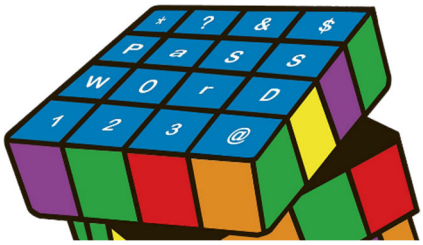
520.743.7554
info@computerdimensions.net
www.computerdimensions.net

How Do You Create A Strong Password?



Almost everything we do online requires a login, and every login requires some kind of authentication to verify that we are who we say we are. As such, your password should be as unique (and complex) as you are! Here are a few tips from the experts:

- **Do use long passwords and passphrases.** Passwords should be at least 8 characters long, but not so long that you can't remember them (see the tip below). Check that your password hasn't been exposed in a data breach at https://haveibeenpwned.com/Passwords.

- **DO use unique phrases and special characters.** A short phrase consisting of 30 or more characters (perhaps with some numbers, capitalization and punctuation) that you can remember is far better than an 8-character word with common substitutions (like a '3' for the letter 'e').

- **DO use a password manager program (free or paid).** A password manager can be helpful for creating, storing, managing, and remembering unique, strong passwords for your various device, system, and application logins. It can also help to eliminate the common practice of writing down passwords in documents or on sticky notes.

- **DO use passwords you can remember.** Overly complex, completely random passwords that are difficult to remember can actually be counterproductive and make your account less secure, because it tends to lead to bad practices such as writing down passwords and using the same passwords across different personal and work accounts.

- **Do use multi-factor authentication (MFA).** When possible, MFA should be enabled on your accounts instead of, or in addition to, passwords. MFA incorporates two or more authentication factors ("something you know," such as your username and/or password, and "something you have," such as a hardware or software token, or a smartphone). When you log into an MFA account, a one-time code is generated on your token or sent via SMS text message to your smartphone. The code can only be used one time, and only within a limited period of time (typically within one to five minutes). This makes it extremely difficult for an attacker to intercept your code and use it to log into your account without your knowledge and before the code expires.

- **DO NOT use the same password twice, regardless of how good it is.** If your password gets compromised in one place (say, your personal Yahoo! email account), cybercriminals will try to use those same credentials in other places (like your online bank account).

- **DO NOT share your passwords with anyone – ever!** Treat your passwords as more sacred than your toothbrush (which you might occasionally share with your significant other – or your dog).

- **DO NOT use common dictionary words.** Automated password cracking programs make easy work of dictionaries – including foreign languages and medical, legal or engineering terms. Also avoid repetitive characters (for example, 'aaaa'), sequential characters (for example, '1234'), and recognizable patterns (for example, 'qwerty').

- **DO NOT use personal information in your password.** Social media makes it easier than ever for cybercriminals to learn personal details about you – including your middle name, birthdate, address, school, spouse's or child's name, and what you did last summer!