PRIVILEGED AND CONFIDENTIAL

Q&A: What to do in the event of phishing in connection with your Tropical Islands booking via a booking portal

Status: October 30, 2024

Dear customers,

We would like to inform you here about how you can deal with phishing in connection with bookings of our services or if you notice such phishing attempts. We are currently experiencing an increase in phishing activities in connection with bookings at Tropical Islands via the booking portal. In this context, please always observe the data protection regulations and security warnings of your booking platform.

What are the current scams in connection with bookings at Tropical Islands?

If you have booked a service at Tropical Islands via a booking platform, you may be contacted via the chat function of the booking platform app or receive emails in your personal inbox. These emails/chats may, for example, ask you to confirm your booking or remind you to make a payment. A link will then take you to a fake website that mimics the appearance of the booking platform you have booked with. There you will be asked to make payments with your credit card or other means of payment and you may also be asked for additional personal information.
These emails and chats are fraudulent and do not originate from Tropical Islands.

How can you recognize a suspicious email/chat post or fake website?

The emails and chat posts can look very realistic - without the usual spelling and grammatical errors. If you are contacted in a language that is foreign to you, this is very noticeable. You will certainly recognize a fake communication if you are asked to follow a link and enter data and/or make payments.

Please report any suspicious mail / chat contribution **directly to your booking platform** and to us at:
betrugsmeldung@tropical-islands.de

What is the correct and authorized payment procedure when booking via a booking platform?

If Tropical Islands requests payment from you, we will ask you to do this in your personal Tropical Islands account on our website. You will need your personal login details and double verification. There you can carry out transactions in a secure environment.

What should you do if you have clicked on a suspicious link?

If you are on a fake website, there are potentially several dangers lurking:

Misuse of your means of payment: If you have entered your credit card or payment details, you will be debited an amount and transferred to the fraudsters. Unfortunately, you will still have to pay your bill to Tropical Island. If the attackers have your data, they will also be able to make purchases with your credit card outside the booking platforms.

Identity theft: If you enter personal data in the form fields on the site, this data is not transmitted to Tropical Islands or the booking platform. Fraudsters steal this data and can sell it on. The more of your data is circulated, the greater the likelihood that you will be further attacked: by phishing and fraud attacks in other contexts or possibly also by identity theft.

Malicious code: In principle, a fake site can also be infected by malicious code and attempt to infiltrate your electronic devices. We are not currently aware of this. However, it is possible.

The BSI explains how you can generally protect yourself against malicious code here:

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.

How do you recognize a fake website?

The BSI (German Federal Office for Information Technology) provides information on how to recognize a fake website and phishing. There are also clear 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

What can you do if you have left data on a fraudulent site?

You should take action.

- If you have left payment or access data, you should change them immediately or block your cards and check your account transactions.
- If you have left contact information, such as your e-mail address, you should clarify how you can protect your inbox. You can find further information on the websites of the police and consumer protection authorities.
- You should check your technical devices for malware.
- If you have suffered damage, you can file a complaint with the local police.

What is Tropical Islands doing to protect you?

We are taking various measures to counter the high volume and quality of cyberattacks on our systems and those of our partners. We monitor our systems and adapt our processes. We train our employees and invest in cyber-attack detection and the expansion of our cyber-defense strategy. Even though Tropical Islands has state-of-the-art security measures in place, it cannot be ruled out that new types of attacks could lead to problems. It is therefore essential that you also exercise caution and actively inform yourself about protective measures.