NEW PASSWORD GUIDELINES

For the longest time, security experts have recommended long, complex, and sometimes random, passwords. Unfortunately, those guidelines create a dilemma for individuals and organizations alike. Of course, the more complexity you add to a password, the harder it is to crack. But a more complex password also means it's harder to remember.

Complexity often fosters frustration, which in turn promotes laziness and tempts people to use the same password for multiple accounts. But there is hope! The National Institute of Standards and Technology (NIST) released a special publication of updated best practices for creating passwords. Here are the highlights:

Ditch the complexity.

Passwords that feature a bunch of random characters and capitalization no longer get the stamp of approval. Instead, passphrases that feature simplicity, now top the list of recommendations.

For example, the previous guidelines recommended developing a passphrase like, "The dog wants to play fetch."

- Use a mixture of upper and lowercase letters: **TheDogwantstoPlayFetch**
- Next, add some numbers: **TheD0gwantst0PlayFetch**
- Then, some symbols: **TheD0gw@ntst0PlayFetch!**

And finally, your passphrase is complete. The problem? You've effectively complicated a supposedly uncomplicated process and created a hard-to-remember password.

Now let's apply the new guidelines to this same passphrase: **thedogwantstoplayfetch**

Done. No random characters. No random capitalization. No numbers or complicated features. Just an easy to remember passphrase. There will still be systems that insist you use a combination of symbols, numbers, and letters. But when you have the option to use simplicity, NIST suggests you do it!

Screen new passwords for weaknesses.

NIST recommends screening passwords against a list that contains commonly used or compromised passwords. ***Here are examples of what that list may include:***

- Passwords obtained from previous breaches.
- Dictionary words.
- Repetitive or sequential characters.
- Context-specific words, such as the name of the service, the username, and derivatives thereof.

While this process mostly falls on the shoulders of management, individuals should apply it to their personal accounts.

End arbitrary password replacement.

Say goodbye to periodic or frequent password changes, a process that NIST suggests does more harm than good. Creating unique passwords for every account is already a difficult challenge. Requiring those passwords to be changed routinely creates frustration and encourages poor behavior (such as reusing passwords across multiple accounts). ***The new guidelines recommend only forcing changes if a security incident occurs which compromises existing accounts.***

Above all, follow organizational password policy. Our policies may not favor or adhere to everything NIST recommends (even the highlights listed above), but the password processes we have in place are for the benefit of everyone within our organization. If you have questions, please ask!