Regular password changes make things worse

More like this

-

RELATED TOPICS

Security experts have been saying for decades that human weakness can trump the best technology.

Apparently, it can also trump conventional wisdom.

Since passwords became the chief method of online authentication, conventional wisdom has been that changing them every month or so would improve a person’s, or an organization’s, security.

Not according to Lorrie Cranor, chief technologist of the Federal Trade Commission (FTC), who created something of a media buzz earlier this year when she declared in a blog post that it was, “time to rethink mandatory password changes.”

She gave a keynote speech at the BSides security conference in Las Vegas earlier this month making the same point.

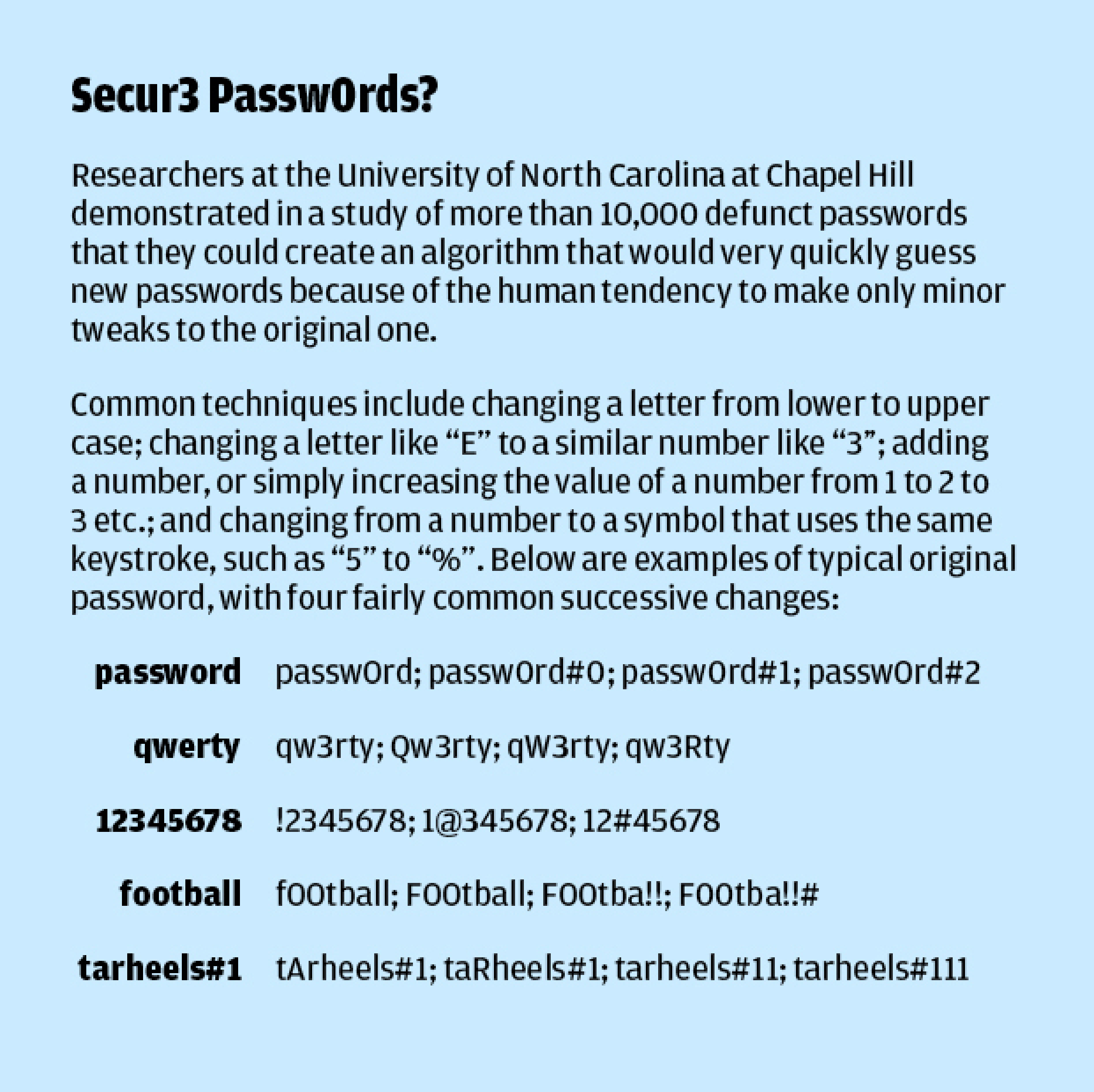
But the message was not new – she has been preaching it for some time. Cranor, who before her move to the FTC was a professor of computer science and of engineering and public policy at Carnegie Mellon University, gave a TED talk on it more than two years ago.

She contends that changing passwords frequently could do more harm than good. Not because new passwords, in and of themselves, would make it easier for attackers, but because of human nature.

She cited research suggesting that, “users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily.”

This, she said, was demonstrated more than six years ago in a 2009-2010 study at the University of North Carolina at Chapel Hill. Researchers, using passwords of more than 10,000 defunct accounts of former students, faculty and staff, found it much easier to crack new passwords if they had cracked an older one, since users tended create a new password with a minor tweak of the old one.

Those tweaks included changing a lower-case letter to upper case, substituting a number for a letter, such as a “3” for an “e,” or simply adding a couple of letters or numbers to the end of the previous password.



Secur3 Passw0rds?

Researchers at the University of North Carolina at Chapel Hill demonstrated in a study of more than 10,000 defunct passwords that they could create an algorithm that would very quickly guess new passwords because of the human tendency to make only minor tweaks to the original one.

Common techniques include changing a letter from lower to upper case; changing a letter like “E” to a similar number like “3”; adding a number, or simply increasing the value of a number from 1 to 2 to 3 etc.; and changing from a number to a symbol that uses the same keystroke, such as “5” to “%”. Below are examples of typical original password, with four fairly common successive changes:

password	passw0rd; passw0rd#0; passw0rd#1; passw0rd#2
qwerty	qw3rty; Qw3rty; qW3rty; qw3Rty
12345678	!2345678; 1@345678; 12#45678
football	f00tball; F00tball; F00tba!!; F00tba!!#
tarheels#1	tArheels#1; taRheels#1; tarheels#11; tarheels#111

Cranor said the researchers found that if they knew a previous password, they could guess the new one in fewer than five tries. A hacker who had also stolen the hashed password file would be able to guess new ones within three seconds – and that was with 2009 technology.

The UNC study is not the only one reaching that conclusion. Researchers at the School of Computer Science at Carleton University in Ottawa, Canada, in a paper published in March 2015, concluded that security advantages of password expiration policies were, “relatively minor at best, and questionable in light of overall costs,” for the same reason the UNC researchers found.

"(W)hen password changes are forced, often new passwords are algorithmically related to the old [password], allowing many to be found in few guesses," they wrote.

And the National Institute of Standards and Technology (NIST), in a draft publication from April 2009 (although it was marked "Retired" this past April), said password expiration policies frequently frustrate users, who then, "tend to choose weak passwords and use the same few passwords for many accounts."

Not surprisingly, attackers are very much aware of these vulnerabilities. The latest Verizon Data Breach Incident Report (DBIR) found that 63 percent of all data breaches involved the use of stolen, weak or default passwords.

A report released earlier this month by Praetorian found that four out of the top five activities in the cyber kill chain had nothing to do with malware, but with stolen credentials, thanks to things like weak domain user passwords and cleartext passwords in memory.

All of which would seem to be even more ammunition for organizations like the FIDO Alliance, which has been crusading to eliminate passwords entirely since its formation four years ago. The Alliance has been pitching two passwordless authentication options it hopes will be irresistible to both users and service providers.

But even with increasing interest and acceptance of those options, Brett McDowell, FIDO's executive director, has acknowledged that there will be a "long tail" for password use.

And during that long transition, he and others say there are multiple ways to improve security that don't involve creating a new password every couple of months that is easier to crack than previous ones.

Zach Lanier, director of research at Cylance, cites Apple's TouchID and Google's Project Abacus as mobile options to wean users off passwords, but said passwords are obviously, "still around, and they're likely to be for a bit longer. It's just that they're so 'standard' for people and enterprises, and have been for so long, that it's really hard to make them completely disappear."

In the interim, he said, organizations can improve their password security through a combination of employee training and, "actively testing their authentication mechanisms and auditing users' passwords – cracking them – whether it's through internal infosec teams or external firms. In my opinion, it should be both," he said. "This can give the organization a better idea of where things are broken, from people to technology."

The users can be brought into this as well, he added, by, "making available the tools to enable, if not force, users to test the strength of their own passwords."

McDowell agrees that education is, "a laudable endeavor, especially to help users avoid falling victim to phishing and/or social engineering attacks." But he said the "shared secret" authentication model is vulnerable to too many forms of attack – not just social engineering – hence the need to eliminate them as soon as possible.

Tom Pendergast, chief strategist, Security, Privacy & Compliance, at MediaPro, said organizations can and should have much more rigorous password policies. "Current policies set the bar far too low for complexity in passwords and don't require multi-factor authentication, acknowledged as the best commonly-available solution," he said.

Lanier agreed. “There are some really awful organizations, sites or services that can’t seem to move past the year 1998 with authentication,” he said.

“Things like not allowing certain characters, or limiting the length of the password to something ridiculously low, all because the developers, database admins, and/or designers are using outdated or deprecated mechanisms.”

Pendergast said he sees the same thing. “There is plenty of existing technology designed specifically to prevent users from repeating passwords, using common passwords, and enforcing password rules. A surprising number of companies don’t use these basic password reinforcement functions,” he said.

And, Lanier noted that, “password managers are, of course, a huge boon for generating complex passwords without the fuss of having to remember them or write them on a Stickie note. This at least reduces the risk that a person might serialize their password choices. Certainly not a panacea, but for the average person, it’s a great idea.”

Still, as McDowell noted, even rigorous passwords can’t compensate for a person being fooled by a skilled attacker. “Many times, passwords are simply given away in a phishing or social engineering attack,” he said. “I saw a recent stat from the SANS Institute that 95% of all attacks on enterprise networks are the result of successful spear phishing.”

All agree that the weaknesses of human nature mean it would be better to move beyond passwords. But, as McDowell notes, human nature also requires that whatever replaces passwords must be, “easier to use than passwords alone.

“User experience is going to win over security every time so the key to building a secure password replacement system is to build ease-of-use into its foundation,” he said.

Until then, Lanier said, organizations should, at a minimum, not rely on passwords alone.

“At the very least, if/when that poor password gets cracked or guessed, two-factor authentication raises the bar for the attacker,” he said.