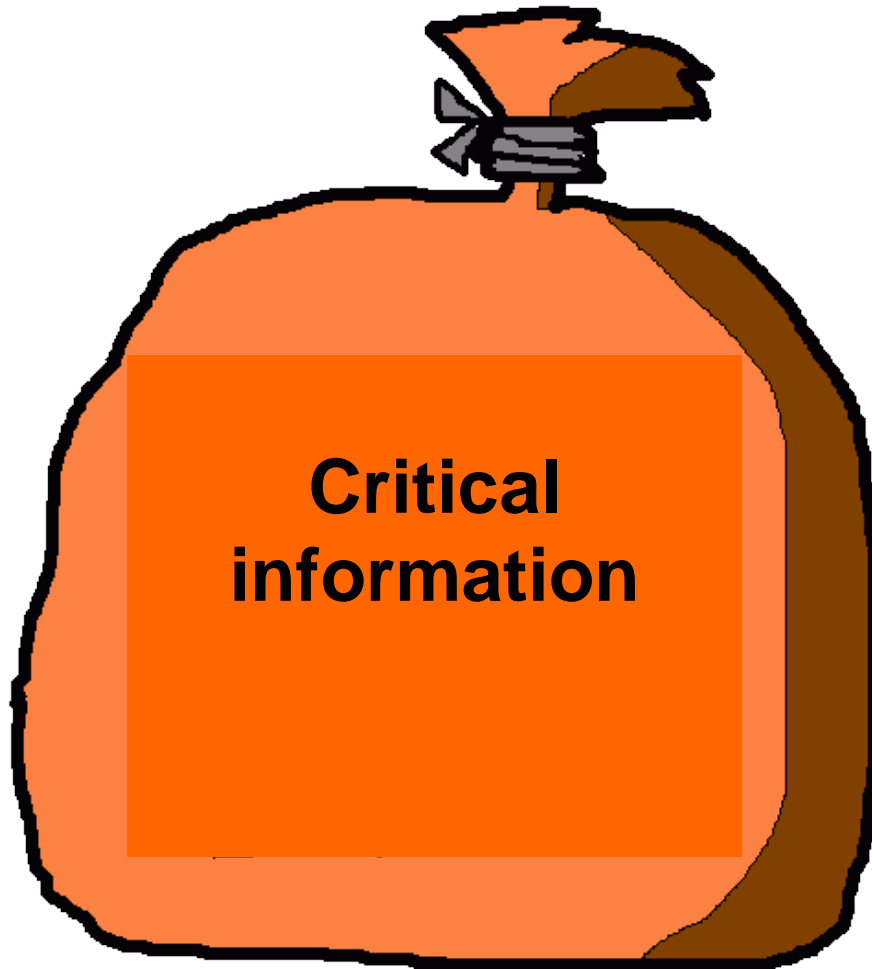
### <Learning tool>

-  **Learning Points for Information Security. It Takes Only 5 Min**  
- Learning Security Measures for Small-to-Mid-Sized Enterprises through Case Examples -  
[http://www.ipa.go.jp/security/vuln/5mins\\_point/](http://www.ipa.go.jp/security/vuln/5mins_point/)

## **IPA Countermeasure Guide Series**

<http://www.ipa.go.jp/security/antivirus/shiori.html>

- (1) Countermeasures on Computer Virus
- (2) Countermeasures on Spyware
- (3) Countermeasures on Bots
- (4) Countermeasures on Unauthorized Access
- (5) Countermeasures on Information Leakage
- (6) Countermeasures against Risks Associated with the Use of the Internet
- (7) Countermeasures against Risks Associated with the Use of Electronic Mails
- (8) Security Countermeasures for Smartphone
- (9) Guide for First-Time Information Security Countermeasures
- (10) Countermeasures against Targeted Attack Mails



Critical information

**IPA**

独立行政法人 情報処理推進機構  
セキュリティセンター

Bunkyo Green Court Center Office, 16t Floors,  
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan 113-6591  
URL <http://www.ipa.go.jp/security/>

[Worry-Free Information Security Consultation Service]

URL <http://www.ipa.go.jp/security/anshin/>  
E-mail [anshin@ipa.go.jp](mailto:anshin@ipa.go.jp)