PIN & PASSWORD MANAGEMENT

PINs and Passwords protect your sensitive data. Therefore, it's crucial to maintain them secure. Try out these three suggestions.

With the ever-increasing amount of data security breaches and regulations, organizations are becoming more and more strict about data security. Keeping password management a top priority for your team will prevent many headaches and issues with data security.

If you are using the same password on multiple websites or email addresses, it's high time you started using different passwords for each account. Users should also avoid sharing their passwords with anyone, as it's easy for hackers to break passwords by pretending to be a friend and asking for password details.

When creating new passwords, ensure they are something you would not likely use in real life. For example, make sure the password you choose is not something your family would use, such as your mother's first name. Keeping your passwords secure will prevent someone from accessing your data through a cyber-attack.

THREE TIPS TO SAFEGUARD:

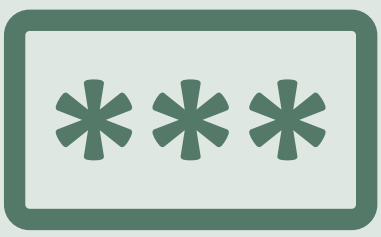
TIP 1

DON'T DISCLOSE YOUR CREDENTIALS

Passwords and PINs shouldn't be written down or shared. When logging in, cover your keypad or keyboard. Do not keep passwords that can be easily guessed.

TIP 2

CREATE UNIQUE PINS & PASSWORDS



Make a strong, one-of-a-kind password and PIN for each account and device. Your other accounts and devices are secure even if one password or PIN is revealed.

TIP 3

STORE YOUR CREDENTIALS SECURELY

Passwords shouldn't be saved in your browser. Instead, think about using a password manager to track all those logins. (Ask permission from your employer before using one at work.)

Example- Create a password that is at least 8 characters long, contains a combination of upper and lower case letters, and includes a number or unique character. Also, create a hard guess PIN, such as a sequence of numbers, letters, or symbols.

PROTECTED HARBOR