

CYBER SECURITY

Newsletter

BROWSING THE INTERNET SAFELY

Problem

The Internet has become a powerful tool for numerous activities, including searching for information, shopping online, and managing 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 also a primary target for cyber criminals. Cyber criminals have developed new attacks and built malicious websites designed to hack your browser and infect your computer. Once hacked, attackers quickly gain total control of your computer and all 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:

1. Your Browser

A key step to protecting your browser is to always use the latest version. The company who developed your browser is constantly adding new security measures and features to enhance its protection. By using the latest version, you ensure you have the latest security mechanisms in place.

In addition to running the latest version, always make sure your browser is updated. Cyber criminals are constantly finding new weaknesses in browser software. As a result, your browser vendor is constantly releasing new patches to fix these known weaknesses. To ensure your browser is always current, enable automatic updating. Automatic updating 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.



Protecting Your Browser

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

Idaho State
UNIVERSITY

This newsletter is published by
Idaho State University, for more
information please contact us at:

help@isu.edu

Avoid Bad Neighborhoods

In a lot of 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 any big city, the Internet has good neighborhoods and bad neighborhoods. Good neighborhoods are made up of friendly websites you know and trust. These are websites that will not intentionally harm you.

Unfortunately, just like in most large cities, there are also bad neighborhoods on the Internet. These neighborhoods are parts of the Internet where websites are designed to attack or harm you or your computer. Some of these websites distribute infected software, such as fake screensavers or infected games that take over your computer. Other malicious websites will attempt to attack and hack into your computer when you simply connect to them.

Just like in a big city, one of the simplest ways to stay safe is to avoid 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. Sometimes it is hard to tell if a website is good or bad. That is why it is important to follow all the precautions described in this newsletter.

2. Avoid Plugins.

Plugins, or Add-ons, are additional programs you can install in your browser to give you more functionality. For example, 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, because very few of them have auto-updating features. Install only authorized plugins and those you absolutely need, and always be sure you have the latest version installed.

3. Scan All Downloads

A key step to protecting yourself is scanning all downloaded files 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, but will attempt to silently infect your computer. This is very common, especially with free files, such as free screensavers or games. Be sure to scan anything you download with anti-virus before opening or running it.

4. Website Filtering and Protection

Browser website filtering (sometimes called Smartscreen Filtering, blacklisting, or phishing protection) will block you from visiting websites that may try to attack your browser and you. You may not realize it, but there are websites on the Internet that are designed to hack into your browser or computer just by visiting them. Website filtering is a list of these dangerous websites you should not visit.

At any point in time, there are thousands of known malicious websites on the Internet. If you try to visit one, website filtering will block your attempt and explain you were trying to visit a known, malicious site. Most Internet browsers have enabled this feature by default. However, you should double check to be sure yours is enabled.

5. Additional Security Settings

In addition to what we have discussed so far, one more step you can take is to change the security settings on your browser. Some browsers, such as Internet Explorer, have additional browser security settings. You may want to consider configuring your security settings to a higher level. While it might stop some legitimate sites from working, it will go a long way in keeping your system secure.

6. Mobile Devices

Keep in mind that these guidelines are not just for your computer, but also for any mobile devices you may use, including smartphones or tablets. While browsers on mobile devices may have far less features and fewer options, you must still keep them secure. As we discussed on the first page, one of the most important steps to be secure is to always run the latest mobile browser.