How many passwords can you remember? Get ready to remember more

December 16 2018, by Tim Johnson, Mcclatchy Washington Bureau

Credit: CC0 Public Domain

Got too many passwords to remember? Just wait. It's going to get a lot worse.

Average consumers five years from now may face double the demands for passwords, said Emmanuel Schalit, chief executive of Dashlane, a consumer password security company.

Schalit and other experts predict that passwords will explode in further use before they eventually fade, replaced by new technology.

Digital devices in homes are growing more numerous, but Schalit said the real driver behind the steady increase in the need for passwords are the sprawling number of accounts for consumers to obtain public services, interact on healthcare and education websites and deal with retailers.

"The problem is not passwords. The problem is to ask humans to memorize and manage hundreds of them," Schalit said.

Dashlane, headquartered in New York City, estimates that the average American currently has about 200 accounts that require some sort of password identification, and that number will rise to 400 within five years or so.

One expert believes Dashlane's forecast is low.

"I think they are being conservative. I think we will have more," said Tom Galvin, executive director of the Digital Citizens Alliance, a nonprofit focused on internet consumer safety.

Some consumers simply give up at the constant demand for passwords, re-using the same password over and over again, a practice that makes cybersecurity experts cringe. If hackers compromise any single account, they can access a victim's other accounts.

That's why some financial institutions, big retail outlets and other

businesses are moving toward biometric identifiers such as fingerprints, iris and voice scans, and facial recognition tools.

But those identifiers aren't foolproof either.

"Your fingerprints are exposed. Your voice is exposed. The iris of your eye is exposed. ... If your biometric information is stolen, you can't replace it. ... It is compromised forever," Schalit said.

Those dangers were underscored when foreign hackers in 2015 filched about 21.5 million personal records from the Office of Personnel Management, which is essentially the human resources office for the federal government. Among the records stolen were usernames, passwords, Social Security numbers, and home addresses, but also the detailed, deeply personal information that is included in applications for security clearances, including the contact information for all the applicants' friends and family. Hackers also got away with at least 5.6 million fingerprints. Chinese hackers were later charged in the breach.

The pace of hacks is only quickening. Last month, Marriott International acknowledged that personal data of up to 500 million guests had been lost during a four-year period in which hackers lurked in the Starwood guest reservation system. Secretary of State Mike Pompeo last week confirmed that China was also behind that breach.

Schalit said since roughly two-thirds of consumers re-use variations of the same password on multiple sites, in all likelihood hundreds of millions of Marriott guests are likely to have other accounts that are potentially easily vulnerable to hackers.

For many consumers, password fatigue set in long ago. Some simply click on "forgot password" on less-used websites and start the process over again.

Then there are those like music impresario Kanye West who opt for the simplest passwords imaginable. During a meeting with President Donald Trump in the Oval Office on Oct. 11, West typed his passcode into his iPhone as television cameras zoomed in. It was "000000." Dashlane dubbed that the worst password blunder of 2018.

Only some 20 million consumers worldwide use password managers offered by companies like LastPass, 1Password, Dashlane, EnPass, LogmeOnce and True Key. In most cases, those services create a unique password for each site a consumer visits and stores them in an encrypted repository with a master password. The consumer only has to remember one password.

Andrea L. Limbago, chief social scientist at Virtru, a data protection company in Washington, said passwords are likely to be phase out within a decade.

Passwords today are limited to letters, numbers and symbols, she said, but data scientists are already working on other identifiers.

She said she witnessed a recent demonstration of the use of colors, emojis, videos and images, sometimes in combination, as passwords.

"It worked well. It's not something that's commercially available. But it works," Limbago said.

Future log-in sites may show consumers things like a large palette of colors, she said, and allow them to combine those with other nearly limitless identifiers.

"That's much easier for us as humans to remember versus the super long passwords that are more rigorous and secure but are really, really super hard to use," Limbago said.

In the meantime, though, Galvin said one of the best thing consumers can do is to change passwords routinely. If hackers obtain older, obsolete passwords, they will prove useless.

"It's like having an old key to my house. It really doesn't matter," Galvin said.