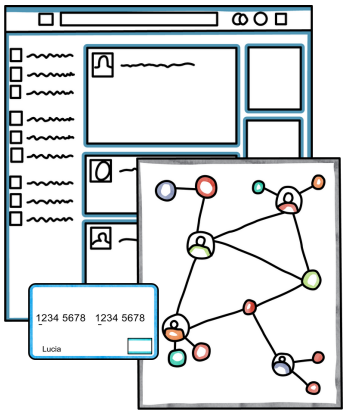
Office of the Chief Information Security Officer
Risk Advisory: Web Browsing

BACKGROUND

Whenever you use your web browser to access information on the Internet, you are also exposing your device, your data, and your privacy to an opportunity for surveillance and intrusion. This is not being alarmist; it is a factual observation. Members of the University community should exercise due care in their browsing habits, endeavor to maintain a securely configured web browsers, and pay attention for indicators of compromise.

BEST PRACTICES

The Office of the Chief Information Security Officer (CISO) encourages you to be aware of the following when browsing the Web:



- Keep operating systems and applications **up to date** by applying all critical software patches to protect against viruses, spyware, and other malicious software that may infect your system through the browser.
- **Secure applications** that are called on by the web browser (e.g., QuickTime, Adobe Reader) by installing updates and patches as they are released.
- Software add-ons that provide functionality to a web browser (e.g., Java, Flash, etc.) may also introduce vulnerabilities to the computer system. Consider enabling add-ons on a case-by-case basis.

- Review web browser **default configurations** and disable or limit features that make your computer vulnerable.
- Multiple web browsers may be installed on your computer and some file types may open with a browser that is not the one you typically use. **Securely configure each browser** that is installed on your computer.
- Use **anti-virus software** and keep it updated to protect against the latest threats, including adware and spyware.

Office of the Chief Information Security Officer
Risk Advisory: Web Browsing

- Only enter personal information, including usernames and passwords, on secure websites. Secure website addresses **start with https://**, and your web browser will display a padlock symbol. Check with your particular browser to see where the padlock should be displayed.
- Don't use the same password for multiple websites, accounts, and applications.
- Don't use the "remember my password" feature or save any personally identifiable information you enter on a form.
- Websites use cookies to collect information about you. If you don't want to be tracked, configure your browser to **delete cookies** – either periodically or when closing the browser.
- To reduce the risk of exposure to malicious files or programs, configure your web browser to **block pop-ups** by default and only allow them on a case-by-case basis.
- Be cautious when playing online games or downloading free software as **spyware** may be bundled with those programs.
- Enable **phishing filters** or the **safe browsing feature** when available in your web browser.
- Keep an eye on the web browser address bar. Be cautious if the address changes unexpectedly or if you click on a link and are taken to an unfamiliar address.
- Before clicking on any links within an email, **verify** that the email is from a sender that you know and trust.
- Exercise caution if an email or website looks suspicious, is out of the ordinary or unexpected, or contains an offer that is too good to be true.

RESOURCES

UW IT Connect Security

Malware Online Training

help@uw.edu