How to pick a new password, now that Twitter wants one

May 4 2018, by Anick Jesdanun

This April 26, 2017, file photo shows the Twitter icon on a mobile phone, in Philadelphia. Twitter says it discovered a bug that stored passwords in an internal log in an unprotected form. Though Twitter says there's no indication of any breach or misuse of passwords, the company is recommending a change as a precaution (AP Photo/Matt Rourke, File)

Yet another service is asking you to change your password.

Twitter said Thursday it discovered a bug that stored [passwords](#) in an internal log in plain text, without the usual encryption. Though Twitter says there's no indication that anyone has stolen or misused those passwords, the company is recommending a change as a precaution.

Here are some tips on coming up with a new password and safeguarding your account—even if your password is compromised.

——

COMPLEXITY COUNTS

Don't even think of using "password" as your password. Picking any common word as your password should be avoided because it's easily guessed using software that tries out every word in the dictionary.

However, you can get a good password by combining two or more words, such as "rocketcalendar." Sprinkle in some numerals and punctuation marks, and make some of those letters in caps, and you've got a strong password. So "rocketcalendar" becomes "rocket44!calendaR." (But don't use that one; the fact that it's in this article means hackers probably already have it in their databases.)

Some services will even require your passwords to have certain characteristics. As you type a new password on Twitter, the [service](#) will tell you whether it's "Too Obvious" or "Weak." Go for "Very Strong."

——

KEEP PASSWORDS FRESH

Each service should have its own password. If you use "rocket44!calendaR" on Twitter, don't use it on Facebook. Once hackers

get your password on one service, they'll try it on other services, too. Outsmart them by using a fresh password each time. It can be as simple as adding the first three letters of the service's name, so Twitter gets "rocket44!calendaRtwi" and Facebook gets "rocket44!calendaRfac."

You can turn to a password-manager service to help you keep track of various passwords, though make sure the one you use hasn't had its own security problems . If you're storing passwords in a spreadsheet or other document on your computer, be sure to protect it with its own password (Microsoft Office lets you encrypt files). Avoid naming the file "passwords." Call it "badmovies" or something innocuous.

——

RESET AND REFRESH

Some security experts recommend that you change your passwords frequently, though treat that advice with caution. When there's a breach, it doesn't matter whether that password is two weeks or two years old. And if you change passwords too often, you risk forgetting them and falling back on simpler, less-secure passwords.

——

A BETTER SAFEGUARD

You can ignore much of this advice if you just do one thing: Turn on two-factor authentication, which Twitter calls "login verification." You'll get a text with a code each time you try to log in from a new device or web browser. So even if hackers get your password, they can't do much unless they have your phone—or some other way to intercept the code.

Of course, this makes it even more important to protect your phone with

a passcode, so that no else can get these texts if your phone is lost or stolen.

Citation: How to pick a new password, now that Twitter wants one (2018, May 4) retrieved 23 April 2024 from https://phys.org/news/2018-05-password-twitter.html