

Hello,

This email is regarding the recent data breach in your organization and the action plans on how to make your organization more secure.

We tried the password dump and as all the passwords were secured though MD5 cryptographic algorithm to obfuscate the password in the database we were able to brute force the password dump and uncover all the passwords.

As all the passwords being used by your organization are minimum 6 characters long also we know that MD5 is the most vulnerable hashing algorithm, and particularly vulnerable to Collisions. Ouch. The main reason you shouldn't use MD5 is because it is a general purpose Hash.

In this case, we suggest a password policy change and the details are as follows:

1. Don't reuse your passwords
2. Do not use sequential numbers or letters
3. Do not include your personal information in your password
4. Use a combination of at least eight letters, numbers, and symbols
5. Use a password manager

Thanks and Regards,

Dheeraj Kashyap