



**No matter what your role in the UOC Biological Sciences Division - Internet browsing is essential to everyday life and work but it can harbor some hidden dangers to you and your computer. These risks can include exposure of sensitive personal information and infection by malware, which includes viruses, spyware, and adware.**

### What is safe browsing?

Safe browsing means being aware of these online threats and taking the necessary steps to avoid them. It only takes a little bit of effort, a few tools, and some basic information to be safe as you browse the Internet. Follow these guidelines to protect your personal information and your computer online.


#### 1. Update Web browsers regularly and enable security features

- Choose "Yes" when browser programs like Firefox, Internet Explorer, or Safari prompt you to update; current versions of these browsers protect you against security vulnerabilities in older versions
- [Adjust security settings](#) for Firefox, Internet Explorer, or Safari browsers to warn you about annoying and potentially dangerous threats to your security, like popups, spyware, and malicious add-ons

#### 2. Install protective software

- [Symantec Endpoint Protection](#) is comprehensive security software that includes additional protection against spyware

#### 3. Guard personal information

- Look for signs of an encrypted Web page when providing sensitive personal information (credit card or banking information, SSNs, etc.) online; key identifiers include a URL for the Web site's login page that begins with "https" and a padlock icon  in your browser status bar (the location of this icon will vary based on browser)

#### 4. Be wary of Internet downloads

- Streaming media Web sites might seem harmless, but watching or listening to streaming media may mean downloading a special media player that could contain malware
- Downloaded files like software or other media can hide malware on your computer without your knowledge

### What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about the University or downloaded malware contact the BSD-ISO team via the following phone numbers or e-mail addresses:

Plamen Martinov, BSD Chief Information  
Security Officer

O: 773-834-1714

[pmartinov@bsd.uchicago.edu](mailto:pmartinov@bsd.uchicago.edu)

Kim Cooke, IT Security and Compliance  
Analyst

O: 773-834-7897

[kcooke3@bsd.uchicago.edu](mailto:kcooke3@bsd.uchicago.edu)

You may also send an e-mail to the BSD Security mailbox: [security@bsd.uchicago.edu](mailto:security@bsd.uchicago.edu)

Visit the BSD-ISO website: <http://security.bsd.uchicago.edu>