FRAUD INSIGHT

JULY 2024

auditone

SCAM ALERT: AIRBNB/HOLIDAY LET SCAMS

Airbnb/holiday let scams are fraudulent activities that target Airbnb/holiday let hosts or guests. These scams can take many forms and may involve fake listings, phishing scams, overpayment scams, theft and damage scams, or identity theft scams. Fraudsters often create fake Airbnb listings or impersonate legitimate hosts in order to trick users into sharing their personal and financial information, or to steal their money or property.

TYPES OF HOLIDAY LET SCAMS

Fake listings: Fraudsters create fake listings to trick guests into booking and paying for a property that doesn't actually exist. They may use photos and descriptions from real listings to make the fake listings look more legitimate.

Phishing scams: Fraudsters send emails or messages that appear to be from Airbnb/a holiday let company, asking for personal or financial information. These messages often contain links to fake websites that mimic the genuine website.

Overpayment scams: Fraudsters pay for a booking with a fraudulent credit card and then ask the host to refund them the difference via a wire transfer or other untraceable method. The host later finds out that the original payment was fraudulent and they are left responsible for the overpaid amount.

Theft and damage scams: Guests intentionally damage or steal items from the host's property or claim that items were damaged or missing when they weren't.

Identity theft scams: Fraudsters use personal information obtained from Airbnb/holiday let users to commit identity theft or fraud.

Multiple listings: Fraudsters create multiple listings for the same property, often with different prices and descriptions, in order to confuse or deceive guests.

Airbnb account hacking: Fraudsters may gain access to an Airbnb user's account and use it to book fraudulent listings or steal personal information.

Fake reviews: Fraudsters may post fake positive reviews to make their listings look more appealing to potential guests.

HOW TO AVOID AIRBNB & HOLIDAY LET SCAMS

- Research the host and listing: Before booking a property, research the host and the listing. Look for reviews from previous guests and check the host's verification status. If a host has no reviews or verification, it may be a red flag.
- Use Airbnb's/holiday let messaging system: Communicate with the host through the company's messaging system, rather than through email or phone. This ensures that your conversations are recorded on the platform and can be used as evidence if there is a dispute.
- Be cautious of requests for money outside of Airbnb: Fraudsters may try to get you to pay outside of the company's secure payment system. This is a red flag, as it means that you won't be protected by the company policies if something goes wrong.
- Be wary of deals that seem too good to be true: If a deal seems too good to be true, it probably is. Fraudsters may offer discounted rates or other incentives to entice guests to book their fake listings.
- Use Airbnb's payment system: Always pay through Airbnb's secure payment system. This ensures that your payment is protected and that you can be refunded if something goes wrong.

HOLIDAY FRAUD

In 2023, 6,640 reports of holiday fraud were made to Action Fraud and data shows July and August saw the highest number of reports made. Holiday makers lost a combined total of £ 12.3 million, meaning there was an average loss of £1,851 per victim.

This has shown a decrease of £3 million from the previous year, which suggests awareness in the area is helping reduce this type of fraud. Action Fraud has again started a campaign to alert travellers to the risk of holiday fraud and advised how to protect yourself when booking a trip away.

Pauline Smith, Head of Action Fraud, said:

"As people think ahead to book their holidays, understandably everyone is increasingly on the lookout for the best deals. With the cost-of-living crisis squeezing our finances, it's easy to forget to stay vigilant against fraudsters offering cheaper deals and great prices that are too good to be true. We want to avoid people losing their hard-earned money and help raise awareness of the signs of holiday fraud. Before booking any trips or signing up to any deals, do your research and check for ABTA and ATOL logos before clicking the confirmation button. Remember: stay alert online and be wise to fraudsters."

Mark Tanzer, ABTA Chief Executive, said:

"Fraudsters are using increasingly sophisticated methods to target consumers, with a particular focus on destinations and times of year when demand is high and availability limited, as they know people will be looking for good deals. Victims will often only find out they have been defrauded just before they are due to travel, or even in a resort, when it can be very difficult to find a legitimate replacement leading to yet more cost and potential disappointment. One of the simplest ways to protect yourself when booking is to look for a company that is a member of ABTA when booking your holiday."

Top tips to help prevent falling victim to holiday fraud:

- Do your research: before committing and booking your holiday, make sure that you do a thorough online search to ensure the company is credible.
- Pay safely: use a credit card when shopping online, if you have one. Most major credit card providers protect online purchases.
- Look for the logo: make sure they're a licensed company and check that they are properly accredited. Look for an ATOL (Air Travel Organiser's Licence) or a membership of ABTA, The Travel Association. Double check that information by searching on the ATOL or ABTA websites. The ABTA website has a section about companies who are showing the ABTA logo on their website and marketing materials when they have no right to use the logo as they are not ABTA members.

- Stay safe online: use three random words to create a strong password for your email that's different to all your other passwords. If a 2-step verification option is available, always set it.
- Beware of suspicious messages: be cautious of unexpected emails or messages offering unrealistic holiday deals. If you receive a suspicious email, report it by forwarding it to report@phishing.gov.uk
- Protect personal information: only fill in the mandatory details on a website when making a purchase. If possible, don't create an account for the online store when making your payment.
- Book with confidence: be sceptical of unrealistic holiday deals. If it sounds too good to be true, it probably is. Exercise caution and research before making purchases.

For further tips from ATOL and ABTA, visit https://www.atol.org/about-atol/how-to-check-for-protection/ or https://www.abta.com/tips-and-advice/planning-and-booking-a-holiday/how-avoid-travel-related-fraud

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at https://www.actionfraud.police.uk/ or by calling 0300 123 2040.

ACTION FRAUD ARTICLE - Don't lose out before flying out: Action Fraud urge holiday makers to watch out for fraudsters online | Action Fraud

SCAM ALERT: WHATSAPP GROUP CHATS TARGETTED BY FRAUDSTERS

WhatsApp group chat members are being warned they could be targeted by criminals. Action Fraud has revealed it has already received 636 reports from victims of the messaging app between January – April 2024. This is a 960% increase from the previous year. The fraud often begins when a member of the group receives a WhatsApp audio call from the fraudster, pretending or claiming to be another member of the group. This is done to gain the individual's trust, and often the scammer will use a false profile picture and/or display name, so at first glance it would appear to be a genuine member of the group. The fraudster will tell the victim they are sending them a one-time passcode which will allow them to join an upcoming video call for group members. The criminal then asks the victim to share this passcode with them so they can be "registered" for the video call. In reality, the criminal is asking for a registration code to register the victim's WhatsApp account to a new device so they can take over their account.

Once the fraudster has access to the victim's WhatsApp account, they will enable two-step verification which makes it impossible for the victim to regain access to their account. Other members of the group, or friends and family in the victim's contacts, will then be messaged asking them to transfer money urgently as they are in desperate need of help.

What can you do to avoid being a victim?

- Set up two-step verification (2SV) to give an extra layer of protection to your account. Tap Settings > Account > Two-step verification > Enable.
- CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person outside of WhatsApp to confirm their identity.
- Report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.

ACTION FRAUD ARTICLE – Action Fraud issue warning as WhatsApp group chats are targeted by fraudsters | Action Fraud

STAYING SAFE ONLINE

Action Fraud have confirmed that more than 22,500 people had their social media or email account hacked in 2023 with victims losing a total of £1.3 million. Pauline Smith, Head of Action Fraud, said:

"Anyone with a social media or email account can be a target for fraudsters or cyberattacks. It is important to take action to secure your accounts, as fraud becomes even harder to detect with technology on a global scale. Protect your information by ensuring your email and social media passwords are secure and different from all your other passwords. You can also set up 2-step verification for a layer of extra security. Remember, prevent the potential for fraud and hacking, never share your password or any 2-step verification code with anyone."

In the reports made to Action Fraud, there were various different methods of hacking reported, including:

On-platform chain hacking

This is when a fraudster gains control of an account and begins to impersonate the legitimate owner. The goal is to convince people to reveal authentication codes that are sent to them via text. Many victims of this type of hacking believe it's a friend messaging them; however the shared code was associated with their own account and the impersonator can now use it to access their account. Usually when an account is taken over, fraudsters monetise control of the account via the promotion of various fraudulent schemes, while impersonating the original account owner.

Leaked passwords and phishing

The other predominant method of hacking reported is leaked information used from data breaches, such as leaked passwords, or account details gained via phishing scams. This becomes prevalent as people often use the same password for multiple accounts, so a leaked password from one website can leave many of their online accounts vulnerable to hacking.

What can you do to avoid being a victim?

- **Use a strong and different password for your email and social media accounts**. Your email and social media passwords should be strong and different from all your other passwords. Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.
- **Turn on 2-Step Verification (2SV) for your email and social media accounts.** 2-Step Verification gives you twice the protection so even if cyber criminals have your password, they can't access your email or social media account. 2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password. You won't be asked for this every time you check your email or social media.

⇒ If you have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040.

⇒ Suspicious emails should also be sent to report@phishing.gov.uk

⇒ Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

⇒ For more information on cyber-crime and how to protect yourself against cyber-crime, please watch the attached awareness video created by the AuditOne counter fraud team:

⇒ https://www.youtube.com/watch?v=kTI7Wm5waNw&feature=youtu.be

ACTION FRAUD ARTICLE - Action Fraud issues a new warning to stay safe online after £1.3 million lost from hacked email and social media account scams last year | Action Fraud

HOW STRONG IS YOUR PASSWORD?

More and more victims are hacked, as the password they use is either easily hacked through information obtained through social media or the same password was used on other hacked accounts or websites. Try using Password Strength Meter (passwordmonster.com) to check how strong your password is or how easy it could be hacked and Have I Been Pwned: Check if your email has been compromised in a data breach to check when your email address has been in a data breach?

Both are free to use and will provide information on if you should change or strengthen your passwords.

IN THE NEWS

In this section we share details of recent fraud news articles from across the UK.

You can access the full article by clicking on the link at the bottom of each story.

Click on the link below to read how an NHS nurse narrowly avoided a prison sentence by defrauding her NHS employer out of £30,000 by working for another NHS trust 9 miles away when on sick leave. The nurse also gave a false reference to land the job at the other NHS employer

NHS nurse's £30,000 sick pay scam laid bare: Pregnant mother-of-four, 44, claimed thousands of pounds while working at two hospitals at the same time, then splashed the cash on TWO holidays to Cuba - as she's spared jail | Daily Mail Online

Click on the link below to read how a psychiatrist was struck off after he defrauded his NHS employer out of £40,000 by falsely claiming NHS work shifts when he was actually on holiday

Psychiatrist, 45, is struck off after he fiddled timesheets and falsely claimed £40,000 worth of NHS work shifts when he was actually on holiday | Daily Mail Online

Click on the link below to read how a nurse was struck off after claiming £50,000 over two years for 144 shifts she didn't actually work

Nurse struck off for claiming £50,000 over two years for 144 A&E shifts she didn't work - Mirror Online

Click on the link below to read how an agency nurse was struck off the NMC register by defrauding an NHS trust out of over £25k by claiming for 77 shifts that she never worked

Nurse faked timesheets to pocket £26k in wages - BBC News

Click on the link below to read how an NHS doctor was jailed for 4 years and made to repay £100,000, after he was caught submitting false invoices to NHS trusts, which could have earned him up to £4 million

Doctor jailed for four years for NHS fraud | Daily Mail Online

Click on the link below to read how a healthcare assistant received a 15 month prison sentence after pleading guilty to five counts of fraud by using cancer patients' bank cards to make fraudulent purchases

Health care assistant who used cancer patients' bank cards is "pure evil" says victim | City of London Police

Click on the link below to discover how a doctor, who has been struck off and sentenced to 12 months in prison (suspended for 2 years) defrauded his NHS employer out of a significant amount of money by claiming for overtime which was never worked

Hospital doctor caught claiming for overtime he never worked - Wales Online

PRESENTATION - CAN YOU HELP?

One of the best ways of helping the NHS prevent fraud is to know what to look out for in your day to day job. One good way of doing this is to arrange a fraud awareness presentation for your team, department/ward or directorate. Our team of trained counter fraud specialists will provide you with an interactive presentation focusing on real life fraud cases. The presentations can be tailored to suit the audience and time available. So, if you have a monthly/quarterly team meeting and fancy hearing from a team you might not ordinarily consider, why not give us a go. To arrange a session please click on the link below

Why not add something different to the next team meeting?

https://forms.office.com/e/i213cpCW9c

auditone
assurance . counter fraud . advisory

MEET THE COUNTER FRAUD TEAM

Rebecca Napper

Head of Operations (Proactive)

T: 07980 726 508

E: rebecca.napper@audit-one.co.uk

Michelle Watson

Head of Operations (Reactive)

T: 07580 589 024

E: michelle.watson@audit-one.co.uk

Laura Fox

Counter Fraud Manager

T: 07976 759 637

E: laura.fox@audit-one.co.uk

Kathryn Wilson

Counter Fraud Specialist

T: 07973 814 205

E: kathryn.wilson@audit-one.co.uk

Gemma Collin

Counter Fraud Support

T: 07920 590 180

E: gemma.collin@audit-one.co.uk

Martyn Tait

Counter Fraud Specialist

T: 07976 433 667

E: martyn.tait@audit-one.co.uk

Steven Sherwood-Hodgson

Counter Fraud Specialist

T: 07977 065 338

E: steven.sherwood-hodgson@audit-one.co.uk

Stephen Veitch

Counter Fraud Specialist

T: 07973 814 475

E: stephen.veitch@audit-one.co.uk

Simon Clarkson

Counter Fraud Specialist

T: 07980 729 654

E: simon.clarkson@audit-one.co.uk

Sarah McCloud

Counter Fraud Specialist

T: 07979 814 713

E: Sarah.mccloud@audit-one.co.uk

Michelle Acuna-Ocana

Lead Investigation Officer

T: 07974 096 752

E: michelle.acunaocana@audit-one.co.uk

Gareth Davies

Lead Investigation Officer

T: 07977 595 677

E: gareth.davies@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060