Strong passwords

A strong password is the first line of defense for an individual computer user's account. Follow these guidelines to keep your account and NCAR computers secure.

Page contents

Creating a strong password

You can generally create strong, memorable passwords or passphrases by building acronyms from a phrase or sentence or stringing multiple random words together with both uppercase and lowercase letters. Mix symbols and numbers inside the words, not just between them or at the ends.

Longer is stronger, so the preference is to use more characters rather than more symbols.

Good passwords should:

- Be memorized or stored in an approved password manager application*.
- Be at least nine (9) characters long.
- Contain both upper-case and lower-case characters.
- Contain numbers.
- Contain other keyboard characters such as !, *, and @.

Good passwords **do not** contain:

- A dictionary word in any language.
- Personally identifiable information such as a name, a login name, part of an email address, a phone number, a date of birth, a license plate, a Social Security number, or similar data.
- Any of the above spelled backwards.
- Any of the above with numbers exchanged for letters or vice versa.
- Any of the above with numbers or special characters appended or prepended.

For example, the following are equally ineffective:

- hello
- 43110
- HeLlO
- olleh
- hello!
- ?hello?

Hackers are well aware of all these tricks and can easily break such passwords.

Protecting your password

Keep your password private. Use a password manager if possible. Written password hints should be secured from view. For example, do not write a password or hint on a white board, especially where it can be seen by a webcam.

Also:

- Do not use Microsoft Office, Google Apps, or similar applications to store passwords even if they have a password protection feature.
- Do not use your browser to store logins and passwords.

---

* NCAR/UCAR staff members can use the Staff Support portal to request installation of an approved password manager application. University users should check with their own system administrators.
