Online password protection

In this article, I will give you some tips to help you avoid two password-related security issues.

Andrew Brandt

Network Administration - *Password protection will be easy with the Password Safe password manager of Bruce Schneier or Portableapps.com version of KeePass software. If I have to use 'infected' public computers? Please scan it first with ClamWin free antivirus software.*

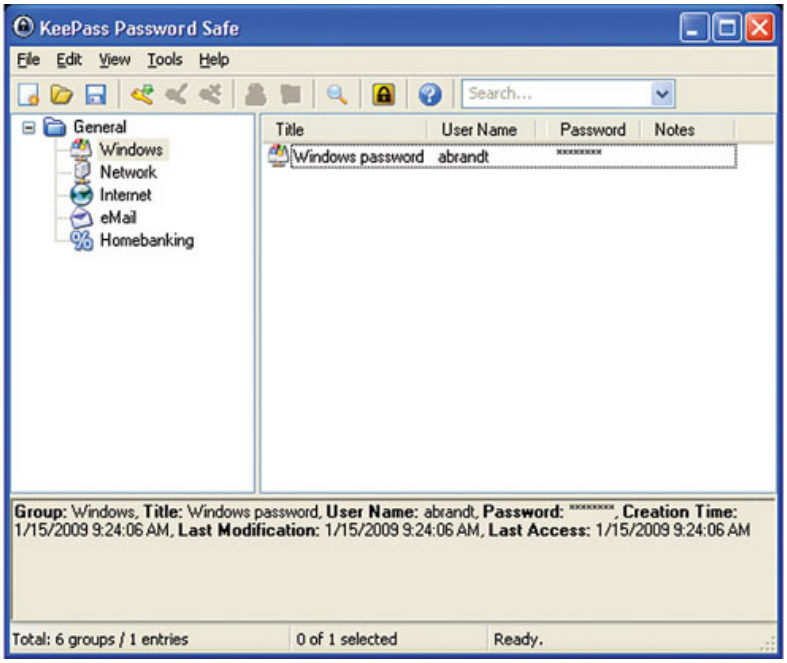
It is very difficult to remember all the passwords that access the sites or the software we use, the loss of control over them will be a big problem for security. Here are some tips to help you avoid two password-related security issues.

Password easy to guess

Reasons to care : Your passwords are the keys to opening everything that you've locked inside.

The report : When someone broke into the Yahoo mail account of Alaska Governor Sarah Palin and published details inside the account, then the incident drew public attention to a serious problem. . You can create a complex, random password for your web mail account, but if the information you provide in the 'secret questions' section of your online profile is too easy or easy. Guess that a bad guy will not be difficult to convince the password recovery mechanism of the service to manage your password.

Today, many people own LinkedIn accounts, Facebook profiles, and Twitter feeds because of the popularity of these social networks, making them easy to guess, such as school. The third level you learned or the name of your favorite dog. You can post a lot of things on your blog.



Remedy : Use a strong password manager and backup your password files. Using the Password Safe of Bruce Schneier or Portableapps.com version of KeePass software is a good solution to this problem. When you create a hard-to-guess, or random password, create a second password in the manager to use when answering a familiar question.

Password protection on public computers

Reasons for concern : You may have to use infected public computers (ie computers that are in unsafe situations) when urgent.

Scenario : On a business trip, check your email at a computer located in the lobby of the hotel. This is why you should not: Public computers in such locations or other locations such as schools, coffee shops, trade shows and libraries are vulnerable to Trojan infections. horse to steal passwords. In many cases, public computers will not be tested by its own management departments, so they are very susceptible to infection and rarely clean up the infection. Based on the number of random visitors using them to log in to email or other services, data thieves will view these computers as an effective source for information theft, then they will sell. for spammers and other types of attacks to exploit your confidential information.

Fix : If you can restart your computer, the safest way is to bring a copy of the operating system that can boot Knoppix on a CD, DVD or flash memory device (USB); You can customize your settings to be around 2GB with Internet tools, production applications and other utilities. However, if you have to use your own Windows installation, it is best to run your applications from a removable drive using the tools available on PortableApps.com. There are a lot of applications here to keep you safe in this case, they store all the temporary files, cache files and history on your drive itself.

To protect yourself from malicious software that may have been secretly installed in public computers, scan the computer with ClamWin free antivirus software (carry) and also need it. Bring your own browser, office applications, IM clients and other secure file transfer tools. There are even useful password management tools, but above all, you should change your password as soon as possible after entering and using the public computer.

You finished reading the article "**Online password protection**" 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.

© 2019 TipsMake.com