Password Tips

Back to Information Security

Table of Contents

- Why is password password security important?
- How are passwords compromised or stolen?
- What is a pass phrase? How does it differ from a password?
- Do's and Don'ts of Passwords and Pass Phrases
- Tips for Creating a Strong Pass Phrase

Why is password security important?

Password security is important to the security of your own identity at CSUCI and beyond. If your password is compromised, an intruder may obtain access to your email, your files, your funds, your personal information or your identity.

Even worse, you may expose others' personal information if your password is compromised, not your own. Once an intruder has your user name and password, they may be able to gain entry or to monitor other restricted or confidential resources on a computer network.

Further, you may actually be held personally liable for breaches of security or compromise of information due to poor password security.

How are passwords compromised or stolen?

Hackers can employ a number of tools to compromise or "crack" passwords. A hacker might use "sniffer" software to watch network traffic for unencrypted passwords sent over a network. Hackers also might use a keystroke logger to keep track of the keystrokes on your computer. Another popular attack vector is the "brute force" or "dictionary" attack, where a hacker will use software which automatically tries every word in a dictionary.

In many cases, users themselves are at fault for creating these situations. Examples of "easy targets" include:

- People who keep their password on a sticky note on their monitor, under their keyboard, or in their desk drawer
- Choosing passwords that are easily guessed, such as the name of a loved one or your telephone number
- People who share their password with others

What is a pass phrase? How does it differ from a password?

A *pass phrase* is simply a phrase that is used in place of a password. While passwords are typically made from single words, pass phrases are made up of multiple words.

Pass phrases are more useful than passwords because, when created correctly, they are usually easy to remember, but much harder for others to guess.

The following table has some examples of how a password can be made into a more secure pass phrase:

Password	Pass phrase
123Banana	1Don'tLikeBananas
Summer	SummertimeandTheLiving$Eazy
Skiier27	SkierFor*27Years

For more information on creating pass phrases, please see Tips on creating strong pass phrases.

Do’s & Don’ts of Passwords and Pass Phrases

DO:

- Use at least 8 characters in your password or pass phrase
- Use a "pass phrase" instead of a single "password" (see "Tips on Creating Strong Pass Phrases")
- Use a mix of upper- and lower-case letters, numbers, and special characters to create your password or pass phrase
- Make your password or pass phrase easy to remember, but hard for others to guess
- Change all passwords and pass phrases every 90 days

DON’T:

- Don't use only letters or only numbers (e.g., butter, 8573985, etc.)
- Don't use any word that can be found in the dictionary — even foreign or technical words (e.g., dog, tincture, polarized)
- Don't use passwords with double letters or numbers (e.g., aabbcc, 111333, etc.)
- Don’t use passwords with number sequences (e.g. 12345, 445566, etc.)
- Don’t use these easily guessed passwords: password, admin, 123456, csuci, or the name of your department.
- Don't use names of spouses, children, girlfriends/boyfriends or pets.
- Don’t use your full name or any part of it in your password
- Don't use phone numbers, Social Security numbers, birthdates, or other personally identifiable information in your password.
- Don't use the same word as your user ID/user name, or any portion or variation of it in your password.

- Don’t use examples of good passwords as your password (i.e, any examples in the “Tips for creating good passwords” section)
- Don’t share your password with anyone, regardless of circumstances.
- Don’t write down your password.
- Don’t reuse your password. Some systems will enforce a “password history” which prohibits you from re-using previous passwords.

Tips for Creating Strong Pass Phrases

"Pass phrases" are preferred to the use of an individual "password", as pass phrases are typically much harder for others to guess, but usually just as easy to remember.

The key to a strong pass phrase is: *Make it easy for your to remember, but hard for others to guess*.

NOTE: DO NOT use any of the pass phrases words in any of the examples below as your password. They are meant as a guideline only.

- Make sure your pass phrase contains 8 or more characters
- Take a phrase and remove all the vowels (e.g. “40 hours per week” becomes “40hrsprwk”
- Substitute numbers or special characters for letters in a phrase (e.g. “I feel so good” becomes “1f33l$0g00d”)
- Take a line of poetry or a favorite song and use the first letters in the first line (e.g. “Do not go gentle into that good night” becomes “Dnggitgn”
- Use a mix of upper-case letters, lower-case letters, numbers, and special characters (such as !, #, $, *, etc).
- Use transliteration, i.e., use phonetic sounds to spell words (e.g., “Seize the Day” becomes “SeasThaDeigh”