SAYRE AREA SCHOOL DISTRICT TECHNOLOGY TIPS
VIRUS PROTECTION BEST PRACTICES

Purpose

This handout is to briefly instruct how protect your SASD PC from computer viruses.

Please read this entire document to ensure that you are following best practices with respect to protecting your PC against a computer virus.

Important Notice - Ransomware

Recently, an increasing number of attempts by cyber criminals to extort organizations by locking computer files and then demanding payment to have them unlocked.

For 2016, these cyber criminals are targeting hospitals and schools.

The following is a sample of how they do it.

This form of extortion is called ransomware. In this particular case the ransomware is called “Locky”. It can be highly disruptive and very difficult to overcome. In reported cases, the bad guys use deceptive emails that have a Microsoft Word document attached.

The email message will contain a subject similar to ATTN: Invoice J-98223146 and a message such as "Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice".

If a victim opens the attachment, the malicious code is executed and locks (encrypts) the files on the machine, including all other drives on this computer for ex: flash drives and network drives. Once this happens, you cannot access any of your files.

KEY POINT: It is critical that you remain vigilant when opening emails and especially email attachments from outside of the organization. If you are not completely sure about the safety of an email or attachment contact the IT department or just delete the email!

What is a virus?

Computer viruses are software programs that were developed to spread from one computer to another and to interfere with normal computer operations.

For example, a virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your PC.

What Virus Protection does SASD Use?

We use a multilevel approach to protection as follows:

1. Each computer and server utilizes ThirtySeven4 as the virus protection software.
2. ProofPoint SPAM system scans all of our email for potential viruses.
3. iBoss Web Filtering filters inappropriate web sites.
4. MS Server data servers block many of the know types of virus files.
5. All USB drives are scanned when inserted into a computer.
6. Multi-tiered backups are in place in order to restore infected data (please note that SASD policy is to save data to our servers for backup).
7. Juniper Firewall is setup to block virus attacks.
8. ACTIVE DIRECTORY: Our network is secured using Microsoft Active Directory. For example, each user has security to his/her personal folders. This ensures that only authorized users have access to their specific work. This security prevents many viruses from rapidly spreading throughout the SASD network.

Are we 100% Protected Against Viruses?

No!

For example, a new virus could be developed that our antivirus vendor does not know about. Additionally many of the new viruses look like antivirus software screens. For example, if you see the following screen appear – you have a virus:

May I Get a Virus from an Email?

Yes!

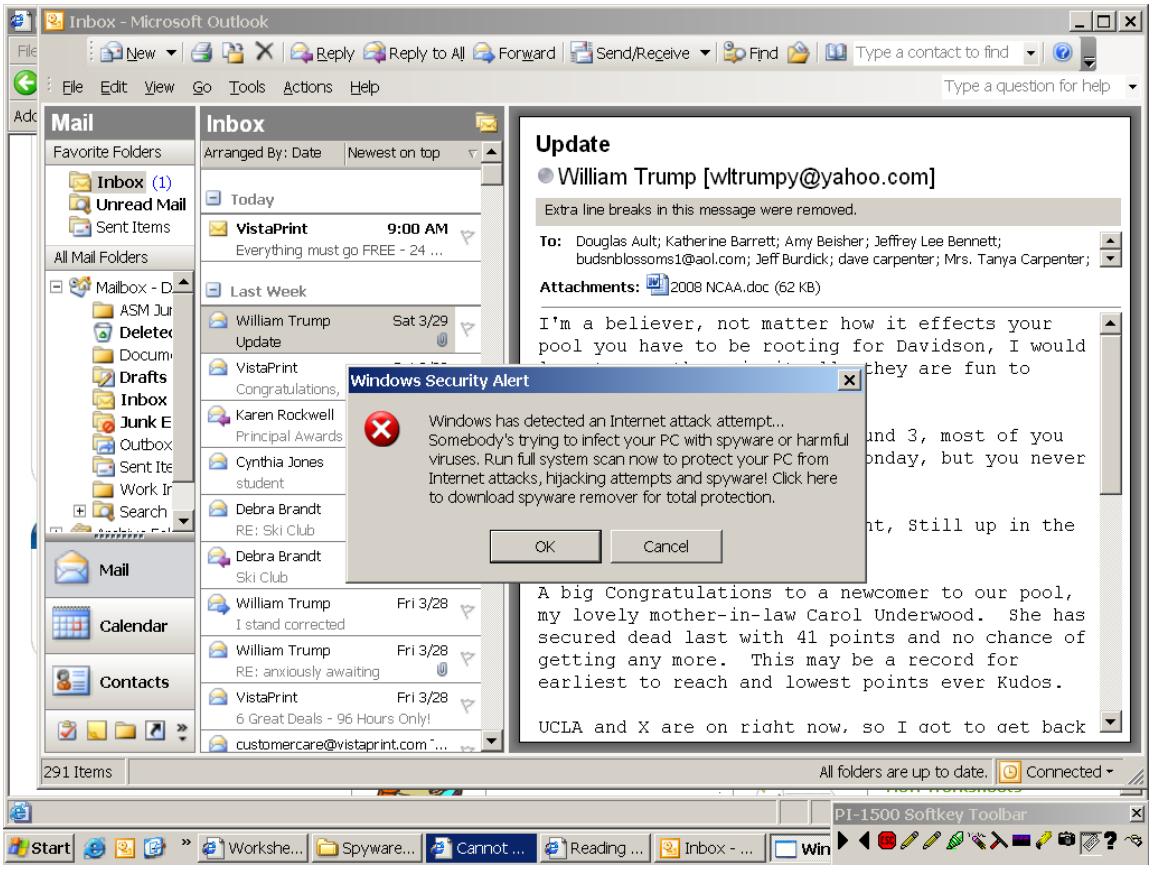
Viruses are easily spread by sending infected attachments in e-mail messages.

That is why it is essential that you never open e-mail attachments unless you know who it's from and you are expecting it. If you receive an email from someone that you do not know, or an email concerning a topic that seems suspicious – please do not open it – just delete it.

Many emails contain viruses that install themselves on your PC and then spread rapidly from your PC to other PCs by attaching itself to email messages that you send out!

If you continue to have a problem with a virus from an email – make sure you notify the Technology Department ASAP by emailing: Group Technology along with the PC Name.

Here is an example of a virus from an Email:



May I Get a Virus from a Web Site?

Yes!

There are many ploys that viruses use. For example, if you go to a web site and it states – "we found a virus on your PC and need you to click on a response to remove it" – it is most likely a virus – in this case shut down your web browser.

If you continue to have a problem with a virus – make sure you notify the Technology Department ASAP by emailing: Group Technology along with the PC Name.

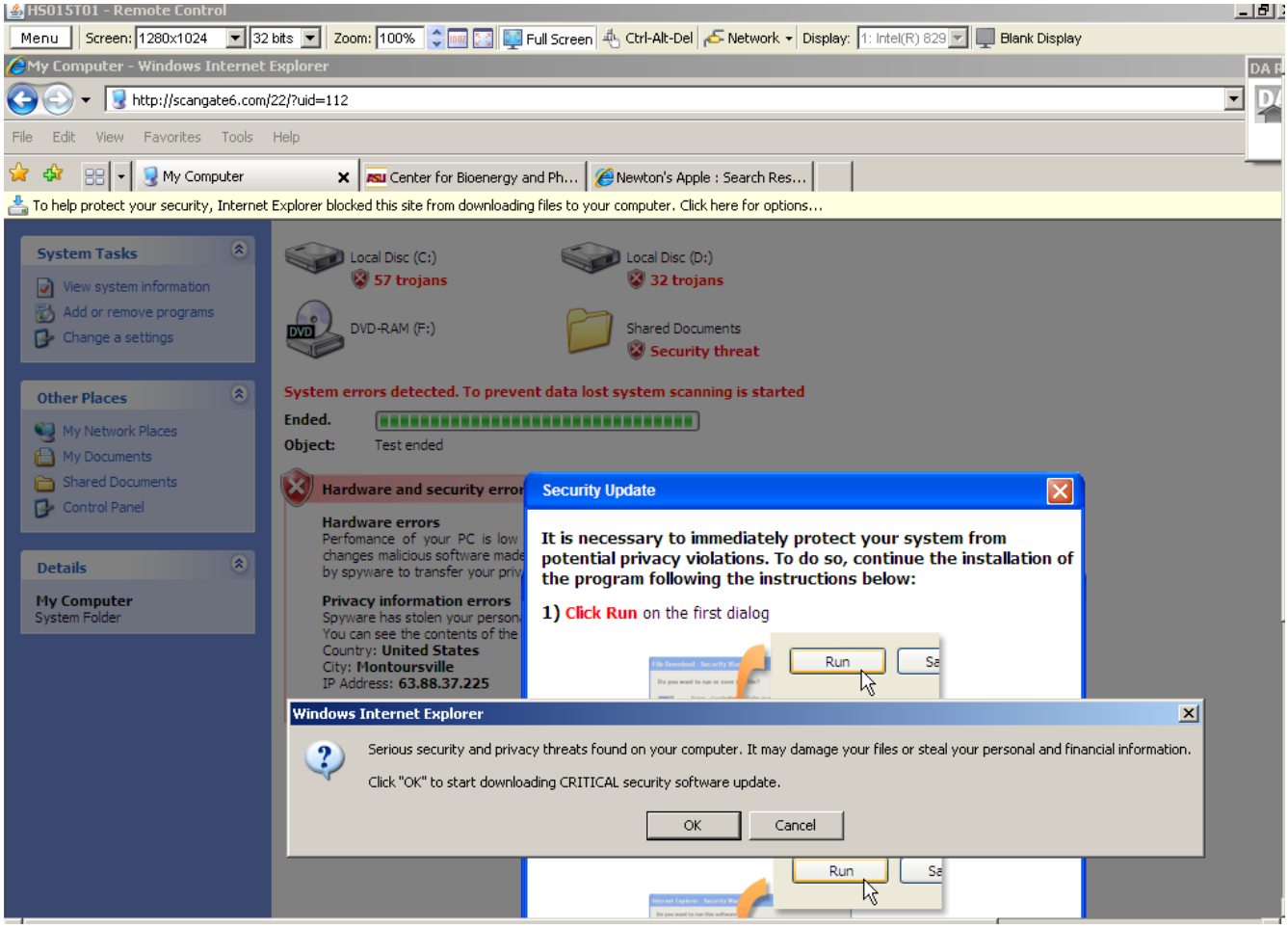


Figure 1 - Sample Virus that looks like an Antivirus Program!