Rag. Renzo Del Rosso

Massa e Cozzile, li 16 novembre 2021

Circolare n°18

Ai gentili Clienti
Loro sedi

La tua password è sicura?
I suggerimenti del Garante della Privacy

Gentile Cliente,

*Il Garante della Privacy ha pubblicato un **vademecum** con poche regole base per creare e gestire le password in maniera corretta e sicura da qualsiasi possibile attacco.*
Vediamo insieme quali sono i consigli del Garante.
Certi di aver fatto cosa gradita, restiamo a disposizione per una consulenza dettagliata.

Premessa

Pochi e semplici suggerimenti di base contenuti in un **vademecum** che il Garante della Privacy ha voluto pubblicare, con lo scopo di dare consigli su come impostare password sicure e su come gestirle in modo prudente.

Il documento spiega quali sono le modalità di scelta di una buona password e le modalità di gestione delle stesse, sia che siano utilizzate in ambito lavorativo o in momenti di vita quotidiana, e ancora come conservarle in maniera sicura.

Il garante precisa che la prima linea di difesa dei nostri dati personali è sempre la **consapevolezza** su come gestiamo, conserviamo ed eventualmente diffondiamo le informazioni che ci riguardano.

I consigli

Una password per essere sicura ed efficace:

- **deve essere abbastanza lunga**: avere almeno 8 caratteri, 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).

Inoltre sarebbe meglio evitare che contenga parole intere di uso comune: è meglio usare parole **di fantasia** oppure parole "camuffate" per renderle meno comuni.

Il garante fa notare che esistono software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue.

Pertanto, sarebbe di fondamentale importanza che la password venga **periodicamente cambiata**, soprattutto per i profili più importanti o quelli utilizzati più spesso, come e-mail, e-banking, social network, ecc..

Altra buona norma consiste nell'utilizzare **password diverse per account diversi** (e-mail, social network, servizi digitali di varia natura, ecc.) in modo tale che in caso di «furto» di una password si eviterebbe il rischio che anche gli altri profili di appartenenza possano essere facilmente violati.

NOTA BENE - Altro punto essenziale è quello di **NON utilizzare password già utilizzate in passato**.

Il documento ricorda inoltre che le eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre **immediatamente cambiate**, scegliendone una personale.

Sarebbe buona cosa infine utilizzare, laddove disponibili, **meccanismi di autenticazione** multi fattore (es. **codici OTP** one-time-password), che vanno a rafforzare la protezione offerta dalla password.

Ragioniere Tributarista qualificato Lapet di cui alla L. N° 04/2013 (N° iscr. 8083047)
Certificato a norma UNI 11511:2020 - Registrazione n°576 FAC Certifica
Via Calderaio n°4 - 51010 Massa e Cozzile (Pt)
Codice Fiscale DLR RNZ 57A05 D612Q - Partita IVA 01791500471
Tel/Fax 0572/050285 - Email scrivi@renzodelrosso.eu - Pec: renzodelrosso@pec.it
Sito web: http://www.renzodelrosso.eu

Rag. Renzo Del Rosso

Come conservare le password in sicurezza

Il garante ha voluto dare dei consigli anche per la fase di conservazione:

- **non scrivere mai le password su biglietti** che vengono conservati nel portafoglio o indosso, o che distrattamente vengono lasciati in giro, oppure in file non protetti sui dispositivi personali (computer, smartphone o tablet);
- **evitare sempre di condividere le password** via e-mail, sms, social network, instant messaging, ecc.. Anche se comunicate a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati;
- se si usano pc, smartphone e altri dispositivi che appartengono ad altri, evitare sempre che vengano conservate in memoria le proprie password utilizzate.

I programmi gestori di password

Il documento consiglia in ultimo l'utilizzo di **programmi specializzati che generano password sicure**: ne esistono di vario tipo, gratuiti o a pagamento e consentono di appuntare in formato digitale tutte le password salvandole in un database cifrato sicuro.

Link utili

Suggerimenti per creare e gestire password a prova di privacy – VADEMECUM
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4248578

Distinti saluti

Lo Studio ringrazia per l'attenzione riservatagli e rimane a disposizione per ogni ulteriore chiarimento, riservandosi la facoltà di tenervi costantemente aggiornati sulle novità e relativi adempimenti di Vostro interesse……

Ragioniere Tributarista qualificato Lapet di cui alla L. N° 04/2013 (N° iscr. 8083047)
Certificato a norma UNI 11511:2020 - Registrazione n°576 FAC Certifica
Via Calderaio n°4 - 51010 Massa e Cozzile (Pt)
Codice Fiscale DLR RNZ 57A05 D612Q - Partita IVA 01791500471
Tel/Fax 0572/050285 - Email scrivi@renzodelrosso.eu - Pec: renzodelrosso@pec.it
Sito web: http://www.renzodelrosso.eu