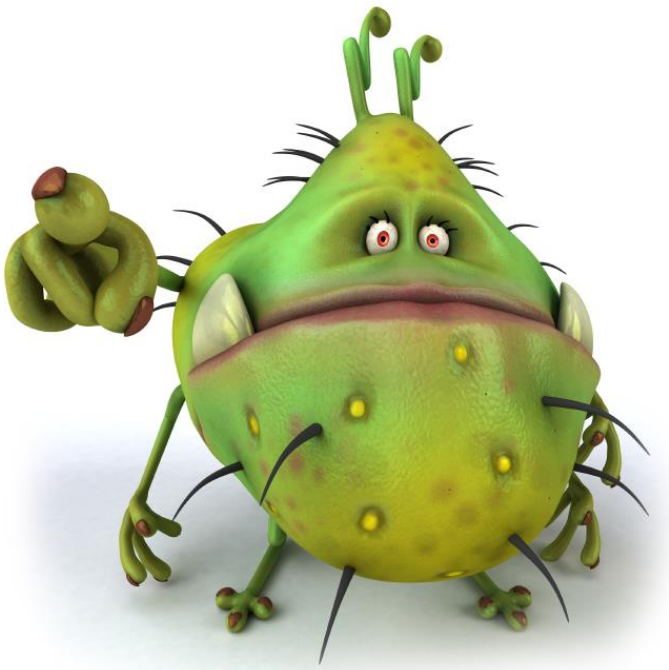


Spotting Email Viruses

SPOTTING VIRUSES

EMAIL BASED VIRUSES

The Problem with Viruses

by Frank Paolino, MayFlower Software

Lately, with the outbreak of CryptoLocker, we have seen a new level of viruses, called "ransom ware" where they lock all of your files on your machine, all of your Word docs and Excel spreadsheets, and you must pay a ransom for the unlock key.

The increase in recent Virus activity has been noticeable, and the sophisticated techniques the virus makers use to evade detection make the job of stopping them that much more challenging.

Many times, a new message appears and I ask "Is this some new attempt to get me to infect my machine"?

Many of my customers ask me the same question, so I put a live stream of recently caught viruses subjects and attachment names on our website at www.maysoft.com. Obviously, I did not put the viruses, just their names.

Viruses are often spread via email the same way spam is spread. The big difference is that the virus wants to steal from you without you knowing in most cases.

Viruses want data on your machine, or they want to make your machine into a "zombie" to send out more spam and viruses to others.

The problem with viruses is that they masquerade as something you want to open by either promising you something you want or scaring you with something you fear.

Most do their work silently. After all, a thief wants to take what they can without you knowing, or you might attempt to stop them.

This short guide explains some of the ways to spot a virus. There are lots of different approaches, and those of us who work stopping these viruses have to be careful or we can infect our own machines (something I have unfortunately done).

I cannot list every tactic, mostly because they change every day. But reading this guide will make you stop and think and possibly delay before opening any attachment, then it will have raised your awareness of this problem.

Good luck, and don't open that attachment!

Scare Me

The "Scare Me" virus wants you to panic and in your panic rush to open an attachment to "fix" the problem, or find out more details.

Yes, the titles of many of these mail messages appear scary and that is what the senders of the email want, to scare you into opening the message and reading the body, then launching the phony "notice".

There are many flavors of this, but here are a few to give you an idea:

Illegal Software Use

Important – Payment Overdue

Judicial Summons

VISA – Recent Transaction Report

Your FED TAX payment (ID : 87VIRS8xxx) was Rejected

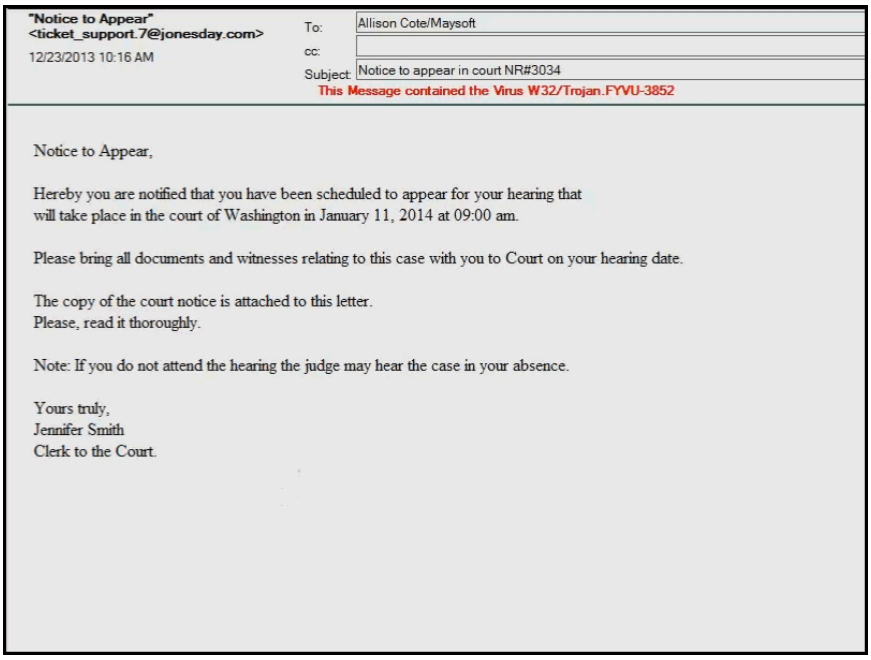
ATTN: Important Bank Documents

Department of Treasury Notice of Outstanding Obligation

FW : DNB Complaint

Order #NR7688 is processed

Notice to Appear In Court


"Notice to Appear"
<ticket_support.7@jonesday.com>
12/23/2013 10:16 AM

To: Allison Cote/Maysoft
cc:
Subject: Notice to appear in court NR#3034
This Message contained the Virus W32/Trojan.FYVU-3852

Notice to Appear,

Hereby you are notified that you have been scheduled to appear for your hearing that will take place in the court of Washington in January 11, 2014 at 09:00 am.

Please bring all documents and witnesses relating to this case with you to Court on your hearing date.

The copy of the court notice is attached to this letter.
Please, read it thoroughly.

Note: If you do not attend the hearing the judge may hear the case in your absence.

Yours truly,
Jennifer Smith
Clerk to the Court.

Here is a sample of a phony notice that appears to come from JonesDay, one of many law firms that were spoofed trying to trick recipients into opening the malware.

Read more about spoofed mail messages here.

TIP

If you are scared by the title, you will be really scared by the damage the virus will inflict if you launch it.

Don't open unknown attachments!

Dear Friend

The "Dear Friend" or any other greeting that does not use your name is a strong indicator that the message is a spam message or if it has an attachment, contains a virus.

TIP

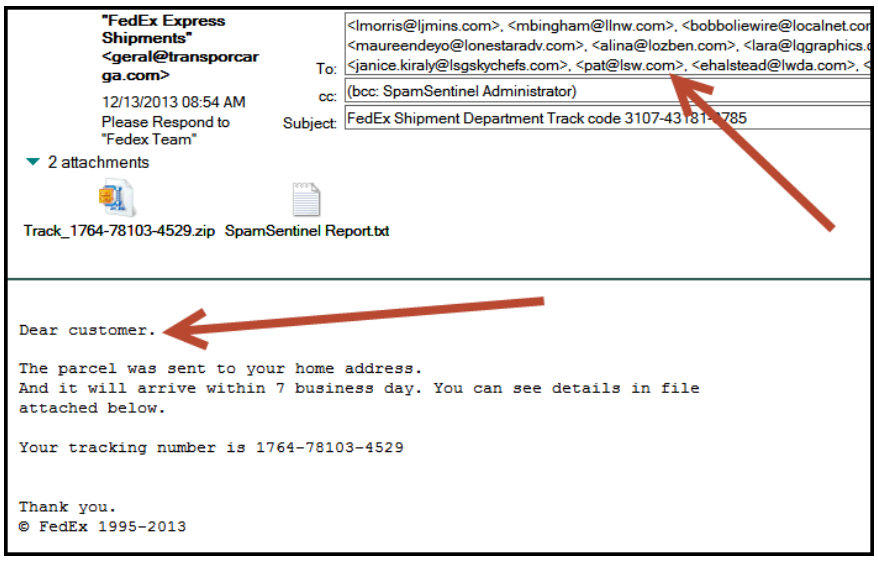
If you don't know the sender, don't open the attachment or click on the links.

Too Many Friends

The "Too Many Friends" is an email that only you should receive, but you find 10, or 20 names in the "To" field, most of whom you do not recognize.

TIP

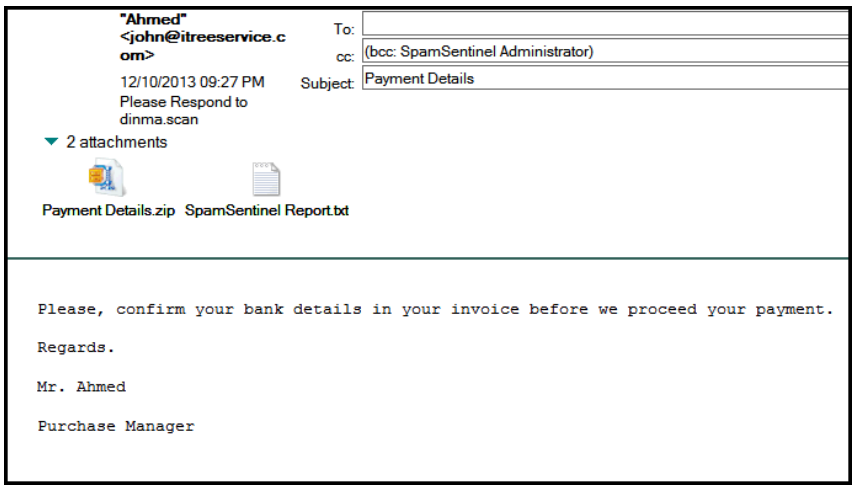
You can have "Too Many Friends" if Viruses are being sent to you.



I Have No Name

The "I Have No Name" is an email that only you should receive, but your name in not in the "To" field. This was probably sent out as a large BCC email.

This most likely has an attachment, and that contains a virus.



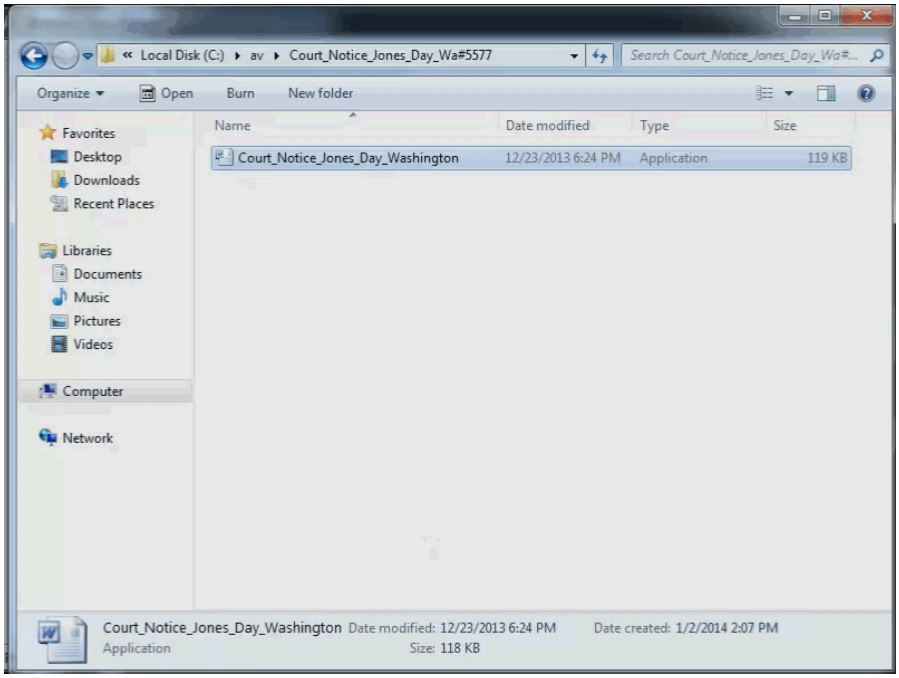
TIP

If it is not addressed to you, don't open it.

Fake Attachments

The "Fake Attachments" pretend to be something safe. Everyone knows (or should know) not to click on and EXE attachment, so many of these are disguised as Word documents or PDF attachments, or a JPG photo.

If strange women are sending "Photos of Me", it is probably NOT your lucky day. In fact, if you open these "photos" they are probably viruses and it is definitely your *unlucky* day.



TIP

If it is inside a ZIP file (or RAR file, another compression format) do NOT open it.

If you are convinced it is a good attachments, detach it to your machine and your anti-virus software might catch it.

Best answer: Send it to IT and infect their machine.

Wrong on So Many Levels

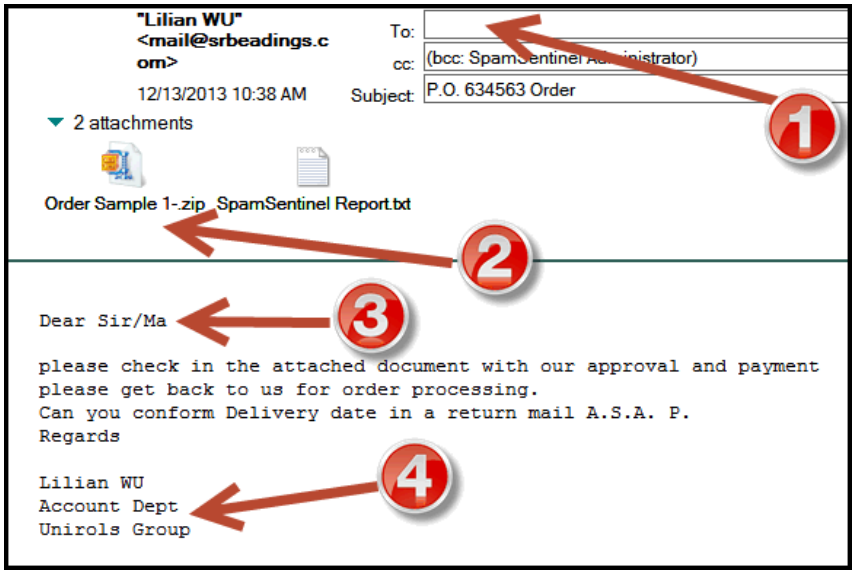
The "Wrong on So Many Levels" breaks all the rules of what NOT to do if you send viruses trying to infect machines.

1. No SendTo

2. Contains a Zip with an EXE inside

3. Not personalized

4. Signature incomplete.



TIP

If you get a "Wrong on So Many Levels", laugh at the virus maker's incompetence and know you are probably having a better day than he is...

...and don't open the attachments.