

## Fake Critical Updates From Microsoft...

**Summary:** Emails that look like a critical update from Microsoft are scams. We'll look at exactly what makes the scam obvious.

*I recently received a "Critical Update" notification for Microsoft Outlook / Outlook Express in my email. I'd not gotten these before, so I wanted to double check. What should I do?*

Delete that email immediately, and ignore any more copies you'll likely get. **DO NOT CLICK ON ANY LINK IN IT!!!**

Malware authors are constantly looking for ways to fool us into clicking on their links. Since I also got the same email, I'll use it as an example of what to look for.

Here's the email in question:

From: "Microsoft Customer Support" <no-reply@microsoft.com>  
Subject: Microsoft has released an update for Microsoft Outlook

Critical Update

Update for Microsoft Outlook / Outlook Express (KB910721)

### Brief Description

Microsoft has released an update for Microsoft Outlook / Outlook Express. This update is critical and provides you with the latest version of the Microsoft Outlook / Outlook Express and offers the highest levels of stability and [security](#).

### Instructions

- To install Update for Microsoft Outlook / Outlook Express (KB910721) please visit [Microsoft Update](#) Center:  
<http://update.microsoft.com/microsoftofficeupdate/isapdl/default.aspx?ln=en-us&id=4073213066266196307501839191291857099795707196499436900323714412165512>

### Quick Details

- File Name: officexp-KB910721-FullFile-ENU.exe
- Version: 1.4
- Date Published: Mon, 22 Jun 2009 15:17:14 -0500
- Language: English
- File Size: 81 KB

### System Requirements

- **Supported Operating Systems:** Windows 2000; Windows 98; Windows ME; Windows NT; Windows Server 2003; Windows XP; [Windows Vista](#)
- **This update applies to the following product:** Microsoft Outlook / Outlook Express

[Contact Us](#)

© 2009 Microsoft Corporation. All rights reserved. [Contact Us](#) | [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

## Here's the problem:

### It's Totally Bogus

*"What scam artists have done is create an email that looks as much as possible like an official email from Microsoft."*

That link that looks like it goes to "http://update.microsoft.com/..."? In the email it looks like that, but if you click on it your browser will really go to "http://update.microsoft.com.ilkihi.com/...". See how there's an extra domain in the URL that's not in the URL that you click on?

That's the single biggest clue that this is a scam. Click on it, and you'll likely get a virus instantly, or be the victim of some other kind of scam - particularly if you accept and install the download.

What scam artists have done is create an email that looks as much as possible like an official email from Microsoft. They've probably even copy/pasted from a real Microsoft email or web page to get the look and feel just right. Many of the other links in that email might happen to be correct, and take you to the corresponding page on Microsoft's web site. That's even a legitimate Knowledgebase identifier, though the real article has nothing to do with what the email claims.

What they're counting on is enough people blindly assuming that the email is legitimate, and clicking on the download link because they think they need this "update".

How do you protect yourself?

- Realize that Microsoft **never** distributes updates via email. Not as an attachment, and not even as instructions to download.
- **Never** click on links in email that you didn't expect, or aren't 100% certain about. Never. Remember, even the technique of hovering over a link to see where it "really" goes can also many times be spoofed - you can't trust even that.
- **Always** keep your machine up to date. If it's updates you want, then enable Windows Automatic Updates, or visit Windows Update yourself. It's also a great way to check out the legitimacy of emails like this: if you visit Windows Update, you'll be notified there if you do indeed need some update.

I'm seeing this scam more and more often, so please - be careful, and watch where you click.