activereach

STRONG AND SECURE PASSWORDS – A QUICK GUIDE

Almost every aspect of our online lives is password protected at some level. Everything from personal details and family photos to corporate secrets and banking access sit behind some form of password. This is why it is important to make sure that your passwords are secure, unique and difficult to crack, not least to protect activereach!

Make sure your password is long enough. The recommended length is at least 8 characters long. A password of 4 standard characters in length has approximately 1.6 million different combinations. This may sound like a lot, but if you have a piece of software trying a new combination every second, that password will be cracked in less than 500 hours.

Always try to avoid using just a normal word. Password for instance, or secret is another common one. Chancers and hackers can and will try to get into your accounts purely just by using the commonest passwords that people pick. Also avoid using words that are easily linked to you, so things based on personal information, including partial words like part of your name or part of your birth date. Also anything easily linked to activereach should definitely be avoided.

Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.

Upper and lower case characters is a simple but very effective way to make your password harder to crack. Try to avoid just putting a capital letter at the beginning.

Adding numbers to your password is also essential, but that in itself does not automatically make the password safe, so avoid Password1 or Secret1 – again very common and very easily cracked by someone with malicious intent. Swap some of the letters out for numbers. Add character symbols from the keyboard also. So ilikefudge could become il!k3F$dg3

Make sure to change your password often. Your password might have already been cracked and someone is rifling through your particulars, but you are unaware. It is good practice to change your password at least every few months, but ideally every few weeks. Make sure that the new password is different from previous ones.

If you don't trust your memory completely and you think writing it down is a must, then make sure you don't label it as a password and keep it safely on your person or locked away. Never store your password on your computer except in an encrypted form.

Don't tell anyone your password, not even members of the Technical team. Never send your password via email or other unsecured channel, and be very careful when entering your password with somebody else in the same room, especially when accessing sensitive information.

activereach

www.activereach.net