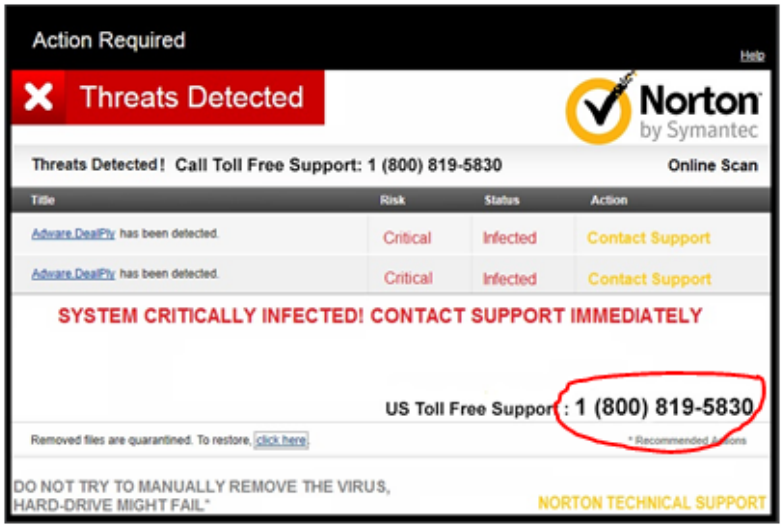
FAKE VIRUS ALERT: WHAT YOU SHOULD KNOW

You've just received this message. Is it the end of the world?

Depending on what you do next, it could be (figuratively speaking of course). The warning message pictured above is **an example of a fake security warning** and it can be quite common to see them as you surf around the internet.

How can you tell if a virus alert is safe? Keep reading:

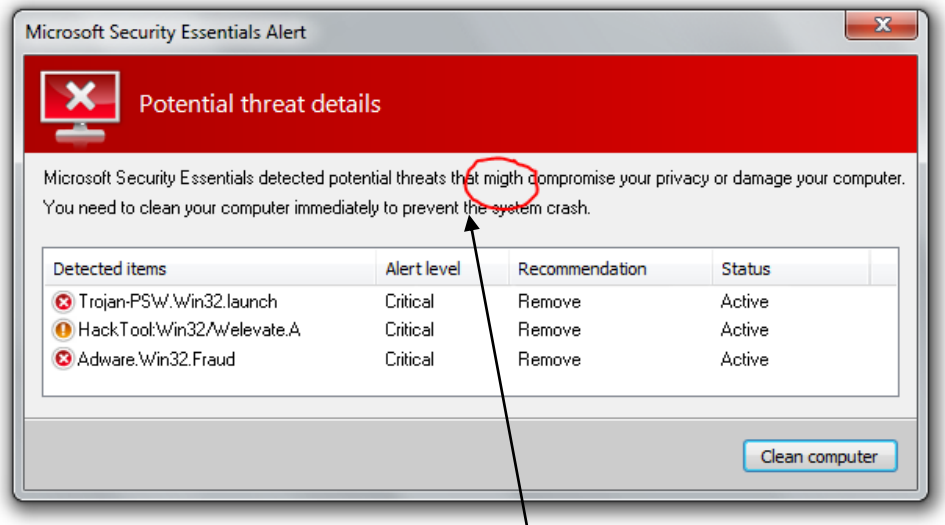
1) HDH uses **Microsoft Endpoint** as its antivirus application. If you see a message from any other source, it is most likely a fake **and potentially dangerous**. Avoid the "Click Here", "OK", etc. buttons on these screens. Malware creators are clever. They can make their alerts look quite convincing and can use what appear to be legitimate sources for their messages (note the "1-800" number – see next item).



2) If you see a “1-800” number on the alert it is a fake. **Calling the number is not recommended**.

3) If you are asked for money, **it is most certainly** a fake. Under no circumstances should you pay the organization for removing a virus.

Other examples of fake virus warnings:



Note the spelling error.

These precautions also apply to your home computer. You should have an antivirus tool running on your computer and it should be receiving regular virus signature updates. If a virus alert message pops up on your screen, stop and carefully examine it. If the message did not come from the antivirus application your are using, then be very suspicious.

IS IT SAFE TO OPEN?

You have just received an email from what appears to be a reputable shipping company (UPS, Purolator, etc.) with the above attachment. You didn't order anything and were not expecting a package to be shipped to you. Should you open the attachment?

The answer is "**no**" and **you should delete the email immediately**. This is just one example of a possible malware source. Many others exist.

A common way to spread viruses is to trick users into opening a file they believe to be legitimate. In cases such as the one above, the file appears to be named "*Shipping Confirmation.zip*". In reality, **the full** filename, **including** its true extension, is **actually** "*Shipping Confirmation.zip**.exe,***" which is **a potentially dangerous** executable file **capable of installing a virus silently on your computer.**

The email system used at HDH does show you the full filename, but other sources such as Gmail, Hotmail, etc. may not. **Extra caution should be used when accessing webmail at work**.

When dealing with email attachments always ask yourself:

1) **Is the email from a trusted source?** If you do not recognize the sender of the email or would have no reason to expect an email from them, **do not open it**.

2) **Are there attachments in this email?** If you do open an email and there is an attachment, use common sense to determine if you should open it or not, e.g., If you did not order anything then you should not have received a shipping confirmation.

3) **What type of attachment is it?** If possible, check the full name of the attachment to determine that it does not contain a**n** ".exe" **in the** file extension.

4) **What else can I do?** Don't trust the antivirus application to do all of the work. None of them is 100% effective when it comes to preventing virus infections from malicious files. **You need to help by being cautious and trying to stop nefarious software before it gets to the antivirus application.**

These guidelines apply to your work PC & your home computer. Viruses can cause a lot of damage. Knowing what to watch means you can stop them before they cause any harm.