

TOP 10 TIPS TO CREATE SECURE PASSWORDS

BITS and ITAC offer the following tips to increase strength and security of online passwords:

- **Take advantage of complexity. (Be Complex.)**
Use a combination of lower and upper case characters, numbers and symbols. Passwords with many types of characters are more difficult to guess..
- **Use the maximum length of the password offered. (Go long.)**
Use the maximum number of characters the site allows. Generally, the longer a password, the harder it is to guess.
- **Create a phrase instead of a specific word. (Phrase it.)**
Use passwords that remind you of an event rather than a name or date. Instead of choosing a name or an event, like a child's name or birthday, pick a phrase that reminds you of the person or birthday, such as "3rdpartySarah".
- **Different passwords for different sites. (Diversity is key.)**
Though tempting, do not use the same password for all your online sites. Remember, if someone ever determines your password, they now have full access to all of your online information and accounts.
- **Create smart combinations. (Smart combos.)**
For example, take the first two letters of your car's make and combine it with the first two letters of your first school, and the first few digits of a number you know well to make up a password.
- **Create a private acronym. (Think texting.)**
Consider using the first letters of a phrase you can easily remember. For example, "my grade school was Oak Hill Elementary" becomes "mgswOHE". Then add in digits and special characters to make it strong.
- **Use capitalization and substitution creatively. (Be creative.)**
Instead of the first letter, choose to capitalize somewhere in the middle. Substitute a number for a letter. For example, use a "5" where you might use an "S" or use an "8" where you might use a "B".
- **Change initial passwords assigned to you. (DIY.)**
When you first register to use some online sites, the site will issue you an initial password. Some sites issue the same password to many users, potentially making your password easy to guess. Change the assigned password immediately.

- Avoid entering your password on a “public” computer. (Private not public.)
Computers in public places used by many different people are often unsafe to use to access sites containing private information or for financial transactions. They may be infected with computer viruses that can capture and store your password without you knowing it.
- Change your password often. (Keep it fresh.)
Change passwords periodically, but avoid “patterns” of change. For example, do not use “somebodysname1” then “somebodysname2” and do not recycle passwords you used recently.

AVOID these easy to guess passwords:

- Family member and pet names.
- Public information such as your birthday or address.
- Words in the dictionary. Many automated programs used to “guess” passwords check for words in various dictionaries including medical, scientific and other dictionaries.
- Sequential characters. A password such as “asdfghjkl” is easy to guess.
- The user identification you use for the site. This is often one of the first things someone will guess as your password.

And, finally, do not share your passwords. Now that you have maximized the protection a strong password offers, don’t compromise your security by sharing your passwords.

For more information contact Ann Patterson, Ann@fsround.org, or Paul Smocer, PaulS@fsround.org.