

Tips for Safer Web Browsing

1. Upgrade your Web browser to 128-bit encryption.
2. Read Web site privacy policies carefully and make sure you understand them. Look on your favorite Web sites for privacy seals of approval from BBBOnline, TRUSTe, ePublicEye, or CPA WebTrust.
3. If you're reluctant to provide certain information on an online form, don't.
4. Set up a special free email account with Yahoo, Hotmail, or other free services and supply those addresses when you fill out forms.
5. Before you give your credit card number to any commerce site, make absolutely sure it's secure. Look for a closed padlock icon at the bottom of the screen or https in the URL.
6. Delete all the cookies in your cookie directory (generally c:\windows\cookies) frequently.
7. Disable cookies in your browser (an extreme measure) or set your browser to alert you to cookies, or to accept only cookies that return to their original server or, better yet, install cookie management software (such as Webroot Software's WindowWasher or The Limit Software's CookieCrusher) to control which cookies your PC will accept.
8. Use an anonymous browser such as Anonymizer to hide your identity and filter cookies.
9. If a Web site gives you the option to opt out of tracking, take it.
10. If you have a fast and constant DSL or cable connection, get some personal firewall software, such as Symantec's Norton Personal FireWall or Network ICE's BlackICE Defender, and install it, FAST!
11. Turn off file and printer sharing in Windows if you're not using it. Intruders will have an easier time accessing your files if this is activated.
12. Elect not to accept news or updates from Web sites you visit.
13. Fake your return address when you use chat or newsgroups.
14. Turn off your Instant Messaging software when you're not using it.
15. Set your Instant Messaging software to allow only people you trust (in your buddy list, for example) to access you.