

# UK Extension IT Computer Security

Even a computer is setup with all of the necessary software still requires certain things to keep it running well and keep your data secure. The purpose of this document is to help you prevent loss of personal information, annoying pop-ups, viruses, and other issues your computer faces. The following sections will help you keep your computer fully secure and running at peak efficiency. As usual if you have questions about any of this, feel free to contact the Helpdesk or your DEITC for more information.

## Updating your computer

The first step to keeping your computer secure is to make sure that windows and other important programs are up to date. Microsoft, Apple, and other software companies constantly release updates to fix security holes within their software as well as to add new functionality. Your computer can be setup to install some updates automatically. However, some updates require you to manually install them. Some examples of important updates that need to be run along with their System Tray Icon:

-  Windows update
-  Java
-  Adobe Flash
-  Adobe Acrobat

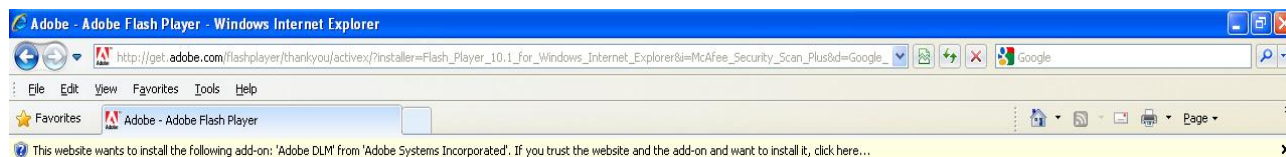
If these programs need to be updated, there should be an icon in the lower right-hand corner of windows; this will be located on the task-bar next to the clock. Clicking on these icons will bring up the update that needs to be run. Unfortunately, some malware will add similar icons to the same area. For this reason it is very important you install only legitimate updates. If you are unsure if an update is legitimate, please contact the Helpdesk or your DEITC **before** running the update.

## Malware

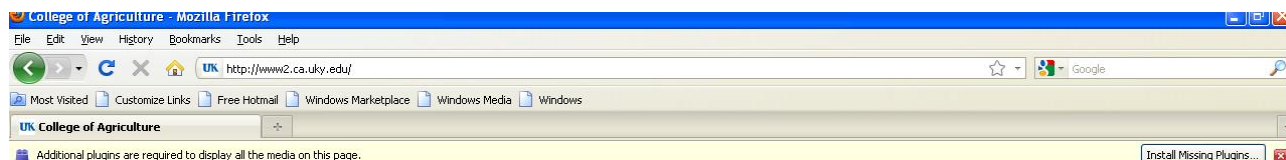
Unfortunately, software exists that may try to infect your machine with harmful software. This software is called malware. Malware can range from harmless and annoying to harmful to your machine or your personal information. There are several different ways that can install itself onto your machine. Some of these ways include browser installation, trojans, or tricking you into running an executable.

*Browser Installation:*

Sometimes while surfing the web, your browser will pop up with a box asking you to install something. In Internet Explorer it looks like:



In Firefox it looks like:



Whenever you see this come up, make sure to look at what it's wanting to install and decide how much you trust this site. This box is here to protect your computer from programs being installed without your knowledge or permission. These aren't always harmful programs, but is one way that you Malware can infect your machine. One rule of thumb, if you are not expecting to install something, do not allow it to install. If you aren't sure what it's wanting to install, don't click the box to install the software and contact your DEITC if you want more information.

### *Trojan:*

A trojan is a program that installs useful software, but at the same time puts something malicious on your machine. So while you may be getting a cool screensaver program, you may also be getting something that causes annoying popups, or worse sends your personal information to a hacker somewhere. Common examples would be screensavers, games, and coupons. Not all free programs contain malware, but whenever you install something that you download from the Internet, you're taking a chance. The best thing to do is only install software from trusted sources. There are many good sources for downloads on the Internet, such as [www.download.com](http://www.download.com), but in this scenario it is best to use your better judgement. If a site feels like the contents may not be completely trustworthy (remember you could be dealing with your own personal information) it is best to not download anything from that site.

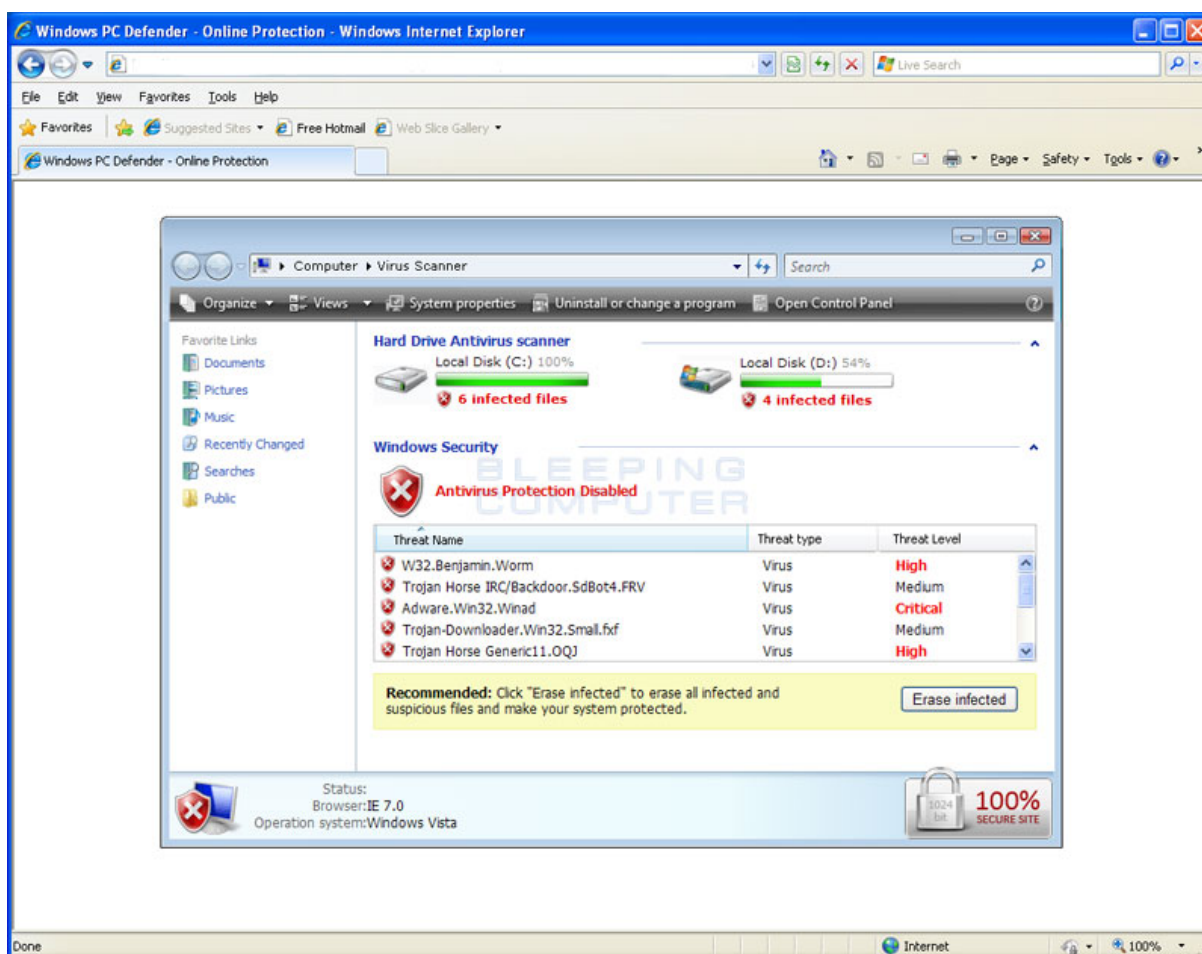
Some programs will include other free programs, that while not technically malware are unwanted and may slow your computer down. If you do install something from the Internet, make sure to read over what it wants to install and uncheck anything that you didn't ask for or don't want.

### *Tricking the User:*

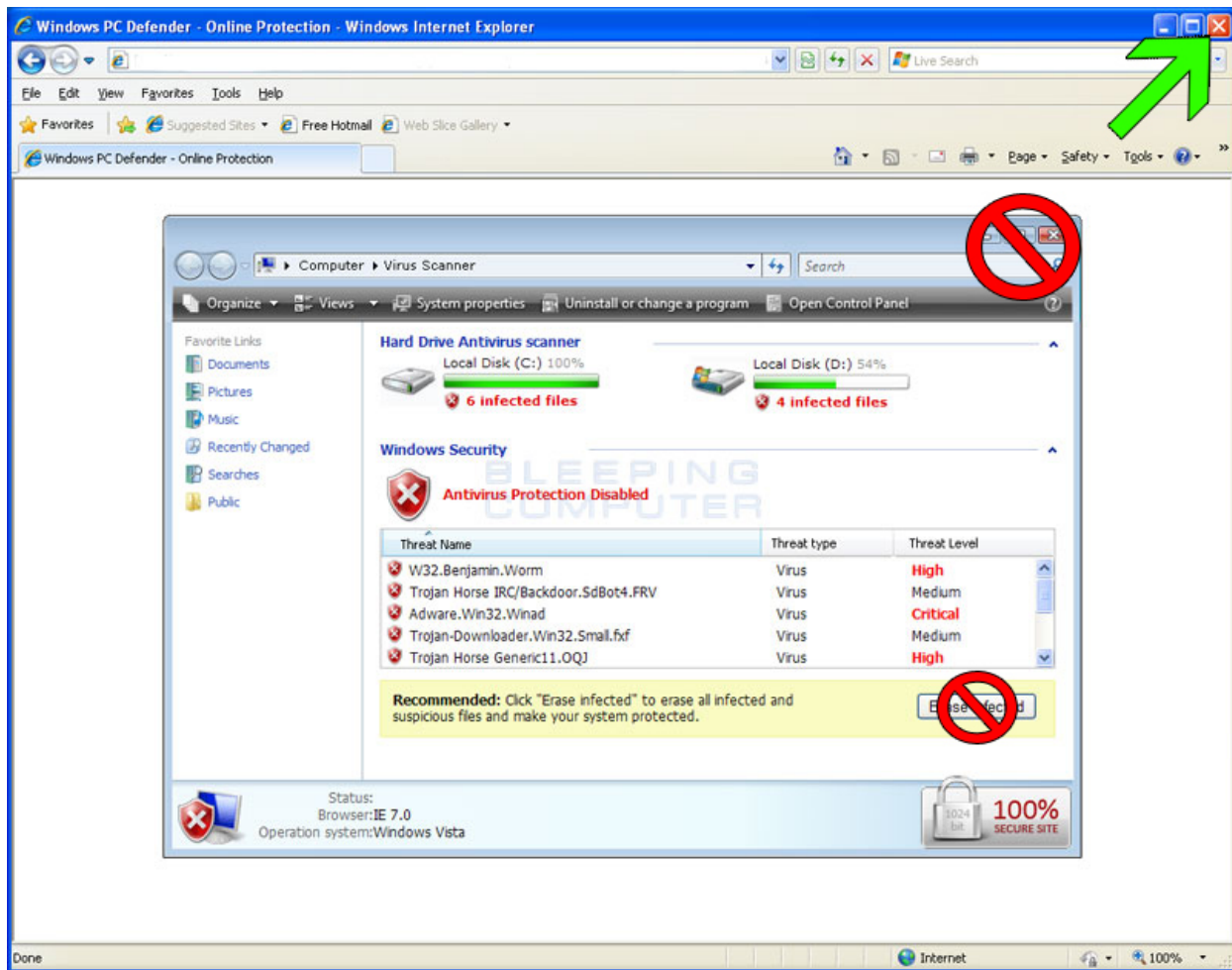
Another common way to get malware on your system is to download something from the Internet and run it. This can be similar to the trojan except that you don't even get something

useful for your troubles. Just because it's labelled goodstuff.exe doesn't mean that the installed program will actually do what they claim it will do. This is much less common than the other methods listed above and is usually found when downloading mp3s, free versions of pay software, or pretty much anything that isn't normally obtainable for free; again use your better judgement. Be careful about what sites you frequent and what sorts of things you are downloading and you should greatly limit your exposure to malware.

Another example of a site trying to trick a user into infecting their computer are fake virus scans. Visiting some websites will cause a pop-up (or sometimes within the same website) that attempt to look like a virus scan. These sites try to get the user to click on something to clean their computer when in fact it does the opposite. Example:



This is not actually your computer performing a scan, it is a fake attempt by this website to try and get you to click. If you click anywhere on here (the "Erase infected" button for instance) you will be **infected**, the opposite of the website leads you to believe. Notice how the screen is actually within Internet Explorer, this is because it is a website *not* a scan. If you see something like this, close your Internet browser immediately - do NOT run the scan, erase or whatever it wants you to do. Also you should not click on the "X" that looks like it is part of "My Computer" instead click the "X" to close your browser, or push ALT+F4 to end the program.



## Safe web browsing

Unfortunately even keeping your system up to date and having anti-virus protection isn't always enough. For this reason, there are a few things that you can do to minimize your risk when browsing the web. First, you may want to use another browser than Internet Explorer. Internet Explorer is the most used web browser and because of that fact more malicious attacks are targeted specifically to Internet Explorer. Firefox, Google Chrome, or Safari are all excellent web browsers that will prevent many attacks simply by not using Internet Explorer.

You can also protect yourself by limiting what sites you go to and what you download. Doing a web search on a topic is a great way to find information, however you never know what type of sites will show up in the results. Using your better judgement again comes into play; there's always a risk that an unknown site may try to infect your machine. If the site is offering free mp3s, screen savers, coupons, or other software, the risk is generally higher than other sites.

Social sites such as Facebook are also popular targets for malware. If you receive a message from someone you don't know asking you to check out their cool video or something similar, you should avoid clicking that link and just delete the message. Be cautious about running any file or

clicking on any link from people that you don't know and it will go a long way towards protecting your computer. It is important to be careful about clicking links that your friends send you as well. Their accounts may have been infected and a hacker can use them to send links out to all of their friends to try and infect others. One clear indication of this type of scam is if the message is only a link, or uses vague language or language your friend wouldn't normally use. For example: "LOL! Check this link out! [www.iwillinfectyourcomputer.com](http://www.iwillinfectyourcomputer.com)" If you are unsure whether or not your friend is actually trying to send you a link, simply ask them.

## Email security

Email is another area where you should be very cautious in terms of security. Email is a very common medium for people to perform scams. Microsoft gives us six signs to spot a scam (<http://www.microsoft.com/protect/fraud/phishing/reduce.aspx>):

1. Generic greetings such as "Dear Customer," which indicate that the sender does not know you and should not be trusted.
2. Alarming or urgent statements that require you to respond immediately.
3. Requests for personal or financial information, such as user names, passwords, credit card or bank account numbers, social security numbers, dates of birth, or other information that can be used to steal your identity.
4. Misspellings and grammatical errors, including Web addresses. The Web address might look very similar to the address of a legitimate business, but with a minor alteration. For example, instead of **www.microsoft.com**, the scammer might use **www.micrsoft.com**.
5. The text of the link in the e-mail message to you is different from the Web address that you are directed to when you click the link. You can identify the actual Web address in a link by hovering over the link without clicking it. The Web address appears in a text box above the link.
6. The "From" line in the original e-mail message to you shows a different Web address than the one that appears when you try to reply to the message.

The next concern is what to do to protect yourself from these scams. The same Microsoft document (<http://www.microsoft.com/protect/fraud/phishing/reduce.aspx>) gives us some advice:

- Delete spam. Do not open it or reply to it. When you reply, you confirm to the senders that they have reached an active e-mail account and make yourself vulnerable to further abuse.
- Use caution when you click links in e-mail messages, text messages, pop-up windows, or instant messages. Instead, type Web addresses in a Web browser.
- Do not open e-mail attachments or click instant message download links unless you know who sent the message and you were expecting the attachment or link. ***(This one is especially important. Many scams will claim to be shipping information from a legitimate source, or something else you may trust in order to get you to download an attachment or click on a link. Unless you know exactly what it is and are expecting the attachment or link DO NOT OPEN IT.)***
- Be cautious about providing your personal or financial information online. Do not fill out

- forms in e-mail messages that ask for personal or financial information.
- Create strong passwords and avoid using the same password for your bank and other important accounts.

As a policy, UK administrators will never ask for your user-name or password. The only email you will receive from UK would be letting you know your password is about to expire. Even this will not ask you to send your password and won't ask you to click on a link; it will not even require a reply. Here is an example of this email:



**---ATTENTION!---ATTENTION!---ATTENTION!---**

The password for link blue account **username** ('Lastname, Firstname') will expire in 10 days.

Please change it as soon as possible. Instructions are below.

Thank you,  
Administrator

If you have specific instructions for changing your password, please follow them.

If your computer is in either the AD or MC domain and you are logged on as a domain user, please use "Ctl-Alt-Del" and select "change password".

If your computer is not in the domain, please navigate to the University of Kentucky Home Page and click the "link blue" link. From that link blue page, select the "Account Manager" link, then the "Manage Your Account" link, log in with your current password, and then click the "Change Password" link.

**Note: This message does not contain any links and it does not ask you to reveal your password. If you receive any messages that contain links or asks you to enter or e-mail your password, the message is not a valid request and you should never click on any of the links, or reveal your password to anyone via a web page, e-mail or telephone.**

You can obtain additional information by navigating to the University of Kentucky Home Page and clicking the "link blue" item.

To change your password please see the password section of this handout.

As always if you have any questions about whether or an email is legitimate, do not hesitate to ask the Helpdesk or your District Tech **before** you do what it says.