Date: June 2, 2021

To: Goldman Sachs Executive

From: Pramod Sheoran, B.E Computer Engineer Graduate

Subject: Review of the Password Leak and Policy Changes.

Dear Sir/Ma'am

After trying to crack all the leaked hashes, I found several vulnerabilities in your password policy and this email concludes all the findings and suggestions to improve your password policy.

1. **Type of hashing algorithm used to protect passwords -** MD5 (Message Digest)

2. **Level of protection this mechanism offers for passwords -** MD5 provides very low level of protection as it has been cryptographically broken and considered insecure. For this reason, it should not be used for hashing passwords.

3. **In the Event of a future password database leak following controls should be implemented to make the cracking much harder:**
    - Use a much more secure hashing algorithm like Secure Hash Algorithm (SHA) or a Symmetric Cryptographic Algorithm.
    - Improve the current Password Policy of the organization.
    - Make Employees aware of the password ethics that should be followed while deciding a password.

4. **Following Observations were made regarding organization's password policy:**
    - The Smallest password length allowed appears to be 6 characters.
    - No checks made to ensure capital characters in the password.
    - No checks made to ensure Special characters in the password.
    - Employees seem to be unaware of basic password ethics i.e., not using very simple frequently used words as password.

5. **Following Changes are suggested in password policy for better security of passwords:**
    - All Password should be at least 9 characters long to increase variations in combinations and increase time required to crack the password.
    - There should be at least 1 Capital Letter in the password.
    - There should be at least 1 Special Character in the password.
    - Password should not contain common password elements like same as username, sequence of numbers etc.
    - Don't let users include their username, actual name, date of birth and other personal information while creating a password.

Thanking You,

Pramod Sheoran

B.E Computer Engineering

Cracked Passwords:

edi_tesla89 : 6c569aabbf7775ef8fc570e228c16b98 : password!

experthead : e10adc3949ba59abbe56e057f20f883e :123456

interestec : 25f9e794323b453885f5181f1b624d0b : 123456789

reallychel : 5f4dcc3b5aa765d61d8327deb882cf99 : password

bookma : 25d55ad283aa400af464c76d713c07ad : 12345678

popularkiya7 : e99a18c428cb38d5f260853678922e03 : abc123

ortspoon : d8578edf8458ce06fbc5bb76a58c5ca4 : qwerty

heroanhart : 7c6a180b36896a0a8c02787eeafb0e4c : password1

eatingcake1994 : fcea920f7412b5da7be0cf42b8c93759 : 1234567

simmson56 : 96e79218965eb72c92a549dd5a330112 : 111111

liveltekah : 3f230640b78d7e71ac5514e57935eb69 : qazxsw

johnwick007 : f6a0cb102c62879d397b12b62c092c06 : bluered

blikimore : 917eb5e9d6d6bca820922a0c6f7cc28b : Pa$$word1