SECURE PASSWORDS

How do I create a secure password? With password theft becoming more and more widespread, security experts recommend using a strong, secure password for financial transactions such as those that involve PayPal, iTunes, or bank accounts. A strong, secure password is one that is easy to remember but difficult to crack. Figure 1-44 offers guidelines for selecting secure passwords and avoiding ones that are easily crackable.

FIGURE 1-44

Tips for Creating Secure Passwords

- Use passwords that are at least eight characters in length. The longer the password, the tougher it is to crack.
- Use a combination of letters, numbers, and special characters such as $, #, if permitted.
- Use uppercase and lowercase letters if the hosting computer is case sensitive.
- Use a passphrase based on several words or the first letters of a verse from a favorite poem or song. For example, the words from the nursery rhyme "Jack and Jill went up the hill" can be converted to jjwuth. You can then insert special characters and numbers, and add some uppercase letters to create a password that still makes sense to you personally, such as J&J w^th!ll. This type of password appears random to anyone else but you.

- Do not use a password based on public information such as your phone number, Social Security number, driver's license number, or birthday. Hackers can easily find this information, and other personal facts such as names of your spouse, children, or pets.
- Avoid passwords that contain your entire user ID or part of it. A user ID of bjeffe coupled with a password of bjeffe123 is an easy target for password thieves.
- Steer clear of words that can be found in the dictionary, including foreign words. Dictionary attacks can utilize foreign language dictionaries. Even common words spelled backwards, such as drowssap instead of password, are not tricky enough to fool password-cracking software.

How do I protect my password? Once you have selected a strong password, you must take steps to keep it safe. Do not share your password with anyone. Avoid writing down a password. If possible, memorize it. If you must write down a password, do not leave it in an obvious place such as under your keyboard or mouse pad. Recording passwords in an unencrypted file stored on your computer is risky, too, especially if you have more than one password. A hacker who gains access to that file can use the passwords to access all your accounts.

If you think one of your passwords has been compromised, change it immediately. Even if you have no evidence of password tampering, security experts recommend that you change passwords periodically, say every six months. When you change your passwords, do not just make a slight variation to your current one. For example, do not change just4Me1 to just4Me2. You should not reuse your old passwords either, so it's best to keep a password history list.

TRY IT!

Which password for Dave Meyers is most secure?

○ DaveBMeyers

○ Dave12345

○ Gilgamesh

○ Ih2gtg8pw

○ HomeGilgamesh

Aside from good password maintenance habits, computer maintenance is also essential. Make sure that your entire computer is protected by security software, which is explained in the Software chapter.

◗ How do I deal with all my passwords and user IDs? You can accumulate many passwords and user IDs—for logging in to Windows, accessing online banking, using e-mail, shopping online, downloading music, and getting into your Facebook account. The more passwords and user IDs you have, the more difficult they become to remember.

How many times have you had to click the "I forgot my password" link when you logged in to an online account? Your passwords provide the most protection if they are unique, but accessing even 25 different Web sites that require 25 different user IDs and 25 corresponding passwords requires quite a memory. To add to the confusion, you must also regularly change passwords to your critical accounts!

Instead of using 25 different user IDs and passwords, you need some way to reduce the number of things you have to memorize. First, strive to select a unique user ID that you can use for more than one site. Remember that people with your name who selected user IDs before you might have already taken the obvious user IDs. For example, when John Smith selects a user ID, you can bet that other people have already used johnsmith, jsmith, and john_smith. To keep his user ID unique, John might instead select jsl2wm (the first letters in "John Smith loves 2 watch movies").

Next, you can maintain two or three tiers of passwords—the top level for high security, the second level for medium security, and the third level for low security. If you do not have too many accounts, you can opt for just two tiers—for high and low security. You can then select two passwords. Use the high-security password for accessing critical data, such as online banking, for managing an online stock portfolio, or for your account at an online bookstore that stores a copy of your billing and credit card information.

Use your low-security password in situations where you don't really care if your security is compromised. Some places on the Internet want you to establish an account with a user ID and password just to add your name to a mailing list. At other sites, your user ID and password provide access to information, but none of your critical personal or financial data is stored there. It is not necessary to change your low-security password very often. Figure 1-45 provides more information about tiered passwords.

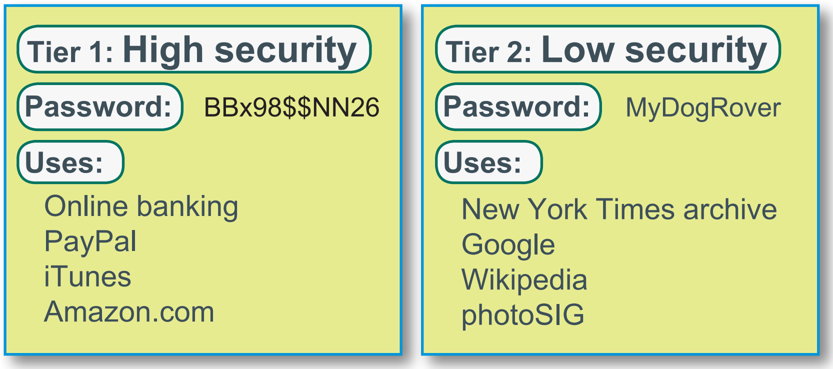


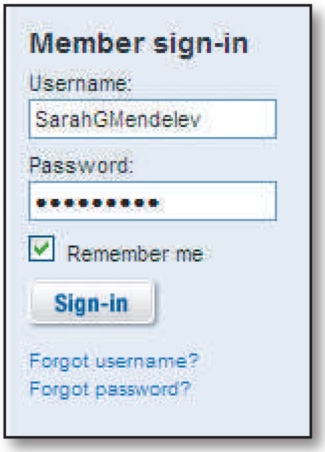
FIGURE 1-45

Tiered passwords reduce the number of user IDs and passwords that you have to remember; however, the disadvantage is that a hacker who discovers one of your passwords will be able to use it to access many of your accounts.

Can my computer help me to remember passwords? Your computer's operating system, Web browser, or other software might include a password manager to help you keep track of user IDs and passwords. A **password manager** (sometimes called a keychain) stores user IDs with their corresponding passwords and automatically fills in login forms. For example, when you register at a Web site while using a browser such as Internet Explorer, the browser stores your new ID and password in an encrypted file on your computer's hard disk. The next time you visit the Web site, your ID and password are automatically filled in on the login screen (Figure 1-46).

FIGURE 1-46

Checking the *Remember me* box saves your user ID and password for the next time you log in, but you have to be using the same browser.



Member sign-in

Username: SarahGMendelev

Password: ●●●●●●●●●

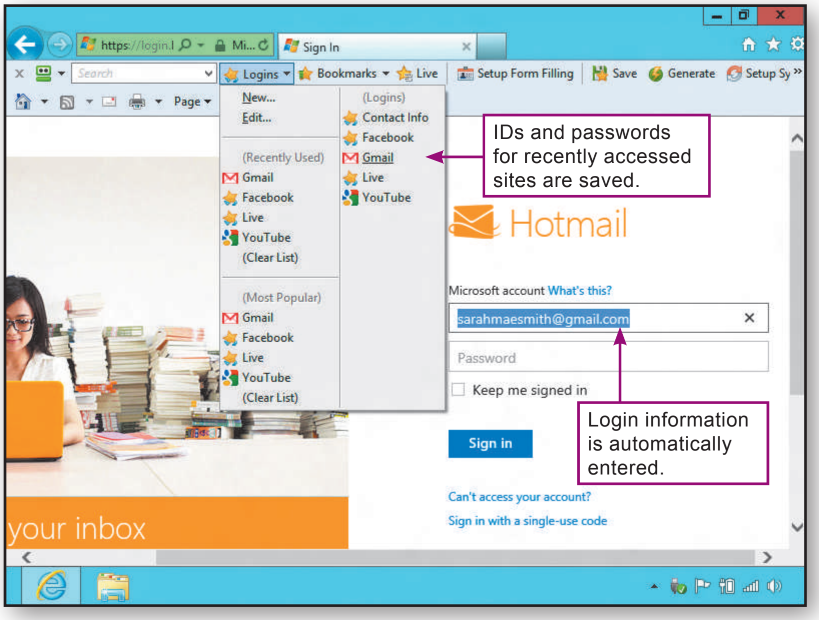
☑ Remember me

The drawback to password managers that are built into browsers, operating systems, or other software is that if you switch to different software or to a different computer, you will not have access to the stored passwords. For example, if you usually work with the Safari browser on your MacBook Air, it stores your passwords; but if you use a public computer in a coffee shop, your passwords are not accessible from that machine.

Standalone password manager software offers a more inclusive approach to creating and retrieving passwords.

What is password manager software? A standalone password manager is a software application that feeds passwords into login forms regardless of the software you're using. As with built-in password managers, a standalone password manager stores user IDs and passwords in an encrypted file. You can access this file using a master password. This type of password manager can be moved from one computer to another, for example, if you purchase a new computer.

A standalone password manager can also generate secure "nonsense passwords." You don't have to worry if the passwords are difficult to remember because the password manager software can keep track of them (Figure 1-47).



IDs and passwords for recently accessed sites are saved.

Microsoft account What's this?

sarahmaesmith@gmail.com

Password

□ Keep me signed in

Login information is automatically entered.

FIGURE 1-47

Password managers help you keep track of all your passwords. ▶ If you've never used a password manager and want to see how one works, start the guided tour for this figure in your interactive eBook.

In addition to generating and tracking your passwords, most password manager software provides other features, such as password strength meters and form fillers.

A password strength meter indicates whether your passwords are secure enough—a feature that is useful if you've created your own passwords, rather than using your password manager to generate them.

Form fillers automatically enter data into online Web forms such as those that request billing data when you order at an online shopping site. Many form fillers also match a Web form's URL against a set of valid URLs that you have provided in order to avoid sending data to a fake Web site that you have been lured to visit by a phishing message. When entering passwords, form fillers are not collecting your password from the keyboard; therefore, a hacker's keylogger cannot secretly record keystrokes.

There are several free, shareware, or open source password managers, such as KeePass, RoboForm, DataVault, and Kaspersky Password Manager. Some password manager software is portable, which means that it does not have to be installed on a computer before it is used. Instead, you can carry it around on a USB flash drive so that your passwords are available wherever you use a computer, such as in your school lab, at the library, or at work. When you remove the flash drive, your portable password manager leaves no traces of passwords behind (Figure 1-48).

For extra protection against intruders who might search your computer for passwords, a flash drive that contains a password manager can be unplugged when you are not accessing password-protected sites. You can also remove the flash drive from your computer when you're out so that your nosy roommate can't snoop through your computer files.

◗ Should I store passwords in the cloud? New password management techniques are being developed, but some offer their own set of potential security problems. For example, Web-based password managers can be attractive targets for password thieves. By breaking into a single site, a password thief could harvest thousands of passwords. As new password management technologies appear, make sure you evaluate them carefully before trusting them with your valuable data.

FIGURE 1-48

Some password managers are portable so that you can carry them with you on a USB flash drive.

Vydrin/Shutterstock.com

TRY IT!

Smartphone access can be controlled by a password. Would you recommend a password manager to your friend with an iPhone?

○ No. The phone's password is all my friend will need

○ Yes, especially if my friend wants to access Facebook or other subscription sites from the phone

QuickCheck

SECTION E

1. An authentication ______ is any method that confirms a person's identity using something the person knows, something the person possesses, or something the person is.

2. On a(n) ______ -sensitive server, the user ID BJP is different from bjp.

3. A(n) ______ attack can guess your password if you are using common passwords or everyday words.

4. A(n) ______ scam looks like a request from your bank or an online payment service, but is actually a hacker who wants you to disclose your user ID and password.

5. Most browsers include a built-in password ______ that remembers the user IDs and passwords you use when logging in to Web sites or online e-mail.

▶ CHECK ANSWERS