Outlook Security Update and Elliott Mass Email

Introduction

In recent years, there have been major Email virus outbreaks that specifically target the Microsoft Outlook platform. These include I-Love-You and Melissa virus. Hackers who write viruses tend to target the Microsoft Outlook platform simply because it is widely used.

To combat this situation, Microsoft has introduced a security update for Outlook 98/2000 to prevent virus programs from using Outlook to send out Email. For Outlook 2002, the security update is built in. There are various features to this security update. One of the security features that will severely impact Elliott is called "**Simple MAPI Guard**". Simple MAPI is a set of function calls that programmers for Windows can use to send e-mail and access address information. Elliott uses Simple MAPI to send Email.

As a result of this security update, when Elliott tries to send an email, it is considered by Outlook to be a possible "virus" and Outlook will prompt the user to determine if this is OK. If you are trying to send one email, this is annoying, however, it still will work if you answer "yes" to the prompt. On the other hand, if you try to use certain Elliott Mass Email functions to send out hundreds or thousands of emails, this simply will not work. We do not recommend that you install this security update if you intend to use Elliott's Email functions. However, with Outlook 2002, the security update is built in and you have to confront this issue. This document tries to explain what you need to do to solve this security update problem.

Who Will Be Affected?

If you are using either Outlook 2002, or Outlook 98/2000 and have downloaded and installed Microsoft Email Security Update, then you will be affected. If you are using Outlook 97, Outlook Express, GroupWise or another Email package, then you will not be affected.

How Will You Be Affected?

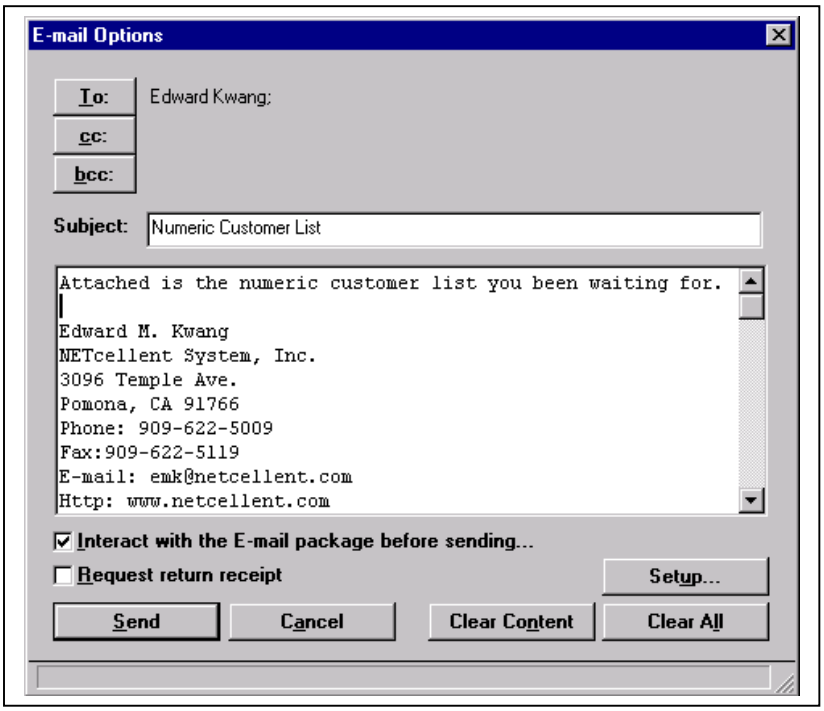
Sending Email through Printing

If you are affected by this security update, when you try to send a printing document as an Email, Outlook will consider this a possible virus and prompt you with the following dialog box:

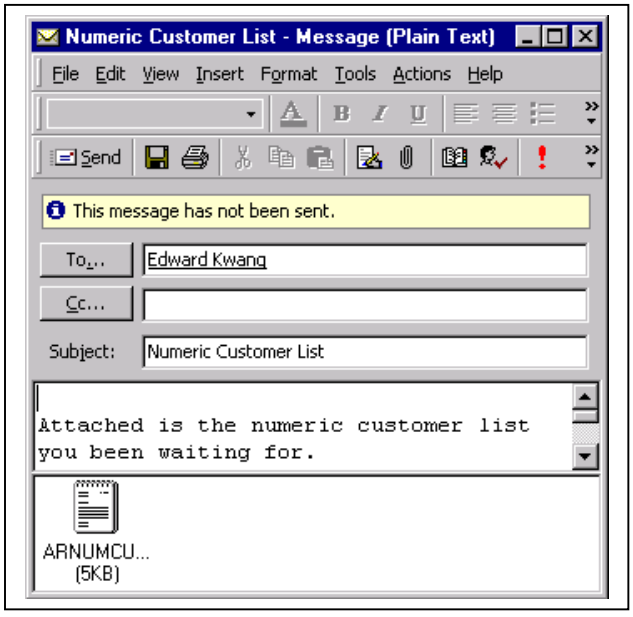
When this message displays, the **Yes** button is disabled for five seconds, and the user can only select **No** or **Help**. After the five-second period is over, the **Yes** button is enabled and the user can click it to allow an email to be sent. If you do not mind waiting for five seconds and manually answer "Yes" to send out your email, you might continue to send out your email this way without taking any action.

Alternative Solution

One alternative to this problem is to check the box "Interact with the E-mail package before sending…"



When you choose **Send**, the Outlook email screen will show up:



At this point, you can simply confirm and send the Email. Since you are now sending email through the Outlook user interface, this email is no longer considered a potential virus and you will not get the annoying message.

Event Handling

In Elliott V7.0, based on users' requests, the system can automatically send out email when certain events take place. The email that is sent out by the event is intended to be a background operation. In most cases, the user is unaware when an event is being triggered and email is sent. After the Outlook security update, the user for sure will know because they will get the following message when the event is sending email:

Also, in many cases, a single Elliott function can trigger many events and many emails. This security update will severely limit the usage of Event Handling in Elliott.

Mass Email in Elliott

There are several Mass Email functions in Elliott V7.0:

- Order Acknowledgement
- Shipping Acknowledgement
- Hold Inventory Purging
- Event Expiration Purging
- Elliott Mass Email Utility

With the exception of Elliott Mass Email Utility, these events are designed to work in the background and have no ability to interact with the Email client. These functions will be severely affected by the security update.

Elliott Mass Email Utility

If you are affected by the security update, then when you use Elliott Mass Email Utility (NW32MSEM.EXE), you might want to consider checking "Interact with email client". By doing so, email recipients will be sent through Outlook as "BCC" (Blind Carbon Copy) addressees. Since the email is sent through Outlook, there will not be a security block.

Also, you may consider using the **Export** function to export email addresses and then import them into Outlook. Then, you can send your emails from Outlook and bypass the security block.

Strategy for Dealing with Security Update

If you need to use any of the Elliott functions that are severely affected by this security update, and the above alternative solutions will not work for you, you should consider the following:

- **Uninstall Security Update** – you may do this if you were using Outlook 98 or 2000. However, with Outlook 2002, the security update is built in.
- **Isolate the running of the affected Elliott functions to a computer** that is not used for a regular user account, secure it physically, and then leave it unprotected by the Outlook Email Security Update.
- **Use the customization tools** to create modified security setting for specific users to allow for functionality that would otherwise be prohibited.

Uninstall Security Update

Outlook 2002

- Removal is not possible. All the security features are integrated into the program.

Outlook 2000

- You must remove Outlook and perform a complete reinstall. If you installed Outlook as part of Office 2000, you must remove Office 2000 completely -- not just the Outlook components -- and reinstall Office. Check the following URL links for more information:
  - http://support.microsoft.com/support/kb/articles/q252/5/66.asp
  - http://support.microsoft.com/support/kb/articles/Q239/9/38.asp
- Interestingly, several people on newsgroups have reported good results from just replacing two Outlook application files with the corresponding files from the original Office CD or Office 2000 SR-1. (SR-1 probably would be better -- you could copy them before you run the SP2 update.) The two files are **Outllib.dll** from the Office folder and **Outllibr.dll** from the Office\1033 folder. This is an unsupported method and probably does not fix all the aspects of the patch, however. It may also cause other problems on your system. Implement at your own risk.

Outlook 98

- Use **Control Panel | Add/Remove Programs** to remove the patch and automatically reinstall the necessary original Outlook 98 components. If you installed Outlook 98 from a CD, it's a quick and painless process. If you installed Outlook 98 via the web, you may have to connect to the Internet to complete the reinstallation process.

Run Elliott Mass Email on an Isolated Computer

On an isolated computer, you will not install the Outlook security update. All of Elliott Mass Email functions are batch oriented and you should be able to run them on an isolated computer without major inconvenience.

This solution will not solve the Elliott Event Handling issue. In order for Event Handling to work properly, every single computer that uses Elliott will need to have the security update problem fixed.

Customizing the Outlook Security Features

If your organization is using Microsoft Outlook with a server that has server-side security, such as Microsoft Exchange Server, you can customize the security update. For example, you can customize the security setting to allow simple MAPI to send Email without the prompt. At the moment of writing, Lotus Development Corporation has agreed to enable this level of customization and Hewlett-Packard Company and Novell, Inc. are currently evaluating implementing the customization capabilities. In cases where you cannot customize the setting, all restrictions enabled in the security update are applied to your Outlook installation.

Microsoft provides administrative tools for the Outlook E-mail Security Update on the Office Resource Kit Web Site. The administrative tools consist of the following three files, packaged into one self-extracting executable:

- **OutlookSecurity.oft** is an Outlook form that enables you to customize security settings on the Microsoft Exchange server.
- **Readme.txt** is a document that provides information on the values and settings available in the template and describes how to deploy the new settings on Exchange Server.
- **Outlk9.adm** is an updated system policy file that is required for client computers that have been set up with system policies.

The administrative tools are available in the Office Resource Kit Toolbox at:
http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#secupd

Implementing Custom Security Settings

Before you begin customizing the settings, you must create an Exchange public folder on an Exchange Server. Customized Outlook security settings are stored in the **Outlook Security Settings** folder, which is a top-level folder in the public folder hierarchy. All organizations that have implemented Exchange Server have public folders, whether they use them or not. To create the Outlook Security Settings folder, create a new folder called **Outlook Security Settings** in the root of the **All Public Folders** folder.

All users can see the Outlook Security Setting folder in the list of public folders and they can open the items that contain the settings. Although users cannot change these settings, there is no way to hide this folder.

Creating Custom Security Settings

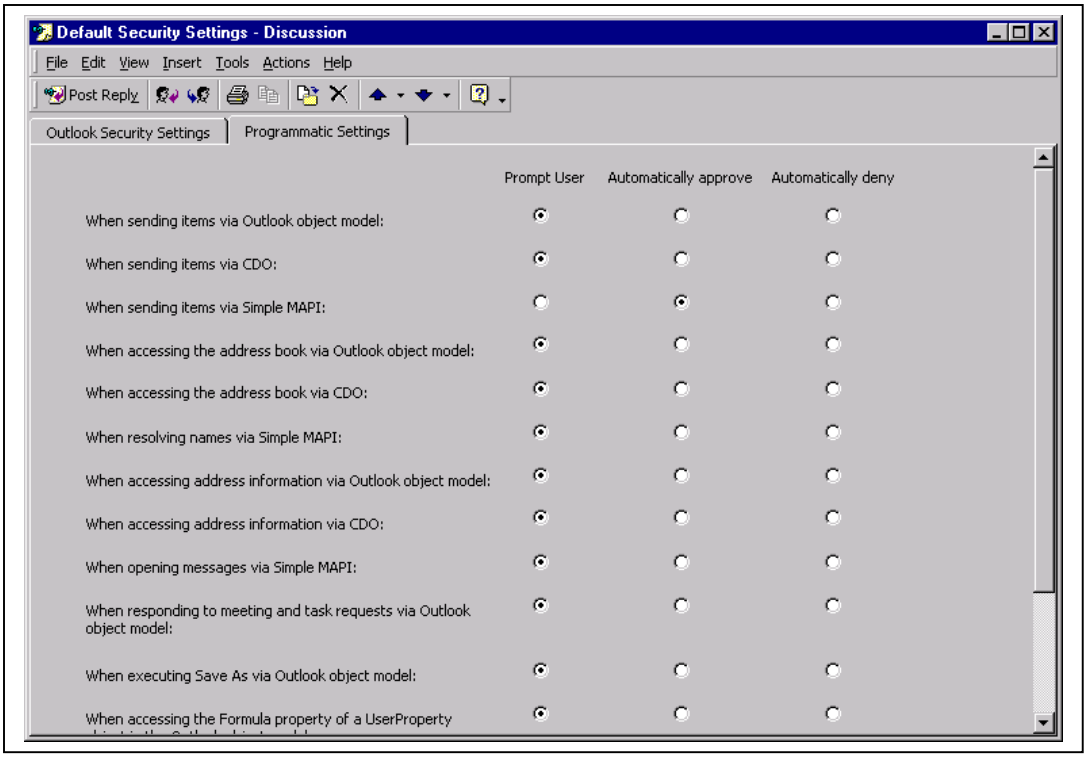
The template (**OutlookSecurity.oft**) can be used to make it easier for you to create custom security settings. Note that the template (OutlookSecurity.oft) is not actually implementing any security. It is simply the storage location for the customized security settings.

To use the template, do the following:

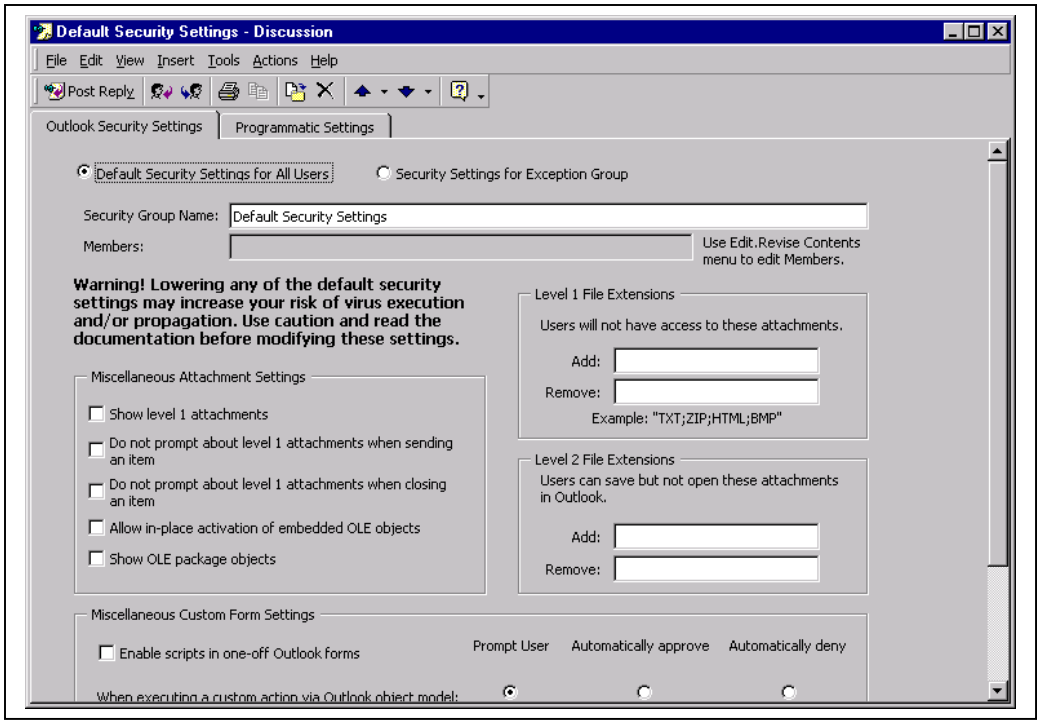
1. On a computer running Outlook, open OutlookSecurity.oft from the file system.
2. When asked to select a folder, select the Outlook Security Settings public folder that you just created. The form will then open in Compose (design) mode.
3. On the Tools menu of the form, point to Forms, and then click Publish Form. (The folder selected should be your current folder, Outlook Security Settings.)
4. In the Form Name box, type "Outlook Security Form".
5. Click the Publish button. The security form is now published in the Security Settings folder.
6. Click the New button to open up a new security form.
7. Create either a default security setting or custom settings for a specific set of users.

Make sure you access Programmatic Settings and change the following setting from "**Prompt User**" to "**Automatically approve**":

When sending items via Simple MAPI



Even though you can customize the security settings user by user, for Elliott's purposes, we only require you to create a default security setting that will be used by all users. Click Default Security Settings for All Users, and then click the Close button.



Since we only open the door for sending Email without allowing the program to lookup Email addresses, we believe this won't compromise the effectiveness in blocking viruses.

Deploying Customized Outlook Email Security Settings To Client Computers

After configuring the security on Exchange Server, you must enable the customized setting for your users. To enable the changed settings, deploy a new registry key to the client computers. How you deploy the registry key depends upon whether or not Microsoft Office was initially deployed with system policies.

- If Office was deployed with system policies, you must change the policies on Exchange Server.

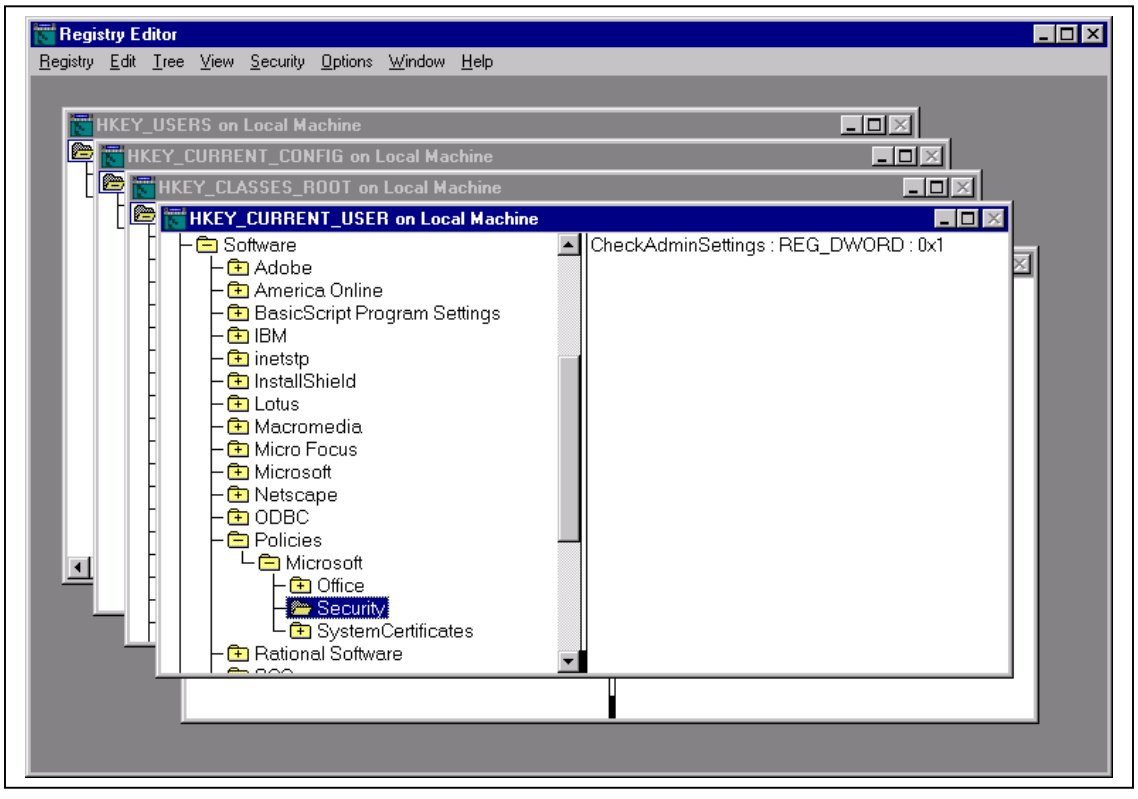
  This involves removing the current ADM file, replacing it with the new one from the download, and then updating the settings. The new ADM file will automatically pass your customized security settings to client computers each time users log onto the system, and enforce these settings.

- If Office was deployed without system policies, you must modify a registry key directly on the client computers. There are many ways of deploying this new key to client computers including using Microsoft System Management Server or adding a command to the user logon script for a sufficient period of time to cover all users.

The registry key holds a DWORD value and is in the following location:

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Security\CheckAdminSettings

You may use regedit.exe or regedt32.exe to add and show this key in registry:



Because the registry key is located in the HKEY_CURRENT_USER\Software\Policies tree of the registry, Outlook respects the new registry key even if you are not using policies. This is a special tree that Office 2000 applications are aware of and that is usually used for system policies. Office 2000 applications all check this section of the registry upon boot, and enforce these settings over any other values the user tries to create for the same item. In other words, the user cannot change this setting through the Outlook user interface. For more information on registry settings and system policies in Office 2000, see the Office Resource Kit.

The following list describes the Outlook behavior for the registry key and its various values:

- **No Key**: Outlook will not check the server for any potential customizations, so the full set of restrictions introduced by the update are applied.
- **Value of 0** (zero): Outlook will not apply customized settings; rather it uses the full set of restrictions as they are designed in the update.
- **Any other value**: Outlook searches for custom administrative settings and applies the settings found in the Outlook Security Settings public folder.

For more information on customizing Outlook security settings, see Customizing the Outlook 98/2000 EMail Security Update at
http://www.microsoft.com/office/ork/2000/journ/outsecupdate.htm

Known Limitation

Delivery Store

Users must use either an Exchange mailbox or an offline folder (OST) to implement custom settings for the Outlook Security Update. Otherwise, the full set of restrictions in the Outlook Security Update is applied. For example, users who have their email delivered to a PST can install the Outlook Security Update, but an administrator cannot customize any of their settings to relax the restriction.

Additional Resources

For more information on Microsoft Outlook 98/2000 security update, refer to the following URL link:
http://www.slipstick.com/outlook/esecup.htm
http://www.microsoft.com/office/ork/2000/journ/outsecupdate.htm

To download the Microsoft Outlook 98/2000 EMail Security Update white paper, refer to the following URL link:
http://www.microsoft.com/office/ork/2000/download/OutSecWP.doc

For more information on customizing Microsoft Outlook 2002 security features, refer to the following URL link:
http://www.microsoft.com/office/ork/xp/four/outg03.htm