PASSWORD POLICIES

A clear, understandable and strong password policy is essential for all businesses. Whether your company is big or small, the business's internal networks will be protected by passwords and your password policy will assist in protecting your business further - preventing unauthorised access to your data, information and networks.

Below we have provided some top tips that could be incorporated into your business's password policy:

- Ensure that as many 'common' passwords (eg: ***password123***) that you can think of are blacklisted. This list should be reviewed and updated regularly to help you and your staff consider what else could be considered 'common'. Another example here wouldn't be an exact password, but blacklisting use of birthdays as passwords.
- Ensure that all passwords used are at least 12 characters long and contain a variety of lower case letters, upper case letters, numbers and symbols (eg: ! $ £, etc.).
- Encourage the use of phrases rather than words. For example; !***TogetherWeAREanOcean100$***
  This will help the password to be memorable to the user but still secure in its length and use of varying cases, numbers and symbols.
- Encourage the substitution of letters for numbers where it can make sense. For example; ***TH3_better_Bu51ne55_n3tw0rk***
- If passwords being used are complex, then regular changing of your passwords won't be necessary and instead you'll likely only need to change them if you believe that your password may be known / your security compromised.
- Where possible, enforcing a temporary lockout feature when incorrect passwords have been inputted after five attempts (for example) will help if someone is attempting to log into one of your systems. These can be undone after a set period of time, or via an admin overview / IT department check.
- For access to your business data / information that will happen outside of your business (ie: emails on an employee's phone, or cloud drive access), ensure two-factor authentication is activated. This will add an additional layer of protection to your accounts and assists in blocking login attempts from new / unknown locations and people.
- Use a password manager to assist in the creation of and storage of strong passwords that will be complex enough to provide a high level of protection.
  Please note: the master password for any password manager must be especially strong / complex for this to be effective.
- Ensure that any default usernames / passwords are updated for any equipment (for example, WiFi routers) or software that you use and install.
- Ensure that the user with admin access has two accounts. One with full admin access and one with basic access for day to day use. This means that the admin account will only be used for admin activities and won't be logged in as often and so therefore will protect you against any malware that could affect you.

- Ensure that neither you or your employees write down passwords on post-it notes, etc. No matter how complex a password is, it's unsecure if it's readily visible to anyone who looks for it. Again, a password manager can help here.
- Do not use the same password for multiple online accounts. Request that staff do not use any of the passwords they use within the business for passwords within their personal lives.

The above ideas, implemented into a clear Password Policy will assist in keeping your business secure from cyber threats. However, it is important to note that it is impossible to negate all risks entirely.

All employees, from the top down must be regularly reminded of and retrained on the policies, with everyone ensuring that they are followed consistently.

USEFUL LINKS:

- https://haveibeenpwned.com/
  This website tracks worldwide data breaches and will alert you (once registered with them) if the email address that has been registered appears in said data breaches.
- https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
  Password strategies that can help your organisation remain secure from the government's National Cyber Security Centre.