Forget Tough Passwords: New Guidelines Make It Simple

npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple

All Tech Considered

Tech, Culture and Connection

August 14, 20174:51 PM ET

Heard on All Things Considered

Here's what we've been told about passwords:

- Make them complicated.
- Use numbers, question marks and hash marks.
- Change them regularly.
- Use different passwords for each app and website.

These guidelines often leave users frustrated and struggling to remember them all.

Now the National Institute of Standards and Technology is about to make all of our lives much easier. The organization recently revised its guidelines for creating passwords, and the new advice sharply diverges from previous rules.

"The traditional guidance is actually producing passwords that are easy for bad guys and hard for legitimate users," says Paul Grassi, senior standards and technology adviser at NIST, who led the new revision of guidelines.

The organization suggests keeping passwords simple, long and memorable. Phrases, lowercase letters and typical English words work well, Grassi tells NPR's Audie Cornish. Experts no longer suggest special characters and a mix of lower and uppercase letters. And passwords never need to expire.

"We focus on the cognitive side of this, which is what tools can users use to remember these things?" Grassi says. "So if you can picture it in your head, and no one else could, that's a good password."

While these rules may seem suspiciously easy, Grassi says these guidelines help users create longer passwords that are harder for hackers to break. And he says the computer security industry in both the public and private sectors has received these new rules positively.

"It works because we are creating longer passwords that cryptographically are harder to break than the shorter ones, even with all those special character requirements," Grassi says. "We are really bad at random passwords, so the longer the better."

Previously, security experts recommended the use of password manager apps to ensure users' accounts were protected. Grassi says these apps are useful because they completely randomize the password, but he says they aren't necessary to maintain security.

Grassi stands by these new guidelines because, he says, previous tips for passwords affected users negatively and did not do much to boost security. When users change their passwords every 90 days, they often aren't dramatically changing the password, Grassi says.

"I'm pretty sure you're not changing your entire password; you're shifting one character," he says. "Everyone does that, and the bad guys know that."