Dear Concern,

Hop you are doing well. I have analyzed the leaked passwords and presenting my overview here.

The hashing algorithm used to protect passwords is MD5. While MD5 is a generally a good checksum, it is insecure as a password hashing algorithm because it is simply too fast. You will want to slow your attacker down. So, the mechanism offer medium level of protection for passwords. The controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again is to use better algorithms and make use the user uses a strong password by checking password strength. What can I tell about the organization's password policy is – it is not good and strong enough. A password must be at least 8 letters length and use of capital letters, small letters, digitals and special characters is required. I will change these.

Thanks,

Azmine Toushik Wasi

Attachments:

Cracked Passwords:

experthead:e10adc3949ba59abbe56e057f20f883e - 123456

interestec:25f9e794323b453885f5181f1b624d0b - 123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password

simmson56:96e79218965eb72c92a549dd5a330112 - 111111

bookma:25d55ad283aa400af464c76d713c07ad - 12345678

popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1

edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered