13.03.2026

Attenzione al phishing via HTML

È in circolazione una forma di phishing particolarmente insidiosa: il phishing via HTML. A differenza degli attacchi classici, la pagina di login contraffatta si trova direttamente in un allegato HTML.

Come funziona il phishing via HTML

A differenza dell'attacco di phishing consueto, le e-mail contengono come allegato un file HTML che una volta aperto mostra nel browser un sito Internet dal design professionale e dall'aspetto molto credibile. Agli utenti viene poi chiesto di inserire i loro dati d'accesso. Nella realtà, però, i dati vengono trasmessi direttamente ai malintenzionati. Oltre a questo, i file HTML possono contenere script che causano ulteriori danni al dispositivo.

Il phishing via HTML è particolarmente pericoloso perché la pagina Internet viene aperta localmente e la barra del browser non riporta un indirizzo Web tipico. Molti filtri di sicurezza hanno difficoltà nel riconoscere gli allegati HTML e l'aspetto professionale aumenta di parecchio la credibilità del messaggio.

Come proteggersi

In generale, trattate con scetticismo gli allegati HTML inattesi. I dati d'accesso vanno inseriti solo su siti Internet noti e sicuri. In caso di dubbio, meglio verificare l'autenticità di un messaggio tramite i canali di contatto ufficiali.

Il phishing via HTML è un'evoluzione degli attacchi di phishing tradizionali, particolarmente insidioso per la combinazione di autenticità visiva e pressione psicologica. Attenzione, prudenza e sistematicità sono le risorse più importanti per prevenire questo genere di attacchi.

Ulteriori informazioni, anche su altre varianti di phishing, sono disponibili qui (https://www.ebas.ch/phishing) .