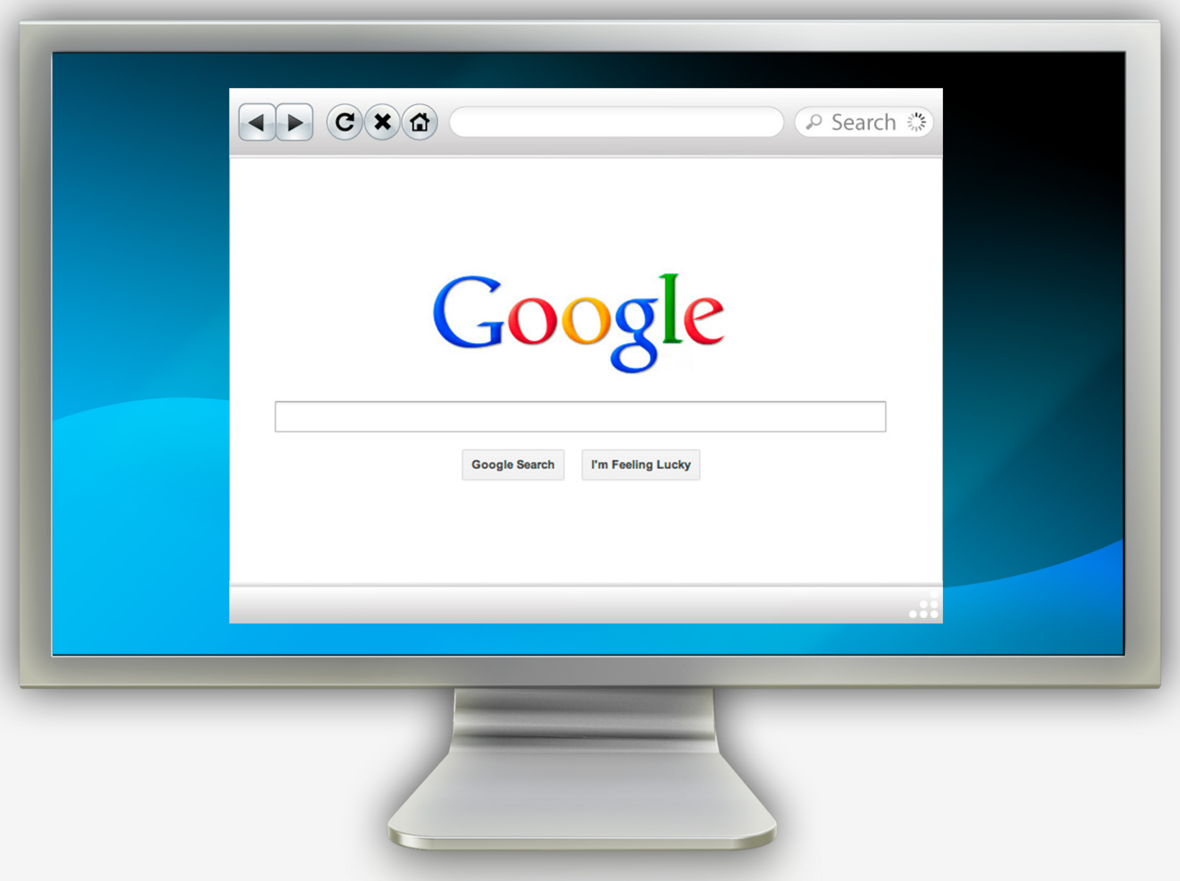
Browsing

Your web browser is your primary tool for using the Internet. It is also the number one target for cyber attackers. By protecting your browser, you protect yourself against many of today's attacks.



This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE
TECHNOLOGY SOLUTIONS & SERVICES

Browsing

The Internet has become a powerful tool for your daily activities. You use it to search for information, shop online, watch movies and manage your finances. In almost all of these cases, the primary tool you use is a web browser, such as Internet Explorer, Chrome or Firefox. Your browser is, in many ways, your gateway to the Internet.

Because so many people around the world use and depend on browsers for their daily Internet activities, your browser is a primary target for cyber attackers. These individuals have developed specialized hacking tools and built malicious websites designed to silently hack into your browser. Once hacked, attackers quickly gain total control of your computer and all of your information without you knowing. By protecting your browser and using it wisely, you can protect yourself against these threats and safely use the Internet for your daily activities.

Solution

You should always follow these steps to protect your browser and yourself.

Your Browser

A key step to protecting your browser is to always use its latest version. The vendor that developed your browser is constantly fixing new vulnerabilities and adding new security features to enhance its protection. By using the latest version, you ensure you have the latest security mechanisms in place. Enable automatic updating to ensure your browser is always current. This feature allows your browser to continually check for new patches. As soon as a new patch is released, your browser or operating system will download these patches and update the browser.

Avoid Plugins

Plugins, or add-ons, are additional programs you can install in your browser to give you more functionality. Common plugins include Adobe Flash, Java and Apple QuickTime. Every plugin you add becomes another window for attackers to break into your computer. In addition, it can be difficult to keep these plugins current; very few of them have auto-updating features. Install only authorized plugins you absolutely need, and always be sure you have the latest version installed. If you are no longer using a plugin, delete it from your browser.

Scan All Downloads

Scan any files you download from the Internet with updated anti-virus. When you download and install or run a new program, that program could be infected. It may appear to work just fine, but it can silently infect your computer. This is very common, especially with free files, such as free screensavers, video players or games. Be sure to scan anything you download with anti-virus before opening or running it.

Website Filtering and Protection

Browser website filtering (sometimes called Smart Screen Filtering, blacklisting or phishing protection) is a feature most browsers support. It helps protect you from visiting websites that are known to be malicious. You may not realize it, but there are security organizations that are constantly scanning the Internet and looking for any malicious websites. Whenever they find a malicious website, they add that site to their database. Most modern browsers have access to these databases. If you attempt to visit one of these websites, your browser will give you a warning. If you get one of these warnings on your browser, do not visit the website. Instead, simply close the browser tab or window. Keep in mind that this feature can only protect you against known malicious websites. It cannot protect or warn you about malicious websites no one knows about.

Avoid Bad Neighborhoods

In some ways, the Internet is a like a big city. It has everything you need, from banks and shopping centers to sporting events and movies. However, just like most big cities, the Internet has good neighborhoods and bad neighborhoods. Good neighborhoods are made up of well-known websites that are trusted. Bad neighborhoods are websites designed to attack or harm you or your computer. They do this by hacking your browser or distributing infected software, such as fake screensavers or infected games. Just like in a big city, one of the simplest ways to stay safe is to avoid these bad neighborhoods. If you have never heard of the website, if the URL information looks incorrect or suspicious or if the website looks like it has dodgy information, then do not download any software or submit any information to it.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE
TECHNOLOGY SOLUTIONS & SERVICES