

How to Tell If a Microsoft Security-Related Message Is Genuine

Published: September 19, 2003 | Updated: August 10, 2004

Microsoft sends e-mail to subscribers of our security e-mail notification services when we release information about a security software update or security incident.

Unfortunately, malicious individuals have been known to send fake e-mail notifications that appear to be coming from Microsoft, a tactic known as spoofing. Some of these messages lure recipients to Web sites to download malicious code, while others include a file attachment containing a virus.

Learn What to Look For

Fortunately, there are ways to spot the imposters. Here's how to verify that a Microsoft security-related message is legitimate.

The Message Contains No Attachments

We never attach software updates to our security e-mail notifications. Rather, we refer customers to our Web site for complete information on the software update or security incident. Most Microsoft software updates are provided through Microsoft Windows Update, Microsoft Office Update, or the Microsoft Download Center.

The Information Is on Microsoft.com

We never send notices about security updates or incidents until after we publish information about them on our Web site. If you are ever in doubt about the authenticity of a Microsoft security e-mail notification, check the [HYPERLINK "http://www.microsoft.com/security/default.aspx"](http://www.microsoft.com/security/default.aspx) [Security site on Microsoft.com](http://www.microsoft.com/security/default.aspx) to see if the information is listed there.

The URL Is a Valid Microsoft Web Address

If you suspect that an e-mail message is not legitimate, do not click any hyperlinks within it. Those links may be spoofed so that they appear to be sending you to a trusted Web site when they are actually sending you to a malicious Web site. Always cut and paste the text of the link from the e-mail to the address bar on your browser; or better yet, type in the address of the site yourself. If the complete URL is too cumbersome, try using the beginning of the address, such as [HYPERLINK "https://www.microsoft.com/security"](https://www.microsoft.com/security) <https://www.microsoft.com/security>.

However, hackers also have ways to display a fake URL in the address bar of your browser, so even though it may appear you are on a trusted Web site, you may in fact be on a malicious one. To help limit this risk, begin on a Web site's home page and try to navigate to the information you're looking for. The Microsoft security update announcements are

always posted on the Microsoft.com home page.

The Certificate Is Current and Accurate

Microsoft and most commercial Web sites use certificates as part of a system for securing online transactions. Typing **https://** as opposed to the standard **http://** into the Web site address activates the certificate. (Your browser may display an alert that you are about to view pages over a secure connection.)

Once you are on the secure site, Internet Explorer allows you to check the certificate. Double-click the lock icon on the status bar at the bottom of your browser. This displays the security certificate for the site.

```
INCLUDEPICTURE "http://www.microsoft.com/security/images/padlock.jpg" \*  
MERGEFORMATINET
```

Secure site icon. If the lock is closed, then the site has a certificate you can check.

This certificate is proof of the site's identity. When you check the certificate, the name following **Issued to** should match the site you think you are on. If the name is different, you may be on a spoofed site. When you click the lock icon on a Microsoft.com Web page, you can match the **Issued to** domain name (www.microsoft.com) to the Web site domain name in the address bar (also www.microsoft.com).

```
INCLUDEPICTURE "http://www.microsoft.com/security/images/  
Microsoft_certificate.jpg" \* MERGEFORMATINET
```

Do the names match? The **Issued to** domain name should match the domain name in the browser address bar.

Links in authentic Microsoft security e-mail notifications use secure Web site addresses. This allows you to check the certificate to confirm that you are indeed on Microsoft.com and not on a spoofed site.

Example of a Fake Bulletin

Counterfeit security communications can appear quite convincing, as was the case with the fraudulent e-mail that was used to distribute the Swen worm. Its professional appearance and sincere, helpful tone tricked many users into infecting their own computers.

```
INCLUDEPICTURE "http://www.microsoft.com/security/images/bulletin_spoof.jpg" \*  
MERGEFORMATINET
```

Fake bulletin. Many users thought this e-mail notice looked good enough to be a real Microsoft message. It wasn't.

If you have not signed up for any security communications from Microsoft and you receive an unexpected message about a security update, you should treat the message with great caution. When in doubt, delete the message and immediately check the Microsoft.com home

page for the same information.

Update Your Software

One of the best ways to help protect against malicious Web sites and hackers is to keep your programs and antivirus software up to date. Microsoft updates are available at the following locations:

Scan for critical Windows updates: HYPERLINK "http://windowsupdate.microsoft.com/" <http://windowsupdate.microsoft.com/>

Scan for needed Office updates: HYPERLINK "http://office.microsoft.com/officeupdate/" <http://office.microsoft.com/officeupdate/>

Scan for updates to other Microsoft Products: HYPERLINK "http://www.microsoft.com/downloads/search.asp" [http://www.microsoft.com/downloads/search.asp?](http://www.microsoft.com/downloads/search.asp)