Email drafted that can be sent to the organization whose usernames and hashes were leaked. The mail goes over the password policy of the organization and suggests a few changes that could be made to improve security.

Dear Sir/Madam

After cracking a set of leaked hashes from your organization and analyzing them, I would like to report to you my findings and make suggestions in regards to the password policy followed in the organization.
By making use of crackstation.net, which is an online tool that uses its own wordlist to crack passwords, I was able to crack thirteen of the nineteen leaked passwords within just a second. This was all possible due to the fact that the organization was using the MD5 algorithm to hash its passwords. Nowadays, MD5 has been said to be cryptographically broken and considered insecure. Hence, it should not be used for anything, let alone for storing passwords.

By observing the cracked passwords, it seems that the organization has allowed users to keep passwords of a minimum length of six, and allowed them to simply use any combination of letter, lower and upper case, numbers, and a few special characters like underscores, dollar signs, and exclamation marks.

Based on the above observations, I would suggest the organization to

- Increase the minimum length of passwords to eight, as it makes cracking exponentially difficult.
- Impose limitations like the compulsory usage of at least a single lowercase letter, uppercase letter, number, and special symbol in the passwords.
- Forbid users from using their own usernames in their passwords, this is something that has been implemented in the AWS service page.

I would also recommend the organization to use a more secure hashing function like the Secure Hash Algorithm (SHA) or a Symmetric Cryptographic Algorithm. I would also suggest using techniques like salting to make it harder for specific attacks like Rainbow tables to successfully crack passwords in case of a future leak.

Thanking you
Hamza R. Khan
B.E. in Computer Science