Password Safety Tips

Create strong passwords

The first rule of thumb is to use a different password for each of your accounts. It may be easier to keep track of just one password, but if a crook discovers that one password, he or she can access all of your accounts. This tip has been well publicized, but the Accenture consultancy's survey of 800 U.S. and U.K. consumers revealed that 88% use just one, universal password.

The second key to a robust password is to make it lengthy. According to a Microsoft spokesperson, each character you add to your password increases the protection it affords many times over. At a minimum, your passwords should be eight digits long, and 14 digits or more is ideal.

A compromised password could lead to identity theft or other dire consequences.

Using the greatest variety of characters possible in your passwords—letters, numbers, symbols—makes them harder to guess or uncover with malicious software. Microsoft's spokesperson says the fewer types of characters you use, the longer your password needs to be—if you use only letters and numbers make it 15 characters long.

Consider using words and phrases you can remember, but that others wouldn't guess. You can use the first letter of each word in a sentence, plus some numbers, mix upper- and lowercase, and include some misspellings and symbols. Here's one example: "I went to Hawaii in August 2009 with Bob," becomes "iWThI082009wB." Include a few symbols and it's "!WT*h;I082009w%B:." (The exclamation point substitutes for "I" and the randomly selected symbols bracket "Hawaii" and "Bob.") Who would ever guess that one? You can also substitute numbers for letters: "hate" becomes "h8."

After creating your password, you can test its strength with one of the "password checkers" available online such as Microsoft's Password checker and The Password Meter. If your password tests as weak, make it more complex.

Some password *don'ts* include:

- Using personal information such as family names, birthdays, or your address.
- Using sequences or repeated numbers, like abcd, 1234, or 9999.
- Using any words listed in a dictionary—they're easy for scammers to guess.

Keep passwords secret

Of course, the strongest password is useless if you share it with others, so guard yours closely. Don't reveal your passwords to family or friends. Children, particularly, may unwittingly pass them on to others, Microsoft's spokesperson reminds.

You shouldn't type passwords into public computers, such as those at libraries or in hotel lobbies. Even if you instruct the computer not to save the password, there could be malicious software on the computer that records your keystrokes for a criminal's use.

Also, you shouldn't send passwords via e-mail—it isn't a secure delivery channel—and you shouldn't enter a password if requested to do so via an e-mail.

If you see suspicious activity, notify the authorities and contact your credit union for help.

Don't store a list of your passwords on your computer—that would be a goldmine to a crook. Microsoft's spokesperson says it's safer to record your passwords on paper, and then hide the paper where others won't find it. Make sure it's a location you'll remember, though. What about between the pages of a book on your shelf? Another idea is to store the word file on a thumb drive and hide the thumb drive, says Ian Forkash, an information technology manager for the Credit Union National Association in Madison, Wis.

If you add encryption software to your computer, which codes information for privacy, you can store passwords there. Some versions of the software are available at no charge, such as a limited version of RoboForm for Windows. There's a fee for more comprehensive programs, such as Symantec's Endpoint Security.

Change your passwords frequently. While a very strong password can be good for several years, a weak one is only good for about seven days, Microsoft's spokesperson says.

Keep track of passwords

So, how do you remember your many passwords? Your secret list is one way, of course. And using a familiar phrase when creating the passwords, as described above, is another.

Consumer Reports suggests developing a couple of basic passwords you can memorize, and then adding different prefixes or suffixes to them for different accounts or Web sites, or scattering different symbols throughout.

Then, on your password list, you can write down just the add-ons and where they appear in the password. For example, if you add an asterisk as the second character in the password for one account, on your list you can just write: 2*.

Don't store a list of your passwords on your computer—that would be a goldmine to a crook.

Vince, who lives in Louisiana, uses a consistent approach to make his passwords memorable. "I use a combination of the Web site's name, along with recognizable information," he says. "For Yahoo, my password could be the first three letters of Yahoo, the first three letters of my pet's name, and the number of my birth month. So, my password for Yahoo might be: yahspo04. This way my password is always different, but still is easy enough to remember." Vince was one of several *Home & Family Finance Resource Center's* What's Your Story respondents.

Stephanie, from West Virginia, has another approach. "I have a good memory for numbers and things such as passwords, so I can typically remember many of them. But when I first change my password, I enter it in my rolodex as a code," she recounts. "Say my user name is 'username,' I would put down 'un.' If my password is 'password1,' I would put down 'pw1.' If I enter a year behind a password like 'password2009,' I would write down 'pw yr full.' Full means I've used a four-digit number instead of two." (Of course, Stephanie would want to use a combination of various characters rather than words that appear in dictionaries.)

When it comes to password storage, Catherine, from California, has a creative method. She uses a set of small index cards, hole-punched at the corner and attached to a metal ring made for organizing papers. "Every time I sign up on a new Web site I write its name on a card, along with the user name and password and other relevant information," she says.

She stores the cards in a safe place that she can remember. "The cards are small enough to drop in my bag, and easy enough to hide from prying eyes," she says. "It works very well for me."

Paul, from New Mexico, stores his online. "I use the Secure Login add-on available for the Firefox Web browser," he explains. "It uses one master password to give you automatic access to an encrypted database containing all your individual passwords."

Take action if someone gets your password

If, despite your best efforts, your password is compromised—possibly through a security breach at a business—don't panic. Monitor all the information you protect with that password, such as online shopping accounts or investment accounts, and request free copies of your credit reports from the national credit bureaus.

Using a variety of characters in passwords—letters, numbers, symbols—makes them harder to guess or uncover with software.

- Experian; 888-397-3742
- Equifax; 800-685-1111
- TransUnion; 800-888-4213

If you see suspicious activity in any of these places, notify the authorities and contact your credit union for help. If you're a victim of identity theft, the Federal Trade Commission's Web site includes information about what steps to take. But remember, the stronger your passwords, the less likely this is to happen.