

Your password is safe

Online life means always living with passwords and trying to remember them - a lot. Internet accounts, e-mail and instant messaging all require you to enter your username and password. Online banking, credit cards and shopping Web sites have to do the same. Meanwhile, less sensitive sites like Consumer Report (www.consumerreports.org) and New York Times (www.nytimes.com) may require lower login security levels.

Online life means always living with passwords and trying to remember them - a lot. Internet accounts, e-mail and instant messaging all require you to enter your username and password. Online banking, credit cards and shopping Web sites have to do the same. Meanwhile, less sensitive sites like Consumer Report (www.consumerreports.org) and New York Times (www.nytimes.com) may require lower login security levels.

Dealing with so many user names and passwords, many people use a simple solution. They choose a pair of words that are easy to remember and apply everywhere. It could be the name of the pet dog in the house, the date of birth of a child, or the name of the character in the favorite movie. Some people even use tips to enter a 'password', one key to the right (to form '[sddeptf]').

Sorry to report a bad news or password thieves are stalking us. If your password is only 'abc123' or 'iluvm' (I love you very much!), It can be considered that you have no password at all. If the password includes only names or any words that can be found in a dictionary (English or any language) it is also useless. A knowledgeable person equipped with good tools and know your username will be able to quickly deduce a simple password and will be able to access your Internet accounts, e-mail or bank accounts.

Picture 1 of Your password is safe

Figure 1: Create and save passwords using the free Password Safe program

Using the same weak password for multiple sites or servers will enable someone to easily take control of your accounts. Even if your password is relatively strong, using the same password for many different sites reduces security. The site manager or know your data has the ability to access that password, and they can find out where to use it based on your e-mail address or IP address (they may also have). In addition, the user name and password you use to access Web pages or to enter your e-mail can be transferred on the Internet in plain text without encryption, and hackers have You can pick up that password to use it somewhere else.

Safe in numbers

Follow the following three common rules to ensure password security and the data they protect.

Choose strong passwords: Includes six to eight completely random alphanumeric characters. Weak passwords

contain easy-to-guess numbers, or names or words that can be found in a dictionary, even if it is a Latin dictionary. Mixing lowercase and uppercase letters can be important or not, depending on the system that accepts the password, but always combine multiple letters, numbers and dots. For example, 'scott123' is a weak password. And if it hadn't been announced, '8hT \$ 2 @ N8' was a strong password.

Successfully building a random password is really not easy for ordinary people so you may have to use a tool - like Info Tech Professional Random Password Generator (find.pcworld.com/36314) - to create passwords for you.

Keep your passwords safe: Since you can't remember dozens of different troublesome passwords, you have to keep them in a safe place. The first thing to keep in mind is that there is no truly safe place to store passwords: The most convenient place is also the most unsafe, and the safest method is also the most inconvenient.

Writing passwords into paper and putting them in a place or putting them in a book is a good way to store them if no one opens the book - and you don't forget to put them in any book. Storing passwords in a file on a PC may be more convenient, but it is very dangerous if the hard disk fails. To avoid such accidental randomness, print out a copy of the paper and put it in a place with a safety lock or some boring book that no one wants to read.

If you sell your computer or replace the drive, you must delete the file containing the password, then use a file deletion utility to permanently delete the data on the drive, so that the new owner cannot recover your password file. Refer to PCW VN A 6/2003 tr.114 or find.pcworld.com/36629 for instructions on deleting hard drives.

Encrypt and password protect the file that stores your passwords. You can password-protect Word 2002 and Excel 2002 files using a strong 128-bit encryption key. Select Tools, Options, Security in one of the two programs to enter the password, and click Advanced to select the encryption level. Of course, choose a strong enough password that you can remember.

Picture 2 of Your password is safe

Figure 2: Schedule your Web news to IE storage area by setting up daily offline offline favorite sites

If you don't use Word 2002 or Excel 2002, or don't believe these programs are safe enough, you can download the free Password Safe utility from Counterpane Lab (find.pcworld.com/36320). In addition to using Blowfish encryption method to encrypt usernames and password databases, Password Safe also has a handy password generator (Figure 1) that lets you copy the user name and password into Windows Clipboard with just one click. When closing Password Safe, the program will remove the password from the Clipboard.

Use passwords securely: A major obstacle to password security is the ability of people to keep their innate secrets. Once you've created a password, don't reveal it to anyone. No place, including banks or ISPs, requires your password to let them know, whether by phone via e-mail, or by an individual (however, the company's IT supporter you're another story). Don't share your password with coworkers, and don't write it to a notebook in your desk drawer either. Do not let others peek over your shoulder when you are logged in to the network or a protected Web site. And for maximum peace of mind, you should not keep your personal password in your PC at work.

If you suspect that one of your passwords has been compromised, simply use the Web site password

management options to change. In fact, every online site or service related to passwords allows you to log in and select a new password quickly.

Store the items if possible

Are you the type of person who just loves reading laptops instead of reading newspapers while sitting on the train, on the ferry or in the airport? Unless you agree to pay an exorbitant price for wireless connectivity, chances are you can't go online. However with a few operations, you can ask the browser to automatically download your favorite news sites to read while on the road.

To use Explorer 6 to store certain Web sites for offline reading, first go 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. Choose Yes if you want to download pages that link to the main site of the site (or No if you just like reading through the headlines), tell the wizard how deep you want to store the links (little ones) Experience should only select one level deep, and then click Next. Select I would like to create a new schedule, and then click Next again. Select the repeat cycle and the time to perform Web page synchronization (Figure 2). You can also set up this synchronization to automatically connect when you go online the next time (if you accidentally leave online at the pre-set time) and enter the username with the password. Click Finish when you've made your selections.

You finished reading the article "**Your password is safe**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.