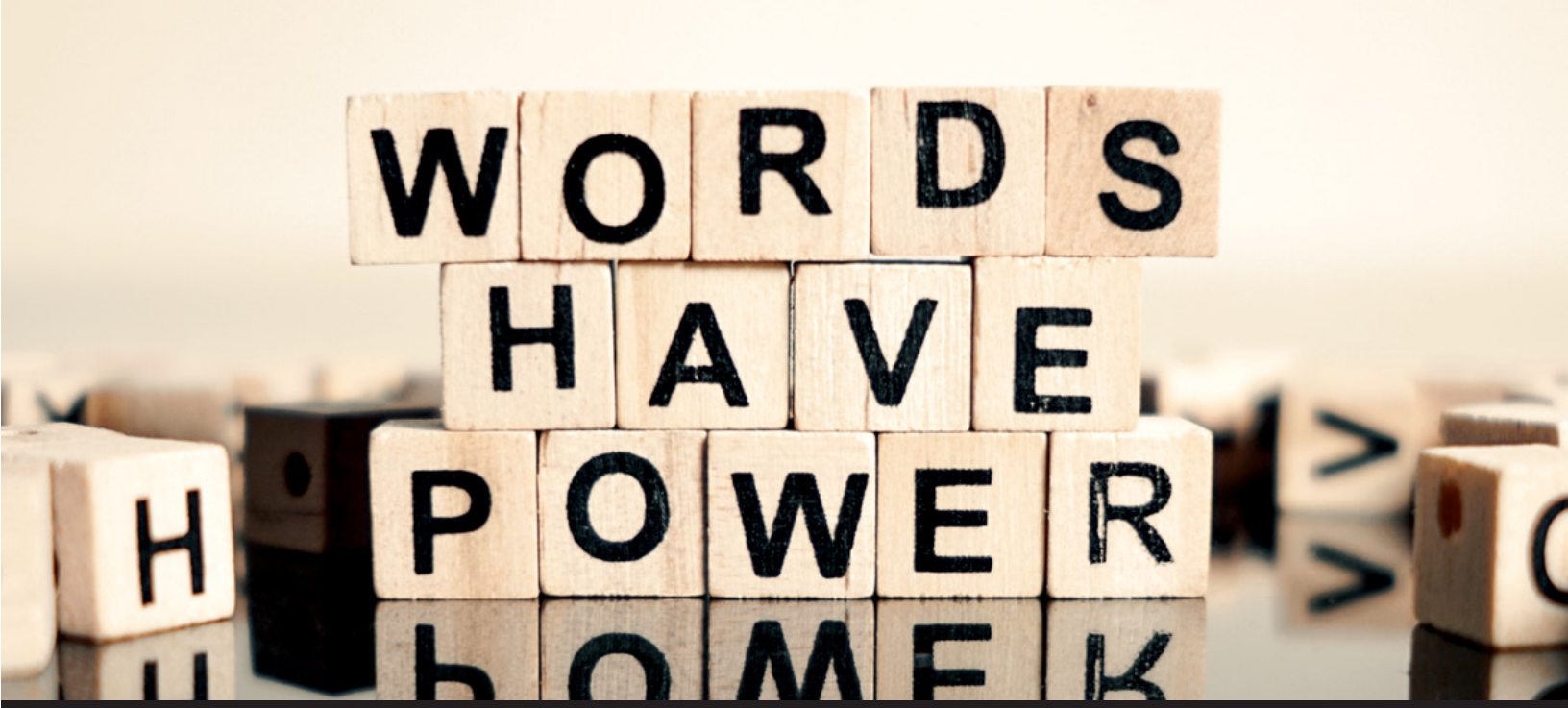

Passwords vs. Passphrases: Let the Battle Begin!

Devolutions

PASSWORDS SHOULD BE STRONG AND COMPLEX, USING UPPER AND LOWERCASE ALPHANUMERIC CHARACTERS TO INCREASE PASSWORD STRENGTH

Welcome fight fans to our main event of the night – the heavyweight championship of the account protection world! In the red corner is the popular fan favorite: PASSWORD.

And in the blue corner is the fearless and powerful contender: PASSPHRASE. For the many fans in attendance and the millions watching around the world: let's get ready to ruummmmmmmmble!

Passwords

A password should be (but often aren't!) comprised of 12 or more uppercase and lowercase letters, in combination with various symbols and numbers. According to a 2010 Georgia Tech Research Institute (GTRI) study, the shorter the password, the easier it is to break. The study showed how a 12-character random password could defeat code-breaking and cracking software. Passwords should also be strong and complex, using upper and lowercase alphanumeric characters to increase password strength and help resist brute-force attacks and guessing. Eventually, though, any password can be compromised.

Passphrases

A passphrase is much longer than a typical password — which takes it well out of the brute force attack vulnerability zone — and contains spaces in between words, which means it could look something like this: "The more complex your password is the better!". A passphrase can contain letters, symbols, and numbers, and it doesn't have to be a proper sentence or grammatically correct. So your high school composition teacher might get offended, but that's a small price to pay for robust security, right?

And the Winner Is...

Passphrases with a first-round KNOCKOUT! And the reason is simple: end users — who are always going to be the weakest link in the information security chain — are pretty bad at choosing long, strong passwords. In fact, NIST's latest guidelines no longer recommend that end users change their password every few months, because they tend to pick worse passwords rather than better ones. Compared to a password, a passphrase is easier for end users to create, and often much easier to remember.

Why Isn't Everyone Using Passphrases?

The reason no one really uses passphrases is because, well, it's a new concept and old habits are hard to break. Think about it, can you name one website that prompts you for a passphrase instead of a password? I'm willing to bet nothing comes to mind. Our brains have been well-trained to think of passwords, and not passphrases. In fact, over the years, when we tried to put a space between characters in a password, whatever software or system we were trying to access would yell at us and say: NO SPACES!

But it's never too late to develop better habits, and so we're hopefully heading into a future where passphrases are everywhere, and passwords are old school.

Always Stronger with Two Factor (2FA)

It's also important to mention that relying solely on passphrases or passwords isn't enough to be fully protected against hackers, phishing and other attempts to bypass authentication. That's why it's wise to add 2FA as an extra layer of security to your accounts. You can never be too secure, right?

What's the Story in Your Organization?

Is your organization using passphrases instead of passwords? Please share your experience with the end users you deal with. Are they changing their behavior to be part of the cyber security solution, or do you spend a lot of time keeping them from being the weakest link in the chain? Please comment below.