IRONSHARE
SECURITY • SIMPLIFIED

Keeping Your Account Secure

Ironshare's Guide To Good Password Practice

Creating a long, strong and hard to guess password is key to account security. In addition Multi-Factor Authentication provides additional security using a random code from your smartphone. This means that an attacker would have to steal your password and your phone to access your account. We recommend enabling MFA wherever possible; you can never be too safe.

How to Manage Your Passwords

It is really important that your passwords are always unique. Reusing passwords, or different variants of the same password, could compromise all of your accounts if just one gets hacked. Minimise the risk by not using the same password more than once.

Writing down passwords is like leaving your keys on your doorstep. You wouldn't let a stranger into your house, so why would you let them into your accounts? If you struggle to remember your credentials, use a password manager to store you passwords.

Sharing login credentials with friends and colleagues is a big mistake when it comes to managing your passwords. Keep your passwords to yourself to avoid any unnecessary risks.

If you're the kind of person who reuses, writes down and shares passwords, you may want to try using a password manager. Not only does this let you securely store your passwords, but it also allows you to randomly generate strong passwords. Keep your accounts secure the easy way.

What Makes a Good Password?

The longer your password, the stronger it is. Using a minimum of 12 characters strengthens your password, and in turn makes it harder for hackers to figure out.

Another way to strengthen your password is using a combination of upper case and lower case letters. Capitalising random letters instead of the first is much more effective as well. For example 'iLovEcoCacOla' instead of 'ILoveCocaCola'

Passwords are great, but passphrases are much more effective. Using multiple words rather than just one will make your password much stronger and make it much harder for a hacker to guess.

Following on from the effectiveness of passphrases, choosing three random and unrelated words greatly reduces the possibility of your password being cracked. For example 'housebluedog'.

Substituting random letters for numbers and symbols is an effective way of making your password even more complex. For example, an 'S' can be easily swapped out for a '5' or a '$'.

It is important that you use random words and phrases in your password so that it is hard to guess. Avoid using birthdays and names of people you know and your password will be much more difficult to crack.