RULE ENFORCEMENT - NIST

Nel rapporto speciale *NIST-SP-800-63-2*, il **NIST** (**N**ational **I**nstitute of **S**tandards and **T**echnology) suggerisce alcune regole (**rule enforcement**) per la scelta delle password:

- la password deve contenere almeno sedici caratteri alfanumerici (**basic16**);
- la password deve contenere almeno otto caratteri, tra cui una lettera maiuscola e una minuscola, un simbolo e una cifra. Non può contenere una parola del dizionario (**comprehensive8**).

UN BUON METODO

È stato provato essere un buon trucchetto usare come password le lettere iniziali delle parole che compongono una certa frase (che si ricorda facilmente).

Per esempio:

<< Con mia moglie Federica ci siamo conosciuti a un concerto di Bob Dylan a New York nel 2005. >>

`Password → CmmFcscaucdBDaNYn2005.`

Oppure:

<< Il mio treno per Milano Centrale parte alle 7 e 5 da Pavia! >>

`Password → ImtpMCpa7e5dP!`

PASSWORD MANAGER

È ormai molto diffuso l'utilizzo di un **password manager** per conservare, in un unico posto e al sicuro, tutte le credenziali, senza la necessità di doverle ricordare a memoria.
Un **password manager** è un programma che archivia in modo sicuro e crittografato le credenziali (*username* e *password*) di accesso ai servizi web (e non solo) in una sorta di **cassaforte virtuale**. Questa è protetta da una **master password**, che serve per aprirla e diventa perciò l'unica password che occorre ricordare.

Un buon **password manager** è sicuro e facile da usare. Due sono i principali possibili rischi:

1. Scegliere un password manager non sicuro: potrebbe essere pericoloso affidare le proprie password ad un software se non se ne conosce e attesta l'affidabilità.
2. Dimenticare la master password: non esiste il solito pulsante "ho dimenticato la password" per recuperare la chiave d'accesso, proprio per ragioni di sicurezza. Quindi dimenticare la master password significa perdere definitivamente tutte le proprie password !

Alcuni password manager sul mercato sono: **LastPass**, **1Password** e (totalmente gratuito perché progetto open-source) **KeePass**.

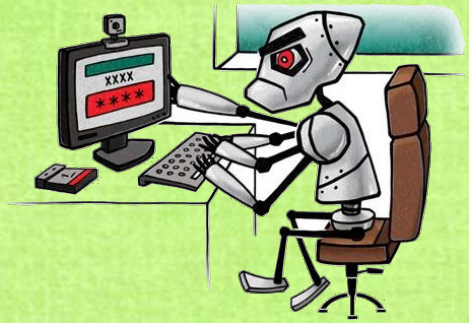
RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/password_buone_pratiche/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

PASSWORD E BUONE PRATICHE

Scopri tutto quello che serve sapere sulle password, come sceglierle, gestirle e non commettere errori.



PERCHÈ LA PASSWORD DEVE ESSERE COMPLICATA?

È una seccatura, anzi è quasi impensabile per molti utenti pensare a password complesse, eppure è l'unico modo per stare veramente al sicuro: se inseriamo un codice di accesso come "ciao", il nostro nome, cognome, data di nascita o codice fiscale o come "password", "12345" o "qwerty", chiunque dovesse provare ad accedere per tentativi avrebbe discrete possibilità di entrare nell'account a nostra insaputa.

Scegliere una buona password è importante, specialmente se si tratta di servizi che includono l'accesso a servizi di pagamento (**eBay, Amazon**) o **e-commerce** in generale.

Il giusto compromesso sta nel trovare una password che sia difficile da indovinare e relativamente facile da ricordare.

PASSWORD DA NON USARE

È altamente sconsigliato scegliere le seguenti password !!!

- *password*
- *password123*
- *ciao*
- *123456*
- *123456789*
- *12345678*
- *12345*
- *111111*
- *1234567*
- *qwerty*
- *iloveyou*
- *batman*
- *superman*

È altamente sconsigliato scegliere le seguenti varianti come password !!!

- *<nome><data-di-nascita>*
- *<nome><giorno-di-nascita>*
- *<nome><anno-di-nascita>*
- *<cognome><data-di-nascita>*
- *<cognome><giorno-di-nascita>*
- *<cognome><anno-di-nascita>*
- *<userID><data-di-nascita>*
- *<userID><giorno-di-nascita>*
- *<userID><anno-di-nascita>*
- *<nome>.<cognome>*
- *<cognome>.<nome>*
- *<iniziale-cognome><iniziale-nome><data-di-nascita>*
- *<iniziale-nome><iniziale-cognome><data-di-nascita>*

COME SCEGLIERE UNA BUONA PASSWORD

Le regole basilari per la scelta di una buona password sono le seguenti:

- usare password **non banali** o corrispondenti, ad esempio, a nomi, date di nascita, numeri o semplici parole come "ciao", "password" e così via;
- utilizzare ogni singola password una ed una sola volta per ogni sito, servizio o email;
- assicurarsi che nella password ci siano **lettere** e **numeri** e, se possibile (e se ammesso) almeno un **simbolo non alfabetico**;
- sfruttare, secondo un criterio facile da ricordare, varianti non scontate di una **password base**;
- se ci stiamo registrando a servizi di natura dubbia, per semplice curiosità o a livello di test, è opportuno registrarsi con email non ufficiali (registratene una per l'occorrenza, magari) ed usare generatori di **password casuali** tipo: *https://passwordsgenerator.net/* .

Ovviamente queste regolette sono delle linee guida basilari, la cui applicazione va più o meno intensificata a seconda delle **esigenze personali** e tenendo presente l'**affidabilità del servizio** di registrazione.

REGOLE DI BUON SENSO E METODI DI SUO COMUNE

È possibile agire seguendo alcune **strategie** per scegliere in maniera sicura le password.

Educazione dell'utente

Nonostante le molteplici raccomandazioni molti utenti tendono ancora ad ignorare tali raccomandazioni riguardo la scelta della password. Molti altri invece non sono neanche in grado di giudicare se una password è buona o meno.

Occorre pertanto **istruire adeguatamente** gli utenti e fare in modo che possano riconoscere una password sicura da una invece più vulnerabile.

Password generate al computer

Un altro modo per assicurarci di aver scelto una buona password è quello di affidarci ad un sistema in grado di **generare automaticamente** password che soddisfano precisi requisiti.
Nonostante dovrebbe essere la normalità e ci siano tool online (come ad esempio quello citato prima) di facile utilizzo per questa proposta, molti utenti ancora faticano ad accettare questa prassi.

Controllo reattivo (e proattivo) della password

Infine sarebbe bello avere un sistema in grado di far reinserire la password all'utente ogni qualvolta esso ritenga sia troppo facile (il sistema prova ad autenticarsi da solo e valuta la complessità, **sistema reattivo**); questo ovviamente è però troppo costoso in generale e si preferisce per cui un **sistema proattivo** che mira a soddisfare un compromesso tra complessità e accettabilità, fornendo delle indicazioni all'utente in fase di inserimento della password.