RATE HAWK

Sensibilisierung für Phishing: So schützen Sie Ihren Zugang vor Cyber-Angriffen

Haben Sie schon einmal eine verdächtige E-Mail erhalten, in der Sie aufgefordert wurden, auf einen Link zu klicken? Höchstwahrscheinlich handelte es sich dabei um Phishing. Um Ihre Daten zu schützen und potenziellen Bedrohungen einen Schritt voraus zu sein, ist es entscheidend, wachsam zu bleiben und proaktive Maßnahmen zu ergreifen. In diesem Artikel erklären wir, wie Sie sich effektiv vor Phishing schützen können und welche Sicherheitsmaßnahmen beim Arbeiten mit unserer Plattform besonders wichtig sind.

1 Phishing in Zahlen: Die Bedrohung verstehen

15%
aller Datenpannen werden durch Phishing verursacht (IBM-Bericht).

$52M+
Verluste durch Phishing in den USA gemeldet (FBI IC3, 2022).

300k
Opfer wurden in den USA im Jahr 2022 gemeldet.

Phishing-Angriffe nehmen weltweit zu und bedrohen sowohl Einzelpersonen als auch Unternehmen. Laut einem Bericht von IBM ist Phishing die häufigste Ursache für Datenschutzverletzungen und macht 15 % aller Vorfälle aus. Die finanziellen Folgen sind alarmierend: Laut dem Internet Crime Complaint Center (IC3) des FBI war Phishing im Jahr 2022 die am häufigsten gemeldete Cyber Straftat in den USA. Insgesamt wurden 300.497 Opfer registriert, mit einem Gesamtschaden von über 52 Millionen US-Dollar.

Die Reisebranche ist da keine Ausnahme. Der Bericht der Anti-Phishing Working Group (APWG) zeigte, dass die Reisebranche zu den zehn am häufigsten betroffenen Sektoren gehört. Forbes warnt davor, dass das Risiko von Cyberangriffen mit der zunehmenden Digitalisierung im Reisebereich steigt – insbesondere bei Online-Buchungen oder der Nutzung unsicherer Netzwerke im Ausland.

Warum ist die Reisebranche also eines der Hauptangriffsziele? Online-Buchungsplattformen verarbeiten große Mengen sensibler Daten, von persönlichen Informationen bis hin zu Zahlungsdaten. Das macht sie zu einem attraktiven Angriffsziel für Cyberkriminelle. Dennoch ist Phishing ein globales Problem, das das gesamte Internet betrifft – und sagt nichts über die Sicherheit unserer Plattform aus. Wir setzen auf fortschrittliche Sicherheitsmaßnahmen, um unsere Nutzer zu schützen. In Kombination mit der richtigen Sensibilisierung trägt dies entscheidend dazu bei, ein Höchstmaß an Sicherheit zu gewährleisten.

2 Wie funktioniert Phishing?

Phishing ist eine Cyber-Angriffsmethode, bei der sich Betrüger als vertrauenswürdige Unternehmen ausgeben, um an sensible Daten zu gelangen. Dabei nutzen sie häufig E-Mails, Nachrichten oder gefälschte Websites, die täuschend echt wirken. Typische Phishing-Methoden sind:

Gefälschte Login-Seiten:
Cyberkriminelle erstellen gefälschte Websites, die den offiziellen Login-Seiten zum Verwechseln ähnlich sehen. Ein nur minimaler Unterschied, wie ein zusätzlicher Buchstabe oder eine geringfügige Änderung der URL, kann selbst die vorsichtigsten Benutzer in die Irre führen.

Betrügerische Angebote:
Phishing-Mails oder Nachrichten enthalten oft verlockende oder dringliche Aufforderungen, auf einen Link zu klicken oder Anmeldedaten einzugeben. Besonders beliebt sind Angebote wie vermeintliche Rabatte oder zeitlich begrenzte Angebote, die den Nutzer zu einer unüberlegten Handlung verleiten sollen.

Schädliche Werbung:
Denken Sie beim Aufrufen einer Website daran, dass nicht alle Werbeanzeigen vertrauenswürdige Quellen sind. Überprüfen Sie vor und nach dem Klicken auf eine Werbeanzeige immer die URL, um sicherzustellen, dass Sie sich auf einer vertrauenswürdigen Website befinden. Betrüger verwenden oft irreführende Werbeanzeigen, um Benutzer auf gefälschten Seiten zu leiten, die echt aussehen, aber nur dazu dienen, Ihre Daten zu stehlen.

Das Wissen um diese Methoden und ein geschärftes Bewusstsein sind der erste Schritt, um sich selbst und Ihr Unternehmen zu schützen.

3 Schritte zum Schutz Ihres Zugangs vor Phishing-Angriffen

Wenn Sie einige einfache Maßnahmen ergreifen, können Sie Ihren Zugang umfassend schützen und Phishing-Angriffe verhindern:

Überprüfen Sie die URL:
Vergewissern Sie sich stets, dass Sie sich auf www.ratehawk.com befinden. Betrügerische Websites enthalten oft kleine Abweichungen in der URL (z. B. ratehwak.com statt ratehawk.com).

Klicken Sie nicht auf verdächtige Links:
Wenn Sie eine unerwartete E-Mail oder Nachricht erhalten, in der Sie aufgefordert werden, sich einzuloggen, klicken Sie nicht auf den Link. Gehen Sie stattdessen direkt zu www.ratehawk.com/accounts/login.

Geben Sie Ihre Login-Daten niemals weiter:
Mitarbeiter von RateHawk werden Sie niemals per E-Mail, Telefon oder über soziale Medien nach Ihren Anmeldedaten oder einem Einmalpasswort fragen. Wenn Sie eine derartige Anfrage erhalten, melden Sie sich bitte sofort**.**

Verwenden Sie sichere und einmalige Passwörter:
Erstellen Sie ein starkes Passwort aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen. Verwenden Sie niemals dasselbe Passwort für verschiedene Konten. Wird ein Dienst gehackt, könnte ein mehrfach genutztes Passwort auch andere Konten gefährden.

Aktualisieren Sie Ihr Passwort regelmäßig:
Indem Sie Ihr Passwort alle paar Monate ändern, reduzieren Sie das Risiko eines unbefugten Zugriffs erheblich.

Indem Sie diese einfachen Sicherheitsmaßnahmen in Ihren Alltag integrieren, schützen Sie sich wirksam vor Phishing und dem Missbrauch Ihrer persönlichen Daten. Bleiben Sie wachsam, handeln Sie umsichtig – und buchen Sie sicher mit RateHawk!