



Smarter Passwords and PINs

By: Elizabeth Rogers,
www.50Plus.com

Do your passwords and PINs need a makeover?

How to pick ones you can remember, but hackers can't easily guess.

Remember how much fun it was to have a secret password for your playhouse? Now it seems we're asked for a password or personal identification number (or PIN) just about everywhere we go. Online banking and electronic payment methods have become a mainstay, not to mention all those websites and online services that require registration...

And, just in case you managed to memorize all your credentials, experts warn to change them every few months to keep criminals out. It's a nuisance -- but the alternative is worse with identity theft and fraud on the rise.

So how can you create passwords you can remember, but criminals can't guess? Here are some tips from experts.

Recognize (and avoid) the weaknesses

According to experts, you're putting yourself at risk if your passwords...

- are too short. Fewer characters means fewer potential combinations, so anything less than six could be problematic.
- use common names, words or character strings. (For instance, Consumer Reports notes that some of the most popular passwords for Twitter include "rosebud", "password" and "123456".) Such passwords are easy to guess because they're widely used.
- include words you can find in the dictionary, even if they are misspelled or backwards. "Dictionary attacks" are a common way to hack passwords, regardless of the language.
- use personal details like your initials, address, birthday, pets' names, phone number, account numbers or digits from a piece of I.D. like your driver's license. This information can often be found through other means, like the phone book or social media.

Create stronger passwords

Maybe you've spotted some red flags already? Here are some ways to create stronger passwords:

- Use at least eight characters. Some experts say that seven, twelve or fourteen are "the best" lengths, but most agree that longer is better.
- Include numbers and symbols. Experts note you can use words as long as you break them up (e.g. "vio\$22let" or "fif50ty%").
- Include upper and lowercase letters, if the site allows (e.g. "vIO\$22let" or "fI50Fty%").
- Have variety. Repeating letters and numbers can be risky.

Many sites have a built in meter to rank your new password, but you can also try sites like The Password Meter to test potential choices. Another alternative is to try a password generator. (As an example, try this one from PC Tools.)

Do you need to go to all this trouble for every account? Perhaps not, but experts warn that the more important the data you're guarding, the stronger your password should be and the more frequently you should change it. Some sources recommend adding "change passwords" to your New Year's resolutions, or changing your online banking passwords each season.

Use tricks to remember them

In short, the best passwords look almost like a random mix of letters, symbols and numbers -- but how can you make them memorable?

- Use a mnemonic. Create a simple sentence (or use a phrase you'll remember) and capture the first letter of each word. For example: "All yellow dogs love to swim" gives you the character string "aydlts".
- Write down *part* of your password. Experts recommend writing down the first and last couple of characters to help jog your memory. If your password is "24violet\$", then jot down "24v...t\$" as a framework.
- Swap the numbers and symbols when you have to update -- and leave the letters and words in tact.
- Keep a secure list -- with caution. Many experts warn not to write down your passwords, especially for financial accounts where you could be on the hook for fraudulent activity if you do. However, some sources say you can write down your passwords if you keep them in a secure place (like a safe) rather than on your computer.

Another big no-no: using password managers or "remember this password" features in your Internet browser. If someone hacks into your computer, you've made it easier to access all of your other accounts.

Websites and online services that manage passwords are also a serious security risk.

Keep separate sets of credentials

You've got a strong user ID and password you can remember -- but don't use it too often, warn experts.

A recent survey conducted by Trusteer (an online security firm) revealed that the majority of internet users reuse their login credentials -- which can put their information at risk. Nearly three quarters of people use the same password for online banking as they do for other websites like social media and email. Worse yet, nearly half of respondents reported using the same password and user ID combination for a variety of purposes.

Admittedly, we don't want to have dozens of user IDs and passwords in our heads, but Trusteer recommends we should have at least three, one each for:

1. Financial websites only. (Use the strongest possible passwords for these websites).
2. Non-financial websites that contain personal information -- like social media websites, online shopping and email.
3. Websites that don't store any personal or financial information about you. (While not as urgent, you'd still like to avoid someone using your account to spam others or commit a crime.)

In addition, we should consider using a separate set for work. Employees who mix professional and personal credentials can put their employers at risk.

Pick better PINs

What about those number-only PINs we use online, in the store or at the bank machine? Many of the above rules still apply. For instance:

- Avoid using all one number, like "9999", and skip sequences like "1234" or "5678". These PINs are too easy to guess.
- Stay clear of your personal information like birthdays, phone numbers and account numbers.
- If you use dates, combine them. For instance, combine the date of your parents' anniversary with the date of your favourite team's big win.
- Turn letters into numbers. Using the keypad on your telephone, turn a code word into numbers to help you remember a numeric password or PIN.
- Use a unique PIN. Avoid reusing a previous PIN within a year or using one from another account.

Protect all of your accounts

One final warning from experts: **don't underestimate the importance of protecting your passwords.** According to the U.S. Computer Emergency Readiness Team (USCERT), many people mistakenly think their information isn't useful to hackers. It might be hard to see why your data is of interest when there are better targets, but criminals target anyone and anything for profit.

In addition, hacking your accounts, even seemingly insignificant ones like social media or email, is often part of a larger attack. Every piece of data leads to other information that can be used against you.

Unfortunately, there's no guarantee that your accounts will be completely safe from the crooks. However, most of us aren't taking advantage of the extra protection that stronger passwords and PINs can offer.

Additional sources: Consumer Reports Electronics Blog, U.S. Computer Emergency Readiness Team website, Microsoft Online Safety, Symantic.com

Copyright © 2010 All Rights Reserved - ZoomerMedia Limited.

The content is reproduced "as is", including links.