Guide for <Avoidance of Risks> When You Use Electronic Mails

For Troubles via Electronic Mails,
These Countermeasures are Required!!

IPA

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

June 8, 2012 4th Edition
Introduction

Nowadays, electronic mail (hereinafter referred to as e-mail) is indispensable for not only corporate activities but also personal use. Thanks to the popularization of antivirus software and spam e-mail filtering software, countermeasures against computer viruses via e-mail and unsolicited (spam) e-mails are effectively implemented by organizations. However, recently, there were information leakage incidents resulting from improper e-mail handling, and virus infection/information leakage resulting from careless handling of suspicious e-mails sent as part of (the after-mentioned) Targeted Attack. Especially, in corporate activities, these problems can develop into the company’s credibility problem.

In order to address the problems like these, it is important to raise security awareness on the part of those handling e-mails and to ensure that basic measures are implemented.

This countermeasures guide explicates the following:

- **To Prevent Wrong E-mail Transmission**
  - Mailer Settings to Prevent Wrong Transmission
  - E-mail Encryption (Attachment Encryption)

- **To Protect Oneself from Computer Viruses and Targeted Attack**
  - Secure Mailer Settings
  - Targeted Attack
  - How to Handle Suspicious E-mails

This guide describes how to strengthen the security of mailers (i.e., an application to read and write e-mails in a secure manner) and the information is based on Microsoft Outlook Express (2003).

Recently, a variety of mailers and Web-based e-mail (applications) are used by people. It is effective to strengthen the security of each application, so we recommend that you strengthen the security of your mailer based on the contents of this guide.

While the previous editions recommended disabling e-mail preview function due to certain vulnerabilities in mailers, this edition omitted such recommendation as those vulnerabilities are not detected in recent mailers.
1. To Prevent Wrong E-mail Transmission

As for major information leakage incidents due to wrong e-mail transmission, the following instances are often observed.

- An incident caused by specifying a wrong destination address
- E-mail address leakage caused by sending a broadcast mail\(^*1\) in the wrong way

\(^*1\) Broadcast mail is an identical e-mail sent simultaneously to multiple recipients.

While the former is often caused by e-mail users' carelessness, the latter is often caused by unaccustomed e-mail handling. In either case, the problems are related to e-mail destination address, so if users exercise caution, they can prevent such problems.

The following countermeasures are effective:

- Prior to sending an e-mail, recheck its destination address and contents as well as the presence/absence of attachment(s);
- Understand the usage of TO, CC and BCC (make it a rule);
- Furthermore, in order to reduce the occurrence of problems, encrypt e-mails.

🚨 Prior to Sending an E-mail, Recheck its Destination Address etc.

■ In the Case of Microsoft Outlook Express

Let's take Microsoft Outlook Express as an example.

General (default) settings are: if you create an e-mail and press the [Send] button on the [Mail Creation Screen], the e-mail is sent immediately. It is recommended to recheck its destination address before pressing the [Send] button, and those who are still anxious may make settings as shown in Figure 1, which gives them an additional opportunity to recheck their e-mail's destination address.
Figure 1: Option Settings to Enable Users to Recheck Their E-mail's Destination Address

On the [Mail Operation Screen], select [Tool] -> [Option] -> the [Send] tab and uncheck the checkbox "Immediately send messages" (this is checked by default), and then click the [OK] button (or the [Apply] button). By making this setting, even if you press the [Send] button on the [Mail Creation Screen], that e-mail is not sent immediately and instead placed in the out-tray. That is to say, you can recheck the content (including destination address) of that e-mail in the out-tray.

Actual e-mail transmission takes place when you press the [Send/Receive] button on the [Mail Operation Screen].
In the Case of Mozilla Thunderbird

In the case of Mozilla Thunderbird, the application itself has no function (setting) to disable immediate transmission, but there are several add-ons*2 that prompt users to check their e-mail's content before sending it. By using these add-ons, you can check your e-mail's content (including destination address) before sending it. This gives you an additional opportunity to recheck your e-mail (Note, however, that add-ons should be used at your own risk.)

*2) Add-on is an extended function that can be added to software. Because Mozilla Thunderbird is open source software (OSS), there are a variety of add-ons by various developers.

Examples of add-ons are:
Check and Send:  https://addons.mozilla.org/ja/thunderbird/addon/2281
Confirm-Address: https://addons.mozilla.org/ja/thunderbird/addon/5582
and so forth.

⚠️ Usage of "TO", "CC" and "BCC"

For e-mail destination address specification, you can use "TO", "CC" or "BCC". Here, we explain by taking Microsoft Outlook Express as an example again.

For "TO" specification, it is common to specify a primary destination address for that e-mail. When you specify a specific person's destination address, you can use this "TO" specification (NB: in the case of Outlook Express, this is called "destination address" instead of "TO").

"CC (Carbon Copy)" specification is used to send an identical e-mail to multiple destination addresses at the same time (i.e., broadcast mail). For example, it would be a pain to send an identical e-mail, one by one, to multiple members within the same company. By specifying multiple members' in the
"CC" field, you can send such identical e-mail at a time. You may also specify each destination address in the "TO" field, but depending on the mail server which sends/receives e-mails or the mail provider, the number of destination address that can be specified in the "TO" or "CC" field may be limited, so, be careful.

In the above example, an identical e-mail is sent to person B as well as C, D and E. What needs to be noted here is that, all the recipients (i.e., person B, C, D and E) would notice that an e-mail to person B was also sent to person C, D and E (The reason why B is specified in the "TO" field is because person B is the primary recipient; if the "TO" field is left blank, this e-mail is regarded by Outlook Express as "undirected" and might be mistaken for a virus e-mail or an unsolicited e-mail. To avoid this, you need to specify at least one person (you may specify multiple recipients).

In this case, if person B, C, D and E did not know each other, they would be embarrassed by receiving such e-mail. For example, person C may not want anybody except A to know his e-mail address. In such case, this e-mail transmission results in e-mail address leakage (personal information leakage).

To avoid this problem, you can use "BCC (Blind Carbon Copy)" specification. "BCC" specification is used to send an identical e-mail to multiple destination addresses at the same time (i.e., broadcast mail). For example, it would be a pain to send an identical e-mail, one by one, to multiple clients. By specifying multiple clients in the "BCC" field, you can send such identical e-mail at a time.
In this case, an e-mail to person A is also sent to person B, C, D and E. However, person B, C, D and E would not notice that the e-mail they received has someone else's address in the "BCC" field (they even don't know if the e-mail was addressed only to them).

At least, the e-mail addresses specified in the "BCC" filed are not disclosed to the recipients, so except for body text and attachment contents, there is no risk of personal information leakage resulting from destination address specification (as mentioned earlier).

The reason why the sender himself is specified in the "TO" field is the same as that of "CC" (if the "TO" field is left blank, this e-mail is regarded by Outlook Express as "undirected" and might be mistaken for a virus e-mail or an unsolicited e-mail.) For "TO", "CC" and "BCC" specification, destination information (e-mail address) is a compulsory input item.

This is a little ingenuity, but if you are going to specify yourself in the "TO" field, you may register in the address book your e-mail address with an explicit owner name (e.g., "Broadcast mail by BCC") so that such explicit destination address is displayed in the "TO" field.

(Caution 1) Cannot Use BCC?

If you have never used "BCC" on your Outlook Express or if you are using your Outlook Express in initial state, the "BCC" entry field is not displayed on the [Message Creation Screen]. In such cases, by selecting [Display] on the [Message Creation Screen] and checking [All the headers], you can make the "BCC" entry field appear.

![Figure 2: How to Make the "BCC" Entry Field Appear](image-url)
(Caution 2) You Checked an E-mail in the [Sent Message] Folder, But You Could not See the "BCC" Content?

Even if you open an e-mail whose destination address specification is "BCC" in the [Sent Message] folder, the "BCC" content is not displayed. If you want to check the e-mail addresses specified in the "BCC" field, select [File] -> [Property] on the [Mail Display Screen], which opens the [Property Screen], and click the [Details] tab. Note, however, that only Base64-encoded information is displayed in the [Property Screen] and the [Message’s Source Screen]. So, while English signage (e.g., e-mail address) is human-readable, Japanese signage needs to be decoded to be readable (if you want to see what is written on the part(s) of Japanese signage, you can use data compression/decompression utility.

Figure 3: Checking a Sent Mail’s BCC Content (in the case of Outlook Express)
**E-mail Encryption or Attachment Encryption**

In order to send/receive e-mails in a secure manner, you may encrypt your e-mail's body text and attachment.

To encrypt an e-mail's body text and attachments, you need to have dedicated software (e.g., PGP*3) and environment (encryption key) for such encryption. A handy way is to encrypt (password-protect) the attachment by using file encryption software or the encryption function provided by the document creation software in use, or the encryption function provided by data compression/decompression software.

*3) PGP (Pretty Good Privacy) is encryption software developed by a development team lead by an American Philip R. Zimmermann and it is a worldwide standard.

■ An E-mail Encrypted by Using Public Key*4 (Advanced Technique)

If the e-mail recipient is making his public key available to the public, you can use it to encrypt your e-mail. In this case, the encrypted e-mail can only be decrypted with the corresponding private key which is held by the one who published the public key. In short, nobody can see the e-mail's content except the recipient. Generally, free software with PGP function is used by the public, but e-mail encryption software products that use this technique are also available.

Because those products involve key management, they are not commonly used, but they certainly provide a reliable means for e-mail encryption.

*4) Public key is a key for encryption and used together with the corresponding private key. What is encrypted by using a public key can only be decrypted with the corresponding private key.

■ An Encrypted E-mail that Uses Password

If the e-mail's sender and recipient have the same key (password) for encryption, they can use it to encrypt their e-mails and exchange them. Generally, e-mail encryption software that automatically generates symmetric key and password at the time of encryption is available in the market. So, you may use it.
An E-mail whose Attachment is Encrypted

This is not about encrypting the e-mail itself but encrypting its attached document in advance and sending it by e-mail, which is also a handy way.

As for the password for decryption, it is important to let the receiving end know by using a communication method other than e-mail, and as for encrypting documents, you can use commercial software, or cryptographic processing (password protection) which is provided by document creation software (e.g., Office products) or data compression/decompression software.

This method is effective because, even if you sent critical information to a wrong address, it would not result in information leakage unless the recipient knew the password for decryption.

For example, if you are using Microsoft Office 2003 Word, you can encrypt your document as follows:

![Figure 4: Encrypting a File (in the Case of Office 2003 Word)](image)

And, if you are using Microsoft Office 2007/2010 Word, you can encrypt your document as follows:
Figure 5: Encrypting a File (in the Case of Office 2007 Word)

1: The [Office] button
2: Prepare for distribution
3: Encrypt this document
4: Password setting

Figure 6: Encrypting a File (in the Case of Office 2010 Word)

1: File
2: Information
3: Protect this document
4: Encryption by using password
5: Password setting

To open this document, password is required.
Furthermore, if you are using Windows OS, you can password-protect the Zip folder as follows (NB: in this case, the files in the folder are also password-protected):

In every case, unless the user knows their assigned password, he cannot open these document files or the files in the Zip folder.

E-mail encryption is not for preventing wrong transmission but for protecting the e-mail's content in case a wrong transmission takes place. From the security aspect, it serves as a countermeasure against unauthorized access such as e-mail/communication interception, so it is good to try on a routine basis.

Furthermore, encrypting (password-protecting) documents and compressed folders is effective in ensuring secure e-mail exchange (i.e., sending and receiving) and protecting the information on your computer, so, give it a try.

Figure 7: Password Protection for the Zip Folder (Files in the Folder)

In every case, unless the user knows their assigned password, he cannot open these document files or the files in the Zip folder.
2. Secure Settings for Microsoft Outlook Express

Here we explain how to make secure option settings on mailers by taking Microsoft Outlook Express as an example, so that readers can use e-mails in a secure manner. Note that Outlook Express uses Internet Explorer's display function (engine) to display e-mail contents. Therefore, we recommend that you strengthen your Internet Explorer's security settings as well.

What you need to do is, open the [Internet Option Screen], select the [Security] tab and click "Restricted sites", and then set "This zone's security level" to "high". For related items, refer to "Figure 10: Security Option Settings", which is described later.
While the [Option Screen] of Outlook Express is also shown in Figure 1, Figure 9 shows how to open the [Option Screen] by selecting [Tool] -> [Option] on the [Mail Operation Screen].

The [Option Screen] has multiple tabs (See Figure 9), but the tabs on which you need to make basic secure settings are as follows:

- Security (optional)
- Read (optional)
- Send (optional)
(1) Outline of Secure Settings

Here we give the outline of secure settings for Outlook Express.

- Sending/Receiving an E-mail in Text Format

  If you use HTML format for an e-mail's body text, you can make the e-mail's appearance much better. However, in the case of an e-mail in HTML format, an attacker can easily embed a malicious script, and if an e-mail containing such malicious script is opened, an unauthorized process might be executed on that PC against the recipient's will. In order to reduce this threat, it is recommended to receive e-mails only in text format. Furthermore, when you send an e-mail, if you know that the recipient is making the same settings as yours, it is a good manner to send it in text format so that the recipient feels safe.

  Most of spam e-mails and direct mails use HTML format in order to attract recipients' interest. Furthermore, in the past, Outlook Express had security flaws in its preview function concerning HTML e-mails and attachment processing; and there was a case where a PC was infected with a virus only by previewing a doctored e-mail. In order to avoid such risk, it is important to not only disable the preview function, but also send/receive e-mails in text format.

  If you want to make your e-mail decorative, put in writing the information you want to convey, obtain the recipient's consent and send it as an attachment.
(2) Security Options

- For security zone, select "**Restricted site zone**" (Details are described later);
- Check the checkbox "**Issues a warning if other applications attempt to send an –mail by using my name**";
- Check the checkbox "**Do not save or open an attachment that is likely to be a virus**";
- Check the checkbox "**Blocks images and external contents in HTML e-mails**".

**Figure 10: Security Option Settings**
As for the preview function of Outlook Express, let's make the following settings for security reason.

- Uncheck the checkbox "Automatically deploys group message";
- Uncheck the checkbox "Automatically downloads messages that are displayed in the preview window";

Furthermore, it is safe to display e-mails in text format …

- Check the checkbox "Reads all messages in text format".

These settings are effective.
(4) Send Options

First of all, to minimize wrong e-mail transmission …

- Uncheck the item "Immediately send messages";
- Uncheck the item "Add return messages' destination address to the address book";

Furthermore, it is a good manner to send an e-mail in text format …

- Uncheck the checkbox "Send a reply in the same format as the received message";
- For mail transmission format, select "Text format";
- In addition, for news transmission format, select "Text format".

Figure 12: Send Option Settings
If you are using a mailer other than Outlook Express, by referring to the examples of Outlook Express, make security option settings for the mailer.

The impact of this closing statement may be weak, but if you are always aware of security issues and do not fail to take the following daily precautions, you will be able to use e-mails in a secure manner. After all, daily attitude is important …

Daily precautions
- Check regularly for security patches for vulnerabilities in your operating systems and applications and apply them accordingly.
- Constantly monitor viruses by using your antivirus software;
- Do not open e-mails from unknown sources or suspicious e-mails (do not even preview them.)

3. To Protect Oneself against Targeted Attack

🌈 What is Targeted Attack?

Targeted attack is a malicious attack method that takes a shot at a specific organization or individual, mainly through e-mail.

A typical example is: sending a bogus e-mail whose subject or body text contains a topic that seems relevant to the recipient’s job, so that the recipients who are interested in it open its attachment. This type has been confirmed in large numbers.

In the case like this, the attachment can be a computer virus itself or a file in which malicious code that exploits certain vulnerability in an application is embedded. If the recipients execute (open) this attachment, their PC might be infected with the virus or the malicious code executed, and then their PC hijacked or the information stored on their PC leaked.
Here we introduce an e-mail which was used for Targeted Attack.

In this instance, the sender is disguised as IPA and this e-mail was sent to e-mail addresses with government-affiliated domain (go.jp). In fact, its attachment was a doctored PDF file which, if opened by older versions of Adobe Reader, executes malicious code that exploits certain vulnerability in such older versions.

Making recipients trust that e-mail and getting them to open its attachment: this fraudulent technique is so subtle that even security-conscious computer users might be trapped.

Furthermore, having no attachment does not mean that the e-mail is safe. There is also a Targeted Attack in which phishing is carried out via HTML e-mails or an e-mail that contains a phony URL link to a malicious Website, so, be careful.

Figure 13: The E-mail which was Used for Targeted Attack
Precautionary Measures against Targeted Attack

Preventive measures against Targeted Attack that targets enterprises/organizations are:

- Educate employees not to open suspicious e-mails;
- Share the information on suspicious e-mails;
- Ensure proper antivirus software operation;
- Filter out spam e-mails;
- Above all, eliminate OS/software vulnerabilities.

To distinguish suspicious e-mails from benign ones, check if:

- The e-mail is from a company with which you don't regularly exchange e-mails;
- The e-mail is from your organization's executive officer with whom you don't regularly exchange e-mails;
- The e-mail is from a free Web-based e-mail account;
- Bumble-headed Japanese (e.g., wrong Kanji characters) is used for the subject/body text/attachment name of that e-mail;
- A signature (including the division name and phone number) is missing in its body text;
- The e-mail's subject contains words such as "Urgent" apparently, to get recipients to open its attachment;
- The e-mail has an attachment which is not the kind of file you usually receive by e-mail.

Derived from the "Research Report on Countermeasures against Targeted Attack" by JPCERT Coordination Center

IPA set up "Worry-Free Information Security Consultation Service", aiming at actively collecting information about "a suspicious e-mail which is sent to a specific organization to steal its information" and providing information on preventive measures and countermeasures so that real damages can be minimized.
4. Worry-Free Information Security Consultation Service

http://www.ipa.go.jp/security/anshin/ (in Japanese, domestic only)
Consultation service for computer viruses and unauthorized computer access

◆ If you receive any suspicious e-mail, contact the sender's organization, and if it is confirmed that the e-mail was not sent by the organization, contact our "Worry-Free Information Security Consultation Service".
◆ If IPA determines that it needs to investigate the suspicious e-mail in question, the person in charge at the consultation service will inform you of its dedicated e-mail address. In such cases, please send that suspicious e-mail to the address.

- Telephone Consultation Service
For the telephone number of "Worry-Free Information Security Consultation Service", please refer to the Web page below.
http://www.ipa.go.jp/security/anshin/ (in Japanese, domestic only)

NB: "Frequently-Asked Questions (FAQ)" information, which was compiled from what has been consulted by many people, is posted on the above "Worry-Free Information Security Consultation Service" page. So, please refer to it first.

For those having information security-related troubles, IPA provides e-mail consultation service.

E-mail : anshin@ipa.go.jp (in Japanese, domestic only)
NB: The above e-mail address is dedicated for its consultation service. So, even if you send an e-mail with an attachment to this address, the consultation service personnel do not open such attachment for security reason.
(Do not send any Specified Electronic Mail to this address)

When you consult with us about suspicious e-mail, please prepare the answers to the following questions as far as you know, so that we can respond quickly.

(1) When did you receive that e-mail?
(2) What are the sender's organization name and e-mail address? And what was the result of the checking with the sender?
(3) What antivirus software do you use? And what is the detection status (including the name of the viruses detected if any)?
(4) What are the subject, attachment name and body text of that e-mail?
(5) How many people received the same e-mail? And how many of them opened its attachment?
(6) When the attachment was opened, what happened?
(7) In reality, what damage was caused?
(8) As for the operating system and applications on the infected PC, what are their versions?
(9) Do you mind if we forward this e-mail to a security software vendor?
5. Reference Information

- If Leaked, it Would Lead to a Serious Problem! Personal Information
- Security Settings for the Secure Use of E-mails
- Worry-Free Information Security Consultation Service
- Investigative research on Recent Targeted Attack - Research Report -
- Research Report on Countermeasures against Targeted Attack
  (JPCERT Coordination Center)
- Information Security White Paper 2011
  (in Japanese)
- This month’s reminder
  □ A new virus that spreads via a variety of routes (e.g., unsolicited e-mail)
    emerged!
  □ As for unfamiliar e-mails, do not open them out of curiosity and discard
    them immediately!
    A variety of damages that begin with unsolicited e-mails are
    on the rise
  □ Watch out for an e-mail disguising as a public institution!!
  □ What's this? Once you opened it, it would be too late.

IPA Countermeasures Guide Series
http://www.ipa.go.jp/security/antivirus/shiori.html
- IPA Countermeasures Guide Series (1) Countermeasures on Computer Virus
- IPA Countermeasures Guide Series (2) Countermeasures on Spyware
- IPA Countermeasures Guide Series (3) Countermeasures on Bots
- IPA Countermeasures Guide Series (4) Countermeasures on Unauthorized Access
- IPA Countermeasures Guide Series (5) Countermeasures on Information Leakage
- IPA Countermeasures Guide Series (6) Guide for <Avoidance of Risks> When You Use the Internet
- IPA Countermeasures Guide Series (7) Guide for <Avoidance of
Risks> When You Use Electronic Mails

- IPA Countermeasures Guide Series (10) Countermeasures against Targeted Attack Mail <Avoidance of Risks>
Bunkyo Green Court Center Office 16th 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] (Computer Virus and Unauthorized Computer Access)

URL  http://www.ipa.go.jp/security/anshin/  
E-mail  anshin@ipa.go.jp