

Greetings Sir/Ma'am,

I discovered multiple flaws in your password policy after attempting to crack all of the leaked hashes, and this email summarizes all of my findings and recommendations for improving your password policy.

The main cryptographic hash functions for data security and authentication are Secure Hash Algorithm (SHA) and Message Digest (MD5). MD5, a weaker hash technique prone to collisions, was used in all of the passwords that were hacked.

Using <https://crackstation.net/> wordlist via terminal and online browsers, it was fairly simple to break. To generate hashes for the password, I recommend using a highly strong password encryption mechanism based on SHA.

After cracking the passwords, I discover the following information about the password policy of the company:

- Minimum length for password is set to 6.
- There are no precise requirements for creating a password. To construct a password, users can use any combination of words and characters.

You can add a few extra features to your password policy. My suggestions are as follows:

- In your password, avoid using common words and character combinations.
- Longer passwords are preferable, 8 characters is a good start.
- Passwords should not be reused.
- In your password, include special characters, capital and lowercase letters, and digits.
- Never include username, actual name, date of birth and other personal information while creating a password.
- Use a password manager.
- Change password every 3 months.

Security Algorithms used:

experthead:e10adc3949ba59abbe56e057f20f883e – **MD5**

interestec:25f9e794323b453885f5181f1b624d0b – **MD5**

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 – **MD5**

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 – **MD5**

simmson56:96e79218965eb72c92a549dd5a330112 – **MD5**

bookma:25d55ad283aa400af464c76d713c07ad – **MD5**

popularkiya7:e99a18c428cb38d5f260853678922e03 – **MD5**

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – **MD5**

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – **MD5**

edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 – **MD5**
liveltekah:3f230640b78d7e71ac5514e57935eb69 – **MD5**
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – **MD5**
johnwick007:f6a0cb102c62879d397b12b62c092c06 – **MD5**
flamesbria2001:9b3b269ad0a208090309f091b3aba9db – **MD5**
oranolio:16ced47d3fc931483e24933665cded6d – **MD5**
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e – **MD5**
moodie:8d763385e0476ae208f21bc63956f748 – **MD5**
nabox:defebde7b6ab6f24d5824682a16c3ae4 – **MD5**
bandalls:bdda5f03128bcbdfa78d8934529048cf – **MD5**

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**

Mentari E.M. Pangkey

Informatics Engineering student at Sam Ratulangi University