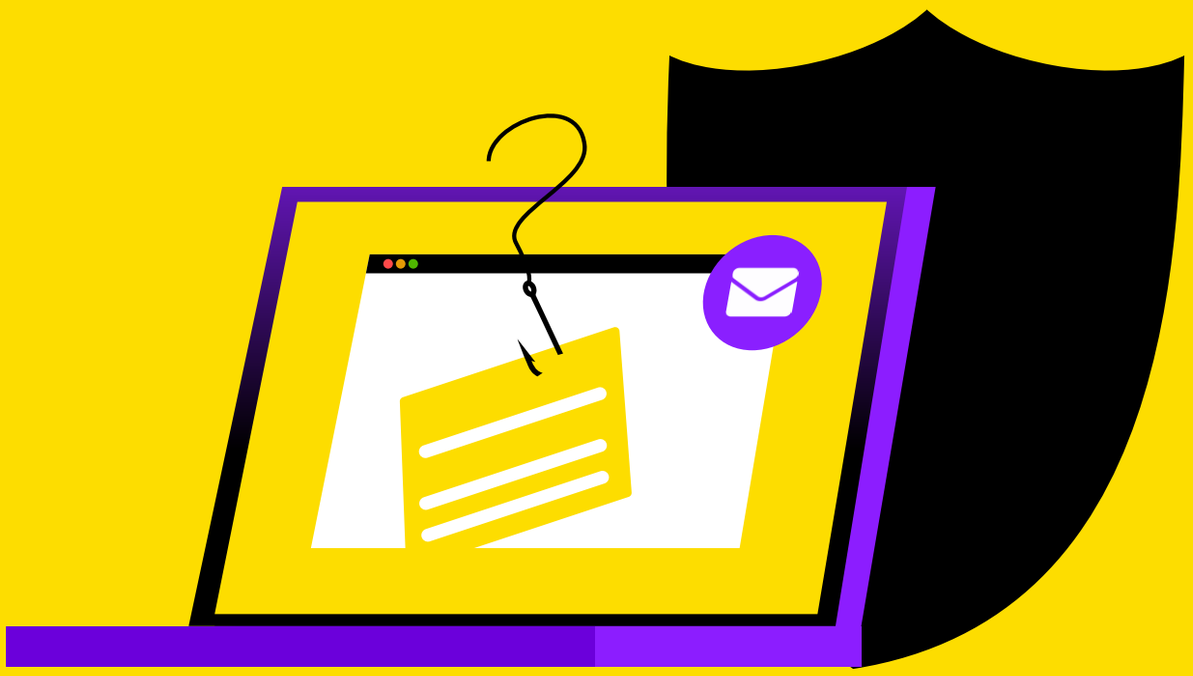
RATE HAWK

Attenzione al phishing: ecco come proteggere il tuo account da minacce esterne



Hai mai ricevuto e-mail sospette che ti invitavano a cliccare su un link? È molto probabile che fossero tentativi di phishing. Per salvaguardare i propri dati e proteggersi da potenziali minacce, è fondamentale informarsi e adottare misure proattive. In questo articolo ti illustriamo i passaggi da seguire per garantire efficacemente la sicurezza informatica e scopriamo i provvedimenti da prendere quando usi la nostra piattaforma.

1 Il phishing in cifre: comprendere le minacce

15%
di tutte le violazioni dei dati è causato dal phishing (rapporto IBM).

$52M+
di perdite segnalate negli Stati Uniti a causa del phishing (FBI IC3, 2022).

300k
vittime segnalate negli Stati Uniti nel 2022.

Gli attacchi di phishing sono in aumento e rappresentano una minaccia sia per i privati che per le imprese di tutto il mondo. Secondo un'indagine di IBM, il phishing è il mezzo più comune di violazione dei dati, rappresentando il 15% delle violazioni totali. I danni finanziari non sono meno allarmanti: secondo l'Internet Crime Complaint Center (IC3) dell'FBI, i tentativi di phishing sono stati i reati più denunciati negli Stati Uniti nel 2022, con 300.497 vittime e perdite per più di 52 milioni di dollari.

Il settore del turismo non fa eccezione. La relazione dell'Anti-Phishing Working Group (APWG) ha rivelato che il turismo è tra 10 settori più colpiti. Forbes avverte che per via della crescente integrazione della tecnologia nelle esperienze di viaggio, vi è un rischio sempre maggiore di attacchi informatici in fase di prenotazione o di accesso a reti non sicure all'estero.

Perché il settore del turismo è un bersaglio primario? Le piattaforme di prenotazione online gestiscono quantità enormi di dati sensibili, dai dati personali fino a quelli finanziari, che rappresentano un bottino allettante per i criminali informatici. Occorre ricordare, però, che il phishing è un problema mondiale che si ripercuote sull'intero ecosistema online e non è legato esclusivamente alla sicurezza della nostra piattaforma. Per proteggere i nostri utenti, ci impegniamo a mettere in atto misure di sicurezza all'avanguardia che, in combinazione con campagne di sensibilizzazione, contribuiscono a garantire i massimi di livelli di salvaguardia.

2 Come funziona il phishing?

Il phishing è una forma di attacco informatico in cui i truffatori si fingono soggetti legittimi allo scopo di indurre gli utenti a rivelare dati sensibili. Questi truffatori utilizzano spesso e-mail, messaggi o siti web falsi che imitano in modo molto simile fonti veritiere. Ecco come funziona solitamente il phishing:

Pagine di login false:
i criminali informatici creano siti web contraffatti che appaiono identici alle pagine di login ufficiali. Una differenza impercettibile, come una lettera in più o una minima modifica dell'URL, possono trarre in inganno anche gli utenti più cauti.

Offerte truffaldine:
le e-mail o i messaggi di phishing contengono spesso un linguaggio convincente e pressante che invita a cliccare su un link o a fornire le proprie credenziali di accesso. Sfruttano di sovente offerte allettanti come sconti, occasioni o promozioni limitate per spronare le persone a cliccare sui link. L'obiettivo è impadronirsi dei tuoi dati personali prima che tu ti accorga dell'accaduto.

Annunci malevoli:
quando accedi a un sito web, ricorda che non tutti gli annunci sono attendibili. Prima e dopo aver cliccato su un annuncio, controlla sempre l'URL per verificare di essere su un sito legittimo. Spesso i truffatori usano annunci fuorvianti per indirizzare gli utenti su pagine false che sembrano vere ma sono progettate per rubare i dati.

Comprendere ed essere consapevoli di queste tattiche è il primo passo per proteggere se stessi e la propria azienda.

3 I passaggi per proteggere il tuo account dai tentativi di phishing

Adottare alcune semplici pratiche può aiutarti in modo efficace a tenere al sicuro i tuoi account ed evitare attacchi di phishing:

Controlla attentamente l'URL:
verifica sempre di essere sul sito www.ratehawk.com. I siti fraudolenti presentano solitamente piccole variazioni nell'URL (ad es. ratehwak.com invece di ratehawk.com).

Evita di cliccare su link sospetti:
se ricevi un'e-mail o un messaggio inaspettati che ti chiedono di eseguire il login, non cliccare sul link. Al contrario, vai direttamente su www.ratehawk.com/accounts/login.

Non condividere mai le tue credenziali di login:
il personale di RateHawk non ti chiederà mai di riferire i tuoi dati di accesso o il codice OTP via e-mail, telefono o social media. Se ricevi una richiesta di questo tipo, segnala l'accaduto immediatamente.

Usa password efficaci e univoche:
crea una password sicura combinando lettere, numeri e simboli. Evita di usare password identiche per accedere a più account. Le password devono essere uniche per ciascuna piattaforma. In caso di violazione di un servizio, l'uso generalizzato della stessa password potrebbe mettere in grave pericolo gli altri tuoi account.

Aggiorna regolarmente la password:
cambiando la password periodicamente diminuisci il rischio di accessi non autorizzati.

Integrando queste pratiche nella tua routine quotidiana, puoi creare una robusta difesa contro i tentativi di phishing e tenere al sicuro i tuoi dati personali. Proteggiti seguendo questi semplici passaggi ed ottimizza la tua sicurezza con RateHawk!

Mantieni la tua sicurezza informatica con RateHawk!