Following the study, it was discovered that the business still uses the antiquated (MD5) password hashing technology, which provides virtually little protection in the event that a password database were to leak.

Additionally, it was found that the present password policy does not follow best practices in the business. allowing users to reuse their usernames as passwords and create short (6 character) passwords.

Following improvements are suggested to raise the general level of password protection as a consequence of the analysis.

Use a password hashing algorithm specifically designed for passwords, such as bcrypt, scrypt, or PBKDF2, as doing so will significantly lengthen the time required to crack each password.

I

Implement salting to prevent usage of rainbow tables to speed up cracking,

Increase the minimum password length requirement to 10 characters-this will increase the computational effort required to crack password and will give additional time to change all passwords in the event of the password database being leaked,

Prevent passwords to be the same as usernames or reused as part of the password-such password combination is easy to check without gaining access to the password database itself.

It is advised to educate users on creating safe and easy try remember passwords. Having a password policy requiring long passwords with a number of special characters results in user writing passwords down or constantly resetting them. The best way to create a strong and user-friendly password is using passphrases (eg.mygrannyschairhadstaples).

The best way to create such passwords is to combine a couple of completely random word It's also advised to use some special characters and numbers as easy to remember substitutions to expand the key space

(eg mYgrannyschaarhadstaples)

Educate users on the benefits of passwords managers. Having a password manager allows having very long and completely random passwords (eg. M>?tk6(fep68/Z41KZWOB) without the need to remember/write down. A strong passphrase is still required as a master key for to access the password manager