ELEARNINGNEWS ARTICLE

Year 6 - number 188 Wednesday 2 february 2022

Cybersecurity: how to set a secure password

Globally, password vulnerability data worsened from 2020 to 2021. Banned easy passwords resulting in the most chosen passwords of 2021

We have often talked about the importance of **cybersecurity** and how much it depends on the **human factor** and can also pass from **passwords**.

Password: the least secure is chosen

Laziness and forgetfulness are two powerful enemies, also when it comes to computer security and passwords. 123456 will be judged by most of us as an **insecure password**, yet, in 2021 it was the most chosen password according to a **report by Nordpass**, along with numeric sequences such as 111111 or 123123. Among non-numeric passwords, depending on the topic, we see that in the world the most chosen are "Ferrari", "Porsche" (in the automotive field), "Michael" (in proper names). In Italy also soccer teams are positioned in the password ranking and the most popular are "Juventus" and "Napoli". Emblematic, as well as paradoxical, also the choice of the password "cambiami" or "password".

Worldwide, the data on the **vulnerability of passwords** have worsened from 2020 to 2021: if in 2020, 73% of passwords could be deciphered in less than a second (with special applications used by hackers, although the measure of the "deciphering time" is indicative and depends on various technological aspects), in 2021 the percentage stands at 84.5%. Already in 2020, 55% of data breaches worldwide were due to vulnerable passwords. **Here** a free virtual calculator that determines in a few seconds how vulnerable our passwords are.

According to Jonas Karklys, CEO of NordPass, "Passwords continue to weaken and people continue to not take care of them properly.It is important to understand that passwords are the gateway to our digital lives, and with the increase in time spent online, it is becoming extremely important to pay more attention to cybersecurity."

On the management of cybersecurity in the company and the strong correlation with the human factor, sometimes mistakenly taken lightly, is based the one-hour **online course " Cyber Security - Company information protection"** created by Mega Italia Media S.p.A., eLearning company very attentive to the technological factor and leader in Italy. The course covers various types of attack and best practices through which the employee or collaborator can manage the situation and avoid risks to corporate or personal data.

In the eLearning environment, the password issue is also very important for the protection of training data and employees' personal data, and affects platform administrators to a greater extent.

Strong passwords: how to manage them

The Garante della Privacy itself, in order to stem the high risks connected to the choice of an unsafe password (due to misinformation, lax attitude or underestimating) has drawn up a **vademecum**.

The choice of the password should follow some precise criteria:

- length: minimum 8 characters (better 15)
- type of characters: at least 4 (maize letters, lowercase letters, numbers, special characters, such as asterisks, exclamation marks ...)
- do not use personal references (name, date of birth ...)
- do not use references to the username
- avoid commonly used words (it is better to use fancy or disguised words, for example "computer" could become "c0mpu!3r") to avoid the easy success of the action of software that systematically tries all the commonly used words in

different languages
- change your password periodically
- use different passwords for different accounts (to avoid that by stealing one password, the cybercriminal has access to all the victim's accounts)
- do not use passwords used in the past
- immediately change temporary passwords issued the first time a computer system or service is accessed
- use multi-factor authentication mechanisms, if available.
- store passwords without writing them down (on a card, unprotected files on a PC, smartphone or tablet, or in the body of emails and messages) or communicating them to anyone

Translated with www.DeepL.com/Translator