

Password solida? Non basta a proteggere il tuo account!



L'importanza di una password solida viene spesso sottolineata dalle risorse di settore e dagli addetti ai lavori in ambito cybersecurity. Indubbiamente, si tratta di uno degli argomenti fondamentali per garantire la sicurezza dei propri account; detto questo, sarebbe erroneo considerarlo l'unico, come una sorta di "proiettile d'argento" risolutivo in qualsiasi contesto.

L'arrivo della pandemia e le conseguenti misure hanno contribuito al raggiungimento di nuovi record di attacchi di phishing e sottrazione di dati online. Con questo articolo cercheremo di offrire una panoramica completa degli strumenti e delle pratiche da applicare per ridurre i rischi di sottrazione dei dati e aumentare la sicurezza dei propri profili virtuali.

Autenticazione a più fattori: definizione e ruolo

L'autenticazione a più fattori (multi-factor authentication, MFA) è un metodo di accesso ai profili online che richiede agli utenti di fornire più informazioni rispetto alla classica accoppiata "nome utente e password".

In pratica, questo significa che oltre alla parola chiave scelta al momento della registrazione, l'utente deve fornire anche un altro tipo di informazione di autenticazione, come ad esempio un codice inviato via SMS o una chiave di accesso fisica.

L'utilizzo dell'autenticazione a più fattori aumenta la sicurezza dei sistemi e degli account online, rendendo più

difficile per gli hacker e le organizzazioni criminali ottenere l'accesso ai dati sensibili. Inoltre, l'utilizzo di questo metodo di autenticazione può aiutare a prevenire attacchi come il phishing, che si basano sul furto di credenziali di accesso.

Sebbene non sia possibile rintracciare una data di nascita precisa dell'MFA, già dai primi anni del XX secolo si iniziarono a vedere sistemi di accesso basati sull'utilizzo di una parola chiave, affiancata dall'uso di una chiave fisica.

I sistemi più semplici, come la 2FA, non sono inviolabili ma offrono un miglioramento sostanziale.

Sistemi di accesso biometrici

Per chi non lo sapesse, i sistemi di accesso biometrici si basano sull'utilizzo dei caratteri fisici unici di un individuo al fine di identificarlo e garantire la sicurezza dei dati. Gli esempi più classici sono le impronte digitali, il riconoscimento facciale o la voce.

Aggiungere il riconoscimento biometrico, ad esempio, per ottenere l'accesso a dati sensibili, come quelli contenuti in un'app bancaria, è un ottimo modo per mettere al sicuro i propri asset di maggior valore.

Connessione sicura a Internet

Se per lavoro o per studio viaggi spesso, ti capiterà sicuramente di collegarti alla rete Internet tramite connessioni pubbliche o reti Wi-Fi non protette. Anche in contesti insospettabili potrebbero nascondersi insidie per la sicurezza dei tuoi dispositivi.

In linea generale, è sempre meglio evitare queste connessioni poco sicure. Qualora non fosse possibile, puoi provare a utilizzare un servizio di connessione VPN per rendere anonima la tua presenza online e ridurre le possibilità di

monitoraggio da remoto da parte dei malintenzionati.

Attenzione al social engineering

Con il termine “social engineering” si intende tutto un insieme di strategie e strumenti utilizzati per ottenere informazioni riservate o per persuadere le persone a compiere determinate azioni.

In molti casi, le organizzazioni criminali che usano social engineering impersonano un'autorità o un'organizzazione affidabile, al fine di ottenere informazioni o di convincere le persone a fare qualcosa che non dovrebbero fare, come ad esempio fornire informazioni personali o accedere a risorse protette.

La formazione delle risorse umane è fondamentale: basta un errore, anche banale, da parte di un dipendente che abbia accesso alla rete informatica aziendale per compromettere la sicurezza operativa di tutta la società.

Seminari e corsi pratici di formazione con test realistici sono alcuni degli strumenti più utilizzati per aiutare i dipendenti a riconoscere i pericoli e disinnescare i rischi all'origine.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/password-solida-non-basta-a-proteggere-il-tuo-account/>