



# ANSWER QUEST TIP SHEET

WE ANSWER YOUR TECHNOLOGY QUESTIONS

BI-MONTHLY NEWSLETTER

AUGUST 2001

## Lions and Tigers and Viruses, OH MY!

Normally, topics aren't repeated in this newsletter but with all the new and improved viruses out there, I thought it's time we talk about it again.

### Virus Protection!

Yes, everyone (that includes you -- at home, at work) should have some sort of Virus Protection on your computer. If you have access to the Internet, you had BETTER have virus protection! If you don't have Internet access, don't feel totally safe yet. All it takes to get a virus is by reading an infected floppy diskette on your PC.

"I would never open up a file that has a virus!" But what if you didn't know it was a virus? Here's how they get you to open those files:

This is one trick

-- Add an extension to the file

You probably know that files ending with .GIF and .JPG are picture files. These are safe; you cannot embed a virus into them.

But what if they sneak on the real file extension of .vbs? The file you are now opening is called cutebaby.GIF.vbs and not cutebaby.GIF.

They use this little trick presuming that you won't notice that they have actually named the file .GIF.vbs. What they are doing is hoping you just see the .GIF or .JPG and not realize it has the little, innocent-looking "real" extension of .vbs (this stands for visual basic script). Any file ending with .vbs is actually a script that, when opened, starts to run a small program.

The problem is, in this case, this little program can be very dangerous. It can do anything from just flashing up HI! on your screen to completely erasing your entire hard drive to mailing itself out to everyone you have in your e-mail address book to giving the person who wrote the virus complete access to your computer! Scary, huh?

Here's another trick (and this one is very new and the delivery of it to your PC is totally new)

-- Embed a virus into a .PDF file

"You can't embed a virus in a .PDF file." Yep that's what I thought. Go on, check out the following URL from McAfee's website (one popular version of Virus Protection software).

---

You are receiving this newsletter because either you requested it or someone you know forwarded this newsletter to you. If you would like to discontinue receiving the Answer Quest Tip Sheet, please call (410) 538-3698 or email [aqtnews@answerquest.com](mailto:aqtnews@answerquest.com)

I'll wait.

[http://vil.mcafee.com/dispVirus.asp?virus\\_k=99179&](http://vil.mcafee.com/dispVirus.asp?virus_k=99179&)

Need more proof? Go to this URL from Norton's website (another popular version of Virus Protection software).

<http://www.symantec.com/avcenter/venc/data/vbs.peachypdf@mm.html>

For those who don't know, any file with .PDF as the extension is a read-only document that was created with Adobe's Acrobat writer program. You can download the Adobe's Acrobat Reader for free (<http://www.adobe.com/support/downloads/main.html>) but you must purchase the writer program.

Here's the good part. Since most people do not own the writer program, this means it will not be wide spread because it can only be activated if you have the writer program installed. The majority of people only have the free reader program.

This virus was just found on August 7, 2001 -- that's just last week. I guess someone must have had some spare time during their summer vacation.

This virus takes a harmless attachment that was being circulated and decided to put it into a .PDF file and turn it into a virus carrier. I'm sure they were hoping that people wouldn't notice it went from being a .JPG attachment to a .PDF attachment. Even if you have the writer program, it won't activate the virus part of the .PDF until you click on the picture when prompted.

Okay, so that's two ways of getting a virus on your computer. How about this old trick:

-- Embed a virus into an executable file (for example, .BAT, .COM, .EXE, .LNK, .PIF)

and what about

-- Embed a virus into a document (for example, Word documents - .DOC or Excel documents - .XLS)

and then there's also

-- Embed a virus in a web page (for example .HTML or .HTM)

Are you convinced yet? See why it is now a MUST to have Virus Protection software on all of your computers?

Have you heard about the SirCam virus? This is directly from McAfee's website describing SirCam ([http://vil.mcafee.com/dispVirus.asp?virus\\_k=99141&](http://vil.mcafee.com/dispVirus.asp?virus_k=99141&)):

*"A list of .GIF, .JPG, .JPEG, .MPEG, .MOV, .MPG, .PDF, .PNG, .PS, and .ZIP files in the MY DOCUMENTS folder is saved to the file SCD.DLL (the 2nd character of the name appears to be random) in the SYSTEM directory. E-mail addresses are gathered from the Windows Address Book and temporary Internet cached pages and saved to the file SCD1.DLL (the 2nd and 3rd character of the name appears to be random) in the SYSTEM directory.*

*The worm prepends a copy of the files that are named in the SCD.DLL file and attaches this copy to the email messages that it sends via a built in for communicating directly with an SMTP server, using one of the following extensions: .BAT, .COM, .EXE, .LNK, .PIF. This results in attachment names having double-extensions.*

*Aside from e-mail overloading, it might delete files on 16 October and/or fill up harddisk space by adding text entries over & over again to a sircam recycle bin file."*

So what do I recommend? There are quite a few Virus Protection programs you can buy. I recommend Norton's Anti-Virus and McAfee's Anti-Virus. Yes, there are some free and shareware (low cost) versions out there, but the most important thing you want be sure of with any of the Virus Protection programs is that they are continually updating their list of virus signatures and are available for you to download at any time.

By the way, have I mentioned that you need to download these virus signature files at least once a month? Oh, you thought you just buy the software, install it and you are finished? NO WAY!

You must download the updated virus signature file from the manufacturer's website. If you don't, you will not be protected from newer viruses. You'll, only be protected from viruses that had been discovered before the date of your last download.

Here's your homework.

Right now, this very minute, everyone should download the latest version of these files. Both McAfee (<http://download.mcafee.com/updates/updates.asp?>) and Norton (<http://www.symantec.com/avcenter/>) have updated virus signature files dated within the last week.

Happy Virus Killing!



Call Answer Quest when you  
need that extra help to get  
your software  
working FOR YOU!

**Answer Quest Technologies is your Total Solutions Provider:  
On-site software training (groups or one-on-one), Technical Writing, Programming,  
Web Development, Technical Services, and Technology Solutions for Small Businesses**

**Need a training facility, call us!**

Copyright © 1998-2001 Answer Quest Technology, Inc. and/or its suppliers, P.O. Box 43494, Baltimore, MD 21236 U.S.A. All rights reserved.

TRADEMARKS. Answer Quest and/or other Answer Quest products referenced herein are either trademarks or registered trademarks of Answer Quest. Other product and company names mentioned herein may be the trademarks or registered trademarks of their respective owners. Trademarked names appear throughout this newsletter. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademark name, Answer Quest states that it is using the names for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon the trademark.