Safe-Surf Guidelines

January 1, 2001 By John Aravosis

When you're doing the safety dance -- whether at the club or on the web -- the more you know, the easier it is to minimize risk. And while the Internet is a valuable resource for people with HIV, it holds particular risks for a community that values its privacy.

The old abstinence saw applies here, too: The only way to ensure you're safe is to stay offline. But then you don't get to reap the Net benefits. Kevin Mischka, an HIVer in Washington, DC, has a friend who recently tested positive and was told to take Viracept (nelfinavir) three times a day. Mischka wanted to lend the newbie a hand, so he logged on and five minutes on The Body (www.thebody.com) was enough for Mischka to realize that his friend's doc had made a dosing blunder.

If you're ready to play with the big kids online, start out by checking to see whether the sites you visit have a privacy policy posted, and then read it carefully to see what's left out. For example, many websites contract out their data collection, among other tasks, and warn that their business partners may not be held to the same standards. Zoe Hudson of Georgetown University's Health Privacy Project conducted a survey of the web's 21 most visited health sites. Nineteen had a privacy "policy," but almost all, including such biggies as WebMD and DrKoop.com, came up short. If these privacy polices are subpar, just imagine those of the Internet's other 17,000 health sites.

A common danger comes from "cookies" (small electronic name-tags that websites often place on the computers of visitors). A cookie can finger you each time you return to a site, keep track of which pages you visit and the data you enter, and even determine where online you just came from and where you're headed next.

The data from various sites' cookies can then be compiled in giant direct-marketing databases that let businesses reverse-engineer not just your true identity, but intimate details of your life, including health status. Your info is then sold to the highest bidder -- be it your insurance company, your employer or some other stalker. While privacy experts don't hold up any real-life terror tales as a result of web spying, many surfers naturally find the practice objectionable in and of itself: A Peeping Tom doesn't have to get you fired to have violated your rights. And as the Internet expands, it's only a matter of time before direct marketers start using the data goldmine so close at hand.

Striking a balance between the dangers and attractions of their online offerings has left those who run HIV-focused websites with few options. Some have cut back in order to ensure visitors' privacy. Russ Toth, director of the California Aids Clearinghouse, is in charge of the site HIVInfo

(www.hivinfo.org). He says that HIVInfo decided not to host online chats or bulletin boards because of the risk that such tools might put them in the position of becoming the “health education police” who would have to unmask users’ identity.

That’s not exactly a scenario out of a sci-fi flick. A syphilis scare in 1999 among San Francisco gay men was traced back to an America Online chat room. Officials from the city health department, working with the website PlanetOut (www.planetout.com), successfully walked a fine line in warning M4M chatters that they may have been exposed without violating their expectation of online anonymity. But such conscientiousness may be an exception.

In the end, safe surfing is like safe sex: It’s up to you to assess the risks, determine what you’re comfortable with and make the call. But Georgetown’s Hudson warns against becoming too complacent. While HIVers are currently protected under the Americans With Disabilities Act, she says, there’s still no federal law that protects the privacy of medical records. Check out the *POZ* resources (below) for tips for tripping safely in cyberland.

© 2026 Smart + Strong All Rights Reserved.
http://beta.docker.poz.com/article/Safe-Surf-Guidelines-1047-5014