Be an informed consumer:

Keep Your Passwords Safe

Penn CASE

Tip 1: Follow the basic password rules.

- Don't pick a short password. Choose one with at least 8 characters.
- Avoid using the same password everywhere. If someone gets hold of your password for one account, they can then gain access to all your accounts.
- If available, use recovery questions that only you know the answer to!

Tip 2: Don’t use obvious words like your name, town or date of birth.

- People trying to discover your password might use words or phrases that they associate with you. These words might be easier to remember, but they are the first guesses that somebody else would make.

Tip 3: Avoid commonly used passwords

- Never use popular passwords such as “password”, “hello”, “123456” or “mypasswordispassword”. Intruders routinely use examples such as these as a starting point when attempting to break into your account.

Tip 4: Choose a combination of random words, and don't use the same technique for every password.

- Using special characters and at least one number (for example, “P@ssw0rd123!”) can be helpful, but people tend to use the same techniques when choosing these combinations. Hackers can predict and target this weakness, so make sure you vary the structure of your passwords.
- A good idea is to choose multiple random words. For example, “correct horse battery staple”.
- These types of passwords are easier to remember, and they are actually much harder for computers to guess.

Be an informed consumer:

Keep Your Passwords Safe

Penn CASE

Tip 5: Keep it simple!

- Think length, not complexity. Keep passwords simple, long and memorable. Phrases, lowercase letters and typical English words work well, according to the National Institute of Standards and Technology.
- if you can picture it in your head, and no one else could, that's a good password.

Tip 6: If you have to change your password frequently, make sure the new password is not similar to the old one.

- Current guidelines no longer suggest passwords should be frequently changed, because people tend to respond by making only small changes to their existing passwords -- for example, switching "monkey1" into "monkey2".

Tip 7: Take advantage of 2-factor authentication.

- 2-factor authentication is a good option on websites that provide it. Each time you log-in, you'll be sent a second password on your phone that you'll need to access your account.
- The password is different each time and only the person with your phone will be able to use it, so it’s very secure. But not every website offers this -- Facebook, Twitter and Google are examples of websites that do.

Tip 8: If you have many different passwords, consider using a password manager app.

- You can download an app on your computer that keeps all your passwords safely hidden, providing them only when you need to log-in to accounts on your computer.
- You’ll still need to remember one password though -- the password used to access the password manager.