cnbc.com

Everything you know about passwords could be wrong

Abigail Ng

4–5 minutes

Having trouble remembering your password after a long holiday? That's just the tip of the iceberg of password-related problems, experts say.

It's not just post-vacation blues. Having to remember a complicated string of characters is a

problem acknowledged by associations such as Fido Alliance, which aims to help reduce the world's reliance on passwords.

Committing multiple complex passwords to memory is a "massive usability challenge," Andrew Shikiar, executive director of Fido Alliance said.

"This usability challenge makes people revert to the easiest password to remember and reuse, which then exacerbates password risks," he added.

Raluca Budiu, director at UX research and consulting firm Nielsen Norman Group, agreed with the sentiment.

Speaking from a user experience perspective, she said: "The biggest problem with passwords is that people have to remember them."

Noting that websites today have "different, relatively sophisticated" requirements, she said: "It's harder and harder to come up with a meaningful password that will be easy to recall."

Security concerns

Even for people with the strongest passwords and photographic memories, security concerns remain.

Passwords are “human readable shared secrets that typically are stored on a central server and thus are susceptible to being stolen and reused,” said Fido Alliance’s Shikiar, adding that the theft could happen in a “myriad” of ways.

Jonathan Knudsen, a senior security strategist at Synopsys Software Integrity Group, said: “People overestimate the ability of websites to protect their passwords. This is why it is so important to use unique passwords for every site.”

“If you reuse the same password everywhere, then a password breach at just one poorly-protected site can be catastrophic for you,” he said.

Unfortunately, an analysis of data from more than 47,000 organizations revealed that employees reuse a password an average of 13 times. That’s according to LastPass’ third annual global password security report.

The solution, experts say, is to move away from

this form of authentication entirely. Instead, users could log in using smartphones, USB security keys and biometric scanners such as fingerprint or voice verification.

In China, QR codes and facial recognition are already being used to make payments.

Fido Alliance's Shikiar, however, pointed out that there would be "behavioral and device upgrade cycles to overcome."

"The 'a-ha' moment will come when people start to realize that the same simple gesture that means 'unlock' on their phone can now mean 'log in' — instead of being dependent on passwords."

Until passwords become a thing of the past, here are three myths, debunked:

1. **Multi-factor authentication is not foolproof**
   "Every security feature can be defeated," Knudsen of Synopsys Software Integrity Group said, when asked about two-factor authentication.
   Hackers can take over a phone number in an attack known as SIM jacking or SIM swapping.

That means one-time passwords would be sent to the attackers and not the rightful owners of the accounts.

2. **Complex passwords aren’t that much better**
   ”Anything is better than the laziest of passwords,” said Shikiar, pointing to the “ever-popular” options of 123456 and password. “But ultimately any password can be stolen.“
   Additionally, people think replacing letters with numbers or symbols to create a more complex password is an effective against bad actors, said Knudsen. “For example, they might believe that ‘secret’ is a weak password but ‘s3cr3t’ will be hard to guess,” he said. “However, hackers are wise to this type of substitution and will have no trouble guessing such a password.”
3. **Frequent changes don’t help with password security**
   Many employees would be familiar with the dreaded email that comes every three to six months — a reminder that your password is expiring soon — and needs to be replaced.

But, according to Shikiar, “forcing frequent password changes or a mix of special characters has actually proven to create passwords that are more susceptible to being forgotten and — surprisingly — to being swiped by hackers.”

— CNBC’s Kate Fazzini, Yen Nee Lee and Annie Palmer contributed to this report.