Q&A Was tun, bei Phishing im Zusammenhang mit Ihrer Tropical Islands Buchung über ein Buchungsportal

Stand: 30. Oktober 2024

Liebe Kunden,

hier wollen wir Sie darüber informieren, wie Sie damit umgehen können, wenn Sie von einem Phishing im Zusammenhang mit Buchungen unserer Leistungen betroffen sind oder wenn Sie solche Phishing-Versuche wahrnehmen. Aktuell stellen wir fest, dass es zu einem vermehrten Aufkommen von Phishing Aktivitäten im Zusammenhang mit Buchungen von Tropical Islands über das Buchungsportal kommt. Bitte beachten Sie in diesem Zusammenhang immer auch die datenschutzrechtlichen Bestimmungen und Sicherheitswarnungen Ihrer Buchungsplattform.

Was sind die aktuellen Betrugsmaschen im Zusammenhang mit Buchungen bei Tropical Islands?

Wenn Sie über eine Buchungsplattform eine Leistung bei Tropical Islands gebucht haben, kann es sein, dass Sie über die Chatfunktion der Buchungsplattform-App kontaktiert werden oder Mails in ihrem persönlichen Posteingang erhalten. Diese Mails/Chats fordern Sie z.B. auf, Ihre Buchung zu bestätigen, oder mahnen Sie, Zahlung vorzunehmen. Über einen Link werden Sie dann auf eine gefälschte Internetseite geführt, die das Aussehen der Buchungsplattform nachahmt, bei der Sie gebucht haben. Dort werden Sie aufgefordert Zahlungen mit Ihrer Kreditkarte oder anderen Zahlungsmitteln durchzuführen und ggf. können auch zusätzliche persönliche Informationen abgefragt werden. Diese Mails und Chats sind betrügerisch und stammen nicht von Tropical Islands.

Woran erkennt man eine verdächtige Mail/Chatbeitrag oder gefälschte Webseiten?

Die Mails und Chatbeiträge können sehr realistisch aussehen - ohne die üblichen Schreib- und Grammatikfehler. Sollten Sie in einer für Sie fremden Sprache kontaktiert werden, ist dies sehr auffällig. Sie erkennen eine gefälschte Kommunikation sicher daran, wenn Sie aufgefordert werden, einem Link zu folgen und dort Daten einzugeben und/oder Zahlungen vorzunehmen.

Bitte melden Sie jede/n verdächtige Mail / Chatbeitrag **direkt an Ihre Buchungsplattform** und an uns unter: **betrugsmeldung@tropical-islands.de**

Wie sieht das korrekte und autorisierte Bezahlprozedere aus, wenn Sie über eine Buchungsplattform buchen?

Wenn Tropical Islands eine Zahlung von Ihnen anfordert, fordern wir Sie auf, dies in Ihrem persönlichen Tropical Islands Account auf unserer Website zu tun. Sie benötigen hierzu Ihre persönlichen Zugangsdaten sowie eine doppelte Verifikation. Dort können Sie in einem geschützten Umfeld Transaktionen vornehmen.

Was ist zu tun, wenn Sie einen verdächtigen Link angeklickt haben?

Wenn Sie auf einer gefälschten Webseite sind, lauern potenziell mehrere Gefahren:

Missbrauch Ihrer Zahlungsmittel: Sollten Sie Ihre Kreditkarten oder Zahlungsmitteldaten hinterlegt haben, wird Ihnen ein Betrag abgebucht und an die Betrüger überwiesen. Ihre Rechnung gegenüber Tropical Island müssen Sie leider weiterhin bezahlen. Haben die Angreifer Ihre Daten, sind sie dazu in der Lage, auch außerhalb der Buchungsplattformen mit Ihrer Kreditkarte Einkäufe zu tätigen.

Identitätsdiebstahl: Wenn Sie persönliche Daten auf der Seite in die Formularfelder eintragen, werden diese Daten nicht an Tropical Islands oder die Buchungsplattform übertragen. Betrüger erbeuten diese Daten und können sie weiterverkaufen. Je mehr Daten von Ihnen kursieren, desto höher ist die Wahrscheinlichkeit, dass Sie weiter angegriffen werden: durch Phishing und Betrugsattacken in anderen Zusammenhängen oder ggf. auch durch Identitätsdiebstahl.

Schadcode: Eine gefälschte Seite kann grundsätzlich auch durch Schadcode infiziert sein und versuchen, Ihre elektronischen Geräte zu infiltrieren. Dies ist uns zwar aktuell nicht bekannt. Es ist jedoch möglich.

Wie Sie sich generell vor Schadcode schützen, erläutert das BSI hier:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/schadprogramme_node.html#:~:text=Webseiten%3A%20Auch%20der%20Aufruf%20einer,sein%20–%20etwa%20durch%20manipulierte%20Werbebanner.

Wie erkennen Sie eine gefälschte Website?

Beim BSI (Bundesamt in der Informationstechnologie) finden Sie Hinweise, wie Sie eine gefälschte Website und Phishing erkennen. Dort gibt es auch anschauliche Videos:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten.html

Was können Sie tun, wenn Sie auf einer betrügerischen Seite Daten hinterlassen haben?

Sie sollten aktiv werden.

- Sollten Sie Zahlungs- oder Zugangsdaten hinterlassen haben, so sollten Sie diese sofort ändern bzw. Ihre Karten sperren und Ihre Kontobewegungen prüfen.
- Sollten Sie Kontaktinformationen, wie Ihre E-Mail-Adresse hinterlassen haben, sollten Sie klären, wie Sie Ihren Posteingang schützen können. Auf den Seiten der Polizei und der Verbraucherschutzbehörden finden Sie weitergehende Hinweise.
- Sie sollten Ihre technischen Endgeräte auf Schadsoftware prüfen.
- Wenn Sie einen Schaden erlitten haben, können Sie Anzeige bei der örtlichen Polizei erstatten.

Was unternimmt Tropical Islands, um Sie zu schützen?

Dem hohen Aufkommen und der hohen Qualität der Cyberangriffe auf unsere Systeme und die unserer Partner setzen wir verschiedene Maßnahmen entgegen. Wir überwachen unsere Systeme und passen unsere Prozesse an. Wir schulen unsere Mitarbeiter und investieren in die Aufklärung von Cyberangriffen sowie in den Ausbau unsere Cyber-Defense-Strategie. Auch wenn Tropical Islands auf dem aktuellen Stand der Technik Sicherheitsmaßnahmen vorhält, kann nicht ausgeschlossen werden, dass neuartige Attacken zu Problemen führen. Es ist daher unerlässlich, dass auch Sie selbst sich vorsichtig verhalten und sich über Schutzmaßnahmen aktiv informieren.