MARIANO ORTU

Sicurezza Informatica

Firma Digitale:

Mariano Ortu

Key ID: 8E0270DF

Key Fingerprint: 6F52 CE06 F752 74C6 3CBD 8E9D FC8E 9FB8 8E02 70DF

Identità Digitale

La mia identità digitale è certificata, verificabile e *riconosciuta a livello internazionale*.

Puoi consultarla direttamente su *Keybase*, una piattaforma affidabile progettata per garantire l'integrità delle comunicazioni e l'autenticità dei contenuti.

Su *Keybase* troverai:

- La mia chiave pubblica PGP,
- I miei messaggi firmati,
- E tutte le informazioni necessarie per verificare in modo indipendente che qualsiasi comunicazione o software provenga effettivamente da me.

Questo approccio garantisce trasparenza, sicurezza e tracciabilità, fondamentali per chiunque operi seriamente nel campo della progettazione e della sicurezza informatica.

Scansiona il QR Code per accedere alla mia identità digitale tramite cellulare o altro dispositivo!

Più avanti troverai i link per accedere dal tuo sistema, sia esso Windows o altro S.O.

Guida al Recupero di un Account Facebook Compromesso

Introduzione

Sovente vengo interpellato da utenti che si ritrovano con il profilo *Facebook* compromesso o addirittura sottratto e clonato.

Personalmente, non ho mai preso "cittadinanza" su quella piattaforma, se non anni fa e non a titolo personale, ma come gruppo di lavoro.

Fu un'esperienza estremamente deludente, per fortuna breve — pochi mesi appena — ma sufficiente per capire a fondo la natura di un sistema di quel tipo: una struttura che espone l'utente a rischi reali, se non si opera con prudenza e non si adottano almeno le misure di sicurezza basilari. Un'autentica stazione di raccolta dati che, all'insaputa degli utenti, vengono trasmessi alle multinazionali che su questi lucrano.

Nel tempo, il numero crescente di richieste d'aiuto, talune molto accorate, mi ha indotto a scrivere questa breve guida, nella speranza che possano beneficiarne tutti coloro che hanno avuto delle esperienze negative con questa piattaforma e gli utenti che intendono cautelarsi e navigare dentro un contesto di relativa sicurezza.

Adotterò una stesura il meno tecnica possibile, con l'intento di offrire uno strumento semplice, diretto e affidabile, affinché — collettivamente — gli utenti di *Facebook* possano usufruirne e imparare a difendere il proprio profilo.

Se sospetti che qualcuno abbia preso il controllo del tuo profilo *Facebook*, è fondamentale intervenire subito. Un account compromesso può essere usato per truffare altri utenti, rubare dati sensibili o diffondere malware.

Facebook è uno degli strumenti più utilizzati per comunicare, condividere e informarsi. Tuttavia, è anche un bersaglio frequente di attacchi informatici, furti d'identità e tentativi di truffa.

Questa guida è pensata per aiutarti a proteggere il tuo account *Facebook*, passo dopo passo, con strumenti semplici e consigli concreti. Ti aiuta a capire se il tuo account è stato violato e cosa fare per proteggerlo o recuperarlo.

Purtroppo l'istinto dell'uomo a fare comunanza, soprattutto su piattaforme digitali che creano una falsa illusione di sicurezza e anonimato, la convinzione che uno schermo ed una tastiera conferiscano una sorta di potere non esercitabile nella vita reale, conducono molti utenti nelle fallaci spire di personaggi senza scrupolo alcuni, perennemente pronti al ricatto, alla truffa, al malaffare. Lo scopo di questa guida è quello di porre un argine a questo squallido quanto dannoso fenomeno.

Diffondi questa guida, falla conoscere, è il solo mezzo che abbiamo per arginare in parte l'attività criminale di questi individui che si celano dentro queste piattaforme. *Io sto facendo la mia parte, voi adesso fate la vostra!*

🗜️ Password e protezione delle credenziali

Il primo aspetto cruciale nella difesa del proprio account è, senza alcun dubbio, la scelta di una *Password* solida.

Non è un consiglio generico: *è il fondamento stesso della sicurezza!*

"Sinceramente, non ho la più pallida idea di quale strategia Facebook adotti per proteggere le credenziali dei suoi utenti." 🤔

Tuttavia, vista la facilità con cui gli account vengono regolarmente e puntualmente compromessi, ho il sospetto che le difese siano quantomeno superficiali.

Per chiarire meglio il concetto, riporto il metodo che applico nei miei progetti quando si tratta di proteggere le credenziali:

- 📝 Riempimento (Padding). Se la password è debole, viene automaticamente integrata con caratteri aggiuntivi fino a raggiungere lunghezze standard (16, 32, 64 o 128 caratteri). Questo rende possibile cifrarla in memoria, vanificando attacchi di tipo *Memory Dump* e *Brute Force*.
- 🧂 Aggiunta di un SALT. Alla stringa ottenuta viene accodato un valore casuale (*SALT*), che rende inefficaci gli attacchi basati su tabelle precalcolate (*Rainbow Table*).
- 🔐 Derivazione con funzione HASH. La *Password* + *SALT* viene sottoposta a derivazione crittografica tramite *Funzione di HASH*, generando una credenziale robusta e resistente a qualsiasi forma di attacco.

Nei miei software questo è lo standard minimo. Non una scelta opzionale, ma una regola inderogabile. *Perché ogni utente ha diritto alla massima protezione, anche se non è un esperto!*

Chi scrive codice per sicurezza, ha il dovere morale di non scendere a compromessi. Questa strategia non è solo efficace: *è l'unico approccio serio e moderno per proteggere le credenziali degli utenti!*

Facebook adotta una protezione simile? Non lo so. Ma alla luce dei continui furti di account, mi sentirei di dire: *probabilmente no*! 😔

Ecco perché la prima cosa da fare è scegliere una password sicura, che rispetti almeno questi requisiti minimi:

- 😟 Non deve contenere nomi propri, date di nascita, parole comuni.
- 🔨 Deve avere almeno 16 caratteri.
- 📑 Deve contenere lettere maiuscole, minuscole, numeri e simboli.
- 📪 Non va mai riutilizzata in altri servizi

Una password debole è come una porta aperta. *E nessun sistema di sicurezza può proteggerti se la porta è già spalancata!*

Segnali d'allarme

Presta attenzione a questi segnali:

- Accessi da dispositivi o luoghi insoliti
- Modifica non autorizzata di email o password
- Messaggi inviati automaticamente
- Post pubblicati che tu non hai scritto
- Disattivazione dell'autenticazione a due fattori (2FA)

Procedura passo-passo

1. Controlla le sessioni attive

Vai su:

Impostazioni e privacy → Impostazioni → Protezione e accesso → Dove hai effettuato l'accesso

- Controlla tutti i dispositivi e le località.
- Se vedi qualcosa di sospetto, clicca su ⋮ > **Termina attività**.

2. Verifica i tuoi dati di accesso

Controlla che non siano stati modificati:

- Email
- Numero di telefono
- Password
- Nome utente
- Domande di sicurezza
- Impostazioni di 2FA

Se noti modifiche non fatte da te, cambia subito la password. Ad ogni modo dovresti prendere in seria considerazione, indipendentemente dagli episodi sopra citati, di cambiare la password almeno una volta al mese, sostituendola con stringhe sempre differenti!

3. Attiva l'autenticazione a due fattori (2FA)

Vai su:

Impostazioni → Protezione e accesso → Autenticazione a due fattori

- 👥 Scegli **un'app di autenticazione** (consigliato: Google Authenticator o Microsoft Authenticator).
- 😨 Evita l'uso dell'SMS, se possibile. (È facilissimo da bucare)

4. Controlla l'attività recente

Vai su:

Menu → Registro attività

- 🕵️ Controlla se ci sono post, commenti, messaggi o accessi che non riconosci.
- 🗑️ Elimina tutto ciò che non ti appartiene.

5. Usa la pagina ufficiale di Facebook

Se sei stato disconnesso o hai perso l'accesso:

🌐 facebook.com/hacked

- 🦾 Segui la procedura guidata per recuperare il tuo account.
- 👀 Non affidarti mai a siti esterni o "servizi di recupero": **sono spesso truffe**.

✅ Consigli preventivi per il futuro

- 🔧 Attiva la 2FA **subito dopo il recupero**
- 🔑 Usa una password **lunga e unica** (evita nomi, date, parole comuni)
- 👤 Non accettare richieste da sconosciuti
- 🔗 Non cliccare su link sospetti, nemmeno se arrivano da amici
- 🧶 Esegui periodicamente un controllo delle sessioni attive
- 😳 Non accedere a Facebook da link ricevuti su WhatsApp o email sospette
- 🤯 Non salvare la password nel browser se usi un PC condiviso
- 📱 Non condividere codici di verifica o SMS con nessuno

Attenzione ai falsi "verificatori di account"

Non esistono strumenti esterni che possano "testare" la sicurezza del tuo profilo. Qualsiasi sito che promette di farlo è potenzialmente una truffa o un tentativo di phishing.

Se ti viene chiesto di inserire la tua password per “verificare il profilo”, *sei già vittima di un attacco.*

Proteggere gli utenti è una responsabilità seria. Se hai dubbi o vuoi saperne di più, visita questa pagina del mio sito.

Diffida dai “professionisti improvvisati”

Quando ti rivolgi a qualcuno che si definisce esperto verifica sempre:

- Che abbia una identità digitale riconosciuta su piattaforme internazionali
- Che firmi digitalmente con una chiave pubblica verificabile
- Che offra strumenti verificabili per la protezione dell’utente, non solo parole
- Non confidare mai la tua password a nessuno, per nessun motivo.

Comunicare con Mariano Ortu

Se hai avuto un’esperienza particolarmente disastrosa, tipo clonazione del profilo o altro e vorresti contattarmi in modo sicuro puoi farlo utilizzando gli strumenti che di seguito ti consiglio. Evita di parlare col cellulare, scrivermi tramite Mail, con SMS!

Canale di Contatto Sicuro: *Keybase*

Per interazioni riservate e sicure, nonché per la verifica affidabile dell'autenticità di qualsiasi Software o Comunicazione proveniente dal sottoscritto, consiglio vivamente l'utilizzo di *Keybase* come piattaforma affidabile per Contatti Crittografati e Verificabili.

Collegandoti tramite *Keybase*, garantisci:

- Crittografia end-to-end, che garantisce che nessuna terza parte possa intercettare o manomettere alcun messaggio o file.
- Verifica crittografica dell'identità, che conferma senza ombra di dubbio che stai comunicando direttamente ed esclusivamente con me.
- Controlli di autenticità a prova di manomissione, che ti consentono di verificare che qualsiasi software, messaggio o file recante la mia firma digitale non sia stato alterato in alcun modo.

Questo Canale offre i più alti standard di integrità, privacy e affidabilità. È l'unico metodo che approvo ufficialmente per le Comunicazioni Sicure e la Verifica dell'Autenticità. Per connetterti, utilizza il mio profilo *Keybase* verificato, dove la mia chiave pubblica PGP e i messaggi firmati sono sempre disponibili e aggiornati. Per ulteriori informazioni, visita questa pagina sul mio sito web!

Comunicazioni Preliminari su Signal (e perché non basta)

Oltre a *Keybase*, puoi anche comunicare con me tramite *Signal*, una chat sicura che utilizza crittografia end-to-end e protegge le conversazioni da occhi indiscreti.

Signal è un ottimo strumento per:

- avviare un primo contatto in modo riservato
- introdurre l'argomento in termini generali
- stabilire la volontà di procedere in modo sicuro

Tuttavia, è bene chiarire un punto fondamentale:

Signal non sostituisce *Keybase* per operazioni che richiedono verifica crittografica dell'identità, firma digitale, scambio di file autentici o verifica software.

Per questa ragione, utilizzo *Signal* solo per comunicazioni iniziali e non tecniche, oppure per accordarsi su quando e come passare a *Keybase*.

Tutto ciò che riguarda software, sicurezza, firme e verifiche deve obbligatoriamente avvenire su *Keybase*, l'unico canale approvato ufficialmente.

Nota importante:

In entrambi i casi, non usare il numero di telefono o email pubblici per scrivermi direttamente. Ricevo solo attraverso i profili verificati. Tutti i link ufficiali, aggiornati e firmati, sono disponibili sul mio sito!

Risorse utili

- Centro assistenza ufficiale: facebook.com/help
- Controllo sicurezza account: facebook.com/security/checkup
- Recupero account compromesso: facebook.com/hacked

Un ultimo consiglio (da chi non ha nulla da vendervi)

Vogliatevi bene, se potete, lasciate *Facebook*.

Non lo dico con leggerezza, né per snobismo. Lo dico perché ogni giorno assisto agli effetti collaterali — spesso invisibili — di una piattaforma che trasforma le persone in prodotti, le relazioni in numeri, e la vita privata in un algoritmo da monetizzare.

Facebook non è solo uno strumento: è un ambiente progettato per indurre dipendenza, alterare la percezione della realtà, e raccogliere ogni singolo dato possibile su di voi, anche quando non ve ne accorgete.

La sicurezza non riguarda solo le password, ma anche la dignità, la libertà e la qualità della propria esistenza digitale.

Ci sono alternative. Ci sono luoghi più sani. Ci sono modi migliori per comunicare, informarsi, costruire relazioni.

Se proprio dovete restare, fatelo con piena consapevolezza.

Ma se potete scegliere, scegliete di andarvene. È un atto di rispetto verso voi stessi!

Voglia di privacy, di autenticità e di tempo ben speso: questa è vera sicurezza.

Quella che nessuna tecnologia potrà mai restituirvi, se l'avete già ceduta.

“Chi rinuncia alla libertà per ottenere sicurezza non merita né l'una né l'altra.”

— Benjamin Franklin

Nota a margine importante

“Se qualcosa è gratis, il prodotto sei tu.”

Questa affermazione è tristemente vera quando si parla di servizi centralizzati e commerciali come *Facebook*, *Instagram*, o quell’altra **schifezza di *WhatsApp***, dove il modello di business si basa sulla raccolta, profilazione e monetizzazione dei dati degli utenti.

Questo principio non vale per i progetti etici e Open Source, dove il codice sorgente è pubblico, la trasparenza è totale, e il rispetto dell’utente viene prima di tutto.

Progetti come *Signal, Keybase* (e molti altri strumenti liberi e verificabili) non ti trasformano in merce, ma ti offrono un mezzo reale per tutelare la tua libertà digitale.

“La tecnologia dovrebbe servire l’uomo, non catturarlo.”

Sono un progettista di sistemi informatici volti alla sicurezza dei dati che lavora solo ed esclusivamente su piattaforma *Open Source*, nella convinzione che la trasparenza del codice sia l'unica vera garanzia di controllo, affidabilità e indipendenza.

Credo fermamente che la sicurezza non possa essere delegata a scatole nere proprietarie, dove l'utente non ha alcun potere di verifica né reale conoscenza di cosa accade dietro le quinte.

L'Open Source, al contrario, offre la possibilità di analizzare, correggere, migliorare e condividere soluzioni nel rispetto dell'intelligenza collettiva, della libertà individuale e della dignità informatica di ogni persona.

È una scelta tecnica ma soprattutto etica, perché difendere i dati significa difendere le persone.

Viviamo in un'epoca in cui ogni informazione personale può essere raccolta, profilata, venduta o sfruttata — spesso a nostra insaputa.

In questo contesto, la progettazione di software libero e sicuro non è solo un mestiere: è un atto di responsabilità verso la società.

Chi sviluppa sistemi ha il dovere di scegliere con coscienza: può contribuire a un mondo più giusto, più aperto, più umano — oppure alimentare il silenzio di strutture opache che trasformano gli utenti in prodotto.

Io ho scelto da che parte stare!

Progetti pubblicati:

- Speedcrypt: cifratura dei dati
- SecureDel: Hard Disk Tool e cancellazione sicura dei dati
- EasyHash: generatore di firme digitali HASH
- Custom Erase: algoritmo per sviluppatori orientato alla cancellazione sicura dei file.

Tutti i miei progetti sono distribuiti con il codice sorgente sotto certificazione OSI.

Siti di riferimento:

- https://www.sicurpas.it/
- https://www.speedcrypt.info/
- Official GitHub Repository!

Articoli tecnici

- https://www.sicurpas.it/articles.html

Integrità pacchetti software

- https://www.sicurpas.it/integrity.html

Download pacchetti Software

- https://www.sicurpas.it/downloads.html

"*Se un malintenzionato riesce a convincerti a eseguire il suo programma sul tuo computer, non è più il tuo computer!*"