

Developing a Strong Password

A strong password is your greatest protection against having your account compromised.

- A strong password is primarily determined by length and not necessarily random characters of short length.
- A password that is easy for you to remember, rather than one you need to write down or store elsewhere is preferable.
- Do not use passwords that are based on personal information that can be easily accessed or guessed (birthdays, anniversaries, parts of names).
- Don't use words that can be found in any dictionary of any language.
- A password should not be shorter than 10 characters in length, and it is recommended that you create a password whose length is as long as the system allows (longer is always better).

Example of a strong password: ther#iz#S0meplyce#!!ke#h0me

This is an easy to remember phrase from a movie using “#” for spaces, phonetically using “iz” for “is”, replacing “No place” with “Someplace”, capitalizing the first letter of the replaced word “S”, and using zeros instead of the letter “o”, replacing the “a” with “y” and “i” with a the character “!”.

For more information on password protection, visit the United State Computer Emergency Readiness Team information website's Security Tip (ST04-002)

Choosing and Protecting Passwords <https://www.us-cert.gov/ncas/tips/ST04-002> .