PILLOLE DI CYBER SECURITY #1

COME IMPOSTARE UNA PASSWORD SICURA.

SCORRI PER LEGGERE I NOSTRI TIPS!

1. CREA PASSWORD FACILI DA RICORDARE MA DIFFICILI DA INDOVINARE.

Non utilizzare parole o frasi di importanza speciale per te, come un compleanno o il nome di un familiare: è esattamente il tipo di informazioni che può essere scoperto.

2. NON CONDIVIDERE LE TUE PASSWORD.

Non darle mai e poi mai ai tuoi amici, nemmeno a quelli più fidati. Un amico potrebbe accidentalmente passare la tua password ad altri o diventare un ex-amico e abusarne.

LumIT
You Believe
We Create IT

3. ASSICURATI CHE LA PASSWORD SIA LUNGA.

Una buona password deve contenere almeno 8-12 caratteri. E ricorda sempre: più lunga è, meglio è!

4. DEVE INCLUDERE NUMERI, LETTERE MAIUSCOLE, LETTERE MINUSCOLE E SIMBOLI:

- Le lettere maiuscole e minuscole non devono essere raggruppate insieme. Se le mischi è più difficile prevedere la password.
- Prova a utilizzare € invece di E, 1 invece di L, (invece di C, 0 invece di O.
- Prova a includere &, % o un altro carattere speciale come [!”£$ /()=?^><@#]

LumIT
You Believe
We Create IT

5. NON USARE UNA SOLA PASSWORD. CREA PASSWORD SIMILI MA DIVERSE PER OGNI ACCOUNT.

Puoi utilizzare parole semplici per ricordare più facilmente le password senza renderle facili da craccare.

6. PROVA A UTILIZZARE UNA “FRASE” INVECE DI UNA SEMPLICE PAROLA COME PASSWORD.

- La frase dev’essere relativamente lunga (circa 20 caratteri).
- Pensa a qualcosa che tu puoi ricordare (ma non gli altri).
- Usa numeri, simboli, lettere maiuscole e minuscole.
- Evita frasi famose che potrebbero essere facili da indovinare.
- Ad esempio, “I really like dark chocolate” diventa “Ir€a11y1ik€DARK(h0(01at€”

LumIT
You Believe
We Create IT

7. ASSICURATI CHE LA TUA PASSWORD SIA CONSERVATA IN UN LUOGO SICURO.

- Non metterla in bella vista e, se devi scriverla, nascondi quella nota dove nessuno può trovarla.
- Considera l'opzione di utilizzare un password manager. Programmi o servizi web come 1Password, Lastpass, RoboForm, Keeper, ecc. ti permettono di creare password molto forti e diverse per ciascun account; tu devi solo ricordarti la password per accedere al programma.

LumIT
You Believe
We Create IT

8. UTILIZZA L'AUTENTICAZIONE A PIÙ FATTORI.

Molti servizi e social media offrono un'opzione per verificare la tua identità nel caso qualcuno accedesse al tuo account da un dispositivo non riconosciuto. Il metodo più tipico consiste nell'inviare un SMS o un altro tipo di messaggio al dispositivo mobile registrato a tuo nome contenente un codice che bisogna digitare per comprovare che sia davvero tu.

LumIT
You Believe
We Create IT

9. ASSICURATI CHE I TUOI DISPOSITIVI SIANO PROTETTI:

- La migliore password del mondo sarà completamente inutile se qualcuno sta sbirciando mentre la digiti o se ti dimentichi di terminare la sessione sul computer di un hotel o di un internet cafè.
- Assicurati di utilizzare un sistema operativo e un software anti-malware aggiornati.
- Stai molto attento prima di cliccare su un link che ti chiede di effettuare l’accesso, di modificare la password o di fornire dati personali, anche se sembra inviato da un sito legittimo. Se hai dubbi, digita quello che sai essere l’URL del sito web nella finestra del tuo browser.

LumIT
You Believe
We Create IT

TI È STATO UTILE QUESTO POST?

Sharing is
Caring

lumit.it