Cybersecurity Awareness Month: Keep Your Passwords Safe

During national cybersecurity awareness month, the College is kicking off a year-long campaign to educate students, employees, and friends of the College about cybersecurity and staying safe online. Here are a few rules on how to keep your passwords safe, provided by our IT staff.

Use the 8 + 4 Rule

This rule helps you to build passwords that are strong and secure. Use at least eight characters with all four types: upper case letters, lower case letters, special characters, and numbers. The more random the better.

Keep Special Characters and Numbers Separate

Here's another hint for an effective password policy to foil hackers. Make sure the numbers and symbols are spread out through the entire password. Bunching them up makes the password easier to hack.

Don't Make it Personal

There's a big difference between security and convenience when it comes to passwords. Using personal information like your first name and birth date is a recipe for disaster. If a hacker ever gets their hands on any of your personal data, this information will be the first set of password combinations they try.

Use Different Passwords for Different Accounts/Websites

It's a bad idea to cut corners by using the same password for more than one website/account. Use a different one for every site or account you have.

Avoid Dictionary Words

It might sound safe to go to the dictionary for a password, but hackers actually have programs that search through tens of thousands of these words. Dictionary attack programs have been used by hackers for years.

Adopt Passphrases

Abbreviations are usually immune to dictionary attacks. Remember to add special characters and numbers. Even better is to have a secure passphrase as your password. Remember, eight characters is a minimum number.

Don't Change Them Too Often

A good strong password will last for six months. Don't change them any more frequently than that (unless you need to), otherwise you can wind up with a password1, password 2 situation. Hackers look for these patterns. This, however, also means you need to use a secure, strong password strategy.

Don't Write Anything Down

Granted, committing all your passwords to memory might get tricky but a discarded Post-It note or even worse, one attached to your monitor would be all that a hacker needs to get into your accounts. There are several reputable password management apps available, some even for free (e.g. Keepass, Dashlane).

Stay Away from Personal Acronyms

Don't use these as a shortcut to identifying your department or who you are. It might be tempting for a student to use DTCCstudent. However, that opens a cybersecurity door wide enough for a hacker to walk right through.

Never Tell Anyone Your Password

A rule good is that no one should ever tell anyone else their password. The college IIT department will never ask you for your password. This also includes someone watching as you type in your password. This is a very common method hackers use (it's called shoulder surfing).