Strong Passwords

Strong Passwords

On this page:

Password rules
Creating effective strong passwords
Other suggestions
Use a pass phrase
Pass phrase hints:
Are password managers a good idea?
Related links

Password rules

Your password or pass phrase **must** conform to the following rules:

- It **must** be different from your current password.
- It **must** be 8 characters or longer.
- It **must** contain characters from at least two different character classes (upper- and lower-case letters, letters and symbols, letters and numbers, etc.)
- It **must** be composed of characters in the Roman alphabet or symbols on the US keyboard.

- It **must not** be based on your Kerberos username.
- It **must not** be a word that appears in the dictionary.

Creating effective strong passwords

- **Longer passwords are better passwords.** The more characters a password cracking program has to crunch, the harder it is to guess. A 12-character password can take 200 years to crack, an 8-character password might only take a few hours.
- **A random mix of alphabetical, numeric and symbolic characters.** - the more "random" your password, the stronger.

Other suggestions

- **Remove all the vowels from a short phrase in order to create a "word."**
  Example: `llctsrgry` ("All cats are gray")
- **Use an acronym:** choose the first or second letter of your favorite quotation.
  Example: `itsotfitd` ("It's the size of the fight in the dog")
- **Mix letters and non-letters in your passwords.** (Non-letters include numbers and all punctuation characters on the keyboard.)
- **Transform a phrase by using numbers or punctuation.**
  Examples: Idh82go (I'd hate to go), UR1drful (you are wonderful).
- **Avoid choosing a password that spells a word.** But, if you must, then:
  - Introduce "silent" characters into the word. Example: `va7ni9lla`
  - Deliberately misspell the word or phrase. Example: `choklutt`
  - Choose a word that is not composed of smaller words.
- **Add random capitalization to your passwords.** Capitalize any but the first letter.
- **Long word and number combinations.** For example, take four words, and put some numbers between them:
  `stiff3open92research12closer`
- **An acronym for your favorite saying, or a song you like.**
  Example: `GykoR-66` (Get your kicks on Route 66) or `L!isn!` (Live! It's Saturday Night!).
- **An easily pronounced nonsense word with some non-letters inside.**
  Example: `slaRoo@Bey` or `klobinga-dezmin`.
- **Change your password at least once a year.** Better yet, change your password every few months to shrink your exposure window. You can make three or four passwords if you like, then switch them throughout the year.
- **Don't use the same password on multiple accounts.** When one site is compromised, hackers try to use those passwords to access accounts on other sites. Don't let one break-in give hackers access to all your accounts.

Note: *Do not adopt any of the sample passwords shown above (`choklutt`, `va7ni9lla`, etc.) as your own Kerberos password. They are, for obvious reasons, no longer secure choices for pass phrases.*

Use a pass phrase

Another common method for securing a password is to use a pass phrase instead of a password. A pass phrase is basically just a sentence, including spaces, that you employ instead of a single pass "word." Pass phrases should be at least 15 to 25 characters in length (spaces count as characters), but no less. Longer is better because, though pass phrases look simple, the increased length provides so many possible permutations that a standard password-cracking program will not be effective. It is always a good thing to disguise that simplicity by throwing in elements of weirdness, nonsense, or randomness. Here, for example, are a couple pass phrase candidates:

> *pizza with crispy spaniels*
> *mangled persimmon therapy*

Punctuate and capitalize your phrase:

> *Pizza with crispy Spaniels!*
> *mangled Persimmon Therapy?*

Toss in a few numbers or symbols from the top row of the keyboard, plus some deliberately misspelled words, and you'll create an almost unguessable key to your account:

> *Pizza w/ 6 krispy Spaniels!*
> *mangl3d Persimmon Th3rapy?*

Pass phrase hints:

Your pass phrase should never contain information that would identify you personally, such as Social Security numbers, telephone numbers, credit card numbers, birth dates, or your Kerberos username. Instead, rely on a phrase that has enough meaning to you that you'll remember it easily--then mix it up.

Try to avoid phrases composed of common, smaller words. For example, "My dog has long toes," though long enough to be a decent pass phrase, contains so many small words that a password cracking program might have a better chance of deciphering it. However, "Provincetown is crowded in August!" or "Revere Beach parking is full!" are both acceptable, and easy to remember.

Note: *Do not adopt any of the sample pass phrases shown above as your own Kerberos pass phrase. They are, for obvious reasons, no longer secure choices for pass phrases.*

Are password managers a good idea?

Yes, as long as you have a strong password protecting all your passwords in your password manager. Most password managers use encryption. If you use a browser-based password manager such as LastPass, you don't have to remember each individual password for your online accounts, but you do need to remember your master password. Be sure to change that master password regularly. Other options for password managers are 1Password, Dashlane, KeePass and RoboForm, among others. The basic versions of these are free. **It is very important to enable Two-factor Authentication in your password manager so that a breach of the master password itself cannot provide an adversary access to your password list.**

Related links

- Remote Domain Computers and Password Changes
- I forgot my password, can I have it reset?
- Password Resets for Lincoln Laboratory Employees