IMQ intuity
SOCIETÀ DEL GRUPPO IMQ

PASSWORD BEST PRACTICES

I nostri account o profili social, definiti da un nome utente e da una password, sono il nostro lascia passare per accedere agli innumerevoli e svariati servizi, siti web e applicazioni che Internet ci offre.
Allo stesso tempo, il nostro account personale ci differenzia dagli altri utenti, rendendoci "unici" per dati, gusti, preferenze di acquisto e moltissime altre informazioni che ci riguardano.
La protezione dei nostri account attraverso password sicure non dev'essere percepita come un impiccio alla veloce fruibilità dei servizi, social network, siti web e molto altro, ma come un impedimento all'accesso, da parte di estranei, alle nostre informazioni.

La password, quindi, è sì un lasciapassare ai servizi che utilizziamo quotidianamente, ma se percepita ed utilizzata correttamente, ci evita di mettere a rischio la nostra privacy ed il nostro portafogli, quando questi accessi interessano credenziali di carattere finanziario.

PRATICI CONSIGLI PER CREARE PASSWORD SICURE, PER MEMORIZZARLE E GESTIRLE CON SEMPLICITÀ.

BY IMQ INTUITY
SECURITY AWARENESS

LE DIFFICOLTÀ PIÙ COMUNI

Una persona utilizza in media 25 profili account che richiedono delle credenziali per accedervi, ma possiede in media dalle 6 alle 8 password. Da questa ricerca di Microsoft si evince come **la stessa password spesso venga utilizzata per account multipli.**

Altro problema è l'utilizzo di **password deboli** o, come spesso c'è capitato di vedere durante le nostre simulazioni di attacco, in seguito alla richiesta di un aggiornamento delle credenziali, l'impostazione di password progressive, ad esempio da "Pippo29" a "Pippo30".

L'impostazione di una password sufficientemente sicura ma allo stesso tempo facilmente memorizzabile, spesso ci scoraggia e per fretta o per pigrizia preferiamo usufruire sempre delle stesse.

BEST PRACTICES

Il primo passo utile è quello di modificare il nostro approccio nei confronti delle proprie password, iniziando a considerarle non più come una scocciatura, un qualcosa in più da dover ricordare, ma come una **vigile sentinella**, di guardia alle nostre aree professionali e private, accessibili solo a noi.

Vediamo allora come rendere sicure e gestire al meglio queste sentinelle al servizio della nostra protezione:

- Utilizzare un **gestore di password**. che permette, attraverso un univoco accesso, di poterle memorizzare, creare ed inserire. Ne esistono diversi, anche in versione free, uno tra questi è **LastPass** (https://www.lastpass.com/it/)
- Non utilizzare la stessa password per accedere ad account multipli.
- Non utilizzare come password riferimenti a persone, animali o altro riconducibili ad aspetti pubblici della propria vita professionale e privata. Ad esempio, evitare di usare il nome di figli, animali domestici, etc.
- Per alcuni account le password devono seguire determinati requisiti (lunghezza, presenza di almeno un numero, una maiuscola o un carattere speciale). Anche se non viene esplicitamente richiesto, facciamolo ugualmente.
- Non memorizzare password all'interno di file salvati nel proprio pc, server o servizi cloud; meglio utilizzare un gestore di password (vedi primo punto).

LA RICETTA PER UNA BUONA PASSWORD

Vi siete mai chiesti se la vostra password è abbastanza sicura?

Il problema che abbiamo tutti è quello di riuscire a pensare ad una stringa di caratteri di media lunghezza, che sia **imprevedibile**, **complessa** ma allo stesso tempo **facile da ricordare**.

Come fare?

1. Pensiamo ad una frase, relativa a qualcosa che facciamo di solito, la frase di una canzone, il passo di un libro, qualcosa che potete ricordare facilmente. Es. "Welcome to the jungle"
2. Utilizziamo solo la prima e l'ultima lettera di ciascuna parola, alternandole tra maiuscole e minuscola: "WeToTeJe".

Il risultato è una password complessa, ma per noi avrà una sua logica e sarà più facile da memorizzare.

Vuoi verificare se le tue password sono mai state hackerate?

Vai a questo link, inserisci l'indirizzo e-mail che utilizzi per accedere ai tuoi account e fai un controllo: https://haveibeenpwned.com/

LO SAPEVI?

Alcuni episodi reali dove una password debole ha causato ingenti danni.

Australian Department of Defence

Un hacker è riuscito a sottrarre 30 gigabyte di informazioni sensibili, riguardanti aerei e navi da guerra della marina australiana, introducendosi in un portale web attraverso le credenziali di accesso di default "admin-admin". (https://www.abc.net.au/news/2017-10-11/hacker-stole-data-from-defence-subcontractor/9040906)

Profilo Twitter di Trump

Un esperto di sicurezza informatica ha dimostrato di essere entrato nel profilo dell'ex-Presidente Trump utilizzando uno dei suoi leit motiv, spesso usato durante i suoi comizi pubblici: "maga2020!". (https://www.agi.it/blog-italia/cybersecurity/post/2020-10-23/hackerato-profilo-twitter-trump-come-ha-fatto-victor-gevers-10044931/)

SOCIETÀ DEL GRUPPO IMQ

IMQ Intuity propone un approccio diverso alla Cybersecurity modificando lo status quo che vede nella soluzione tecnologica l'unico modo di affrontare il problema, quest'ultimo invece sempre più legato all'uomo ed al contesto sociale in cui esso opera.

La sicurezza informatica deve essere approcciata da un punto di vista Culturale, mettendo al centro le persone nel processo di sicurezza aziendale: **People-Centric Security**

www.intuity.it

IMQ INTUITY S.r.l.
Soggetta ad attività di direzione e coordinamento di IMQ Group S.r.l.

Sede operativa
via A. Ceron, 2 35129 Padova
049 817 0850 | info@intuity.it

Sede legale
via Quintiliano, 45 20138 Milano
admin@pec.intuity.it