Information Security Awareness Program

This document is part of a collection of documents that make up the Information Security Awareness Program. The following is a link to the main Information Security Awareness Program document.

Staying Safe & Secure Online

Staying safe and secure online is one of the most important aspects of any information security awareness program. The College has invested in the technology infrastructure to keep our systems and data safe and secure. This section will explain some of the risks associated with the Internet and how you can stay safe and secure online.

Additional Resources

Microsoft's Safety & Security Center
http://www.microsoft.com/security/default.aspx

National Cyber Security Alliance Stay Safe Online
http://www.staysafeonline.org/

Google's Stay Safe Online
http://www.google.com/goodtoknow/online-safety/

Stop, Think, Connect
http://www.stopthinkconnect.org/

What is a Virus?

A virus, more generally known as malware, is software that is designed to harm a computer/network and can copy itself to other computers/networks. You come in contact with malware through the course of accessing the Internet from your computer. Malware can be installed on your computer without your approval or knowledge through deceptive links or from downloading something that sparks your interest such as attachments of funny images, greeting cards, or audio and video files. Once malware has been installed on your computer, cyber criminals try to access your personal information by tracking your keyboard keystrokes or logging your computer's activity. They can control your computer to send spam e-mail, automatically re-directed to view unwanted websites, or perform other actions without your knowledge. The result can simply be a brief annoyance, or something more devastating like identity theft.

CAUTION

To help prevent infection by malicious software, never accept or open any file or link from an e-mail, on a webpage, or in an instant message until you verify its authenticity with the sender.

Once a virus is on your computer, its type or the method it used to get there is not as important as removing it and preventing further infection. If you suspect you have a computer virus, turn off your computer and call the ITS Helpdesk at (513) 569-1234.

Additional Resources

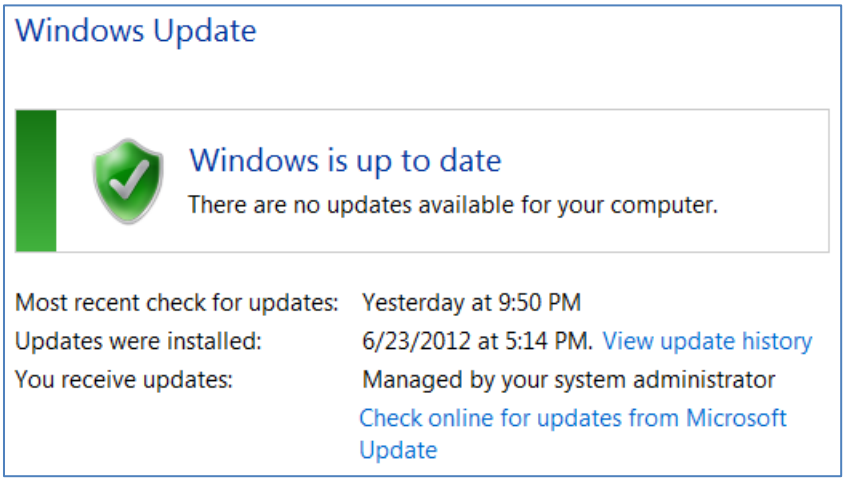
Microsoft's Safety & Security Center: *What is a computer virus?*
http://www.microsoft.com/security/pc-security/virus-whatis.aspx

Google's YouTube Video: 5 tips for staying safe on the web
http://www.youtube.com/watch?v=o5wC826_Z18&feature=player_embedded

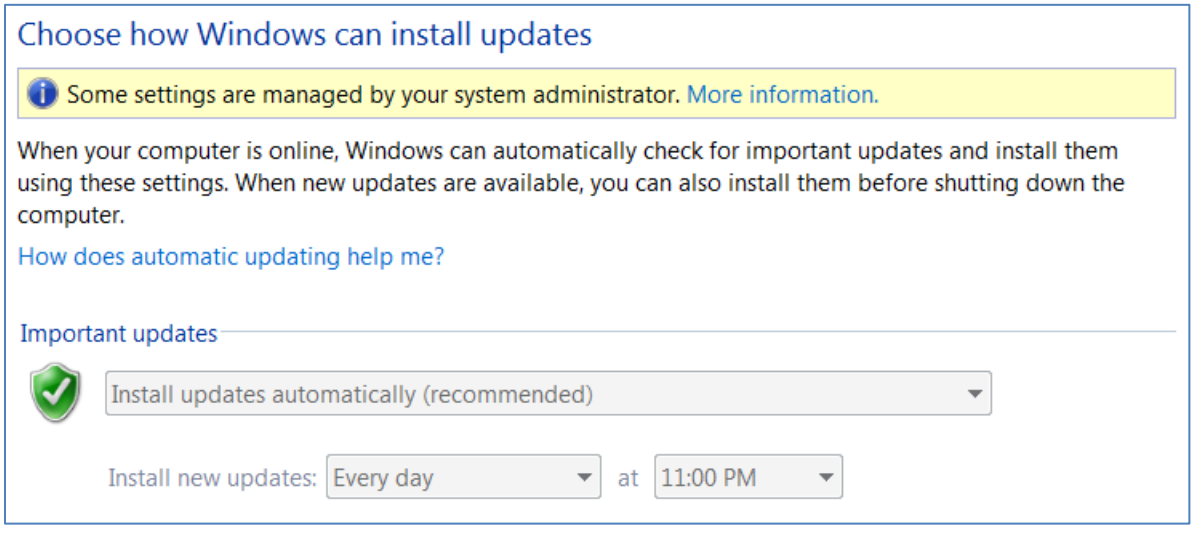
Google's Staying Safe Online: Malware
http://www.google.com/goodtoknow/online-safety/malware

Keep a Clean Machine

The best defense against viruses, malware, and other online threats is to ensure your computer stays current with the latest security software/updates. To verify the Windows Updates on your computer are current, click the Start button, click All Programs, and then click Windows Update. You should see something similar to the image below.



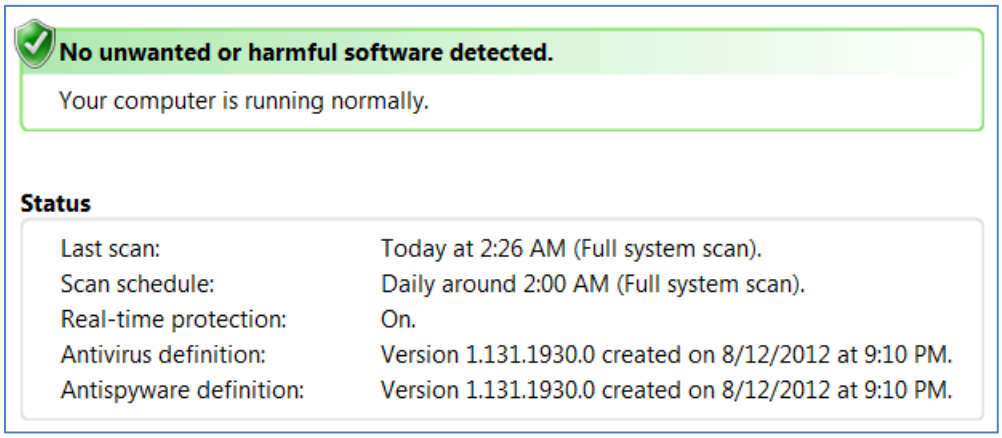
College owned computers are configured to automatically install updates daily. Because this is critically important to the stability and safety of our systems and data, this setting cannot be changed by users. While viewing the Windows Update screen above, click Change settings from the menu on the left. You should see something similar to the image below.



Along with computers, other devices, such as smart phones and gaming systems, should also be protected from viruses and malware. Also, be sure to scan externally connected hardware like USB devices and external hard drives.

Anti-Virus Software

To combat attacks on your computer, be sure to have reputable anti-virus and anti-spyware software installed and up-to-date. The College's anti-virus software is Microsoft's Forefront. Because Forefront is critically important to the stability and safety of our systems and data, some settings cannot be changed by users. To view Microsoft Forefront, click the Start button, click All Programs, click Microsoft Forefront, and then click Forefront Client Security. You should see something similar to the image below.

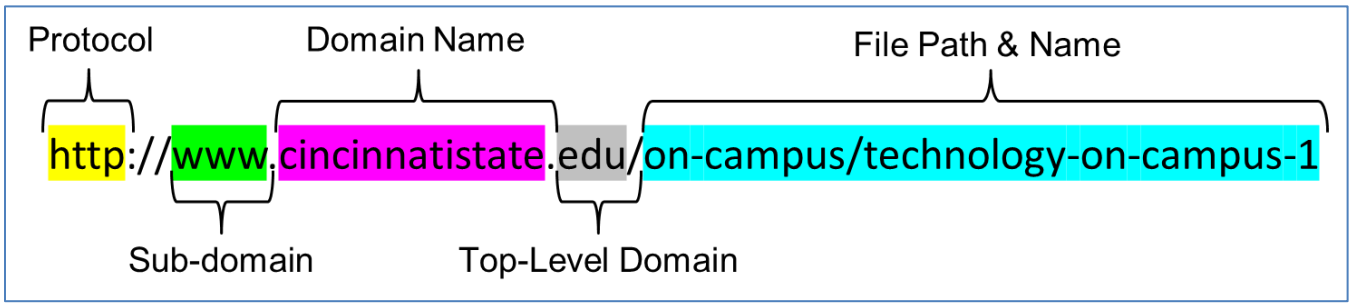


Additional Resources

Microsoft's Safety & Security Center: *How to remove and avoid computer viruses*
http://www.microsoft.com/security/pc-security/antivirus.aspx

Secure Browsing

The internet provides a vast knowledge of information but it doesn't come without risks. Before you enter sensitive data in a web form or on a webpage, look for signs that show the site is secure. This section offers a few suggestions to help you determine if a website is safe and secure. First, let's look at the parts that make up a web address or URL (Uniform Resource Locator).



Protocol: Protocol, also known as schema, is the first part of the URL. The most common protocols are http (Hypertext Transfer Protocol) and https (Hypertext Transfer Protocol Secure). Others include ftp, smtp, and pop3.

Sub-Domain: The next part of the URL is the sub-domain. In this example the sub-domain is www (World Wide Web), which is often the default sub-domain used on many websites. Because of this, the sub-domain is often not

necessary. If you browse to google.com or www.google.com you arrive at the same site. In its simplest form, the sub-domain is a folder on the web server.

Domain Name: The domain name is an easily recognizable phrase to a numerically addressed (IP address) web resource. For example, www.google.com has a unique IP address of 74.125.225.178. If you copy and paste this IP address into a browser, you will open Google's website.

Top-Level Domain: The top-level domain is the name server that your browser will use to resolve the location of the requested site. Most common top-level domains are .com, .org, .edu, and .gov.

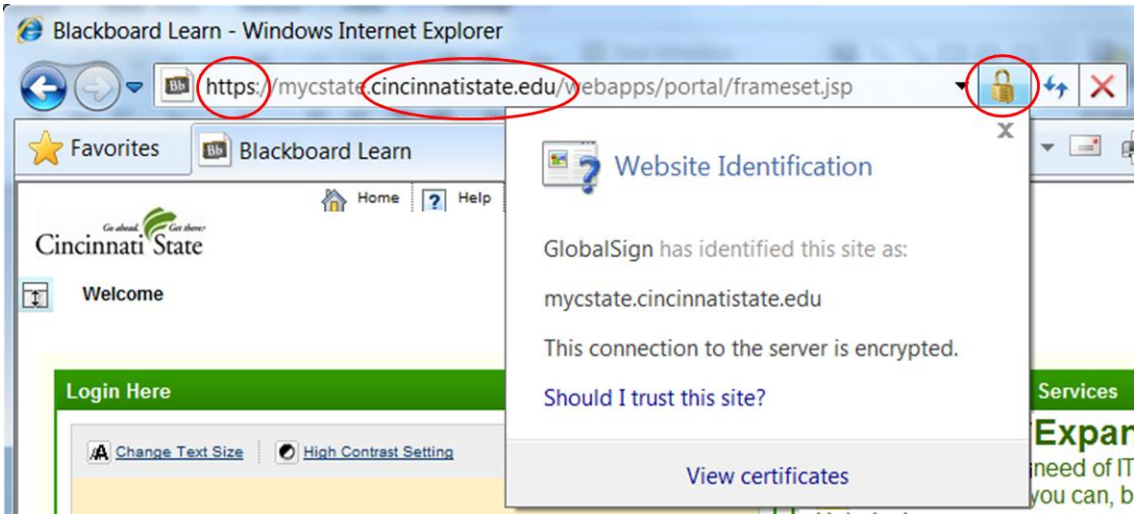
File Path & Name: File path & name is the specific file or resource being requested.

On a secure site, the protocol should be **https** (instead of http). Https presents a secure connection and browsers will often display a padlock near the URL (except for Firefox). You can click this padlock to determine if the site has a verified security certificate. Also, inspect the Domain Name (cincinnatistate) and Top-Level Domain (edu) to ensure you are on the correct site. The following displays how the four top browsers, Microsoft's Internet Explorer, Mozilla Firefox, Google Chrome, and Apple's Safari, show you are on a secure website.

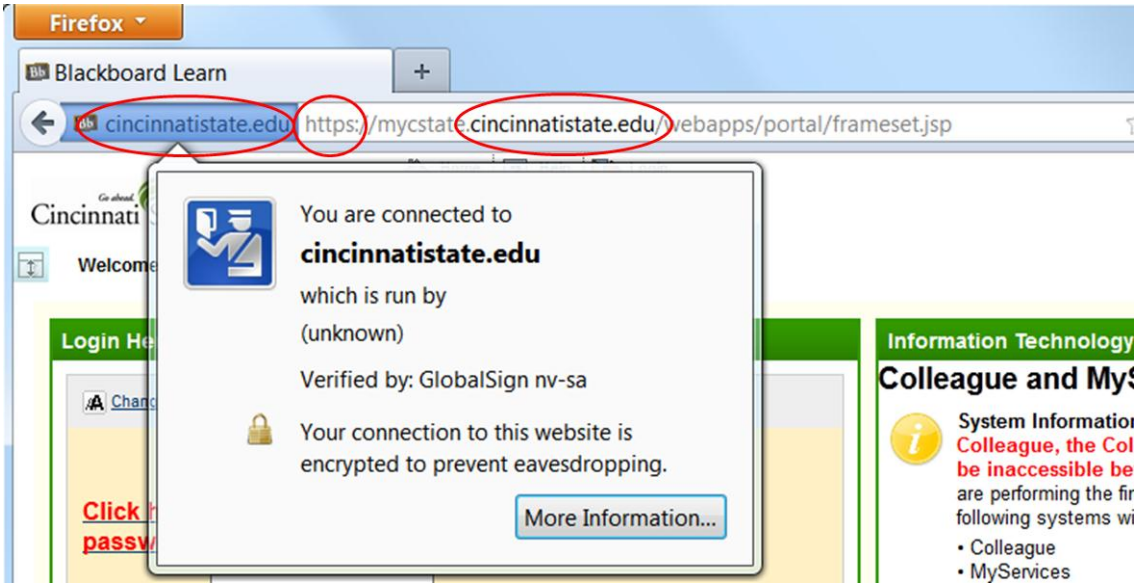
CAUTION

Never disclose your password, credit card number, social security number, or other personal information in an instant message or text message.

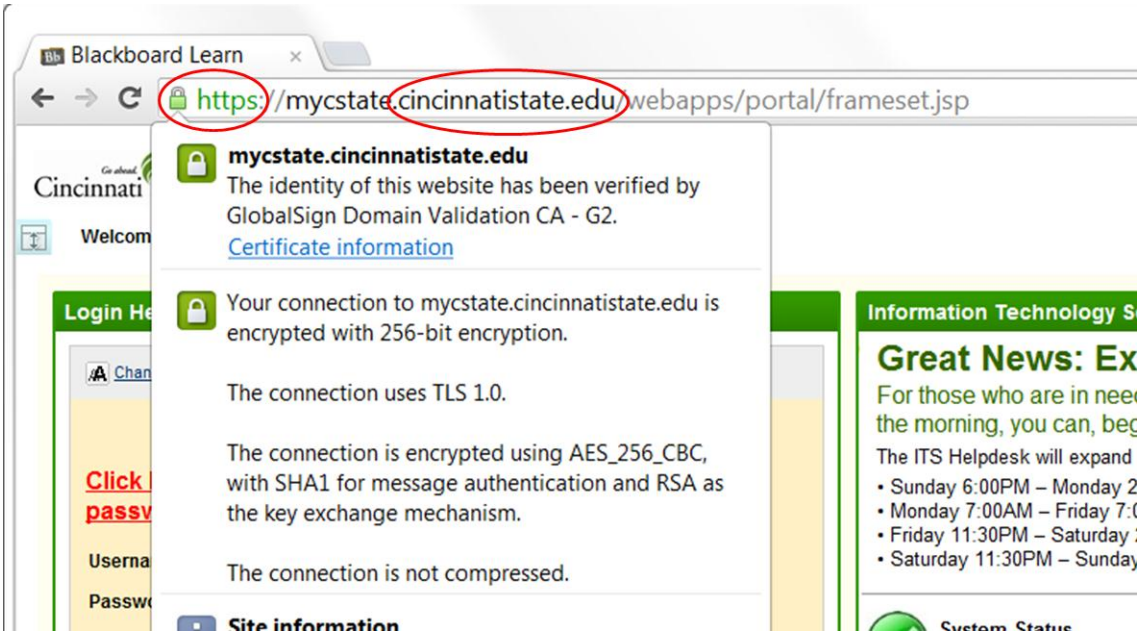
Microsoft's Internet Explorer: The padlock is to the right of the URL. Click that padlock to view the security certificate. The protocol (**https**), the domain name and top-level domain (**cincinnatistate.edu**) are in bold for quick reference that you are on the correct site.



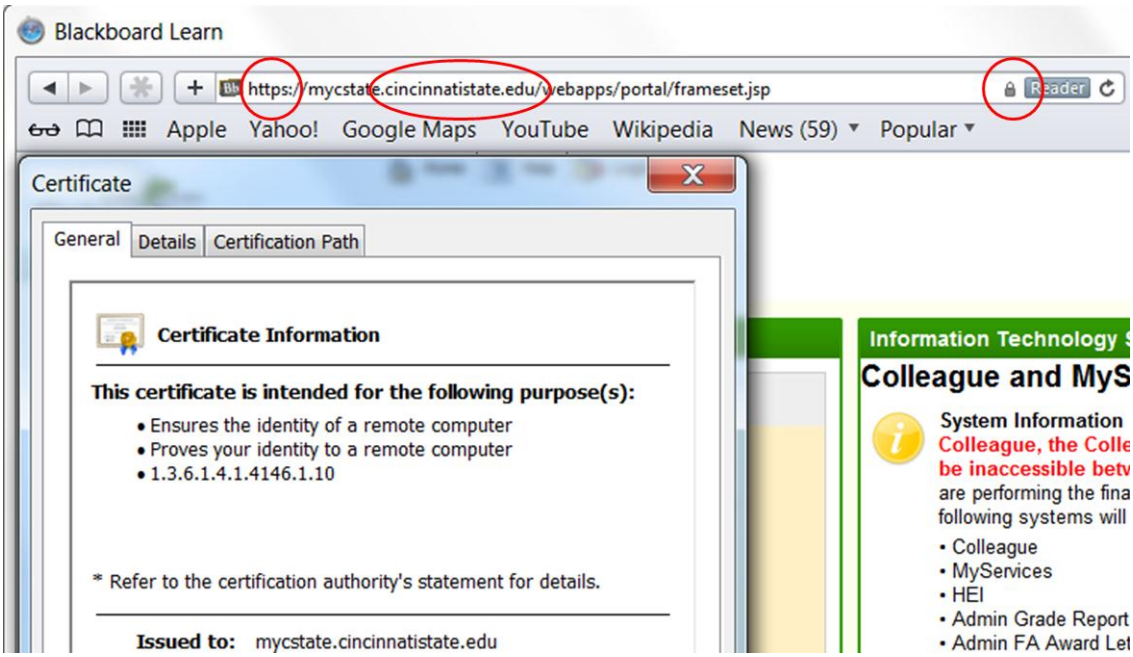
Mozilla Firefox: Firefox does not display a padlock. Instead, it "highlights" the website to the left of the URL. Click that highlighted website to view the security certificate. The protocol (**https**), the domain name and top-level domain (**cincinnatistate.edu**) are in bold for quick reference that you are on the correct site.



Google Chrome: The padlock is to the left of the URL and the color of the protocol (https) is green. Click that padlock to view the security certificate. The domain name and top-level domain (**cincinnatistate.edu**) are in bold for quick reference that you are on the correct site.



Apple Safari: The padlock is to the right of the URL. Click that padlock to view the security certificate. Safari does not bold the protocol (**https**), the domain name, or the top-level domain (**cincinnatistate.edu**).

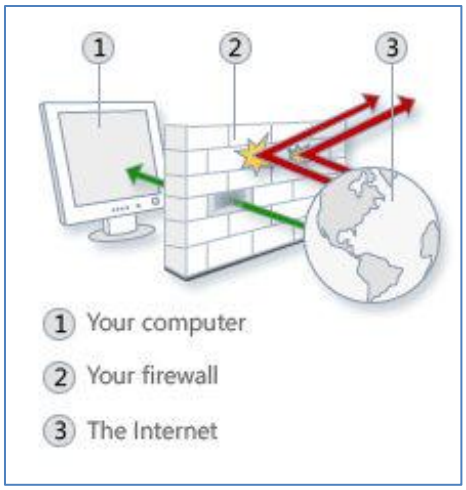


Additional Resources

Microsoft's Safety & Security Center: *Six rules for safer financial transactions online*
http://www.microsoft.com/security/online-privacy/finances-rules.aspx

Firewalls

A firewall (hardware or software) can help protect your computer from would-be hackers trying to delete information, crash your computer, or steal your passwords and credit card information. It also helps to protect your computer from viruses and/or worms that try to reach your computer over the Internet. The image below shows a simplistic view of a firewall.



In the image above, the green arrow represents safe communication coming from the Internet and is allowed to pass through the firewall to your computer. The red arrows represent unsafe communication, such as viruses, and are not allowed to pass through to harm your computer.

The campus network has firewall protection at the entry point to the network. Because this protection is performed at the network level, Windows Firewall is turned off on all campus computers. Firewalls are a strong defense against dangerous attacks via the Internet.

Additional Resources

Microsoft's Safety & Security Center: *Firewalls*
http://www.microsoft.com/security/pc-security/firewalls-using.aspx

Additional Security Measures

The following are a few additional security measures that will help keep you safe and secure online.

- ✓ **Use Complex Passwords**: Combine capital and lowercase letters, numbers, and symbols to create a more complex and secure password; also see the Information Security Awareness Program Username & Password Security document
- ✓ **Use Unique Passwords**: Use separate passwords for each system; if you do this and a cyber-criminal gains access to one of your systems, they won't have access to all of them
- ✓ **Keep Them Safe**: Keep your passwords in a safe and secure place away from your computer
- ✓ **Control Your Information**: When available, set the privacy and security settings on websites to your comfort level for information sharing; always remember, it is a best practice to limit the information you share online
- ✓ **Protect Your Wi-Fi**: Ensure that all Wi-Fi (home and cell hot-spots) are password protected
- ✓ **Be Cautious of Links**: Don't click links or buttons in a pop-up window that seems suspicious