**Subject: leaked password database severity**

Dear Mr. David M. Solomon,

I am writing this email to report to you about the leaked password database. This email covered all the topics that are related to hashing algorithms we used, the level of protection, how to implement security, and our password policy.

Okay, let’s discuss it.

The passwords hash has based on the MD5 message-digest algorithm. It is a cryptographically broken but still widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function.

And the level of protection of md5 as it has a 128-bit hash value and is used as a cryptographic hash function. Now MD5 hashes are no longer considered cryptographically secure, and they should not be used for cryptographic authentication.

To implement more security we have to use passwords rules or passwords that may combination of numbers, capital, and small letters, special chars. Should have a minimum of 15 in length. Also, we can use another algorithm that is more secure.

Password policy should be:

At least 8 characters—the more characters, the better

A mixture of both uppercase and lowercase letters

A mixture of letters and numbers

Inclusion of at least one special character, e.g.,! @ # ? ]

This password policy will make breaking the passwords harder

Thanks,

Shivam Hande,

Intern, Goldman Sach.