Passwords

People use passwords that are often very easy to crack – and often times reuse passwords. People want to use something that is easy to remember so they use their child's name, a birthdate, a pet's name, etc. This information is easily accessible by hackers. The hackers just need to follow your social media to find these answers. If you reuse your passwords, once the hacker finds one ID and password combination that works, they try that same ID and Password at other sites – knowing people reuse passwords. A very common password that is used is password123, this is giving the hacker the keys to your account.

Here are a few suggestions for creating stronger passwords.

- Use a strong password - at least 10 characters including upper- and lower-case letters, numbers, and special characters.
- Do not reuse passwords.
- Use a different password for each account.
- Use a password vault or manager – stores your passwords and you only need to remember one password – the password to your vault.
- Consider creating one strong basic password, then add letters or numbers from the website to make it unique to that site.
    - For Example:
    - Strong Base Password – MyP455w0rd!
    - Website Specific – 1st and 3rd letters from the website URL
    - Example Password for facebook.com = MyP455w0rd!fc

Password managers or vaults are a great tool to store all your passwords and can even help you generate new, random passwords. The PCMag article, "*The Best Password Managers for 2022*" by Ben Moore and Kim Key, updated December 13, 2021, has the pros/cons of 11 different password managers. There are many different password managers, some are free, and some are paid subscriptions. Read the article to learn more and determine which password manager would be best suited for your needs.

Source: PC Magazine
https://www.pcmag.com/picks/the-best-password-managers