## David Heavrin-Brown

**From:** "David Heavrin-Brown" <info@heavrinbrown.com>
**To:** <info@heavrinbrown.com>
**Sent:** Saturday, June 04, 2005 3:07 AM
**Subject:** Wisdom from your Webmaster



# *Wisdom from your Webmaster*

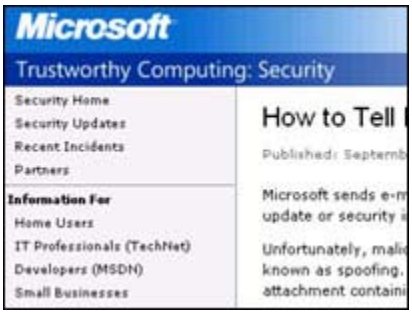
*04 June 2005*

**Dear David,**

It is important for me to keep you apprised of information that is crucial to performing business online in a safe and productive manner. So, I have created this newsletter, that I will publish occasionally, to inform you of issues that I feel are important in your day-to-day dealings on the internet.

## Microsoft Critical Upgrade Spoof

**A bogus e-mail campaign, designed to fool users into installing an attachment containing a virus, is making the rounds.**




An e-mail circulating the internet right now appears to come from Microsoft letting you know that you need to install the attached update to your Windows software. The problem is that the e-mail is not from Microsoft and the attachment is actually a virus. (See a PDF of the actual e-mail I received.)

Counterfeit security communications can appear quite convincing, as is the case with the current fraudulent e-mail that is being used to distribute the "Worm.Gibe.F" virus. Its professional appearance and sincere, helpful tone attempt to trick users into infecting their own computers.

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, do not run the attachment and immediately check the Microsoft.com home page for the same information.

If you cannot find information about the security upgrade mentioned in the e-mail on the Microsoft site, they should be suspicious of the message and delete it.

**STAYING SAFE ONLINE**

- Install anti-virus software
- Keep your anti-virus software up to date
- Install a personal firewall
- Use Windows updates to patch security holes
- Do not open e-mail messages that look suspicious
- Do not click on e-mail attachments you were not expecting

Those clients that have followed our advice and have their site hosting and mail service through AWS Hosting, will find that the virus protection service installed on the servers will kill such attachments before they ever arrive in your mailbox. Rather than receiving the attachment, I received the following message:

```
This is a message from the MailScanner E-Mail
Virus Protection Service
-----------------------------------------------
The original e-mail attachment "Install775.exe"
was believed to be infected by a virus and has
been replaced by this warning message.

At Mon May 30 17:56:47 2005 the virus scanner said:
   ClamAV: Install775.exe contains Worm.Gibe.F
   MailScanner: Executable DOS/Windows programs
   are dangerous in email (Install775.exe)
```

This message lets you know that the virus-containing file has been stripped away and discarded for your safety.

Another way to tell if the e-mail you're looking at is authentic is to check the header information. In Outlook Express you can do this by going to *FILE* | *PROPERTIES* | *DETAILS*. Here you will see information that looks like this:

```
Return-Path: sunbos@f4.dion.ne.jp
Delivered-To: dave@heavrinbrown.com
X-Apparently-From: sunbos@f4.dion.ne.jp
Received: 18 May 2005 01:47:49 -0000
Received: from xlztznnj (K115047.ppp.dion.ne.jp
[211.18.115.47]) by dsmtp3.dion.ne.jp
Date: Wed, 18 May 2005 09:54:36 +0900 (JST)
FROM: "Microsoft Public Bulletin"
[cemrpypfr_fehhdokr@bulletin.com]
TO: "Customer" [customer.kgczxjkwf@bulletin.com]
SUBJECT: Critical Upgrade
```

Note that the "Return-Path" and the "X-Apparently-From" addresses are from Japan (the ".jp" suffix) and that the "FROM" and "TO" addresses are from a domain named "bulletin.com". These are dead give-aways of a fraudulent e-mail. Had this been authentic the "Return-Path" and the "X-Apparently-From" addresses would have shown a microsoft.com domain address. Also, the "FROM" would have indicated microsoft.com and the "TO" would have been my address. Not the fake ones that are showing here.

Remember, it's good practice to always think before you click when there's any

question in your mind about an e-mail. Safe is always preferable to sorry. *We at Heavrin-Brown Consultants are here to answer any questions you might have... no matter how large or small.* ***YOU*** *are the reason we are here.*

All the best,

David Heavrin-Brown
Heavrin-Brown Consultants

email: dave@heavrinbrown.com
phone: 734.327.4125
web: http://www.heavrinbrown.com