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.

ESET®

CYBERSECURITY
EXPERTS ON YOUR SIDE

For more information visit
www.eset.com