



Strong Passwords: How to Create and Use Them

Information from Microsoft.com

Your passwords are the keys you use to access personal information that you've stored on your computer and in your online accounts.

If criminals or other malicious users steal this information, they can use your name to open new credit card accounts, apply for a mortgage, or pose as you in online transactions. In many cases you would not notice these attacks until it was too late.

Fortunately, it is not hard to create strong passwords and keep them well protected.

What makes a strong password?

To an attacker, a strong password should appear to be a random string of characters. The following criteria can help your passwords do so:

- ***Make it lengthy.*** Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal. Many systems also support use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.
- Combine letters and numbers. ***The greater variety of characters that you have in your password, the harder it is to guess.***
- ***The fewer types of characters in your password, the longer it must be.*** A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection.
- ***Use words and phrases that are easy for you to remember, but difficult for others to guess.*** The easiest way to remember your passwords and pass phrases is to write them down. Contrary to popular belief, there is nothing wrong with writing passwords down, but they need to be adequately protected in order to remain secure and effective. In general, passwords written on a piece of paper are more difficult to compromise across the Internet than a password manager, Web site, or other software-based storage tool.

Password Strategies To Avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters.** "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- **Avoid your login name.** Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- **Avoid dictionary words in any language.** Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- **Use more than one password everywhere.** If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.
- **Avoid using online storage.** If malicious users find these passwords stored online or on a networked computer, they have access to all your information.

Keep Your Passwords Secret

Treat your passwords and pass phrases with as much care as the information that they protect.

- **Don't reveal them to others.** Keep your passwords hidden from friends or family members (especially children) who could pass them on to other less trustworthy individuals. Passwords that you need to share with others, such as the password to your online banking account that you might share with your spouse, are the only exceptions.
- **Protect any recorded passwords.** Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.
- **Never provide your password over e-mail or based on an e-mail request.** Any e-mail that requests your password or requests that you go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted company or individual. E-mail can be intercepted in transit, and e-mail that requests information might not be from the sender it claims. Internet "phishing" scams use fraudulent e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more.
- **Change your passwords regularly.** This can help keep criminals and other malicious users unaware. The strength of your password will help keep it good for a longer time. A password that is shorter than 8 characters should be considered only good for a week or so, while a password that is 14 characters or longer (and follows the other rules outlined above) can be good for several years.

- **Do not type passwords on computers that you do not control.** Computers such as those in Internet cafés, computer labs, shared systems, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, bank balances, business mail, or any other account that requires a user name and password. Criminals can purchase keystroke logging devices for very little money and they take only a few moments to install. These devices let malicious users harvest all the information typed on a computer from across the Internet—your passwords and pass phrases are worth as much as the information that they protect.

What To Do If Your Password Is Stolen

Be sure to monitor all the information you protect with your passwords, such as your monthly financial statements, credit reports, online shopping accounts, and so on. Strong, memorable passwords can help protect you against fraud and identity theft, but there are no guarantees.

No matter how strong your password is, if someone breaks into the system that stores it, they will have your password. If you notice any suspicious activity that could indicate that someone has accessed your information, notify authorities and your financial institution as quickly as you can.

