BLISS·MCKNIGHT®

# Are Your Passwords So Complicated They Are Unsafe? The Answer May Surprise You


Complex passwords have long been touted as safer and users have been encouraged to include a variety of upper-case letters, lower-case letters, numbers, and special characters.

However, new research shows that passwords comprising a complex string of numbers and characters are hard to remember and easy to hack. The study found that users are more likely to engage in unsafe cybersecurity practices if they are required to come up with complex passwords.

An associate professor at James Cook University asked study participants to create increasingly complex passwords and then asked them about their password habits in a separate survey.

The professor found that 75 percent of the participants used strategies to remember their passwords that compromised their cybersecurity, such as using the same password for multiple sites.

The "brute force" method is one of the most common ways hackers crack passwords. A computer program will rapidly guess character combinations until it guesses the entire password. Even complex passwords, if they are not long enough, can be easily guessed this way.

As a result, cybersecurity experts are increasingly moving away from recommending complex passwords and instead suggesting passwords that seem simpler but are harder for hackers to guess.

For example, using a password such as "sunlightautumnleaves" is easy to remember and long enough to prevent a successful brute force attack, unlike "TvU4E#k&." Stuart Layt "When it comes to passwords, complex is not always safer, new study shows" brisbanetimes.com (May 9, 2021).

*Commentary*

Let’s start with what the information above is not saying. It is not saying that you should have a simple password or no password. What it is saying that you need to have long and different passwords for different accounts, but ones that are not so overly complicated whereby you make compromises that create a vulnerability.

According to the latest research in password safety, it is better to create passwords that are simple enough that you can remember them without writing them down, but still secure enough to thwart hackers.

It is important to note that password managers do not guarantee that your passwords will be safe from cybercriminals. In May 2021, the password manager Passwordstate announced that hackers had accessed user data. Stuart Layt "When it comes to passwords, complex is not always safer, new study shows" www.brisbanetimes.com.au (May 09, 2021).

Therefore, passwords that are easy to remember so you can keep track of them without writing them on paper or in a document or even relying on a password manager increase your cybersecurity.

This latest guidance has called into question the idea that complex passwords keep you safe, but other password best practices remain in effect.

Namely, it is essential to make your password as long as possible. The longer the password, the more protected you are from brute force attacks. You should still avoid common sayings, quotes, or song lyrics as well as personal information that would be easy for a hacker to look up. Cybersecurity & Infrastructure Security Agency "Security Tip (ST04-002) Choosing and Protecting Passwords" us-cert.cisa.gov (Nov. 18, 2019).

One of the most important tools in protecting yourself from a cyberattack is using unique passwords for every account. US-CERT states that reusing a strong password leaves you as vulnerable as using a weak password.

This is another reason why simple but long is better than short and complex. You must create unique passwords for every account, so choosing ones that you can remember without becoming frustrated and reusing them is critical.

***This article has been adapted from the Bliss McKnight Practical HR Resources website. Articles and other risk management resources are available on the site to members of the AIC Endorsed General Liability Insurance Program. For more information contact risk@blissmcknight.com.***