



Password Security - Top Tips

Whether it is digital devices or dedicated company websites, most of them have some sort of access and authentication control. Many of them use usernames and passwords to gain access. Therefore, if a Hacker can get their hands on these then they can do a lot of harm! Be aware that over the years thousands of company's databases have been hacked releasing usernames and passwords onto the dark web.

You can check if your email address has been captured in any previous attacks at <https://haveibeenpwnd.com>. Just type in your email address to find out. If it has, do not be alarmed, just follow our top tips below.

Also, the way that Hackers try to gain access is by using your username (quite likely to be your email address) and then run a designed programme to "guess" your password. These attacks are referred to as Brute Force and Dictionary attacks. By doing these attacks there is a good chance that they will get a hit and gain access. Therefore, there is a significant need to make sure your password is as complicated as possible. Have a look at <https://nordpass.com/most-common-passwords-list/> to ensure your passwords are not on this list. If they are, or even if they are similar then change them to something more secure by following the details below.

One of the most effective techniques for creating a password is to start with a very long phrase, such as "To be or not to be that is the question". This can then be broken down to: 2Bornot2Btit?. After you have used this new password a few times you should not forget it. However, make sure that you keep it stored in a "safe" place for reference.

When doing this make sure that you contain numbers, lower and uppercase letters, and symbols. No password is unbreakable but by making it complicated it will make it difficult and very time consuming to crack.

Ideally, you do not want to use the same password for each system/device. One method of using a different one for each is to just add the company's name afterwards, for example 2Bornot2btit?Hot for Hotmail, 2Bornot2Btit?Vod for Vodafone etc...

If you find that your email address is on haveibeenpwnd then you need to change your email password ASAP. Regardless, we would also suggest that you change your passwords at least every 6 months, particularly for your email and social media accounts.

At Littoral Risk, we provide bespoke Cyber Security Awareness training.

Hope this helps.

www.littoralrisk.com

