Security :: Create and Maintain Strong Passwords

Information protection starts with account protection. If your account is secure and can't easily be accessed by a stranger, the information you store in that account will also be safe. While you are associated with Humboldt State University, you are responsible for keeping your HSU account information and all activity relating to that account secure.

Be aware that sharing your password and/or other account information is a violation of HSU policy [1]. If your password is shared or stolen, it can be used to compromise your information or hijack your email account. **You will be held liable if your account is compromised as a result of your voluntarily sharing this information.**

How to Create a Strong Password

Passwords are your first line of defense against an unauthorized person gaining access to your personal information. HSU requires that your password contain a minimum of 8 characters and up to 30 characters, including one or more letters, one or more numbers, and at least one special (non-alphanumeric) character. A special character might be one of the following:

#%*+,-. /:=?\^

Note: The following special characters are NOT supported by HSU's password program:

@[]{}$&;()'"<>

Do's and Don'ts for Creating a Strong Password

Do:

- Mix up numbers, upper and lower case letters, and symbols.
- Make it easy enough to type quickly to prevent others from seeing what you typed.
- Create it from a method that makes it easy to remember. Consider choosing a line from a favorite song or poem and using the first letter of each word in that line to generate the password, for example, **r**-e-s-p-e-c-t, **F**ind **O**ut **w**hat **i**t **m**eans **t**o **m**e becomes **rFOwim2m=**. Add numbers or symbols to this to make it even harder to guess.
- Use two unrelated words and separate them with a punctuation mark, symbol or numbers; you could also reverse one or both of the words. For example "surf dent" would become fruS10*tned

If you're interested in mnemonics as a security device, take a look at this white paper on The Memorability and Security of Passwords: Some Empirical Results [2].

Don't:

- Use your login name in any form (reversed, capitalized, and certainly not as-is)
- Use your first, middle or last name, or your pet's, parent's, sweetheart's, or child's name
- Use a common dictionary word

Related Topics

Policy [3], Security [4]

Source URL: http://www.humboldt.edu/its/security-accountprotection

Links:
[1] http://www.humboldt.edu/its/policy-aup
[2] http://www.humboldt.edu/its/sites/its/files/docs/strong_passwords.pdf
[3] http://www.humboldt.edu/its/category/quicklinks/policy
[4] http://www.humboldt.edu/its/category/quicklinks/security