www.garanteprivacy.it/flash

Consigli flash

TUTELARE la tua privacy con buone password

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network*, ecc.).

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet*.
- **Evita 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 pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

4 PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD»

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

Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash e le nostre campagne di comunicazione «Social privacy», «Fatti smart» e «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante:
www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il **phishing** è una tecnica illecita utilizzata per **appropriarsi di informazioni riservate relative a una persona o a un'azienda** - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, **i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare**. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti.

E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e- mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto ditipo bancario, attraverso tali canali.

Se si ricevono messaggi sospetti, è bene **non cliccare sui link in essi contenuti e non aprire eventuali allegati**, che potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri.

Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

Occhio agli indirizzi

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi oaddirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche **grossolani errori grammaticali, di formattazione o di traduzione da altre lingue**.

E' utile **anche prestare attenzione al mittente** (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).

Meglio diffidare dei **messaggi con toni intimidatori**, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

Proteggersi è meglio

E' utile installare e tenere aggiornato sul pc o sullo smartphone un **programma antivirus che protegga anche dal phishing**. Programmi e gestori **di posta elettronica** hanno spesso **sistemi di protezione** che indirizzano automaticamente nello **spam** la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio **non memorizzare dati personali e codici di accesso nei browser** utilizzati per navigare online. In ogni caso, è buona prassi **impostare password alfanumeriche complesse**, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

Acquisti online in sicurezza

Se si fanno acquisti online, è più prudente **usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati** del conto bancario o della carta di credito.

La prudenza non è mai troppa

Per proteggere conti bancari e carte di credito è bene **controllare spesso le movimentazioni** e attivare **sistemi di *alert*** automatico che avvisano l'utente di ogni operazione effettuata.
Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile **contattare direttamente** la banca o il gestore della carta di credito attraverso **canali di comunicazione conosciuti e affidabili**.

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