Cybercriminals Never Go On Vacation (even when you do)

Office of Information Technology
Division of Information Security
JULY 2022

Every summer, millions of Americans go on vacation either locally or globally. Many Americans book their vacations online, which has increased cyber scams in the vacation industry. It is easy to be tempted to score a great deal on a vacation, especially with the rising costs due to inflation. If it sounds too good to be true then it most likely is, and it can cost you more in the end.

Recently, cybercriminals have begun to focus on the vacation rental market by advertising fake vacation rental homes. It has become increasingly popular to book with vacation rental sites such as Airbnb and VRBO. Cybercriminals use real rental listings and advertise them as their own, leaving the renter unaware until they arrive. This allows the cybercriminal to obtain all of your personal information via the fake booking site, which is basically a shell site. This information includes credit card information that the cybercriminal can use to accumulate debt in your name. Your bank may not hold you accountable for these charges, but it takes time and effort to get them reversed. While the majority of websites are trustworthy and valid there are always a few bad apples that spoil the bunch.

Below are a few helpful tips to prevent your dream vacation from turning into a nightmare due to scams.

Tips to Avoid a Vacation Rental Scam

1. Avoid sharing your travel details on social media because cybercriminals often use this information to target your home while you are away.

2. Avoid “super deals”. If the price is extremely below the market, then that is a major red flag.

3. If the website contains grammatical and spelling errors, it is most likely a scam. Most of the time these types of sites are made by people in different countries and they use translators to transcribe the site. Also, verify the images of the listing by conducting a reverse image search to ensure the photos are not stock photos (https://www.pcmag.com/how-to/how-to-do-a-reverse-image-search-from-your-phone).

4. Obtain recommendations only from trusted sources such as family, friends, or reputable travel agencies.

5. Always stick to well-known vacation rental sites such as Airbnb and VRBO. If you are booking a vacation rental on a site other than Airbnb and VRBO, always check to see if there is a contact number and email for the owner prior to booking. If there is only an email, there is a chance it could be a scam. Do not sign or pay for anything until you know the terms of the agreement including cancellation or refund policies.

6. If you are using a well-known vacation rental site such as Airbnb and VRBO, conduct a Google search after you have completed the reservation. Always search the owner's name, address, phone number, and email. If there are any complaints or issues regarding a cyber scam, the search could uncover it. If you find that the listing is fake, report it immediately and cancel the reservation. Airbnb has a rebooking and refund policy that explains how they will assist with rebooking a reservation and handling refunds. VRBO hosts must follow one of the five VRBO cancellation policies, which vary based on the type of listing.

7. Avoid new listings on Airbnb and VRBO if at all possible. Unfortunately, Airbnb does not have a system to go and physically check the listings in place, so the travelers must do their research. If there are no reviews or the reviews have improper wording or grammatically incorrect descriptions of the listing, it is most likely a scam. You can copy and paste the review into a search engine to see if the review is from another listing. If a listing has one bad review or a mediocre review it is most likely to be a legit listing since most fake listings do not have bad reviews.

8. Do not pay outside of the Airbnb or VRBO platform. It is a common practice that a host may want to avoid additional fees, but a cybercriminal could also be attempting to steal your information digitally. Avoid sending any wire transfer payment, a payment through PayPal, Zelle, gift cards, cryptocurrency, or payments to banks. If a cybercriminal is requesting any of these payment methods, it is a red flag. Cybercriminals know that if you pay using any of these methods and attempt to retrieve your money, there is no way to track it or get it back. Airbnb and VRBO platforms protect you in the case you need to cancel or any other issues arise.

9. Take time-stamped photos and videos of the property as soon as you arrive to avoid being scammed for property damage that you did not cause. When this type of scam occurs, the host will often threaten to leave a bad review for the traveler, which could result in being suspended from the site or legal action to recover the cost of damages. In the event that there is damage, report it immediately to the host and keep a record of your communication within the Airbnb message center. That way if the host does try to fraudulently accuse you of damages, you have evidence to protect yourself and to receive assistance from Airbnb.

Lastly, if you have been a victim of a travel scam or suspect a travel scam, you can report it to the FTC (https://reportfraud.ftc.gov/#/), Better Business Bureau (https://www.bbb.org/file-a-complaint), FBI Internet Crime Complaint Center https://www.ic3.gov and your state's attorney general's office (https://www.consumerresources.org/file-a-complaint/). These agencies assist with protecting travelers from misleading, deceptive, and unfair acts and often prevent future scams.

If you have any questions about this article, please send a message to cybersecurity@ihs.gov.

Stay safe and enjoy your summer vacation!