Microsoft

Strong passwords: How to create and use them

Published: March 22, 2006

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, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:

- **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. An ideal password combines both length and different types of symbols.
- **Use the entire keyboard**, not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.

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, such as password managers.

Create a strong, memorable password in 6 steps

Use these steps to develop a strong password:

1. **Think of a sentence that you can remember.** This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old."

   Check if the computer or online system supports the pass phrase directly. If you can use a

2. pass phrase (with spaces between characters) on your computer or online system, do so.
3. **If the computer or online system does not support pass phrases, convert it to a password.** Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".
4. **Add complexity** by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".
5. **Finally, substitute some special characters.** You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word) "M$8ni3y0".
6. **Test your new password with Password Checker** Password Checker is a non-recording feature on this Web site that helps determine your password's strength as you type.

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 using only look-alike substitutions of numbers or symbols.** Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.
- **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.

The "blank password" option

A blank password (no password at all) on your account is more secure than a weak password such as "1234". Criminals can easily guess a simplistic password, but on computers using Windows XP, an account without a password cannot be accessed remotely by means such as a network or the Internet. (This option is not available for Microsoft Windows 2000, Windows Me, or earlier versions) You can choose to use a blank password on your computer account if these criteria are met:

You only have one computer or you have several computers but you do not need to access information on

- one computer from another one
- The computer is physically secure (you trust everyone who has physical access to the computer)

The use of a blank password is not always a good idea. For example, a laptop computer that you take with you is probably not physically secure, so on those you should have a strong password.

How to access and change your passwords

Online accounts

Web sites have a variety of policies that govern how you can access your account and change your password. Look for a link (such as "my account") somewhere on the site's home page that goes to a special area of the site that allows password and account management.

Computer passwords

The Help files for your computer operating system will usually provide information about how to create, modify, and access password-protected user accounts, as well as how to require password protection upon startup of your computer. You can also try to find this information online at the software manufacturer's Web site. For example, if you use Microsoft Windows XP, online help can show you how to manage passwords, change passwords, and more.

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 to 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. Learn more about phishing scams and how to deal with online fraud.
- **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 as quickly as you can. Get more information on what to do if you think your identity has been stolen or you've been similarly defrauded.