Tips for staying cyber safe

Tip 6: Password Management

Password Management has become a hot topic in 2019.

Recent research from the Ponemon Institute's into the State of Password and Authentication Security Behaviours has revealed some frightening statistics:

- 51% of those surveyed reuse passwords across 5 or more business and person al business accounts:

- 69% of respondents admit they have shared passwords with their colleagues

- 57% of those surveyed said that they had experienced a phishing attack but did not change their password behaviour.

Microsoft, NIST and the Department of Homeland Security in the United States have recently revised their password policies.

One of the most frequently asked questions we experience is what is best password practice. So, listed below are the updated best practice tips for maintaining healthy password behaviour.

1. Don't use a password that is the same or similar to on you use for other websites. Try and use a unique password for every site where a password is required.

2. Create a random password for the best security. Don't use common phrases like "password" or "1234" or "Iloveyou".

3. Make passwords easier to remember but hard to guess. Most recent guidelines suggest using a longer phrase rather than a complex password. It is better to create a unique password that is easy to remember, using whatever characters you want, rather than convoluted and complex passwords that are impossible to remember.

4. Use a mix of Upper and lower case, symbols and numbers. New guidelines suggest that passwords can be up to 64 digits long to allow for a favourite phrase to be used. It is still good practice to have a mix of capital and lower case letters and numbers and symbols.

5. Use a secure password manager which can provide stronger passwords and stronger security. It has been recommended by NIST that a "paste" feature be enabled in the password field. If this is enabled, it helps promote the use of password managers.

6. Use multi factor authentications. It is a lot more difficult for a hacker to get past a multi factor password. Download an authenticator app on your smart phone and it will enable you to verify that you are who you say you are instead of just accepting the password is legitimate entered.

7. Do not use dictionary words for your password. It might seem safe to use a dictionary word as a password but hackers have created algorithms that search through tens of thousands of dictionary words.

8. Don't write your passwords down: I understand, committing all your passwords to memory is almost impossible.. Try not to write them down and don't store a list of

passwords on your desk, in your wallet or on a post-it note. If you need to store passwords, do that through a secure password manager app.

9. Have stronger passwords for Sensitive accounts and Bank accounts: it goes without saying that certain kinds of information are more sensitive or confidential than others. When accessing sensitive information, create. Much stronger password and use multi-factor authentication.

10. Never tell anyone your passwords. It is never smart to tell others your passwords and particularly always keep your unique passwords to yourself.

Use these tips to increase your overall security and don't let something as easy to avoid as a weak
password expose you to an increased likelihood of a cyber attack.