

Group 7

Web Browsing

What is "Web Browsing"?

Web Browsing is using a computer's Internet browser as a search engine for exploring websites.

Common Internet browsers include:

Internet Explorer, Mozilla Firefox, Safari, Google Chrome, and Opera.

Common Problems

There are many common problems associated with web browsing, the most common among them is security. According to the United States Computer Emergency Readiness Team (US-CERT), our web browser security is being compromised to insure better function of our browsers. Many users are not aware that their web browsers are configured to increase functionality and not to protect them from security risks. Websites can easily be disguised and just a simple click can lead to exposure of your computer.

Solutions

The solution to this common problem is to become informed about the tools available to deal with the potential security risks such as: enable automatic software updates to keep your computer up-to-date, install and use anti-virus software, avoid unsafe behavior (i.e., clicking on unknown attachments), and don't enable anything you don't need. Users must also become familiar with the features and functionality of the web browser they use. Browsers have different features (i.e., cookies, plug-ins, etc.) and provide varying amount of security to their users.

Security Threats

Anytime software is downloaded from the Internet, your computer is being put at an increased risk. It is difficult to determine which websites are truly safe. Protecting younger children from seeing things they should not or from running innocent searches that return with adult content is another common problem with web browsing. Often, websites our students are using can easily be mistyped and lead them

to an unsafe website. Our students should be taught ways to identify an authentic website versus a website imitation. For instance, any official government website will end in “.gov” instead of “.com.”

Prevention Tips

A simple explanation of this idea to our students could prevent exposure to some of these unsafe websites. In addition, our students should be taught how to identify authentic parts of the website versus an advertisement. A solution to this common problem is the use of parental controls which are available in operating systems, web browsers, computer software-controls, mobile devices, and home/school networking (i.e. software that works with your router to filter Internet content). Parental controls offer a way to make sure that kids’ Internet usage is both safe productive. Another way to prevent web browsing security threats is to interactively teach our students about internet safety. Carnegie Mellon University’s Information Networking Institute created Carnegie Cadets to teach students in grades 3-6 about cybersecurity. Carnegie Cadets is an online game that allows students to learn about internet safety in a fun and engaging way.

Check out these links for helpful prevention tips on dealing with web browsing security threats.

[United States Computer Emergency Readiness Team](#)
[Carnegie Cadets](#)

Technology Plan Application

With all of the dangers and threats available to children on a web browser, a school district now needs to incorporate practices to ensure that a simple click does not lead a child to an inappropriate website. There are many different software concepts that can ensure that web browsers are secure. A tool that is effective in a school district is iBoss.

iBoss

iBoss is an innovative tool that can be used throughout the school district. When a child clicks onto a site such as “Facebook,” iBoss will immediately pop-up based on the sites that are restricted by the school district webmaster. This “blocking” will be on any device at anytime. Users in the district such as teachers or administrators can have a username and password for iBoss in order to access sites such as “Pinterest” that are blocked by school districts.

Another feature of iBoss is that the software can locate and backup any searches in the web browser to ensure that users are not trying to search for inappropriate sites. This is a safety measure for the district to ensure that all employees and students are abiding by the school district's technology policies.

Having a software like iBoss would ensure security at its highest measure and also monitor school employees and students that are breaking the technology policies which will be held up in the user agreement signed by all in the school district.

Beyond a school-wide initiative with software, teachers will be required to teach a Common Sense Media lesson every year to every student. By giving each student a basic understanding of how to search and use a web browser, students at any age level will understand what search engines are safe to use such as kidzsearch.com. By instilling the knowledge to students and staff, web browsers will be used in the way deemed fit in a safe and effective manner.

More Resources on Web Browsing

YouTube Link: [Child Focus 'E-safety'](#)

The YouTube video above shows a girl playing a game on the computer, unsupervised, when a virus link (which looks exciting) pops up! The girl clicks on the link not knowing that it is a virus and it could crash her computer. The lesson learned in this video is a vital one. Children should never be left unsupervised on the computer when the computer is unprotected. The parent should be supervising or playing the game with the child to prevent any accidental viruses from downloading, which is what the parent ends up doing in the video at the end.

Proquest Article: [Correcting and Replacing Free Tool from Dell KACE Thwarts Common Security Threat: Browsing the Web](#)

This article introduces an application from the Dell computer company, that secures web browsing. It prevents users from accidentally installing viruses/malicious software on the computer that is not needed. The article mentions a school in Tennessee that uses the secured browser for their K-12 school, the malicious material gets cleaned from their computer systems by the application called Dell KACE Secure Browser.

Website Tool: [PBS Kids Webonauts Internet Academy for Parents and Teachers](#)

This website was made by PBS Kids to educate children about internet security through game play. Players are sent on a training mission where they encounter enemies

(internet security threats) and in order to win the game they must pass through the cookies to get to the end of their mission. It is similar to real-life situations such as not giving out password information, good internet behavior, and not making public profiles.

ProQuest Article: [CA eTrust Secure Content Manager Education Matching Program Helps Schools Protect Themselves From Internet Dangers](#)

Computer Associates International in California developed a secure content manager program for schools. School computers are a breeding ground for a range of internet security threats. The eTrust threat management program makes it easier for schools to meet the challenge of internet security threats.

ProQuest Article: [Republican Presidential Candidate Senator John McCain and Secure Computing Corporation Discuss Safer Internet Usage Through URL Filtering in Schools](#)

This article explains a program called SmartFilter™, an industry leading URL filtering solution, that is being used in a Utah Education Network. It is overseeing Utah's 300,000 K-12 students' internet browsing. Senator McCain explained that it is important to provide the best internet access to the students, doing so in a safe and learning-conducive environment. Nowadays, the internet is an extremely vital form of technology which is used in all of our classrooms across the United States. However, if unsafe browsing is being used, it negates the purpose of the children's best interest supporting education.

ProQuest Article: [THE DEVELOPMENT AND EVALUATION OF A PEER-TRAINING PROGRAM FOR ELEMENTARY SCHOOL STUDENTS TEACHING SECURE INTERNET USE](#)

This is an article about a peer-training program that was utilized in two different elementary schools in Turkey. 24 students were involved, 12 students being the control group and 12 students being the experimental group. Following the tests and the experiment, peer-trainer communication skills increased and the students developed positive changes in the use of Internet browsing. The students became knowledgeable about secure Internet use.

Website Tool: [Google for Kids-The Safe Search Engine for Kids where Filtered Search is always on!](#)

Google for Kids! I never even knew this existed, however it does. This website overrides computer search settings to help remove potentially dangerous material when searching Google. The best part is there are no changes made to the computer or browser settings. This program is an excellent filtering tool for kids, because they can go on

many different websites to play games, read, and watch videos without you as the parent being concerned about malicious material showing up.

ProQuest Article: [Program Offers Kids a Secure Place on Web; Waldorf School Sees Potential in 'Safe Card' Software for Guarding Students From Internet Dangers](#)

This article brings up a great point about Internet web-browsing security. Kids nowadays are so technologically savvy that even young kids know how to go onto the Internet and search YouTube videos, which can be really scary.

References

iBoss

<https://www.iboss.com/web-security-data-sheet>

Kidzsearch

<http://www.kidzsearch.com/>

Common Sense Media

<https://www.common sense media.org/>

ProQuest

<http://search.proquest.com.authenticate.library.duq.edu/pqcentral/advanced?accountid=10610>

Carnegie Mellon University

<http://www.ini.cmu.edu/about/mysecurecyberspace/index.html#msc.smc-topic.browsing>

United States Computer Emergency Readiness Team (US-CERT)

<https://www.us-cert.gov/publications/securing-your-web-browser>

Pictures

<https://chakchai.files.wordpress.com/2011/12/ranger-web-browser-icons.png>

Google

<http://www.safesearchkids.com>

YouTube

www.youtube.com