WhatsApp Screen Sharing: il cavallo di Troia che espone soldi e identità

Maria Cattini | 04/09/2025 | Sicurezza digitale

Immagina di ricevere una chiamata su WhatsApp: una voce gentile dice di essere della tua banca e ti avverte di “problemi urgenti” sul tuo conto. La soluzione? Condividere lo schermo per una verifica rapida. Sembra normale assistenza, ma è il primo passo di una trappola studiata con cura.

Secondo un’inchiesta pubblicata da India Today, bastano pochi secondi di screen sharing perché i truffatori vedano comparire sul display password, OTP, numeri di conto. È come spalancare il portafoglio a uno sconosciuto.

Come agiscono i truffatori

Il copione è collaudato:

1. Falsa urgenza – L’attacco parte con l’allarme: “Il suo conto è a rischio, agisca subito”.
2. Autorità apparente – Il malintenzionato si presenta come dipendente della banca o di un servizio finanziario.
3. Screen sharing – Con la scusa della “risoluzione errori”, convince la vittima a condividere lo schermo.
4. Raccolta dati in tempo reale – OTP, credenziali e notifiche bancarie diventano visibili.
5. Escalation – Talvolta la vittima viene spinta a installare software di mirroring o accesso remoto, che consegna il dispositivo ai criminali.

La condivisione schermo è uno strumento utile, ma su piattaforme non pensate per l’assistenza tecnica diventa un’arma contro chi non conosce i pericoli. Su WhatsApp, privo di controlli avanzati per l’uso “sicuro” dello screen sharing, un clic può compromettere identità digitale e patrimonio.

Difendersi: tre regole pratiche

• Mai condividere lo schermo con sconosciuti – Nessuna banca chiede di farlo.
• Diffidare dall’urgenza – I truffatori giocano sul tempo e sul panico. Fermarsi, respirare, verificare.
• Canali ufficiali solo dall’app o dal sito – Per problemi reali, contattare la banca attraverso numeri o chat certificati.

Per chi lavora con l’OSINT, il dato interessante è la quantità di informazioni che un solo frame di schermo può rivelare: notifiche push, email in arrivo, movimenti di app bancarie, cronologia di ricerca. Non serve un malware sofisticato: basta una finestra condivisa.

Condividere lo schermo su WhatsApp può sembrare un gesto banale, ma equivale a dare le chiavi di casa a un perfetto sconosciuto. In un mondo dove i criminali digitali perfezionano continuamente i loro stratagemmi, la consapevolezza resta la prima linea di difesa.
Immagina di ricevere una chiamata su WhatsApp: una voce gentile dice di essere della tua banca e ti avverte di “problemi urgenti” sul tuo conto. La soluzione? Condividere lo schermo per una verifica

rapida. Sembra normale assistenza, ma è il primo passo di una trappola studiata con cura.

Secondo un'inchiesta pubblicata da India Today, bastano pochi secondi di screen sharing perché i truffatori vedano comparire sul display password, OTP, numeri di conto. È come spalancare il portafoglio a uno sconosciuto.

Come agiscono i truffatori

Il copione è collaudato:

1. Falsa urgenza – L'attacco parte con l'allarme: "Il suo conto è a rischio, agisca subito".
2. Autorità apparente – Il malintenzionato si presenta come dipendente della banca o di un servizio finanziario.
3. Screen sharing – Con la scusa della "risoluzione errori", convince la vittima a condividere lo schermo.
4. Raccolta dati in tempo reale – OTP, credenziali e notifiche bancarie diventano visibili.
5. Escalation – Talvolta la vittima viene spinta a installare software di mirroring o accesso remoto, che consegna il dispositivo ai criminali.

La condivisione schermo è uno strumento utile, ma su piattaforme non pensate per l'assistenza tecnica diventa un'arma contro chi non conosce i pericoli. Su WhatsApp, privo di controlli avanzati per l'uso "sicuro" dello screen sharing, un clic può compromettere identità digitale e patrimonio.

Difendersi: tre regole pratiche

• Mai condividere lo schermo con sconosciuti – Nessuna banca chiede di farlo.
• Diffidare dall'urgenza – I truffatori giocano sul tempo e sul panico. Fermarsi, respirare, verificare.
• Canali ufficiali solo dall'app o dal sito – Per problemi reali, contattare la banca attraverso numeri o chat certificati.

Per chi lavora con l'OSINT, il dato interessante è la quantità di informazioni che un solo frame di schermo può rivelare: notifiche push, email in arrivo, movimenti di app bancarie, cronologia di ricerca. Non serve un malware sofisticato: basta una finestra condivisa.

Condividere lo schermo su WhatsApp può sembrare un gesto banale, ma equivale a dare le chiavi di casa a un perfetto sconosciuto. In un mondo dove i criminali digitali perfezionano continuamente i loro stratagemmi, la consapevolezza resta la prima linea di difesa.