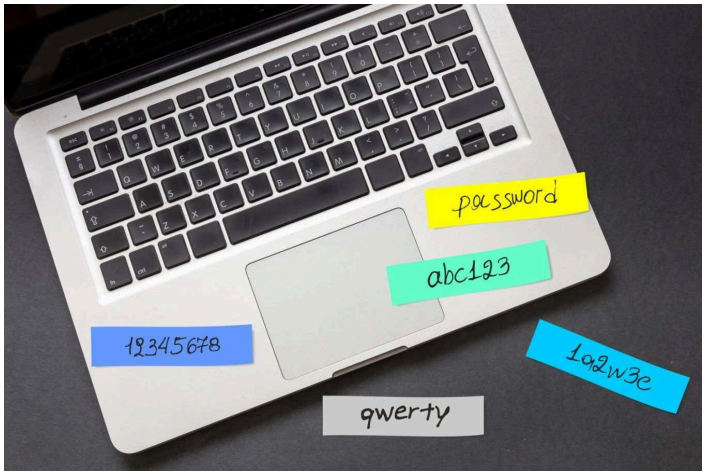
Forcing people to change their passwords is officially a bad idea

A US standards agency has issued new guidance saying organisations shouldn't require users to change their passwords periodically – advice that is backed up by decades of research

By Matthew Sparkes on September 27, 2024



Many people struggle to think of new passwords and remember them. rawf8/Shutterstock

Many organisations make staff regularly change their computer passwords for security reasons. Now the US government is saying those who make and run software and online tools should stop the practice. So, what should people really be doing?

The latest advice from the US National Institute of Standards and Technology (NIST) isn't coming out of the blue. It is based on decades of research showing forcing website and software users to periodically change their passwords actually harms security.

Alan Woodward at the University of Surrey, UK, says enforcing regular password changes goes against all official advice, but it is still widely done. Research has shown many times it leads to users picking poor passwords that are easy for hackers to guess, he says. "If you make security difficult to use, or awkward to use, or you put the onus on the user all the time, it slowly becomes less and less effective," says Woodward.

Angela Sasse at University College London says the debate was settled a long time ago: her own research over many years, as well as that of colleagues, points to enforced, regular password changes being bad for security. People can't remember the endless passwords and begin

making bad decisions like simply appending incrementing numbers to simple words or phrases – “password1”, “password2” and so on.

“We observed the memory load and annoyance it caused from interviews and self-reported data over 20 years ago. People told us coping strategies that lead to weaker passwords,” says Sasse. “The mystery is why that established scientific knowledge and official advice has not managed to shift outdated advice from certain certifications, the minds of auditors and a big part of the security industry.”

The latest pressure to drop the practice comes from the NIST, which spends its time vetting the next generation of encryption algorithms and other standards, and is currently consulting on “digital identity guidelines“, which govern how software and websites verify users.

In those new standards, NIST says online tools and software “SHALL NOT require users to change passwords periodically” for the same reasons highlighted by Sasse and Woodward.

The UK’s National Cyber Security Centre (NCSC), which is part of the Government Communications Headquarters (GCHQ), published documents in 2018 advising companies that continually forcing users to create new passwords was unhelpful. “Regular password changing harms rather than improves security,” the report says. “The user is likely to choose new passwords that are only minor variations of the old.”

NIST was not available for comment at the time of writing, and the NCSC did not respond to *New Scientist’s* questions.

Woodward thinks relying solely on password security is essentially a “dreadful idea” anyway, and that best practice is to have two-factor authentication requiring a password and another layer of security like a one-time code sent in an SMS message. “That just kind of kills all the attacks dead in the water, really,” says Woodward.