



Tuesday's Tip

information provided by Adriance Memorial Library to make your life a little bit easier

Internet Safety and Strong Passwords

August 9, 2016

Visit GCFLearnFree (<http://www.gcflearnfree.org/internetsafety/>) for a tutorial about safety on the Internet. The site also has a tutorial about internet safety for kids (<http://www.gcflearnfree.org/internetsafetyforkids/>).

By the way, GCFLearnFree is a great place for tutorials on computer topics as well as basic skills such as math, money management, resumes, and more.

A key step for internet safety is using strong passwords, ones that are difficult for a hacker to guess. One way to create strong passwords is to use a password generator. Here are two to try:

- Strong Password Generator (<https://strongpasswordgenerator.com/>)

Strong Password Generator

Strong Password Definition / Requirements

A strong password **has:**

1. at least 15 characters
2. uppercase letters
3. lowercase letters
4. numbers
5. symbols, such as '!'

A strong password **is not:**

- your login or username
- your name, your friend's name, your family member's name, or a common

Password Generator

Generate password

Your new password is:
[password will appear here]

Show options...

- Random Password Generator (<https://www.random.org/passwords/>)

Random Password Generator

This form allows you to generate random passwords. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs.

The passwords generated by this form are transmitted to your browser securely (via SSL) and are not stored on the RANDOM.ORG server. Nevertheless, the best data security practice is not to let anyone but yourself generate your most important passwords. So, feel free to use these passwords for your wi-fi encryption or for that extra Gmail account, but you shouldn't use any online service to generate passwords for highly sensitive things, such as your online bank account.

Part 1: The Passwords

Generate random passwords (maximum 100).

Each password should be characters long (minimum 6, maximum 24).

The passwords will not contain characters or digits that are easily mistaken for each other, e.g., '1' (the digit one) and 'l' (lowercase L).

Part 2: Go!

Be patient! It may take a little while to generate your passwords...

A potential problem with strong passwords, especially ones generated for you, is that they can be difficult to remember. Other than writing the passwords down (in a place that can't be easily found) is to use a password manager. *PC Magazine* has recent reviews of free and paid password managers:

- The Best Free Password Managers of 2016
<http://www.pcmag.com/article2/0,2817,2475964,00.asp>
- The Best Password Managers of 2016
<http://www.pcmag.com/article2/0,2817,2407168,00.asp>