Password Guidelines

From your Friends at CAA Ministries

Quiz: When I create my next password, I will:

(a) Seek a group consensus from my closet friends

(b) Use my new baby's name, which I have just introduced to the Facebook world

(c) Make it easy on myself and go with my usual password, which is "password"

(d) Establish a creative combination of numbers, letters, and symbols that would be at least 12 characters long and known only to me.

If you said "d", you get a passing grade!

Common Sense & Strong Passwords

Passwords should be changed regularly. We suggest every 3 months, if not more often. Like any task that you may dread undertaking, you will feel great when it's finished. In fact, your password-changing effort may just save your bank account, credit card or social media outlet from being compromised.

Here are tips and suggestions for creating passwords.

1. Avoid common passwords. Commonly used passwords include, '123456', 'password', '111111', 'qwerty', 'abc123', 'iloveyou', 'admin', 'God', '123123', 'monkey' and 'sunshine'. According to a recent study, the 100 most commonly used passwords make up over 60% of all passwords in use. Don't kid yourself – cybercriminals are fully aware of our lazy practices.

2. **Steer clear of personal passwords.** When creating passwords, avoid passwords that are based on personal information about yourself or your family and that can be seen readily online on your blog, social networking site (i.e. Facebook), etc. For example, if you post a picture on Facebook of your new puppy 'Roscoe', we suggest that you do not change your password(s) to 'Roscoe'.

3. **Take the time to create a strong password.** Strength of a password is measured by a combination of its length and complexity (mixing in numbers, letters, capitals, symbols, etc.). And believe it or not, length plays a bigger role in password strength than complexity. Passwords should be at least 8 characters in length but 12 characters or more should be the norm. Also, don't use one-word passwords. Believe it or not, 90% of passwords used by all of us today are considered weak.

4. **Get creative with passwords.** Here are some common substitutions in passwords that make them more complicated while still being easy to recall. Take, for example, the simple password made up from two easy words: "house" and "barn" like this: 'house-barn'.

- You want at least one capital letter, but Instead of capitalizing the first letter, try capitalizing the last letter in each word to increase complexity – '**housE-barN**'

- Include the current year in the password to add length and numbers. Even better, change the '0' (zero) in 2018 to 'o' (alpha o), producing '**housE-barN-2o18**' – adds numbers and complexity

- Instead of 'a', substitute '@'; instead of 'I', substitute '!'; instead of 'e', substitute '3'; etc., producing '**hous3-b@rN-2o18**' with special symbols for even more complexity

Individuality can make creating strong and easy-to-remember passwords enjoyable, especially when sharing the importance of strong passwords with children, teens and even young adults.

For example, if your son really enjoys playing “Mario Kart” and if he wants a simple password like ‘mariokart’, get creative as shown in the above suggestions. The resulting password might be something like

‘**m@rio-k@rt-2018**’

by telling him to use ‘@’ instead of ‘a’ when entering his password and add the year at the end. Even younger children can be trained to remember a password based on something they enjoy and yet we have also established a strong password.

Securing Your Passwords

Given the suggestions above for creating strong passwords, below are some tips on how to keep your passwords secure. Most of them are “common sense” but research proves that they are not being practiced.

1. Don’t share your passwords with others. A good rule of thumb may be to treat your password like your house key. It’s probably best not to share your house key with all your neighbors and all your friends at school or work.

2. **Never text, email or post your passwords online.** Any time you share your passwords in this fashion you are essentially allowing full public access to your account information. It would be like leaving your front door wide open when you leave home or go on vacation. Any data that travels through the Internet “unencrypted” can be intercepted and viewed by just about anyone, including all the bad guys (cybercriminals).

3. **Change your passwords regularly**. The hard truth is that no password is truly secure so change them regularly. Consider all the data breaches that are becoming commonplace in the nightly news. You also have the human element (socially-engineered schemes, phishing attack victims, etc.).

4. **Use different passwords for different sites and activities.** As the saying goes, don’t put all your eggs in one basket. The same can be said in relation to passwords — do not use the same one for everything. It’s easy (lazy) but can cost you dearly. If you happen to get tricked into sharing or entering a password, or if an e-commerce site falls prey to hacking – not your fault but it happens – you will not have all your various accounts exploited if you have separate passwords for each account. In other words if the cybercriminals do get one of your passwords, make sure it is not like a master key that gives them access to all your accounts.

It takes work to keep up with new passwords, but it’s worth it! Getting hacked stinks and leads to very real damage and hurt.

When night falls, most of us lock our car doors, deadbolt our front door and shut the garage. Why wouldn’t we take the time to complete a few routine steps to keep our online affairs private and secure as well?

Make it fun and use capitals, symbols and numbers. Set an alarm on your phone to remind you to change your passwords once every three months (or more often). Any increase in switching them up and making them stronger is a bonus to your personal online safety.