Password Awareness

Don’t Share Your Password With Anyone.
You should never share your password with anyone, not your boss, family member, or friend. Social engineering occurs when someone tells you a lie, (e.g. “There is a problem with your account and I need your password to fix the problem”). Bosses don’t need your password to cover your workload when you are on vacation. If access is needed, bosses should contact DoIT for assistance.

Write Passwords Down in a Secure Location. If you must write down your passwords do so in a secure location. In your rolodex under ‘P’ is not a secure location. Under your keyboard or taped to your monitor is not a secure location. The best way to record passwords is through the use of an electronic password vault (a software program that stores confidential information in an encrypted format).

Change Your Password If Compromise Is Suspected.
If you suspect, even mildly, that your password may have been compromised, it should be changed immediately. If you violated one of the above rules and shared your password, it should be changed immediately. If it seems like it has been a long time since your password changed, it should be changed immediately. Changing a password regularly creates stronger password security.

Add Complexity to Passwords.
Adding complexity to passwords creates exponentially stronger passwords. Complexity is increased by using at least 3 of the following 4 character sets when creating a password:
- Upper case letters
- Lower case letters
- Numbers
- Special Characters (!@#$%^*, etc.)

Creating Strong Passwords
Following the above guidelines will help you create a strong password. If you would like further guidance or specific methods to create hard to guess, easy to remember (strong) passwords, please find the Secure IT brochure entitled “Creating Strong Passwords.”

For more information write to infosec@creighton.edu or www.creighton.edu/secureit

Why Use Passwords

Passwords are a critical information security component. Passwords are used to authenticate, or validate, that the person using your Logon-ID is really you. Consequently, passwords are also one of the most common targets of people trying to access information without authorization.
Why Would Someone Want to Steal My Password?

- Passwords are the only keys that prevent unauthorized entry to many Creighton systems.
- Hackers may want to corrupt your files.
- Hackers may want to send embarrassing or offensive emails as you.
- Hackers may want to use your system or systems belonging to Creighton to compromise other systems.
- Hackers may want to steal Creighton resources, like bandwidth, processing power, or storage space.
- Hackers may want to use Creighton to attack others.

Hacking Methods

The easiest method used to “break” a password is to simply guess. It’s usually pretty straightforward because many people use personal information such as family names, birth dates, 111111, “password,” Creighton, Bluejays, etc., as their password.

More sophisticated hacking methods include using software that can decrypt passwords within minutes by using ‘dictionary’ and ‘brute force’ attacks. Dictionary attack software use common English and foreign language dictionaries to guess passwords. Brute force attacks use software to combine every possible letter, number, and special character in every combination possible.

It may seem nearly impossible to prevent an unauthorized person from stealing your password, but having a strong password can slow the attacker to the point that it causes them to give up.

Password DOs and DON’Ts

Give Everything a Password

Many software products come with a blank password by default. Using anything as a password is better than a blank password.

Don’t Make Your Password Too Obvious

Try to avoid passwords with obvious personal significance...your last name for example. And don’t use default passwords such as the words ‘password’ or ‘administrator’.

Don’t Make Your Password Too Short

A combination lock with a one-number combination would not provide much protection. And, just like that one-number combination lock, any password that is less than eight-characters long simply will not hold up under attack for very long.

Don’t Use Common Dictionary Words

Software programs that use dictionaries as the basis for their attack strategy are commonly available. A computer conducting a ‘dictionary’ attack can try every word in its dictionary in a few minutes. Most dictionary attack programs also check proper names, common misspellings, words with numbers appended or preceding, and foreign language words.

Don’t Use the Same Password Over and Over Again.

Passwords should be changed on a regular basis, at least once every 180 days. The primary reason is that if someone has cracked your password without you being aware of it, it makes them have to start all over again. A strong password is never reused.

Categorize your passwords

Categorize your passwords in order to minimize the number of passwords you have to remember but also to provide a barrier between systems with sensitive information and those with non-sensitive information. For example, you can use the same password for Blue domain and Banner, but you should not use the same password for your online banking.