

How to choose an unbreakable password

Despite the current wave of identity theft and corporate security breaches, it's amazing how very few people treat their passwords with any level of seriousness. Most computer users, both at home and in the office, see passwords as a nuisance and therefore make them as easy to remember as possible. This can be a catastrophic mistake.

There are certain specific guidelines you need to follow to choose a safe and secure password. Use the following tips as a "how to" on making your password secure.

1. Your password must be alphanumeric. That simply means a mixture of numbers and letters such as xpf2778z. Why? When a hacker tries to break into a system, they often use what are called dictionary or brute force hacks. A dictionary hack is an application that simply uses standard words and word combinations in an attempt to guess your password. For example, many computer users use the word "password" as their actual password. A dictionary hack would crack that password in a few moments. Using alphanumeric passwords increases the number of possible password combinations by millions.
2. It should be 6 - 8 characters in length. The longer the password the harder it is for a hacking program to get around. If your password was abc then there are 6 possible password combinations. If your password was abc123 there are now over 720 password combinations possible. If your password was abc1234, there are now almost 6,000 possible combinations. Never, ever use a short password only comprised of letters.
3. Never use personal details in your password. People often use their home address, their age, husband or wives name, their social security number or their date of birth. These are incredibly easy to get access to by either a fellow employee or potential system hacker. Your password needs to be secure and hard to guess and personal details meet neither of these criteria.
4. Do not write your password down anywhere. Keeping a record of your password for somebody to find is as dangerous as keeping a copy of your ATM pin number in your wallet beside your ATM card. Create a memorable password that you will have no problem recalling. This is not as hard as it sounds and if you jot some password ideas down you will quickly come up with some good ones. Obviously burn the piece of paper you jotted your ideas down on.
5. Do not use the same password for more than 90 days. Create several variants of the same password and recycle them every 60 - 90 days. This adds an extra layer of security to your data. By recycling your password frequently, you make your data 1000% more secure. You will notice that most large corporations force their employees to change their password every month for this exact reason.

Hopefully these tips will help you choose a password that is both safe and secure and that you will have some fun creating your new passwords too!

About the Author

Did you find this article useful? For more useful tips, hints, points to ponder and keep in mind, techniques, and insights pertaining to

www.spam-blocking.infozabout.com www.infozabout.com

Source: <http://www.zogol.com>