Countermeasures against Unauthorized Access

Is your computer really safe? (For PC Users)

IPA
Information-technology Promotion Agency
IT Security Center
http://www.ipa.go.jp/security/
What is Unauthorized Access?

Unauthorized Access is an act of illegally gaining access into any computer, network etc, or promoting such activity, which is banned under the “Unauthorized Access Prohibition Law” (*1), enforced on February 13, 2000. For more details, please refer to the description below:

- Compromising a computer by bypassing its access control (*2), exploiting a vulnerability (a security hole) (*3) in the operating system, hardware, or applications running on it.
- Illegally using services available only to legitimate users, by using their user IDs and passwords (*4) without their consent. (Masquerading or impersonating)
- Providing a third person with users' IDs and passwords without their consent.

This guide is intended for PC users. Please note that the countermeasures against unauthorized access, presented in this guide, may not be sufficient (or applicable) for company networks.

For example, these are true stories.

• Pitfalls of Simple Passwords

  Mr. A, a regular user of Internet Auction, was trading baseball cards at frequent intervals. He was using his name as password (for logging on to the auction site) so as not to forget it.

  One day, when he supplied his password to log on to the auction site, he saw the message “Invalid Password!” He tried again but the result was the same. Because he had no recollection of changing his password, he contacted the management company and found that the password had actually been changed.

  He was using such a simple password that it was easily guessed and abused by a malicious user.
• Pitfalls of Constant Internet Connection

Ms. B was using a CATV Internet service. Because it was a flat-rate service, she left her computer connected to the Internet.

She did not care about security and did not take any steps to mitigate security holes (vulnerabilities), such as by applying the Windows Update.

One day, she received a phone call from the Information Security Response Center, informing that her computer was attacking a government facility, and instructing her to stop accessing the Internet and take necessary steps. In a hurry, she disconnected her computer from the Internet.

Because she left the unprotected computer connected to the Internet, it was compromised without her knowledge and used as a stepping stone for the attack.

• Pitfalls of Wireless LAN

Mr. C has several personal computers at home. His family wanted to place a computer for each room, and therefore, they applied wireless LAN, which does not require cables. As soon as connected, it was ready to use, so they tried it without reading the manual.

Several weeks later, when they were playing an online game, their computers became less responsive and the access lamps started blinking for a long time, even when not accessing data.

One day, they were unexpectedly billed for online-shopping by a credit-card company. After the investigation, they learned that the shopping had been done by a third party.

A few days later, they found that a shared file containing their credit-card number had been accessed by a malicious user via the unprotected wireless LAN to perform online-shopping.

In this way, because of “Using a simple password”, “Not applying security patches”, “Inappropriate Access controls”, you might fall the victim of unauthorized access. Anybody who accesses the Internet can encounter such incidents. For a secure, comfortable Internet access, apply the following minimum-required countermeasures.
1. **Apply Security Patches (Countermeasures against intrusion)**

Operating Systems (such as Windows, Macintosh, Linux etc), Web browsers (such as Internet Explorer, Firefox etc), and other software programs could have some defects (vulnerabilities) that might allow breaches of computer security.

These security defects are called **Security Holes or vulnerabilities**. If you are using an operating system or application having a security hole, it might allow the penetration of computer viruses or unauthorized access, due to which data on your computer might be deleted or personal information stolen.

To prevent such incidents, it is important to apply a patch to fix the detected security hole. These patches are provided by software developers to mitigate such vulnerabilities.

Windows users should periodically perform the Windows Update/Microsoft Update, or turn on the Automatic Update feature. You can apply the latest patches provided by Microsoft for their operating systems, Internet Explorer, and Office products.

- **Windows Update**
- **Office Update**
- **Microsoft Update**

For information on how to apply the Windows Update, Office Update, and Microsoft Update, please refer to the following Web sites:

- **How to apply the Windows Update**
- **How to apply the Office Update**
- **How to apply the Microsoft Update**
2. **Password security should not be overlooked** (Countermeasures against Masquerading/Impersonation)

User IDs and Passwords supplied by users are checked by information systems (services) to verify their identity. Generally, a unique user ID is assigned to each user, but passwords are something you must set (or change) by yourself. If your User ID and Password are compromised or stolen, somebody else might use them to access your system or other systems, masquerading as a legitimate user.

There have been incidents in which attackers illegally withdrew users' money by accessing online banking, or bought expensive items via Internet auction.

Your User ID and Password are used by systems to verify your identity, so do not use a simple password, do not tell your password to anyone else, and change it on a regular basis.

---

**Example of Passwords:**

1. **Combination of alphabet characters (upper and lower cases), numerals, and symbols**
   - Use a password with symbols (such as “!”, “#” etc), numerals, and alphabets mixed.

2. **A long password**
   - Use a password with at least 8 characters.

3. **A hard-to-guess password that you can remember**
   - Use a password with a random, meaningless sequence of characters.

**Measures to prevent your password from being stolen:**

1. **Change it on a regular basis**
2. **Do not write it down on a paper**
3. **Do not save it on your computer**
4. **Do not tell it to anyone else**
3. Points to remember when accessing the Internet (Countermeasures against Intrusion)

While accessing the Internet from your home or an office, your PC might allow another user to gain unauthorized access (intrusion), depending on how you connect it.

If you are accessing the Internet using a telephone line (or cell-phone line) and a modem, there is a high possibility that your PC might be accessed by an unauthorized user, exploiting the direct Internet connection. To avoid this, it is recommended to make security settings on your computer (as described later) or use security software.

If you are accessing the Internet using ADSL and a relatively-new ADSL modem, the possibility of your PC being accessed by unauthorized users becomes low, because such modems have a router function to block unauthorized access; however, you may still suffer from unauthorized access due to inappropriate modem settings. If you feel uneasy about it, make security settings on your computer (as described later) or use security software.

If you are accessing the Internet using a CATV cable and a cable modem (or an optical fiber and a VDSL modem) and if no device is placed between your PC and Internet, the possibility of your PC being accessed by unauthorized users becomes high. In such cases, it is recommended to use a router or a device that provides a Firewall function. Note, however, that you must chose devices applicable for the line type, and that you may still suffer from unauthorized access due to inappropriate device settings. If you feel uneasy about it, make security settings on your computer (as described later) or use security software.

If you are accessing the Internet using public wireless LAN hot-spot services or a LAN installed in facilities such as business hotels, your computer might allow unauthorized access from other users on the same LAN, because such network environment can be accessed by unspecified number of users.

In this case, it is recommended to make settings to protect your computer against unauthorized access (as described below) or use security software.
4. Settings to Protect against Unauthorized Access

(1) Disable the file-sharing feature

If you connect your PC to a LAN within a business hotel, and then open the “My Network” window and look through the Entire Network, you may see other person’s computer’s folders. It’s just like asking “Look into my holder.” This is because the user’s PC is connected to the LAN with its folder-sharing feature enabled. If you are going to connect to a LAN that allows unspecified number of users to connect to it, disable the folder-sharing feature.

If the folder is set to be shared, its icon will look like the figure on the left.

To set a folder to be shared, right-click on the folder’s icon, select [Property] and click the [Sharing] tab. The folder’s property window will appear.

If you are using Windows XP Professional Edition, the window on the left side will appear. For Windows XP Home Edition users, the window on the right side will appear. Note that these two windows are slightly different.
(2) Change the Properties of Local Area Connection

In addition, it is recommended to make your computer invisible on the Microsoft Windows Network by changing the properties of ‘Local Area Connection’.

Operations:
Select [Start] > [Settings] > [Control Panel] > [Network Connection], right-click on [Local Area Connection], and click [Properties]. The Local Area Connection Properties window will appear.

(Caution) When switching from the current network environment to your own network environment, be sure to restore the settings. Otherwise, you cannot set folders or printers to be shared as you did before changing the settings. If you are not using network printers or the file-sharing feature, you do not have to restore the settings.

5. **Use of Firewall Software (Integrated Security Software) Recommended**

Firewall is a key tool to prevent unauthorized access.

Apart from manually implementing countermeasures against virus and Spyware, it is recommended to use Integrated Security Software having a Firewall function or Personal Firewall Software.

Firewall is designed to monitor data exchanged between a computer and the Internet, display warning messages if it detects data communication that may affect the system, and block unwanted access to the computer.

Even in the case where your computer has been compromised and a malicious program such as Spyware attempts to send personal information (stored on the computer) to the outside, Firewall displays warning messages so that you can prevent further damage.
For mobile devices, install and utilize Personal Firewall Software or Integrated Security Software, because there is no router available and no Firewall is pre-installed.

If you are using Windows XP, use embedded Windows Firewall.

Windows Firewall blocks malicious data coming from outside but cannot prevent such data from going out. (Windows Vista is expected to block malicious data transmitted in both directions.) However, it is an effective tool for protecting against external attacks that exploit vulnerabilities in the operating systems and application software. If you cannot install Personal Firewall Software or Integrated Security Software for some reason, use this tool.

Operations:
Select [Start] > [Settings] > [Control Panel] > [Windows Security Center] > [Windows Firewall]
6. ABCs of Wireless LAN

Wireless LAN does not require network cables and can be used anywhere within a house or office as long as it is within the reach of electric waves.

However, if no security settings are made, there is a risk that data on the computer is stolen or the wireless LAN used without permission.

The latest Wireless LAN equipment allows users to make minimum-required security settings.

It's recommended to implement the following measures: *(For more details, please refer to the wireless LAN equipment manual.)*

- **Wireless Access Point Device**
  - Set the SS-ID (*5)
  - Set the Key for WEP (WPA/WPA2) (*6)
  - Enable MAC Address Filtering (*7)
  - Deny a connection request from an anonymous terminal

- **Make settings on the client in accordance with the settings on the Access Point Device**
7. **Backup Important Data**

A computer that has received an unauthorized access (or intrusion) can allow a malicious program to be embedded or the system altered. In such case, the user may have no choice but to initialize his (or her) computer. **Make it a rule to back up data on a regular basis.** In addition, keep in a safe place the original CD-ROMs of application software. Should the contents of the hard drive be damaged, you can restore them using the CD-ROMs.

(System Recovery Function)

Windows XP has a system recovery function. Using this function, you can restore your system to its previous state. For example, if your system has been altered by an attacker gaining unauthorized access (intrusion), you can use this function to restore your system to its previous state. It can also be used in the case where the system began to malfunction after opening a file. For the detailed procedures, please refer to the following site:

💡 - Recovering Windows XP using the System Recovery Function (Microsoft)

http://support.microsoft.com/default.aspx?scid=kbja;306084

---

![Backup Important Data Diagram](image)
8. If you have fallen victim to ...

If you think a malicious program has been embedded on your computer by means of unauthorized access (intrusion), scan it by using the security software (antivirus software or anti-Spyware software) with its virus definition files updated. If you have been able to identify the name of the virus but do not know how to eliminate it, visit the Web site of your antivirus software manufacturer and look for the information related to the virus, and then follow the instruction presented on the Web page.

If you have no security software at hand but can access the Internet, you can still use free-online scan services provided by some vendors to identify the name of the virus. If identified, look for the information on the virus and follow the instruction presented on that Web page.

If you have further questions, contact the “IPA Computer Virus 911 call” service, where you can consult IPA consultees about virus-related problems.

■ IPA Computer Virus and Unauthorized Access 911 Call Number

For information related to unauthorized access, call the following numbers or email us:

03-5978-7509

(Japanese language only)

Weekdays: 10:00 - 12:00, 13:30 - 17:00
E-mail : crack@ipa.go.jp

💡 If you have fallen victim to spoofing (or masquerading), contact your ISP (Internet Service Provider) or the cyber-crime consultation service of Prefectural Police Headquarters. For incidents involving credit cards, consult with a Local Consumer Affairs Center (National Consumer Affairs Center) or your credit-card company.
9. References

For further information, please refer to the following materials:

- Unauthorized Access Prohibition Law (Japanese language only)
  http://www.ipa.go.jp/security/ciadr/law199908.html
- Unauthorized Access will be Punished! (Japanese language only)
- Countermeasures against Unauthorized Access (Japanese language only)
  http://www.ipa.go.jp/security/ciadr/faq01.html
- Computer Unauthorized Access FAQ (Japanese language only)
  http://www.ipa.go.jp/security/ciadr/law199908.html
- Security at Home: Protecting Your Computer (Microsoft)
  http://www.microsoft.com/athome/security/yourself/default.mspx
- “Enhancing Browsing and Email security” (Microsoft)

IPA Countermeasure Guide Series
  http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA Countermeasure Guide (1) Countermeasures against Virus
- IPA Countermeasure Guide (2) Countermeasures against Spyware
- IPA Countermeasure Guide (3) Countermeasures against Bots
- IPA Countermeasure Guide (4) Countermeasures against Unauthorized Access
- IPA Countermeasure Guide (5) Countermeasures against Information Leakage

10. Terminology
(*1) Unauthorized Access Prohibition Law

A law to prohibit unauthorized access and relevant activities, which
was passed by the Diet on August 6, 1999 and came into force on
February 13, 2000, except for Article 6. As of July 1, 2000, Article 6
was also put into practice. To read the Articles, please refer to the
following sites: http://www.ipa.go.jp/security/ciadr/law199908.html (Japanese
language only)

Explanations are given by the National Police Agency in the
following two sites:
  http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm (Japanese language only)
  http://www.npa.go.jp/cyber/english/legislation/ucalaw.html (English)

The “Regulations on Assistance by Regional Public Safety Commissions
for the Prevention of the Recurrence of Unauthorized Access”, which was
established by the National Public Safety Commission, can be found on
the following site:
http://www.npa.go.jp/cyber/legislation/kitei/enjyo_kitei.htm (Japanese language only)
In addition, if a computer was caused to malfunction or data corrupted due to an unauthorized access, the person who performed the access would be charged with “Forcible Obstruction of Business”.

(*2) Access Control
From the aspect of computer security, access control is implemented to limit access to computer resources to authorized users having a privilege required.

(*3) Vulnerability
Vulnerability in terms of information security is a security hole that may degrade the security level of systems, networks, applications and protocols, which can bring unexpected, unwanted events, or design and implementation errors. Vulnerabilities are classified into “vulnerabilities in the operating systems”, “vulnerabilities in applications”, etc. Inadequate security settings are also referred to as vulnerability. In general terms, it is called “security hole”.

(*4) User ID and Password
User ID and password are referred to as “Identification Code” in the Unauthorized Access Prohibition Law. In the broad sense, this could be code, fingerprint, signature, voice, image etc. that is used to confirm the person’s identity. In this document, we simply call it user ID and password.

(*5) Service Set ID (SSID)
An Id to identify an access point (AP).

(*6) Wired Equivalent Privacy (WEP)
An optional encryption standard defined by the IEEE. WEP uses a secret key cryptography that is based on the RC4 algorithms. The length of the encryption key is 64, 128 or 152 bits; however, it is recommended to use the longest one, because WEP itself has a known vulnerability. Recently, as an alternative to WEP, a wireless LAN encryption system called Wi-Fi Protected Access (WPA) have come into use.

(*7) MAC Address
In this case, mac address is a unique ID assigned to the wireless LAN adaptor.