

Suite 3  
Woodhouse Corporate Centre  
935 Station Street  
Box Hill North, Victoria  
3129, Australia  
**ABN:** 83 078 025 813  
**Tel:** +61-3-9896-7800  
**Fax:** +61-3-9896-7801  
**Email:** sales@eb2bcom.com  
**Web:** www.eb2bcom.com



## The PC World password safety test

Scott Spanbauer, IDG News Service  
05/01/2004

Life online means living with--and trying to remember--passwords. Lots of them. Your Internet, e-mail, and instant messaging accounts require you to enter a user name and a password. So do secure online bank, credit card, mutual fund, and shopping Web sites. Meanwhile, less-sensitive sites such as those of Consumer Reports and the New York Times may require a lower level of log-in security.

Faced with retaining so many user names and passwords, most of us take the easy way out: We pick one memorable pair of terms and use them everywhere: Our dog's name, our kid's birthday, our favorite Star Trek character. Maybe if we are feeling really tricky, we move our hands one key to the right and type "password" (that produces "[sddeptf]").

I'm sorry to be the bearer of bad tidings, but the password stealers are on to us.

If your password is "abc123", "iluvjlo", or "OU812", you might as well not have one at all. If it consists of names or any words that can be found in a dictionary (English or otherwise), fuhgeddaboutit. A knowledgeable person equipped with the right tools and your user name could deduce your weak password and gain access to your Internet account, e-mail, or bank account in no time.

Using the same weak password at multiple sites or servers compounds the likelihood that someone will take control of your accounts. Even if the password you use for your ISP account is fairly strong, using the same password at various sites reduces your security. The people who manage a site or otherwise are privy to your data in one place undoubtedly have access to the password, and they may be able to figure out where to use it based on your e-mail or IP address (which they also probably have). Moreover, the user names and passwords that you use to access Web pages or to enter your e-mail may travel over the Internet in the form of unencrypted plain text, so devious folk can grab your password and give it a try elsewhere.

## There's Safety in Numbers

Follow these three commonsense rules to ensure the safety of your passwords and the data they protect.

**Choose strong passwords:** These consist of six to eight completely random alphanumeric characters. Weak passwords contain easily guessed number sequences, or names or words that can be found in a dictionary, even if the dictionary is Latvian. Mixing upper- and lowercase may or may not matter, depending on the system that accepts the password, but you should always combine letters, numbers, and punctuation. For example, "scott123" is a weak password. And except for the fact that it now has been published in PC World, "8hT\$2@N8" is a strong one.

Since coming up with a truly random password is difficult for humans, you may want to use a tool--such as the Info Tech Professional Random Password Generator --that can create such passwords for you.

**Store passwords securely:** Since you can't possibly remember dozens of unique, gibberish passwords, you need to record them and store them somewhere safe. The first thing to recognize is that there is no truly safe location to store passwords: The most convenient place won't be the most secure, and the most secure methods won't be terribly convenient.

Writing passwords on a piece of paper that you file away somewhere or stick into a book will work okay as long as no one else is likely to open the book--and you don't forget which book it's in. Storing passwords in a file on your PC may be more convenient, but not if the hard disk dies. To prepare for that contingency, print out a paper copy and store it in a safe, a locked cabinet, or a safety deposit box, or in an innocuous book that nobody is likely to browse through, such as *Do-It-Yourself Brain Surgery: A Narrative or Scranton on \$50 a Day*.

If you sell your computer or replace its hard disk, you'll need to delete the password file, and then use a file-wipe utility to permanently erase the drive so that the new owner can't restore your password file. The June Answer Line gives instructions on wiping a hard drive.

**Encrypt and password-protect the file you save your passwords in.** You can password-protect Word 2002 and Excel 2002 files using a fairly strong 128-bit encryption key. Choose Tools, Options, Security in either program to enter the password, and click Advanced to select the encryption strength. Obviously, choose a strong password that you'll remember.

If you don't use Word 2002 or Excel 2002, or if you aren't convinced that these programs are secure enough, download Counterpane Labs' free Password Safe utility. In addition to using Counterpane's bulletproof Blowfish encryption to encrypt the company's user name and password database, Password Safe includes a handy password generator that lets you copy user names and passwords to the Windows Clipboard with a single click. When you close Password Safe, the program clears passwords from the Clipboard.

**Use passwords safely:** One major stumbling block in password security is the innate human inability to keep a secret. Once you have created a password, reveal it to no one. Your ISP, your bank, and no one else should ever need you to tell them your password, whether by phone, via e-mail, or in person (your company's IT support person, however, is another story). Don't share your password with coworkers, and don't write it on a note that you leave in your desk drawer. Don't let others "shoulder-surf" you by observing you as you log in to a network or secure Web page. And for maximum peace of mind, keep your personal passwords off your office PC.

If you suspect that one of your passwords has been compromised, simply use the Web site's password-management options to change it. Practically every online site or service that relies on passwords allows you to enter your account and select a new one instantly.

Are you one of those people poring over a laptop instead of a newspaper while on the train or ferry, or at the airport or coffee shop? Unless you pay through the nose for a wireless connection, you're probably not online. But with a little effort, you can have your browser automatically preload your favorite news sites for you so that they're available during your commute.

To use Internet Explorer 6 to cache a Web site for offline reading, first browse to the site, choose Favorites, Add to Favorites, check Make available offline, and click Customize to open the Offline Favorite Wizard. Click Next to start moving through the wizard. Select Yes if you wish to download pages linked to the site's main page (or No if you're happy just to read the headlines), tell the wizard how many levels deep you wish to cache links (I recommend just one level deep for starters), and then click Next. Select I would like to create a new schedule, and click Next again. Choose a frequency and time to perform the Web synchronization. You can also set the synchronization to connect automatically when you next go online (if you happen to be offline at the preset time) and to enter a user name and password. Click Finish when you've made your choices.

Internet Explorer's AutoComplete feature handily remembers the user names, passwords, and other data that you need to enter repeatedly in online forms, so you don't have to type the data in every time. But what if a certain password you recorded there has changed, or if you don't want to make your passwords available to other users of the PC? To remove a user name and password from IE's encrypted database, visit the site where you enter them, double-click the site's user name or user ID field, select the user name you want to remove in the drop-down field, and press Delete. To erase all AutoComplete data, choose Tools, Internet Options, Content, AutoComplete, Clear Passwords.