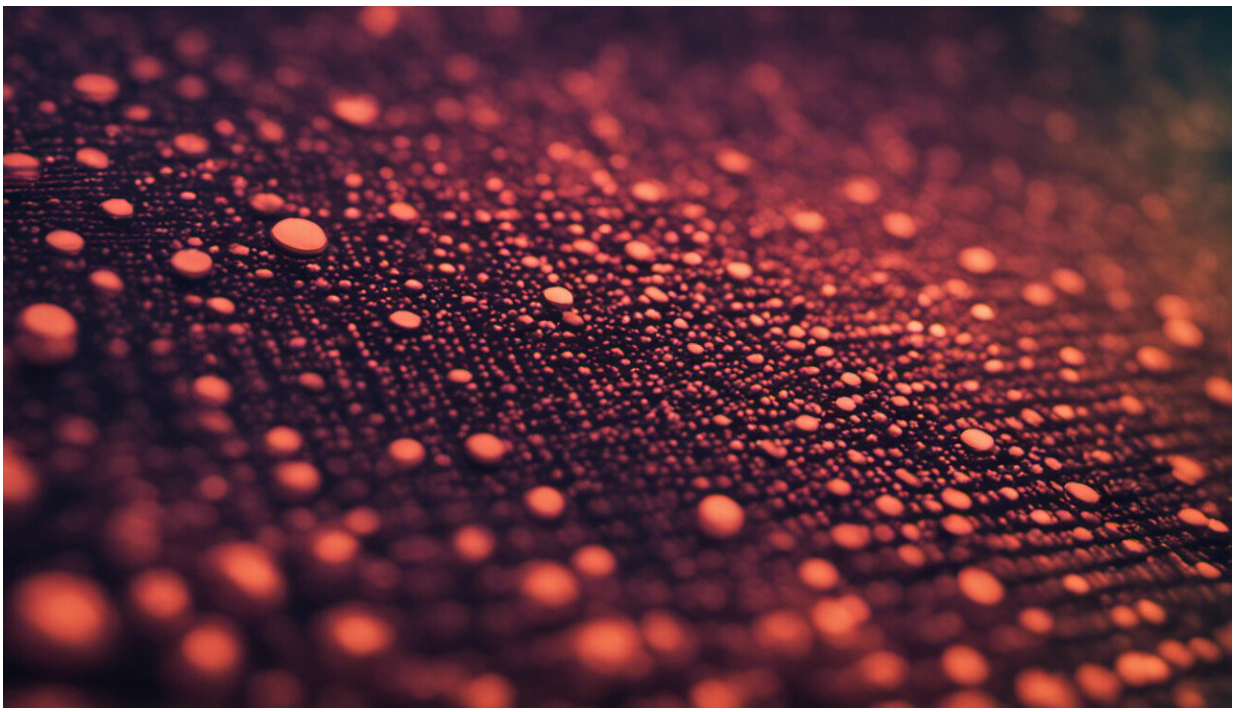
Stop blaming people for choosing bad passwords. It's time websites did more to help

January 3 2022, by Steven Furnell



Credit: AI-generated image (disclaimer)

Year after year, passwords like "123456," "qwerty" and even "password" are found to be the most popular choices and 2021 was no exception.

These reports generally come with the same advice to users: create better

passwords to protect your security online. Although this is may well be true, it's also time to realize that years of promoting this message has had little or no effect.

To improve things, I believe we need to stop blaming people and instead put the onus on websites and services to encourage and enforce better "cyber hygiene."

Of course, it's easy to point the finger at the users—they're ultimately the ones making the poor password choices. But at the same time, it's now well known that people commonly make these choices. So it's fair to assume that without guidance or restrictions to prevent weak passwords, they're likely to continue with the same habits.

Nonetheless, we have successive generations of users who are not told what a good password looks like, nor prevented from making lazy choices. It's not hard to find examples of websites that will accept the very worst passwords without complaint. It's similarly easy to find sites that require users to create passwords—yet give them no guidance in doing so. Or sites that will offer feedback that a user's password choice is weak, but allow it anyway.

How providers can do better

If you're responsible for running a website or a service that will accept the likes of "123456," "qwerty" or "password," it's time to rethink your system. If you let users get away with bad choices, they will believe that they are acceptable and continue this bad practice.

On the contrary, by implementing stronger protocols, you can help to address the problem at its source. Websites should have processes in place to filter out poor passwords—a "blacklist" of common choices.

And while it can be useful to offer guidance for users at the point of password creation, sites should stop insisting on things that authoritative organizations like the UK National Cyber Security Centre and the US National Institute of Standards and Technology now say ought not to be enforced. For example, they advise against the requirement for password complexity (like including upper and lower case letters, numbers and punctuation symbols).

Both organizations indicate that increasing password length is more important than complexity. This is because longer passwords are more resistant to brute force cracking (where attackers try all letter, number and symbol combinations to find a match) and less complex passwords can be easier to remember.

Yet many sites continue to demand complexity and impose upper limits on length, in the process often blocking perfectly reasonable password choices that our browsers and other tools can automatically generate for us.

You may wonder why this is important. If people want to choose weak passwords and put themselves at risk, then why should that become the provider's problem? One argument is that if a service is charged with protecting users' personal data (as providers are through GDPR) then it doesn't make a lot of sense to allow users to leave themselves vulnerable by choosing weak passwords.

It's also worth noting that in some cases one user's weak password could give an attacker a foothold into the system from which to exploit other weaknesses and increase their access. So it's arguably in the provider's interest to minimize these opportunities and protect other people's data in the process.

Passwords aren't going anywhere

We're now seeing a move towards passwordless authentication, but this name in itself emphasizes the dominance of password-based methods. Their death was predicted more than 15 years ago, and yet they're still here. It's safe to assume they're going to be with us for some time yet.

So we have a choice: take collective responsibility to get the basics right—which involves action by users and providers—or maintain the collective effort to shrug our shoulders and complain about users' behavior.

For those providing and operating password-based systems, sites and services, the call to action is hopefully clear: check what your site permits and see if it should do better. If it lets weak passwords pass, then either change this, or at a minimum do something that tries to deter users from choosing them.

If you are reading this as a user and you're looking for some good advice on creating better passwords, the UK National Cyber Security Centre provides some useful tips. These include combining three random words to give yourself longer but more memorable passwords, and saving your passwords securely in your browser to further reduce the burden of remembering passwords across multiple sites. So even if providers are not doing enough, there are still some things you can do to protect yourself.

Provided by The Conversation

people-bad-passwords-websites.html