FAIRDINKUM

LEVERAGING INNOVATION WITH TECHNOLOGY

Creating Secure Passwords

Although password minimum characters and complex password requirements are in place, weak passwords can still be created that conform to these policies. They are present to merely enhance all passwords to attempt to allow employees to create stronger passwords. The below tips will help to avoid weak passwords and explain why passwords that appear to be strong are not.

Methods Used to Decrypt / Guess Passwords

Using consumer available technology. As an example relatively inexpensive equipment can test 30 MM passwords per second on an offline encrypted password, this number can increase exponentially with the addition of various equipment.

1. Automated Brute Force Dictionary Attack

Attackers utilize this type of attack on both online and offline attempts. This attack tests various potential passwords taken from very large wordlists and the addition of rules which add common password formats against a live login or obtained encrypted password (these can be taken from computers that were logged into previously or pulled from discarded hard drives as well as other techniques).

2. Automated Brute Force Attack

Similar to a dictionary attack, in this scenario every combination within a specific range of characters is tested against an encrypted offline password or online portal. This type of attack is less common, as minimum character count is increased. As the minimum character count increases the time needed to test all possible combinations increases exponentially and time to decryption is not feasible.

Password Creation Tactics

1. The Use of Plain Dictionary Words Within a Password

Using a single dictionary word even if it exceeds minimum password character length with your password is not recommended. The format of these passwords allow for automated dictionary attacks to decrypt these within a short amount of time.

Example weak password: Abbreviation2020!

This password would meet character minimums as well as complexity requirements, however this is considered a weak password.

It is advisable to use multiple dictionary words that have no combined association, this will prohibit dictionary attacks from discovering the password.

Example stronger password: Mondaypotato2020!

Although the above password is similar in length and added character types the “strong” example gains effectiveness since it can better avoid current methods.

2. Character Password Format

Through research it has been found that users often conform to similar password patterns

Examples of most common formats

- Capitalized first character
- 1-4 digits used in the beginning or end of a password (commonly used is the current year or most recent past year)
- Symbol used in the beginning or end of password (commonly used ! or @)
- Replacing letters with symbols or digits (Alex to @l3x)

As mentioned in the dictionary attack method “rules” can be used to more efficiently decrypt/guess password. These rules add common format types to dictionary words to create potential password matches that are seen commonly.

Our example of Mondaypotato2020!, while more secure can be further enhanced with a change in format.

Example: moNdaypotatO20!20

This example further strengthens the password by removing commonly used formats

3. Special Character (Symbol) Use

The last item to assist in strengthening passwords is to use uncommon allowable special characters.

Commonly used special characters: !@#$

Allowable characters in most cases are: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Try replacing common symbols with relatively unused characters such as | ; : . < >

Example: moNdaypotatO20:20

Example: 20moNnday:20potatO

Please do not use any of the passwords listed in this document or copy exact formats. Instead create passwords using similar techniques.