

# Computer Security-Strong Passwords

*Keep your computer, data and accounts safe with strong passwords.*

To protect your computer, your data and your online accounts or mission critical data for your business, make a strong password your first line of defense. Most people know that strong passwords are a good idea, but don't realize hackers are becoming increasingly sophisticated at password "cracking." You have to change your password frequently, and stay aware of what techniques hackers are using to steal passwords, if you want to stay ahead of the bad guys. Remember, your computer is a tool (as well as an entertainment device) and as such, proper use is paramount.

Internet security is based on a "weakest link" principle, and passwords are often the only thing standing between a hacker and access to your computer or the home/business network. If your password is weak or non-existent, you make it easier for someone to break in. Hackers make their livelihood by automating ways to continually search out the weakest link to gain access to a network or computer. Don't let your password be the weak link!

There are real consequences to not having a **strong** password. If someone steals your password, they may find a way to access your e-mail or IM messages, your bank accounts, your research, your contact lists, confidential memos and whatever else you have on your computer. Your files may be altered or destroyed or in some cases, lock you out of your own system. Sometimes hackers even take over a computer and turn it into a zombie, using it to perform malicious tasks such as sending out large amounts of spam.

## How Passwords are stolen

When you are creating a strong password, it can help to know the tactics hackers use to steal them. Here are some of the most frequently used techniques:

- **Guessing.** Believe it or not, this is usually number one. Programs designed to guess a user's password are common. They often use personal information found online—such as names, birth dates, names of friends or significant others, pet names or license plate numbers—as a starting point. These programs can even search for a word spelled backwards.  
TIP: It's best to **NEVER** use any personally identifying information when creating a password.
- **Dictionary-based attacks.** Programs and software also exist that run every word in a dictionary or word list against a user name in hopes of finding a perfect match.  
TIP: Staying away from actual words, even in a foreign language, is recommended.
- **"Brute Force" attacks.** By trying every conceivable combination of key strokes in tandem with a user name, brute force attacks often discover the correct password. Programs can execute a brute force attack very quickly.

TIP: The best way to beat such an attack is with a long, complex password that uses upper and lower case letters, numbers, special characters and punctuation marks.

- **Phishing.** Phishing scams usually try to hook you with an urgent IM or e-mail message designed to alarm or excite you into responding. These messages often appear to be from a friend, bank or other legitimate source directing you to phony Web sites designed to trick you into providing personal information, such as your user name and password.

TIP: Best advice is don't click a link in any suspicious e-mails, and don't provide your information unless you trust the source.

- **"Shoulder surfing."** Passwords are not always stolen online. A hacker who is lurking around in a cybercafé, library or any open or public wireless access points, may be there for the express purpose of watching you enter your user name and password into a computer.

TIP: Try to enter your passwords quickly, without looking at the keyboard, as a defense against this type of theft.

- **Inadvertently exposing you password.** Once you have created your really strong password, keep it to yourself. Don't write it on a post-it and stick it under your keyboard.

## **Never, Never and I mean NEVER....**

**Never** write your password down or store it electronically in an unencrypted file-such as in a spreadsheet or text file.

**Never** leave any password blank or unchanged from its initial or default value.

**Never** make your password trivial (e.g., "password", "passwd").

**Never** make your password repetitive (e.g., "AAAAAAA", "aaa111").

**Never** make your password sequential (e.g., "abcdefgh", "12345678", "qwerty").

**Never** base your password on any of your personal information such as all or part of your Social Security number or telephone number.

**Never** use the name of a family member, nickname, pet name, birth date) or word associated with your interests (carfixer123) as your password.

**Never** use any word in any dictionary or any common given name (e.g., John, Mary, Tommy) as your password.

**Never** construct your password by taking any word in any dictionary or any common given name and substituting numeric characters or symbols for similar looking alphabetic characters (e.g. "p@ssw0rd", "C@rfiXer"). Many of these can be found in many of the popular search engines on the web.

**Never** build your password by following or preceding any of the above with by a number or symbol (e.g., "movie10", "1kerri").

**Never** use the same password over again. Think of them as disposable.

**Never** send your password through email. A new trick that hackers use is to try to get people to give away their passwords and other personal information through email. Reputable companies will never ask you to send a password through email. If you receive such a request, notify the company immediately by phone or through their Web site.

## **Tips for Creating and Using Safe Passwords**

If you work in an office or have multiple home users of your computer, it's important to remember protecting your computer and accounts with strong passwords. This helps protect other users as well. If just one password used to access the company network is breached, all of the computers connected to the network are put at risk for viruses, worms and other forms of malicious attack.

In addition to the suggestions offered above, follow these guidelines for creating and using strong passwords:

### **Creating a strong password:**

- Use BOTH upper- and lower-case letters.
- Place numbers and punctuation marks randomly in your password.
- Make your password long and complex, so it is hard to crack. Between 8 to 20 characters long is recommended (of course this makes it more difficult to commit to memory).
- Use one or more of these special characters: ! @ # \$ % \* ( ) - + = , < > : ; " ' `
- Make your password easy to type quickly. This will make it harder for someone looking over your shoulder to steal it.
- A passphrase could be a lyric from a song or a favorite quote. An example of a strong passphrase is "Superman is \$uper strOng!". A nonsensical word can be built using the first letter from each word in a phrase (e.g. C\$200wpG., represents "Collect \$200 when passing Go."). These typically have additional benefits such as being longer and easier to remember.

### **Using your password safely:**

- Create different passwords for different accounts and applications. That way, if one account is breached, your other accounts won't be put at risk too.
- Don't use your computer password for online shopping sites or free e-mail accounts (Hotmail, Yahoo!, Gmail).
- Change your passwords regularly, about every six months. Don't share your password with anyone else. Once it's out of your control, so is your security.

- Don't enable the "Save Password" option, even if prompted to do so. Pre-saved passwords make it easy for anyone else using your computer to access your accounts.
- Never walk away from a shared computer without logging off. This will ensure no other users can access your accounts.
- Don't use sample passwords given on different Web sites, including this one.
- Another safe password technique is to create a new, strong password for every Web site or login that requests one. You might consider creating a few strong passwords and use those at sites you want to keep most secure, such as your bank, brokerage, or bill-paying company. Then create another small set of passwords that are easier to remember that you can use everywhere else.
- A *social engineer* will try to manipulate a computer user by using trust rather than exploiting computer security holes. Be aware of anyone who wants to log on to your machine to send a quick email or anyone who claims to be an administrator and requests a password for various purposes.
- Use a password generator
- Using a password manager to store your password is not recommended unless the password manager leverages strong encryption and requires authentication prior to use. Be sure to use a strong password for your password manager. KeePass password safe (<http://keepass.info/>) is a fine example.

A good password is more than just a complex password. A good password is one that is not easily guessed but still easy to remember. It should be long and should consist of letters, number, and symbols, but still easy to type quickly with few errors. It should have elements of randomness that only a computer can provide while still having familiarity that only a human can provide.

But the best password of all is the one that the user chooses based on an educated understanding of passwords - a password that is hard to crack, but never forgotten. And the best password policy is one that helps users in creating these passwords.

**Links:**

[http://en.wikipedia.org/wiki/Password\\_strength](http://en.wikipedia.org/wiki/Password_strength)

<http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/>

<http://www.pctools.com/guides/password/>

<https://www.grc.com/passwords.htm>

[http://sourceforge.net/project/showfiles.php?group\\_id=28391](http://sourceforge.net/project/showfiles.php?group_id=28391)

<http://supergenpass.com/>

