MINISTERO DELL'ISTRUZIONE E DEL MERITO
ISTITUTOCOMPRENSIVOROMBIOLO
Vial°Maggio151-89841Rombiolo(VV)
E-mail: vvic81300p@istruzione.it-PECvvic81300p@pec.istruzione.it
Telefono:0963367184-CF 96012580799Sitoweb:http://www.icrombiolo.edu.it

ISTITUTO COMPRENSIVO STATALE ROMBIOLO - -ROMBIOLO
Prot. 0008444 del 19/09/2023
II (Uscita)

Ai Docenti
Al Personale Amministrativo
Alla DSGA
Al Team digitale
All'Animatore Digitale
Alla FS Area 3
Al Sito Web

Circolare N° 20

Oggetto: corretta impostazione e utilizzo delle password

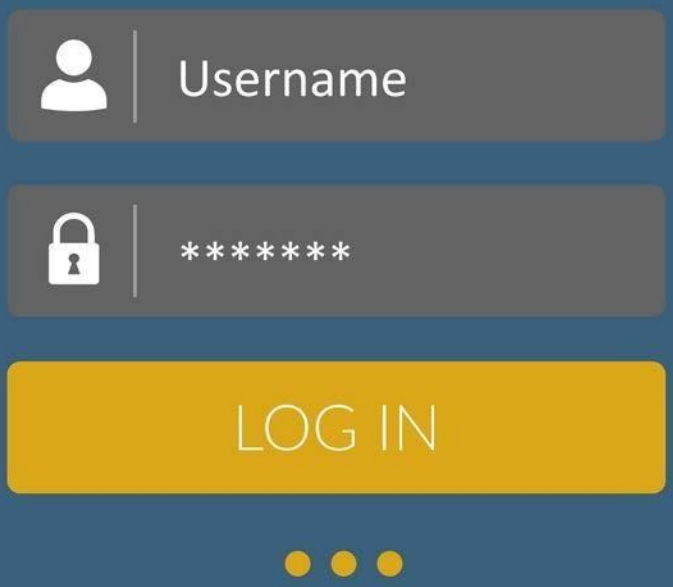
Si informa il personale in epigrafe che, al fine di una corretta gestione delle password usate nella pubblica amministrazione, si allega alla presente il Vademecum del Garante.
L'occasione è gradita per augurare a tutti un buon lavoro.

Responsabile dell'istruttoria
Ins. Ventura Francesco

Responsabile del Procedimento
La DSGA, Mariarosa Contartese

IL DIRIGENTE SCOLASTICO
Prof. Giuseppe Sangeniti
(firmato digitalmente)

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Suggerimenti per creare e gestire password a prova di privacy

IMPOSTA BENE LA TUA PASSWORD

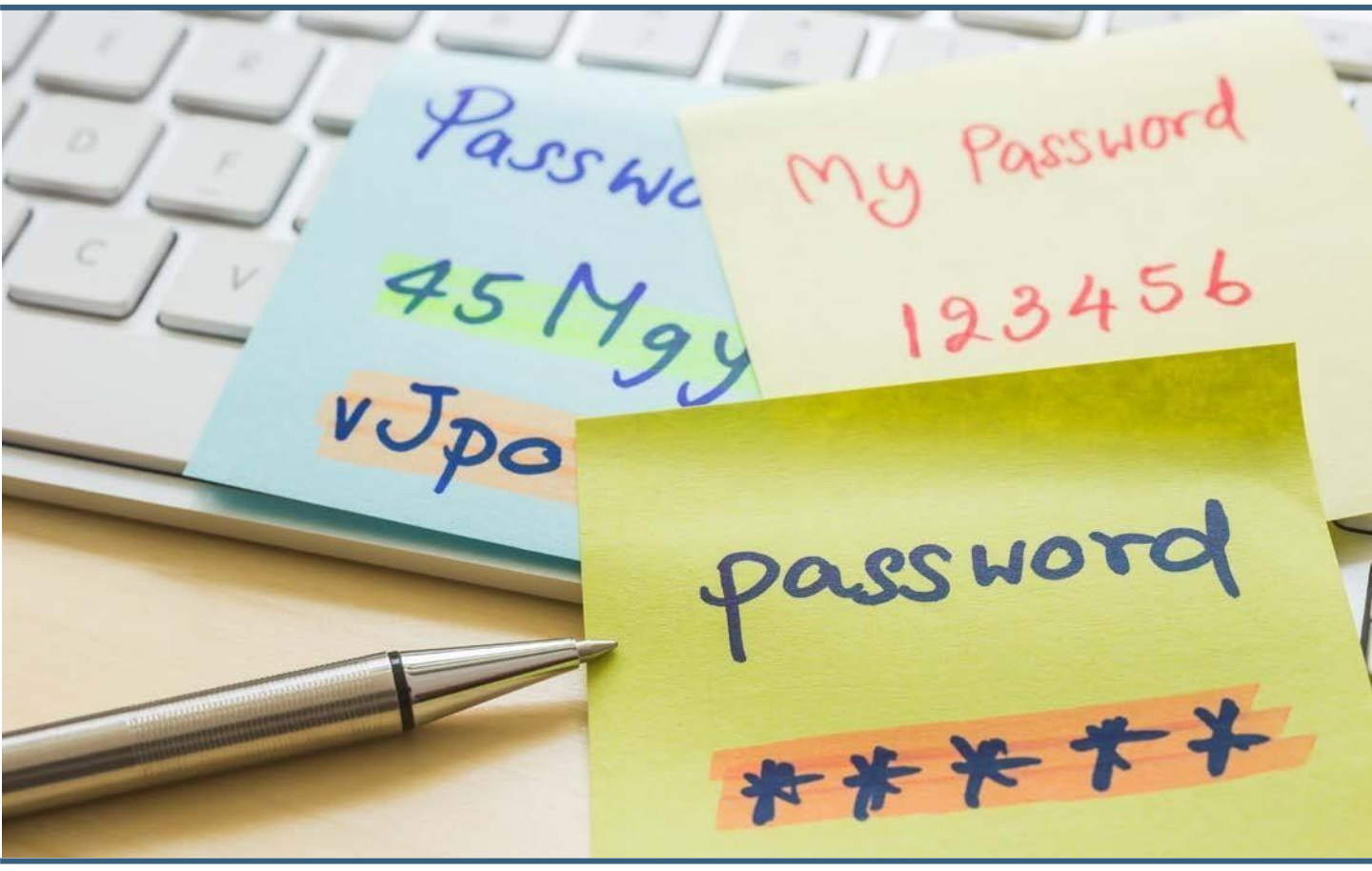
Una buona password:

- **deve essere abbastanza lunga**: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);
- **deve contenere caratteri di almeno 4 diverse tipologie**, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
- **non deve contenere riferimenti personali facili da indovinare** (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
- **meglio evitare che contenga parole "da dizionario",** cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
- **andrebbe periodicamente cambiata**, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GESTISCI BENE LE TUE PASSWORD

- **Utilizza password diverse per account diversi** (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.
- Altra accortezza importante è quella di **NON utilizzare password già utilizzate in passato**.
- Occorre poi ricordare che le eventuali **password temporanee** rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.



SE VUOI STARE PIU' TRANQUILLO

Utilizza (laddove disponibili) **meccanismi di autenticazione multi fattore** (es. codici OTP one-time-password), che rafforzano la protezione offerta dalla password.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

CONSERVA CON CURA LE TUE PASSWORD

- **Non scrivere mai le password su biglietti** che poi magari conservi nel portafoglio o indosso, o che puoi distrattamente lasciare in giro, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet).
- **Evita sempre di condividere le password** via e-mail, sms, social network, instant messaging, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati.
- Se usi pc, smartphone e altri dispositivi che non ti appartengono, **evita sempre che possano conservare in memoria le password da te utilizzate**.

VALUTA SE USARE «GESTORI DI PASSWORD»

Si tratta **di programmi specializzati che generano password sicure** e consentono di appuntare in formato digitale tutte le password salvandole in un database cifrato sicuro. Ce ne sono di vario tipo, gratuiti o a pagamento.

La scheda ha finalità meramente divulgative e sarà aggiornata in base agli sviluppi tecnologici e normativi