How Safe Are Your Passwords?

Is your favorite password secure? Could a hacker quickly crack it? For most of us, the answers to these questions are "no" and "yes, much faster than you think."

The table below shows estimates of the time a hacker would need to guess a password depending on the number and type of characters used. If your passwords consist of numbers only or lowercase letters only, or are shorter than seven characters, you're vulnerable to cyber-surprise.

Maximum time needed to guess password (assuming computing speed of 1 million guesses per second)	**Number of characters in password**						
	4	**5**	**6**	**7**	**8**	**9**	**10**
Password with numbers only	0.01 seconds	0.10 seconds	1.00 second	10.00 seconds	1.67 minutes	16.67 minutes	2.78 hours
With lowercase letters only	0.46 seconds	11.88 seconds	5.15 minutes	2.23 hours	2.42 days	62.84 days	4.48 years
With lowercase and uppercase letters	7.31 seconds	6.34 minutes	5.49 hours	11.90 days	1.70 years	88 years	4,584 years
With lowercase and uppercase letters plus numbers	14.78 seconds	15.27 minutes	15.78 hours	40.76 days	6.92 years	429 years	26,614 years
With lowercase and uppercase letters, numbers, and common punctuation symbols	1.36 minutes	2.15 hours	8.51 days	2.21 years	210 years	19,985 years	1,898,582 years

The estimates on the table are best-case scenarios. Your clever eight-character password is probably still easy to crack, for several reasons:

- Estimates shown on the table assume a "brute force" attack is used, wherein a computer program methodically tries to guess each character of a password. Since most computer-users pick passwords that incorporate words or names, hackers often use programs that utilize a "dictionary" attack, which tries to guess passwords by trying all the words in a dictionary and a name database—an approach vastly faster than brute force.
- The table shows the *maximum* time needed to guess a password using the brute-force method, but a hacker might get lucky and guess it early in the process. Times on the table indicate what happens when a hacker gets incredibly unlucky and captures your password only after trying every other possible combination of characters.
- The amount of time needed to solve a password is strongly tied to the hacker's computer speed. For the table, we assume a hacker's computer makes 1 million guesses per second, a somewhat arbitrary assumption; the hacker's computer could be much faster since many have several computers—often hijacked for the purpose—working together. Using 10 computers instead of one would reduce the time needed to guess a password by a factor of 10.

- Protections for some software are so weak that hackers don't even have to guess: They simply steal passwords or reset or circumvent them.
- A common password is likely to be guessed right away. Hackers usually try the most common passwords first, hoping to get lucky.

On the other hand, the times shown on the table are somewhat oversimplified in that the calculations assume a hacker somehow knows the length of the user's password, that it is constructed of numbers or lowercase letters only, and so on, and sets up an attack accordingly. Since hackers seldom have that information, they often try to guess passwords by using all keyboard characters. So in some ways, the length of your password—and avoidance of common passwords, words, and names—is what really matters.

Some password pointers:

- The most secure passwords consist of at least eight characters and include numbers, uppercase letters, lowercase letters, and punctuation.
- Avoid incorporating a word or name in your password. The more random your selection of characters, numbers, and symbols the better. Since at times many parents can't even quickly recall the names of their children, it's unrealistic to count on remembering 10 random keyboard characters. One approach is to pick a relatively obscure but easy-to-remember secret phrase or sentence, add numbers and punctuation, and then use only the first (or last) letter of each word in the phrase. For example, if your secret phrase is "One day Ashley Judd will marry me," your password could be "OdAJwmm!32." Another option is to misspell a memorable word—for example, "&Waldcats*98!" instead of "&Wildcats*98!".
- Choose a different password for your computer, email, and every website you use. If you use the same password every time, then a lot of databases store your master password, and anyone who steals your password from one site has access to your entire digital existence. Because most of us can't realistically expect to remember dozens of passwords, one way to control password chaos is to pick a complicated password and then incorporate into it part of the URL of each website to make it unique. For example, if your password is "OdAJwmm?32," when accessing *www.checkbook.org* your password might be "chOdAJwmm?32," "OdAJwmm?32ch," "cOdAJwmm?32k," etc.
- Another option is to keep track of everything using password management software. Examples include Password Depot (*www.password-depot.com*), Roboform (*www.roboform.com*), and Splash ID (*www.splashdata.com*). Current operating systems for Macs come with a built-in password management system called "Keychain."

Complex passwords are just one step toward maximizing security, but they'll do nothing if you carelessly let someone take control of your data—the hacker could simply record every action you take and every keystroke you input. Our article "Healthy Computing Habits," published in *CHECKBOOK*, Volume 15, No. 4, and available at *www.checkbook.org*, details ways to minimize the risk of attacks.