Passwords - The First Step to Safety

Most people don't put a lot of thought into creating a password. It's usually easiest just to create a short, easy-to-remember password, or even just to use the same password for every account you have. After all, the average person probably won't be able to guess your password.

However, hackers often use password-cracking software that can keep testing many different passwords until they find the correct one, and they can easily crack weak passwords. By creating strong passwords, you can greatly reduce the chance that your personal or financial information will be stolen.

Common Password Mistakes

Many people create passwords based on their spouse's name, a hobby, or a simple pattern, since those types of passwords are easy to remember. Unfortunately, they are also very easy for hackers to guess. To create a strong password, you will need to avoid these types of common mistakes.

Review the infographic below to learn some common password mistakes.


Common Password Mistakes
Preventing your passwords from getting cracked
Weak Passwords
DO THESE SOUND FAMILIAR?
Hackers
WORK HARD TO GET YOUR PASSWORD
PASSWORD: CodyBanks8
"No one will guess the password to my banking account. I used my grandson's name and age."
Hal
"It only took me 10 minutes to guess Hal's password. He posted his grandson's name on a photo sharing website."
PASSWORD: ILuvFishing
"I use my favorite hobby as my Facebook password."
Jarrod
"Jarrod's Facebook profile picture shows him fishing. People leave so many clues on social media websites!"
PASSWORD: BrAveZ!2
"I use the same password for all of my accounts. That way, I only have to remember one password."
Bryan
"Once I cracked his iTunes password, I was able to get into his Facebook, Amazon.com, and email accounts."
PASSWORD: 123abc123
"My Twitter password is really easy for me to remember. It's just a pattern."
Emilia
"A lot of people use passwords that have some kind of pattern. They don't realize that I try those first!"
STRONG PASSWORD: m&t7T5$dAY
"I used to write down my passwords, but now I use a password manager that encrypts all of them. It lets me use stronger passwords like m&t7T5$dAY that are harder for hackers to guess."
Jazmin
"I'm still working on figuring out this person's passwords. She doesn't seem to have any clues for me anywhere!"
GCF LearnFree.org

Common

To see more examples of common password mistakes, check out 25 Worst Passwords of 2011 Revealed.

Tips For Creating Strong Passwords:

Never use personal information such as your name, birthday, or spouse's name. Personal information is often publicly available, which makes it much easier for someone to guess your password.

Use a longer password. Your password should be at least six characters long, and for extra security it should ideally be at least twelve characters (if the site allows it).

If you need to write down your passwords, keep them in a secure place. It's even better if you "encrypt" your passwords or just write down hints for them that others won't be able to understand.

Don't use the same password for each account. If someone does discover your password for one account, all of your other accounts will be vulnerable.

Try to include numbers, symbols and both uppercase and lowercase letters (if the site allows it).

Avoid using words that can be found in the dictionary. For example, "swimming1" would be a very weak password.

Random passwords are the strongest. Use a password generator instead of trying to think of your own.

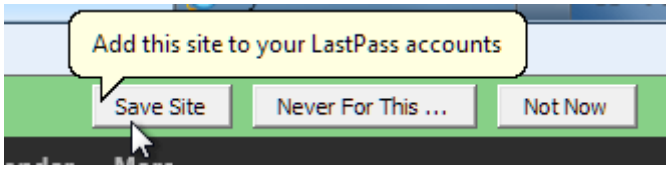
Random passwords are harder to remember, so create a mnemonic device. For example, "H=jNp2#" can be remembered as "HARRY = jessica NOKIA paris 2 #." This may still seem random, but with a bit of practice it becomes relatively easy to memorize.

Using Password Managers

Instead of writing your passwords on paper where others can easily see them, you can use a password manager to encrypt and store them online. Some password managers can also generate random passwords, making your information even more secure. Examples of password managers include LastPass, KeePass,Firefox's password manager, and Chrome's password manager.

For example, when using LastPass, you will first need to install the LastPass browser plugin. Whenever you type a password on a website, the browser plugin will ask you whether you want to save it. The next time you go to the website, LastPass can automatically enter the password

for you. If someone else wants to use your computer, you can simply log out of LastPass to prevent the other person from accessing your information.



Saving a password with LastPass