SWCP Portal
January 2012

Start the New Year Right

Passwords and Protection

Despite the various security threats out there, many experts do not suggest elaborate or expensive schemes to protect yourself and your identity online. Most simply emphasize the **basics** of online security.

There's little anyone can do about cyberwar, but you can do a lot to foil criminal access to your computer. Your most important means is often the one often given the least consideration – your **passwords**.

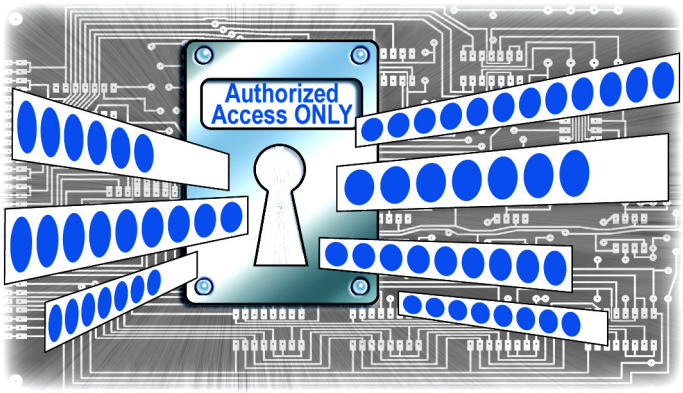
There's a lot of debate about how to make them strong but still useful, preventing malicious hackers from discovering them, and so forth, but surprisingly little about how vitally important they are. Because if your passwords are compromised, then any other security steps are generally useless.

As long as Internet services depend on character strings for authentication, your passwords are truly magic words – a literal "**open sesame**" to your life.

Back to basics

There are many rules for choosing good passwords:

- Do *not* use names or words from *any* language that can be found in *any* dictionary.
- The longer the better – at least 5 characters, 8 is better, and our system can handle up to 12.
- Upper or lower case *do* matter – "a" is not "A". Mix them up together randomly.
- Substitute numbers or symbols for letters like "3" for "E" or "+" for "t".
- A good method to generate passwords is to create an acronym from a memorable phrase by stringing together the first letters, especially with substitutions. For instance, a secure password such as "rRw4aTr?" could be readily remembered if made from "Romeo, Romeo, wherefore art thou, Romeo?"
- Use different passwords and usernames for different accounts — not the same one for everything.
- Remember that the account you think *least* important might be the most important one, if it easily allows access to other parts of your online life.
- Change your passwords every 3 to 6 months, too.



Trying to recall this all the time could drive a person crazy. Fortunately, there is a simple trick and online tools that can help greatly. But before discussing them, here's a few things you should *not* do:

- Again, *no names*, including your pet's, any nicknames – or any strings of numbers. Half of the Top 10 *Worst* Passwords commonly used are numbers; "123456" being most common. Other poor choices in the Top 10 are "password", "pussy", "dragon", and "qwerty". You get the general idea.
- If you use Wi-fi at home, be sure to change the default password on your router. Contact SWCP Tech Support for how to do this and other important protective steps, like disabling ad hoc mode, SSID broadcast, and enabling WPA2 encryption.
- Do *not* write your passwords down on a sticky note under your keyboard or on the monitor frame.
- Never, ever give passwords out in an email or instant message.

The last two points bring up an important consideration: how insecure your computer actually is. For instance, instant messaging passwords are often stored in **plain text**. You just need to know where to look. In fact, any application or webpage that you are required to log in to access usually has an option to remember your username and password that is almost as vulnerable. When you click "Remember me", that information is either stored on your computer in plain text or in a static key that can be hacked in minutes with free tools easily available online. Therefore, controlling **physical access** is as necessary as controlling online access.

Continued on back

Continued from front

It should also be noted that there is no password that *cannot* be broken given enough time, by sheer brute force number-crunching if nothing else. The best you can accomplish is to make your password so hard to crack that it's not worth the bad guys' pains.

Password management

One strategy to making good passwords is to base them on something **meaningful only to yourself**. That's the idea behind choosing the name of your favorite kitty from childhood, but "Snowball" could be cracked easily, and "8N0vv6A1L" is tough to recall – for instance, was it the *letter* "O" or the *number* "0"?

Yet such techniques *are* effective. It's calculated that even with a fast computer and highspeed connection, an 8-character string of lowercase letters altered to include just one capital letter and one symbol would increase the time needed to crack it from 2.4 days to 2.1 centuries – by which time it won't matter.

There are a number or websites offering to check your password's strength – even Microsoft has one. These should be used with caution as a way to find out what makes a password strong or weak; *don't submit any password you actually use online*.

You can use our own Password Generator to make some to try out. Just log on our **Members Tools** page, **https://members.swcp.com/** where you can safely whip up any number of secure or softer keywords to choose from. It's conveniently listed beneath the link to change your SWCP passwords. Please note that our system needs about 15 minutes for any alterations to your passwords to take effect.

Unless you're lucky enough to concoct a string that is somehow easy to remember, the problem of exactly recalling it persists. One clever way around this that is said to create an even more difficult-to-crack password than a random one of similar length is based on age-old memory enhancement techniques.

Simply think up a string of several words that would never come up in a sentence, yet together create a striking visual image. For "blindradishballetmule", for instance, all you'd have to do is picture a radish with sunglasses next to a donkey in a tutu. What could be easier? Even *without* substitutions, such a password would be long enough to be reasonably secure.

Yet even so, remembering a half-dozen or more bizarre images could be confusing. So they still need to be written down and stored somewhere. The only secure method to do so is to use a **password manager**. They can make your machine safer and reduce the number of passwords you must recall to one.

For Firefox users, the **Firefox Master Password** option can store all your website passwords behind a single 8+ character master key. Just go to Tools > Options > Security and click "Use master password".

For physical security, the **Master Password Timeout Extension**, an add-on that you can freely download from Mozilla.org, allows you to set your computer to require the master password to unlock it after whatever time period you choose.

There are a number of free manager applications available online. Two open source Windows password managers that have been recommended by reputable sources are the lightweight **Password Safe**, **passwordsafe.sourceforge.net** and **KeePass**, **keepass.info**, which is more robust and also portable – it can be handily used from a flash drive on other computers as well as installed on your own.

Other safety steps

- **Virus protection** remains important. While Macs and Linux have been relatively untargeted and no new killer viruses have surfaced recently, this could change at any moment. There are still some excellent free antivirus programs like AVG available; call or email Tech Support for more info.
- **Firewall** defenses are absolutely essential to keep out intruders, especially if you use Wi-fi. Modern devices have a firewall built in. If not, free and commercial software firewalls are available.
- **Using email safely** is a good habit to get into. Be careful about opening attachments, especially from strangers, and do not ever respond to spam. Never give out *any* personal information online. Feel free to check out any suspicious emails with our Tech Support. Take full advantage of the suite of powerful customizable **antispam filters** SWCP has put together for more precise control over your inbox, **https://members.swcp.com/mailfilter/**.
- SWCP offers one *free* **Virus Scan** per box per year for our members. Other Computer Repair services include **Tune-ups** to remove the garbage, defragment the drive, and so on, available for a reasonable fee. See **http://www.swcp.com/computer-tune-ups-and-virus-scans/** for full info; call if you have questions or to schedule a visit.
- And keep visiting our website! The **SWCP Blog**, **www.swcp.com**, has new articles all the time on security topics and a wide range of other helpful information for all our friends and members.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) • **SWCP.com** • **Help@swcp.com**

5021 Indian School NE, Suite 600, Albuquerque, NM 87110