Multi-factor Authentication and Password Security

Did you know?

A password-cracking expert has unveiled a computer cluster that can perform up to 350 billion guesses per second.

What is Multi-Factor Authentication?

You understand the saying, “a chain is only as strong as its weakest link.” This is no different when it comes to protecting your assets. A one-factor authentication (1FA) system, such as a password, offers a single layer of protection. This means that if someone steals your password, they have access to your assets. Multi-factor authentication (MFA) is added layer(s) of protection, that confirm you are who you say you are. MFA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

Why should I care about MFA?

You should care about MFA as it protects you from bad actors, but works whether or not you have been targeted. This does not eliminate your password - you can still access your assets. However, when both a password and a second factor are required, it is much more likely that the second factor will be unique to you, the user, to confirm you are who you say you are. Most MFA allows you to choose how to perform the second factor - from you, the user, to quick single click or touch authentication requests, username and password, plus something you have - like a smartphone app to approve authentication requests, and something you know - like a personal identification number (PIN) or other easy-to-remember number.

Password Security Do's and Don'ts

PASSPHRASE EXAMPLES:

PASSPHRASE DO'S:

Don't use common words spelled backwards.
Don't use less than sixteen characters. More characters are harder to break.
Don't use predictable phrases like the name of your first pet or high school mascot.
Don't use common words, system commands, sites, companies, hardware, or software.
Don't use personal information such as birthdates, addresses, phone, yubikey, etc.)
Don't use work-related information such as building names, and personalization of this added security you are accommodating your desires.
Don't use your username or email. It is a common password in lists.
Don’t use work-related information such as building names, computer, or system commands.
Don't use your favorite song, book, movie, TV show, website, or other personal information.
Don't use work-related information such as building names, computer, or system commands.
Don't use your favorite song, book, movie, TV show, website, or other personal information.
Don’t use work-related information such as building names, computer, or system commands.

PASSPHRASE DON'TS:

Don't use dictionary words or terms that can be found in a dictionary, including foreign language, or system commands, sites, companies, hardware, or software.
Don't use work-related information such as building names, computer, or system commands.
Don't use personal information such as birthdates, addresses, phone, yubikey, etc.)
Don't use common words spelled backwards.
Don't use less than sixteen characters. More characters are harder to break.

Do's and Don'ts

Use a different password for every account. Otherwise, a single data breach can compromise passwords for other accounts.
Consider using a passphrase, which is an easier, better way to choose a password. Passphrases are often longer than an acronym or series of numbers.
Use at least one special character (like $, #, %, and $) in your password.
Use at least one number in your password.
Use both upper and lowercase letters.
Use three or more words in your password.

Aim for 20 to 30 characters in length. Passwords with more characters are harder to break.

When available, use multi-factor authentication (MFA) to maximize its strength.
Lengthen your password periodically. Change your multi-factor authentication (MFA) when available.

Password Management

If you need to save or “Remember” your passwords, consider using a password manager. Password managers help you to store, organize and even generate strong and unique passwords. They can also be associated with each account.

Multi-factor Authentication

More and more entities are adding MFA or No-Way!

MFA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

If you have MFA options available, understand the security features offered to you where your most valuable assets are housed.

If MFA is not offered where your most valuable assets are housed, consider choosing a provider who offers MFA for your best protection.

MFA protects assets.

Trust?

For more information, visit trust.cisco.com.