https://www.wsj.com/articles/complex-password-cyber-security-risk-11631051077

JOURNAL REPORTS: TECHNOLOGY

# The Problem With 'Complex' Passwords

They make it too hard for users, who in turn make it too easy for hackers.

*By Karen Renaud*
Sept. 8, 2021 8:30 am ET

We all know the drill when creating a password. In the name of "complexity," we're typically asked to use a minimum of eight characters, including at least one uppercase letter, one lowercase letter, a number and a special character. Oh, and we need to memorize the password and not use the same one anywhere else.

Here's the problem with these instructions: They do the opposite of what was intended. They make it too hard for users, who in turn make it too easy for hackers.

The issue, as we all know too well, is that the passwords most organizations ask for are essentially nonsense strings, without any meaning. But that creates all sorts of problems.

First, the human brain deliberately prunes nonsense, typically when we sleep. That complex nonsense string evaporates overnight.

Then there is Zipf's Law: Humans always expend the least possible effort in carrying out tasks. Given the brain's propensity to prune things, it requires a great deal of deliberate memorization to force the brain to retain a complex password, and extra effort to reset the password when it is inevitably forgotten. So, people find ways around it—using the same password everywhere or writing it down (often in the computer itself).

## Forced change

Forcing people to change their passwords on a regular basis—as most companies do—further compounds the problem. People don't want to just throw away all the time they spent memorizing a password, so they often simply regress toward using something like "May2021!" and then merely change the month each time they are forced to change their password.

SHARE YOUR THOUGHTS

*What do you think are the pitfalls of required "complex" passwords? Join the conversation below.*

The situation was only made worse by the global shift to online shopping over the past year due to the pandemic, with people opening more online accounts, all with the same password.

The result is a perfect cybersecurity storm, with people being required to

manage increasing numbers of complex nonsense passwords, employing coping skills, and hackers gleefully taking advantage of the situation.

None of this is a secret. In fact, in 2017, several influential organizations—the U.S. Department of Commerce's National Institute of Standards and Technology, the UK's Centre for the Protection of National Infrastructure, and the UK's National Cyber Security Centre—published updated guidelines about password "good practice." One big change is that the traditional measures of strengthening passwords, using multicharacter-type complexity, were determined to be the wrong way to go, as was forced password expiration. They recognized that while multicharacter complex passwords are indeed strong, they lose that strength when you expect human brains to remember them.

## And yet…

So why do many organizations still mandate the outdated complex password rules, forcing users to provide a nonsense string of letters, numbers and special characters?

It could be a simple lack of knowledge—the person developing the website might have been taught that complex passwords are advisable, and they aren't aware that the advice has changed since then. Or it could be just inertia; people have a tendency to keep doing what they have long been doing.

Whatever the reason, just telling IT administrators that the advice has changed, or pushing them to adopt new protocols, isn't likely to get very far. Abandoning their longstanding practices of requiring password complexity suggests they have been doing the wrong thing for a long time. That's hard for most people to accept.

But there might be another way. Consider, first, the word "complex." The American Heritage Dictionary of the English Language defines it as "consisting of interconnected or interwoven parts."

Perhaps the best way to approach institutions, therefore, isn't to say they have been doing it all wrong and have to change. Instead, it's to say that the best passwords are still complex ones. But instead of complexity as a string of nonsense letters, numbers and characters, the best passwords are those that are composed of interconnected parts.

In essence, this would be a passphrase, composed of at least three different words. Not coincidentally, that's the kind of password that the organizations mentioned above recommended in 2017.

If people use three or more words as their password, they can memorize it more easily, tailor it to the specific account the password is being used for, and then not have to write it down. For example, consider the relative difficulty of memorizing "Ih&Kdxp!" vs. "Rhinos are scarcer than Yellow Jackets." The latter is much easier to recall. It could, say, be your password for the account you have at the local zoo. Or "Good Health Is Peachyl" could be your passphrase for your company-benefits site. Adding humor enhances memorability.

Recent research suggests users can strengthen passwords even more by using two different languages in a single password. So instead of "Rhinos are scarcer than Yellow Jackets," you could use, "Rhinos are scarcer than Gelb Jackets, using the German word for "yellow." That's still easy to remember, but so much harder for hackers to guess.

In other words, instead of trying to tell people to eschew complexity requirements, and risk triggering a resistance to change, we could point out that passphrases are just another way to meet complexity requirements, too. And a lot easier to remember.

*Dr. Renaud is a chancellor's fellow at the University of Strathclyde in Glasgow, Scotland. She can be reached at reports@wsj.com.*