6 BASIC RULES FOR A GOOD PASSWORD POLICY

aka *How to setup a safer organization by IT departments*

01.

DEFINE THE POLICY IN AN EASY-TO-UNDERSTAND FORM

Document the password policy so that it includes all the important information – such as length of the password, complexity as well as acceptable unsuccessful login attempts.

02.

FORCE RESPECTING THE POLICY ON ALL LEVELS

All employees are to follow the company password policy. This includes the owners as well as top management and board members, without exception.

03.

BLACKLISTING BAD PASSWORDS

Create a "blacklist" of the most commonly used and/or previously compromised passwords and reject all attempts to use them.

04.

STORAGE OF USER PASSWORDS

Store the user passwords as salted hashes, and use a hashing algorithm specifically designed for password storage.

05.

CHANGING PASSWORDS NOT TOO OFTEN

Periodic password expiration is no longer an advised security practice. NIST as well as the UK National Cyber Security Centre (NCSC) now recommend changing passwords only in case the subscriber requests it or there is evidence of a compromise. Users forced to change their passwords too often will resort to using simpler and easy-to-remember passwords, or to adopting a trivial strategy such as adding a number or letter to the end of their password and then incrementing that at each change. Both approaches result in weaker protection of the company system.

06.

APPLY POLICY TO THE WHOLE NETWORK INCLUDING IOT

Password security policy should also encompass all passwords protecting the organization's devices and systems, especially IoT devices, such as security cameras, smart hubs and routers. If these are mismanaged or are used with default credentials, there is an ever-growing risk that attackers will find and try to exploit this vulnerability.

8 STEPS TO CREATE STRONG PASSWORDS

aka *How to instruct employees in your organization*

01.

A PASSWORD HAS TO BE UNIQUE

This applies for each account to avoid compromising multiple resources, if leaked. A password should not be written down on sticky notes or in an unencrypted file saved on any company device.

02.

THE LONGER THE PASSWORD THE BETTER

US National Institute for Standards and Technology (NIST) recommends at least 8 characters, offering a reasonable level of protection against brute force attacks.

03.

ENCOURAGE THE USE OF PASSPHRASES

A phrase with 30 or more characters, even if only comprised of alphabetics, is significantly safer than an 8-character word with common substitutions (such as '3' for the letter 'e', "!" for "i" or "l", etc.) Phrases are also inherently easier to remember, so the additional length is not as great a burden to the user.

04.

ELIMINATE COMPLEX COMPOSITION RULES

Requiring users to include both uppercase and lowercase characters, at least one number and a special character, rarely encourages users to set stronger passwords, and rather leads to both weaker and harder-to-remember passwords.

05.

DO NOT SHARE PASSWORDS

Never show your passwords to others, including colleagues, superiors, family or the HelpDesk, since phishers may well pretend to be from IT support.

06.

AVOID REPETITIVE CHARACTERS

"XXXX" is not a good password. Similarly, any sequential characters (e.g. '1234'), and recognizable patterns such as 'qwerty' are to be ommited.

07.

DO NOT USE COMMON DICTIONARY WORDS

These words can be brute forced in a dictionary attack. This includes foreign languages, or expert terms from different fields.

08.

NEVER USE PERSONAL INFORMATION

These can be guessed by the attackers based on information acquired from social media. This includes middle names, birthdates, addresses, schools, spouse's or child's name.