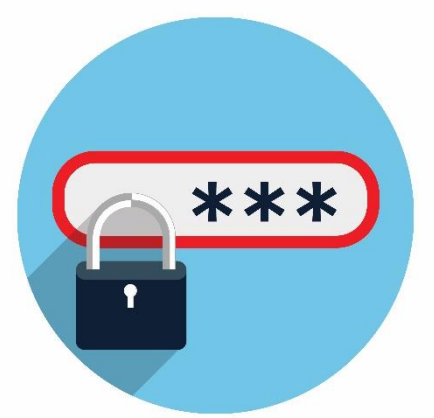
THE FACTS: PASSWORDS & SECURING YOUR ACCOUNTS

Passwords are like keys to your personal home online. You should do everything you can prevent people from gaining access to your passwords.

How do I create a good password?



Remember the phrase "long and strong." Good passwords have a minimum of 12 characters and a mix of upper and lowercase letters, numbers and symbols. And they avoid common or easily guessed words or character combinations. Better yet, say the experts at the National Institute of Standards and Technology, is to create a passphrase that uses a few normal words or phrases that have a unique association to you; words that are connected in your mind, but not the same in others' minds. These are much easier to remember, but harder to guess (as long as your words aren't also a grouping that is easily guessed, such as the names of your children or colors of the rainbow). Better examples might be words that come to mind when you think of your house, such as "bluecornerfamilymaple", or your hobbies, such as "travelboatrelaxsunny".

How do I ensure my password protection stays safe?

-- Never share your passwords with others.
-- It's OK to make your passwords unique to your life, but not something that is easily guessed.
-- Have a different unique password for each account.
-- Get a password manager program to help you generate strong passwords and remember them. Some browsers offer password managers.
-- It's best not to write down your passwords to remember them, but if you do write them down, store them safely, away from your computer.
-- Security experts used to advise that you change your passwords several times a year. Now they say it's not such a good idea, because many users change their passwords in predictable patterns, and frequent changes make passwords harder to remember. You should change your

password only if there is evidence of a compromise.
-- Check to see if your password (or one you're hoping to use) has been compromised by a data breach or hacking. Some browsers and websites offer this service.

Are passwords the only form of protection for my accounts?

Typing a username and password or passphrase isn't the only way to identify yourself. Some web services add to their security features with two-factor or multi-factor authentication that may include an additional form of authentication to verify your identity, such as:
-- Biometrics such as voice ID, facial recognition, iris recognition and finger scanning
-- A one-time security code (usually sent via phone call or text)
-- A security key or token; a small device (most often used via a USB port or in conjunction with a smartphone) that is used when logging in

In some cases, two-step and multi-factor authentication services may be available, but are not required. Ask your financial institution and other online services if they offer these methods or additional ways to verify your identity. If you do use multi-factor authentication, experts recommend that you avoid receiving authentication codes by text or email because they are more easily compromised. Instead they recommend using an authenticator application. Stop.Think.Connect also offers authentication tips and a guide on how to turn on strong authentication for several popular online services at https://stopthinkconnect.org/campaigns/lock-down-your-login

SOURCES: National Cyber Security Alliance, National Institute of Standards and Technology

FOLLOW ARCYBER ON (Click the images to visit sites):

As of 23 March 2022