

HOW TO CREATE A STRONG AND SECURE PASSWORD



Nowadays, it's **more important than ever to have a strong password**. Not only do you need to worry about hackers, but you also need to worry about social engineers that aim **to trick you into providing sensitive information**.



Passwords should be at least 10 characters

Creating a strong password is easier than you might think. First, you will want to choose a password that is at least ten characters long. A common way that passwords are hacked is through a technique called 'brute-forcing' and a longer password will increase the amount of time for this attack method to work.

Passwords should contain alphabetical characters, numeric characters, and symbols

It is important to use a mixture of upper and lowercase letters, numbers, and symbols. If you only use words from a dictionary or a purely numeric password, a hacker only must try a limited list of possibilities.



Avoid using easy to guess passwords

A strong password should be difficult for someone else to guess or crack. You should avoid using generic passwords and the password should have no ties to your personal information. As an example, a popular password combination you should avoid is a surname + year of birth "Jones1980".

Create a unique password for each account

If you use the same password across multiple websites, it will not matter how complex or long your password is. If one account is compromised, all your accounts that share that password become compromised. You should create a unique password for each account.



Avoid sharing your password

Sharing work account passwords can have severe consequences. By granting anyone else your user credentials, you are compromising the security of your account and placing the company's security at risk. As soon as they have access to your account you cannot guarantee what they will do with your access details.