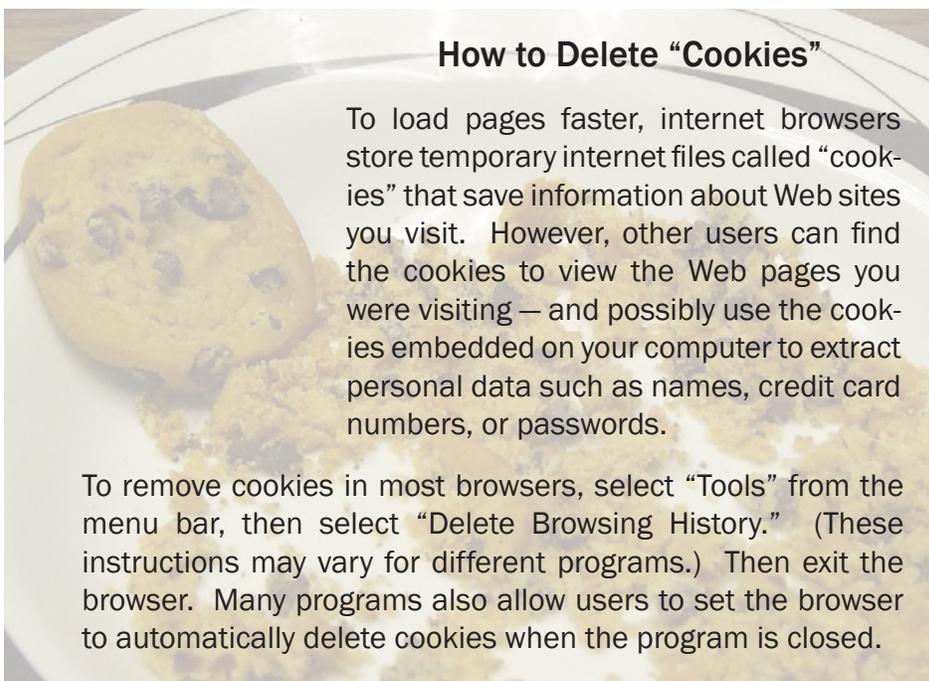


Protect Electronic Devices During Holiday Travel

While travelling during the holiday season, it is important to be aware of the threats against computers and mobile devices, especially if they have wireless capabilities. Protecting your computer does not have to be difficult. The premise is quite simple: first, protect information, and second, protect possessions.

Protect Information. When connecting to the Web wirelessly, connect only to trusted networks. Avoid accessing wireless networks from unknown sources. Ideally, any wireless network should be encrypted and password protected. Thus, a free “wireless hot spot” at the airport might be convenient, but it is a dangerous place to use a credit card to make a purchase.

Just as when you are withdrawing money from your account at an ATM, be alert for anyone “looking over your shoulder” as you use the Internet. In this case, do so literally and figuratively. It is obvious when someone is peering at your computer screen, but it is harder to tell when a hacker is observing your computer screen remotely by intercepting your connection to the wireless network with a specialized antenna. For these reasons, it is not advisable to enter any personal data, access bank accounts, or work on private or sensitive information on a Web site in public. For example, do not make online purchases at a coffee shop or work on sensitive information in an airport.



How to Delete “Cookies”

To load pages faster, internet browsers store temporary internet files called “cookies” that save information about Web sites you visit. However, other users can find the cookies to view the Web pages you were visiting — and possibly use the cookies embedded on your computer to extract personal data such as names, credit card numbers, or passwords.

To remove cookies in most browsers, select “Tools” from the menu bar, then select “Delete Browsing History.” (These instructions may vary for different programs.) Then exit the browser. Many programs also allow users to set the browser to automatically delete cookies when the program is closed.

Also, when using a public computer in a hotel lobby or internet cafe, avoid entering personal information when possible, and erase any personal information that may have been saved on the computer. Before logging off of a public computer, delete temporary internet files such as “cookies,” sign out of any Web site that required a log-in (before closing the browser), and then exit all programs or internet browsers.

Protect Possessions. The potential for theft of laptop computers is also a concern, especially during the hustle-bustle of holiday travel. The following tips can decrease the chance that your computer might be stolen:

- ✓ Never leave your laptop or any portable/wireless device alone in a public place. Use a hotel safe if one is available, and/or purchase a laptop cable lock for added security while in a hotel room.
- ✓ Do not pack electronic equipment or other valuables in checked baggage. When passing through an airport security checkpoint, wait until the laptop has passed under the x-ray machine before passing through the metal detector, then keep an eye out for it to come out of the machine. Retrieve electronics immediately, and then worry about your shoes.
- ✓ Avoid leaving a laptop or other expensive electronic devices in a car, if possible. If you must leave a computer in a car, put it in the trunk to conceal it. Ideally, place it there when getting into the car. Otherwise, moving it to the trunk calls attention to the computer right before you walk away.

Simple measures can reduce an individual’s vulnerability to cyber-crime of any sort. For more tips on keeping your information and systems safe, contact safeschools@csc.com. ■