To **Joanna**,
Goldman Sachs,
Warsaw Office.

Subject: Submission of Cracking leaked password database task provided in Virtual Experience.

The Table summarise the task of cracking the passwords for different hashes provide in dump file.

Username	Hash	Cracked Password	Type of Encryption
experthead	e10adc3949ba59abbe56e057f20f883e	123456	MD4
popularkiya7	e99a18c428cb38d5f260853678922e03	abc123	MD5
ortspoon	d8578edf8458ce06fbc5bb76a58c5ca4	qwerty	MD5
simmson56	96e79218965eb72c92a549dd5a330112	111111	MD5
liveltekah	3f230640b78d7e71ac5514e57935eb69	qazxsw	MD5
eatingcake1994	fcea920f7412b5da7be0cf42b8c93759	1234567	MD5
johnwick007	f6a0cb102c62879d397b12b62c092c06	bluered	MD4
edi_tesla89	6c569aabbf7775ef8fc570e228c16b98	password!	MD5
interestec	25f9e794323b453885f5181f1b624d0b	123456789	MD5
reallychel	5f4dcc3b5aa765d61d8327deb882cf99	password	MD5
bookma	25d55ad283aa400af464c76d713c07ad	12345678	MD5
heroanhart	7c6a180b36896a0a8c02787eeafb0e4c	password1	MD5
blikimore	917eb5e9d6d6bca820922a0c6f7cc28b	Pa$$word1	MD5
flamesbria2001	9b3b269ad0a208090309f091b3aba9db	Flamesbria2001	MD5
nabox	defebde7b6ab6f24d5824682a16c3ae4	nAbox!1	MD5
spuffyffet	1f5c5683982d7c3814d4d9e6d749b21e	Spuffyffet12	MD5
oranolio	16ced47d3fc931483e24933665cded6d	Oranolio1994	MD5
bandalls	bdda5f03128bcbdfa78d8934529048cf	Banda11s	MD5
moodie	8d763385e0476ae208f21bc63956f748	moodie00	MD5

The level of protection offered by MD4 and MD5 are poor and these methods have deprecated.

My conclusions about organisation's password policy:

• Minimum length for password is set to 6 encryption type in MD4 or MD5.

• There is no specific requirement for the password creation.

Users can use any combination of word and letters to create a password.

My recommendations for password policy are:

• Users should avoid common words and character combinations in the password.

• Longer passwords Must be preferred and minimum must be 8 characters.

• Users should not reuse passwords in multiple websites.

• Include special character, capital and small letters, numbers in the password.

• Don't let users include their username, actual name, date of birth and other personal information while creating a password.

• **Using SHA-3, bycrypt, TDEA** etc. more advanced encryption algorithms make it difficult to decrypt hash also spreading awareness among users to follow these policies to keep their passwords strong and safe.

Thank you for providing such an amazing opportunity.

Yours Faithfully

Hitesh Kumar