

Search Web

What Makes a Password Stronger

by Stu Woo
Friday, June 24, 2011

provided by

THE WALL STREET JOURNAL.

With concern about hackers, tools for remembering so many codes; no more pet names or 123456.

For all its benefits, the Internet can be a hassle when it comes to remembering passwords for email, banking, social networking and shopping.

Many people use just a single password across the Web. That's a bad idea, say online-security experts.

"Having the same password for everything is like having the same key for your house, your car, your gym locker, your office," says Michael Barrett, chief information-security officer for online-payments service PayPal, a unit of eBay Inc.

Mr. Barrett has different passwords for his email and Facebook accounts -- and that's just for starters. He has a third password for financial websites he uses, such as for banks and credit cards, and a fourth for major shopping sites such as Amazon.com (Nasdaq: [AMZN](#) - [News](#)). He created a fifth password for websites he visits infrequently or doesn't trust, such as blogs and an online store that sells gardening tools.

A spate of recent attacks underscores how hackers are spending more time trying to crack into big databases to obtain passwords, security officials say. In April, for instance, hackers obtained passwords and other information of 77 million users in Sony Corp.'s (NYSE: [SNE](#) - [News](#)) PlayStation Network, while Google Inc. (Nasdaq: [GOOG](#) - [News](#)) said this month that hackers broke into its email system and gained passwords of U.S. government officials.

So-called brute force attacks, by which hackers try to guess individual passwords, also appear to be on the rise, Mr. Barrett says.

PayPal says two out of three people use just one or two passwords across all sites, with Web users averaging 25 online accounts. A 2009 survey in the U.K. by security-software company PC Tools found men to be particularly bad offenders, with 47% using just one password, compared with 26% of women.

[More from WSJ.com: [Sleevecandy.com Sells Vintage T-Shirts, Hipster Cred](#)]

Another PC Tools survey last year showed that 28% of young Australians from 18 to 38 years old had passwords that were easily guessed, such as a name of a loved one or pet, which criminals can easily find on Facebook or other public sites. Other passwords can be easily guessed, too. Hackers last year posted a list of the most popular passwords of Gawker Media users, including "password," "123456," "qwerty," "letmein" and "baseball."

"If your password is on that list, please change it," says Brandon Sterne, security manager at Mozilla Corp., which makes the Firefox browser and other software. Hackers "will take the first 100 passwords on the list and go through the entire user base" of a website to crack a few accounts, he says.

People typically start changing online passwords after they've been hacked, says Dave Cole, general manager of PC Tools. However, "after a relatively short time, all but the most paranoid users regress to previous behaviors prior to the security breach," he says. He and other security experts recommend people change or rotate passwords a few times a year.

To come up with a strong password, some security officials recommend taking a memorable phrase and using the first letter of each word. For example, "to be or not to be, that is the question," becomes "tbontbtitq." Others mash an unlikely pair of words together. The longer the password -- at least eight characters, experts say -- the safer it is.

Once people figure out a phrase for their password, they can make it more complex by replacing letters with special characters or numbers. They can also capitalize, say, the second character of every password for added security. Hence "tbontbtitq" becomes "tB0ntbtitq."

[More from WSJ.com: [Would Pilot 'Panic Button' Save the Day?](#)]

No matter how good a password is, it is unsafe to use just one. Mr. Barrett recommends following his lead and having strong ones for four different kinds of sites - email, social networks, financial institutions and e-commerce sites -- and a fifth for infrequently visited or untrustworthy sites.

Even the strongest passwords, however, are useless if criminals install so-called malware on computers that allow them to track a person's keystrokes. Security experts say people can avoid this by keeping their antivirus and antispyware software updated

More from Yahoo! Finance:

- [Companies Run Exclusively By Men](#)
- [Things Your Neighbors Won't Tell You](#)
- [Most Dangerous Cities in the U.S.](#)

[Visit the Family & Home Center](#)

and by avoiding downloading files from unknown websites and email senders.

Some security experts recommend slightly modifying passwords within each category of site. Companies such as Microsoft Corp. (Nasdaq: [MSFT - News](#)) offer free password-strength checkers, but users shouldn't rely on them wholly because such strength tests don't gauge whether a password contains easily found personal information, such as a birthday or a pet's name.

It's especially important to have a separate password for an email account, says Mozilla's Mr. Sterne. Many sites have "Forgot my password" buttons that, when clicked, initiate a password-recovery process by email. Hackers who break into an email account can then intercept those emails and take control of each account registered using that address.

[More from WSJ.com: [Start-Up's Camera Allows Photos to Be Refocused](#)]

Some websites, such as Google and Facebook, now let people register a phone number along with their account. If a person forgets his passwords, the sites reset the passwords by calling or sending a text message to that person.

Mr. Barrett says people should be able to remember four or five good passwords. If not, they can write them down on a piece of paper and stick it in their wallet, and then throw the cheat sheet away once all the passwords are memorized.

People who still struggle to remember them all can use a password manager. Several, such as LastPass, are free. LastPass prompts users to create a master password and then generates and stores random passwords for different sites. Some security experts warn against using managers that store passwords remotely, but LastPass Chief Executive Joe Siegrist says hackers can't access the passwords because all data is encrypted.

The worst thing that people can do after creating their different passwords: Put it on a sticky note by their monitor. "That defeats the entire purpose," says Mr. Sterne.

Heather O'Neill, a 27-year-old tech-company employee in San Francisco, had her Google email account broken into earlier this year. She says she used the same password for several sites, and that it was a weak one.

"I can't have one password for everything," she says. "Everything is going to be different."

Write to Stu Woo at Stu.Woo@wsj.com

Popular Stories on Yahoo!:

- [10 Industries Doomed to Disappear](#)
- [Meet the Man With \\$300,000 in Credit](#)
- [How Much You Should Really Be Saving](#)

Follow Yahoo! Finance on [Twitter](#); become a fan on [Facebook](#).

2 comments

Show:

[Post a comment](#)

[Maniac](#) 13 minutes ago | [Report Abuse](#)

0 0

No Password is safe for long term. They need to be changed at least every 60 days.

[Reply](#)

[Jane Doe](#) 17 minutes ago | [Report Abuse](#)

0 0

A much better solution was given in the "Silver Parachutes" book, where you can have only one password to remember yet it would be different every time use use it. The password can be a formula that you create and the formula can have elements of the particular website name.

[Reply](#)
