RATE HAWK

Concienciación sobre el phishing: Cómo proteger tu cuenta contra las amenazas en línea

¿Has recibido alguna vez un correo electrónico sospechoso en el que te pedían que hicieras clic en un enlace? Es muy probable que se tratase de phishing. Para proteger tus datos y estar protegido frente a posibles amenazas, es fundamental ser consciente y tomar medidas preventivas. En este artículo, analizamos detalladamente los pasos a seguir para tu seguridad y te contamos qué medidas puedes tomar cuando utilices nuestra plataforma.

1 El phishing en cifras: Entender la amenaza

15%
de todas las filtraciones de datos se deben al phishing (informe de IBM).

$52M+
en pérdidas reportadas debido al phishing en EE. UU. (FBI IC3, 2022).

300k
víctimas reportadas en EE. UU. en 2022.

Los ataques de phishing van en aumento, amenazando a personas y negocios de todo el mundo. Según un estudio de IBM, el phishing es el vector de filtración de datos más habitual, representando el 15% de todas las brechas de seguridad. El impacto financiero es igual de alarmante — las estadísticas del Centro de Denuncias de Delitos en Internet del FBI (IC3) revelan que las campañas de phishing fueron los delitos más denunciados en los Estados Unidos en 2022, con 300.497 víctimas registradas y unas pérdidas que superan los 52 millones de dólares.

Y el sector de los viajes no es la excepción. Según el informe del Grupo de Trabajo Anti-Phishing (APWG), la industria del turismo figura entre los 10 sectores más atacados. Según Forbes, a medida que la tecnología se va integrando más profundamente en las experiencias de viaje, el riesgo de ciberataques al reservar viajes o al acceder a redes no seguras en el extranjero es una preocupación cada vez mayor.

¿Por qué el sector turístico es uno de los principales objetivos? Las plataformas de reservas en línea manejan enormes cantidades de datos sensibles, como datos personales o información financiera, un botín muy tentador para los ciberdelincuentes. Sin embargo, no debemos olvidar que el phishing es un problema global que afecta a todo el ecosistema en línea — no es un indicador de la seguridad de nuestra plataforma. Nosotros tenemos el compromiso de implementar medidas de seguridad avanzadas para proteger a nuestros usuarios, que, combinadas con la concienciación, ayuden a garantizar un nivel óptimo de protección.

2 ¿En qué consiste el phishing?

El phishing es una forma de ciberataque en la que los estafadores suplantan la identidad de entidades legítimas para engañarte y hacerte revelar información sensible. A menudo, estos atacantes emplean correos electrónicos, mensajes o sitios web falsos, que imitan a las fuentes genuinas casi a la perfección. Así es como suele funcionar el phishing:

Páginas falsas de inicio de sesión:
Los ciberdelincuentes crean sitios web falsos con una apariencia idéntica a la de las páginas de inicio de sesión reales. Una pequeña diferencia, como una letra de mász o una ligera alteración de la URL, puede engañar hasta a los usuarios más precavidos.

Ofertas fraudulentas:
Los correos electrónicos o mensajes de phishing suelen contener un lenguaje apremiante o tentador, incitándote a hacer clic en un enlace o a que les facilites tus datos de inicio de sesión. Con frecuencia, utilizan ofertas urgentes, como descuentos, gangas especiales o promociones por tiempo limitado, para presionarte y que hagas clic en sus enlaces. Su objetivo es obtener tu información personal antes de que te des cuenta de lo que está pasando.

Publicidad maliciosa:
When accessing a website, remember that not all ads are trustworthy sources. Before and after clicking on an ad, always double-check the URL to ensure you're on a legitimate site. Scammers often use misleading ads to direct users to fake pages that look real but are designed to steal your information.

Entender y ser consciente de estas tácticas es el primer paso para protegerte a ti y a tu negocio.

3 Pasos para proteger tu cuenta frente a ataques de phishing

Adoptar unas sencillas prácticas puede ayudarte enormemente
a proteger tus cuentas y evitar ataques de phishing:

Revisa detenidamente la URL:
Asegúrate siempre de que estás en www.ratehawk.com.
Los sitios web fraudulentos suelen tener ligeras variaciones en la URL
(ratehwak.com en lugar de ratehawk.com, por ejemplo).

No hagas clic en enlaces sospechosos:
Si recibes un correo electrónico o un mensaje inesperado
pidiéndote que inicies sesión, no hagas clic en el enlace.
En vez de eso, ve directamente a www.ratehawk.com/accounts/login.

No compartas nunca tus datos de inicio de sesión:
Los empleados de RateHawk jamás te van a pedir tu nombre de usuario
ni tu contraseña de un solo uso por correo electrónico, ni por teléfono, ni en redes
sociales. Si recibes una solicitud de este tipo, comunícanoslo inmediatamente.

Utiliza contraseñas seguras y únicas:
Crea una contraseña segura que contenga una combinación de letras,
números y símbolos. Evita utilizar la misma contraseña en diferentes cuentas.
Las contraseñas deben ser únicas para cada plataforma. Si un servicio
resulta vulnerado y utilizas la misma contraseña en todas partes, todas
las demás cuentas se encontrarían en grave riesgo.

Actualiza tu contraseña periódicamente:
Si cambias la contraseña cada pocos meses, reduces
el riesgo de acceso no autorizado.

Incorporando estas prácticas a tu rutina diaria, puedes construir una sólida defensa
contra los ataques de phishing y mantener tus datos personales bien protegidos.
¡Protégete con estos sencillos pasos y mantente a salvo con RateHawk!