

Este alojamento do Porto está no Booking, mas afinal não é verdadeiro. Cuidado a marcar férias, a fraude tem aumentado e está mais sofisticada

cnnportugal.iol.pt/fraude/burla/este-alojamento-do-porto-esta-no-booking-mas-afinal-nao-e-verdadeiro-cuidado-a-marcar-ferias-a-fraude-tem-aumentado-e-esta-mais-sofisticada/20220616/62aaff4e0cf26256cd2986eb

Sofia Marvão

Ontem às 19:37

Pesquisar
Destino/nome do alojamento:
Porto
Data de check-in:
Data de check-out:
2 adultos · 0 crianças · 1 quarto
Viagem em negócios
Pesquisar

Lamentamos mas este alojamento não está a receber reservas no nosso website de momento. Não se preocupe, ainda encontra milhares de outras opções aqui.

Private Apartment GuestMonro 4.5
Alojamento de acomodação e pequeno-almoço
1680 Rua do Freixo, Campanhã, 4300-214 Porto, Portugal – Excelente localização - mostrar mapa

Situado a 2,2 km do Coliseu do Porto, o Solar Transmontano providencia acomodações com um salão partilhado, jardim e receção 24 horas. A propriedade oferece acesso Wi-Fi gratuito em todas as áreas e estacionamento privado está disponível no local.

Os hóspedes do alojamento de acomodação e pequeno-almoço podem desfrutar de um terraço.

Pontos fortes do alojamento
Excelente localização: os hóspedes recentes deram uma pontuação alta (8,5)

mais 17 fotografias

À medida que o regresso à normalidade devolve os clientes às plataformas de reservas também aumentam as burlas. Saiba quais os cuidados a ter e práticas a evitar para prevenir situações fraudulentas quando marcar as suas férias

Private Apartment GuestMonro: o nome surge na conhecida página de reservas de alojamento Booking.com como uma opção “imperdível” para quem procura passar uma temporada no Porto. Com boa imagem, centenas de comentários positivos, preço acessível, e está até validado pelo próprio site. O que poderia correr mal?

Poucos dias depois da reserva, surge uma mensagem de um número desconhecido no Whatsapp: “O meu nome é Andreas. Fez uma reserva no nosso alojamento, mas o seu cartão está inválido”. A mensagem vem acompanhada de um link para uma página que se parece exatamente igual à do Booking. “Pode inserir os dados do cartão e o problema fica resolvido”, assegura o interlocutor. Depois de voltar a preencher os dados para pagamento, o mensageiro desaparece e fica incontactável.

O caso descrito é real e acabou por bater à porta de Ricardo Moura, dono do Solar Transmontano, o verdadeiro alojamento instalado na morada indicada na página da popular página de reservas como sendo do "Private Apartmente GuestMonro". O solar fica num palacete remodelado a poucos metros da estação de Campanhã e desde 2019 via os seus quartos encherem diariamente. Hoje está vazio, lamenta o proprietário, de 49 anos. "O serviço de reservas foi pirateado no final de maio.

"Não conseguia entrar com os meus dados de acesso", começa por explicar o dono do estabelecimento. "Pensei que fosse algum erro no Booking e que seria resolvido no dia seguinte", mas não foi isso que aconteceu. Ao hostel continuaram a chegar clientes prontos para entrar, mas Ricardo Moura nunca tinha recebido aquelas reservas. É que o nome da sua página tinha sido alterado, bem como as imagens e o contacto telefónico. "Tentavam ligar para o número e ninguém atendia, por isso vinham ter a esta morada", conta. "A identificação do anfitrião era a minha, mas a fotografia era totalmente diferente". Tudo o resto parecia intacto, nomeadamente as avaliações dos clientes e até o selo de licença de Alojamento Local que a plataforma usa para certificar o local.

“Vinham da África do Sul e do Brasil, com malas à porta”

O proprietário diz que tentou contactar o Booking mas de pouco adiantou. "Dizem sempre que nos vão ligar de volta para confirmar o número, mas como o meu registo foi roubado ligavam para o tal indivíduo e não atendia", esclarece indignado. Ricardo chegou a ser insultado por algumas pessoas. "Estava desesperado", assume. Mas compreendia as reações. "Algumas vinham da África do Sul e do Brasil, com malas à porta e sem alojamento. É muito complicado".

Quando propunha que se hospedassem no Solar Transmontano recusavam devido à elevada diferença de preços. "Um grupo que aqui apareceu disse que reservou mais de 20 noites por 600 euros e eu não podia oferecer isso". Já o Booking podia, e assim o fez: "os clientes contactavam o site e em vez de lhes ser sugerida a minha propriedade, era sugerida uma diferente e mais barata".

Sem poder fazer nada para além de alertar aqueles que apareciam, exigiu à plataforma que retirasse o alojamento fraudulento da página até o problema ficar resolvido. "Mande a minha identificação, as faturas, as comissões que pago, tudo o que comprovava que era o dono daquela propriedade", mas até ao momento não houve resposta.

A página deixou entretanto de aceitar agendamentos. "Se não tinham respeito por mim, ao menos que tivessem respeito pelos clientes", queixa-se. Ao fim de uma semana, já mais de 40 pessoas tinham aparecido com reservas falsas, e foi quando decidiu apresentar queixa na Polícia Judiciária. Ter-lhe-ão dito que é uma situação "bastante complicada".

Duas semanas passaram desde que perdeu o acesso à sua conta, mas as perdas com as reservas já terão chegado aos milhares de euros. "Tinha reservas todos os dias, com quartos entre os 60 e os 70 euros por noite", afirma, explicando que 90% das estadias

eram agendadas pelo Booking. As comissões da plataforma também já não as consegue pagar, uma vez que não recebe as faturas. Agora resta-lhe um estabelecimento praticamente vazio e procurar novas alternativas.

O número de ataques com sucesso aumentou

“É um ataque feito de forma muito silenciosa”, quem o diz é Bruno Castro, CEO da VisionWare, empresa especializada em cibersegurança. “Alteram meramente as coordenadas bancárias, depois o dinheiro cai e fica na conta do atacante”. Trata-se de roubo de credenciais, usurpação de identidade e posterior tomada de controlo de sites de alojamento – um ataque muito conhecido, mas de curta duração.

“Localizam as pessoas via Facebook, Instagram, LinkedIn, o que seja, e depois massacram-nas constantemente até caírem numa armadilha”, nomeadamente o chamado phishing. Esta prática criminosa visa a recolha de informações pessoais – como o número do cartão de crédito, dados bancários ou senhas – através de sites aparentemente legítimos. Assim que a vítima é infetada torna-se um alvo acessível para que lhe seja roubado o dinheiro ou a identidade.

Sabe-se que desde o início do ano houve um aumento de ciberataques, mas, pior do que isso, “houve um nível brutal de ataques com sucesso”. Bruno Castro afirma que são bastante comuns aqueles direcionados a plataformas de alojamento, uma vez que visam negócios online levados a cabo por pessoas individuais. “Têm menos tendência para estar protegidas no que respeita à cibersegurança, ao contrário das empresas”, explica. “É perfeitamente normal que, com o crescimento do volume de negócio aumentem também estes ataques”.

Já para os clientes a situação agrava-se: "estão a confiar numa plataforma que se chama Booking, e não na pessoa que está por trás do alojamento que está no Booking". A dimensão da plataforma leva as pessoas a terem menos cautela, mas há sempre alguns cuidados a ter.

Como evitar este tipo de fraude?

Desconfiar por defeito

Prestar muita atenção ao tipo de conteúdos abertos quando são direcionados à própria pessoa, seja através de marketing agressivo, anúncios falsos ou mensagens pessoais. No caso de réplicas de plataformas de alojamento, importa avaliar a legitimidade dos links que são enviados. “É necessário ter sensibilidade e maturidade para perceber se está bem escrito, porque às tantas Booking até pode aparecer só com um 'o'”, alerta o especialista.

No caso que abre o artigo, o link enviado através do Whatsapp ia para uma página cujo endereço começava com "order-booking.com" e não o habitual "www.booking.com" da plataforma oficial. É uma bandeira vermelha.

Comunicação feita apenas através do site

O contacto com o anfitrião deve ser única e exclusivamente estabelecido através dos canais de comunicação oficiais da plataforma. Qualquer alteração na reserva que seja discutida por telefone, mensagem de texto ou email, e que implique o fornecimento dos dados do cartão de crédito merece ser alvo de desconfiança.

Separar o perfil pessoal do profissional

Bruno Castro sugere aos proprietários uma separação "muito bem feita" de toda a informação que envolva alojamentos, num perfil completamente distinto do pessoal. De outra forma, a sua identificação individual estará exposta e a pessoa em questão será "massacrada com ataques" para que lhe sejam roubadas as credenciais e usurpada a sua identidade e o seu negócio.

Se as informações não estiverem ligadas, "atacando o perfil profissional não colocam em causa o perfil pessoal", esclarece. "Este tipo de fraudes é direcionado a pessoas, e por isso estes conteúdos têm que estar segregados".

Credenciais complexas e autenticação multifator

O nível de complexidade dos dados de acesso é um dos pontos mais importantes a considerar no que diz respeito à segurança online, outro é a autenticação multifator - um mecanismo de revalidação de logins que, para além de uma password, envia ainda um código para o telemóvel ou email. "Grande parte destas plataformas já dispõe disso", afirma.

Pagar no momento da estadia

É aconselhável pagar no próprio alojamento sempre que possível, ainda que o especialista considere este um caso "muito raro". Isto porque grande parte das vezes é solicitada uma determinada quantia para assegurar a reserva.

Recorrer a cartões MB NET

A possibilidade de gerar um cartão virtual através da aplicação Mway é vista por Bruno Castro como uma "ótima" alternativa à utilização dos cartões de crédito nestas plataformas. "Permite bloquear pagamentos únicos e de quantias limitadas", esclarece. Basta indicar o valor a carregar no cartão e, por fim, inserir os dados do mesmo na página onde se pretende efetuar um pagamento.

Se o ataque já tiver ocorrido, o proprietário do alojamento deve expor a situação na plataforma e efetuar uma denúncia nas autoridades para que eventualmente lhe sejam devolvidas as credenciais. Por outro lado, os clientes dificilmente receberão o reembolso do valor roubado. O próprio site pode ter mecanismos de indemnização mas, de acordo com Bruno Castro, "a tendência é para que se autoexcluem". "Não será fácil", remata.



Novo Dia CNN

5 coisas que importam

Dê-nos 5 minutos, e iremos pô-lo a par das notícias que precisa de saber todas as manhãs.
[Saiba mais](#)