

Tuesday TechTip:

You decide:

What's more frustrating:

- a) Creating and remembering a strong password
- b) Cleaning up your credit after a security breach
- c) Notifying thousands of Columbia College constituents that their account information has been compromised

Your password is worth as much as what it protects!

General rule of thumb, the more random and longer a password is the more secure it is. Strong passwords are created using all of the following tips:

- *Make it lengthy:* Ideally, passwords should be at least 14 characters long. Every additional character provides more security.
- *Consider using a pass phrase:* It may be hard to find a word that is 14 characters long. Instead, use
 - a mantra
 - a quote
 - a sentence
- *Substitute:* Use numbers instead of characters or vice-versa.
- *Add complexity:* Include a combination of UPPER and lower case letters and numbers.
- *Develop mnemonic phrases.* Use the beginning letter of each word of a sentence, such as the example below from Wikipedia: *Tp4tci2s4U2g!*
The password for (4) this computer is too (2) strong for you to (4U2) guess!

Avoid:

- Weak, easy-to-guess passwords, such as:
 - your username
 - first/last name
- Using the same password for every online application
- Passwords with less than 6 characters.
- Repetitive passwords, such as: Pass11, Pass22, Pass33....

[Check your password's strength](#)

(DO NOT enter your *exact* password. Enter a password with similar structure only!)

Columbia College Password Policy

Columbia College has a single sign on process for Email, Web Advisor, Datatel and Network access. Under this policy *faculty and staff will be required to change their passwords every 90 days*. For more details, check out [Columbia College's Password policy](#).

Register or view February Technology Workshops at <http://training.ccis.edu>