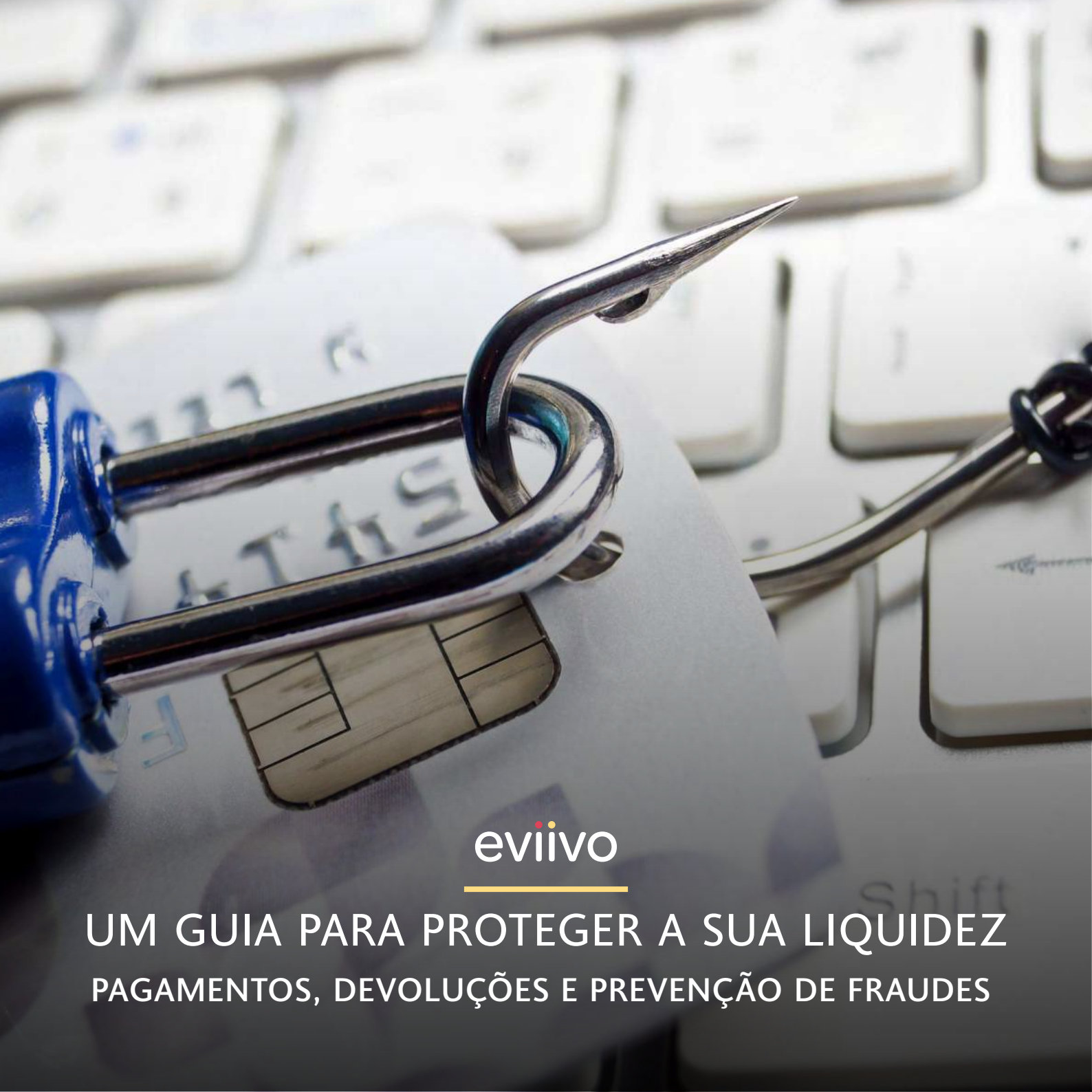


eviivo

UM GUIA PARA PROTEGER A SUA LIQUIDEZ

PAGAMENTOS, DEVOLUÇÕES E PREVENÇÃO DE FRAUDES

Para proteger a sua liquidez, é necessário adotar estratégias operacionais concebidas para:

1. Automatizar pagamentos e cobranças (em vez de depender de lembretes humanos)
2. Evitar estornos
3. Evitar fraudes

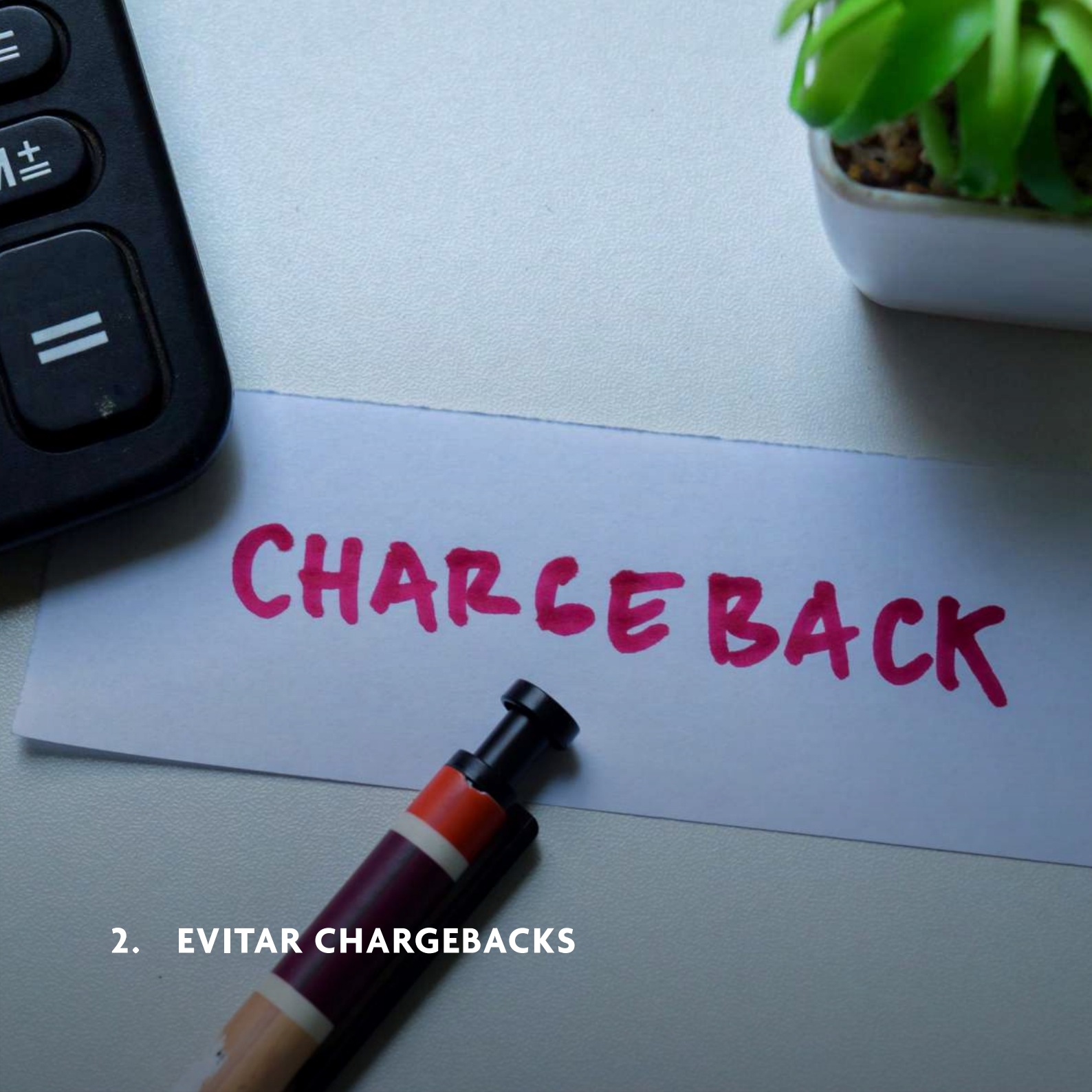
Este guia oferece conselhos de especialistas nas três áreas, adaptados a hoteleiros, anfitriões e gestores de propriedades. Continue a ler para começar a proteger o seu fluxo de caixa.

1. AUTOMATIZAÇÃO DOS PAGAMENTOS

A melhor forma de otimizar a sua liquidez é utilizar um PMS (sistema de gestão de propriedades) que ofereça um portal de pagamento totalmente integrado.

Este PMS deve ser capaz de:	eviivo Suite
Automatizar a cobrança de pagamentos com base em qualquer calendário definido pelo utilizador (entre a data da reserva e a partida), sem intervenção humana ou erros.	✓
Confirmar automaticamente qualquer pagamento.	✓
Enviar automaticamente um lembrete ao hóspede antes da data de vencimento.	✓
Determinar automaticamente se é devido ou não um reembolso quando uma reserva é cancelada.	✓
Processar automaticamente o reembolso correspondente.	✓
Confirmar automaticamente os cancelamentos e o valor dos reembolsos.	✓
Controlar automaticamente a entrega das chaves e dos códigos de acesso se os pagamentos previstos não tiverem sido recebidos.	✓
Pré-autorizar automaticamente os cartões (por exemplo, através de uma comunicação eletrónica completa com o banco do hóspede para [1] validar o cartão e [2] verificar e autorizar a existência de fundos suficientes no cartão para a reserva).	✓
Indicar automaticamente qual a parte da reserva que foi cobrada através de uma OTA e, em seguida, apresentá-la ao anfitrião e na fatura do hóspede, indicando qualquer saldo remanescente a cobrar no check-in ou posteriormente.	✓

Este PMS deve ser capaz de:	eviivo Suite
Indicar automaticamente se um cartão de crédito virtual (VCC) fornecido pela OTA está disponível e pode ser cobrado.	✓
Fornecer relatórios simples sobre depósitos pendentes; saldos de reservas não pagas; pagamentos em dinheiro/transacções por fonte de reserva e/ou método de pagamento.	✓
Proporcionar a reconciliação instantânea de pagamentos OTA - por VCC ou transferência bancária direta.	✓
Distinguir automaticamente entre uma reserva OTA pré-paga e um depósito antecipado, e identificar quando um pagamento VCC pode ser considerado um depósito antecipado e quando não pode.	✓
Gerar ou inverter automaticamente e com precisão os registos contabilísticos necessários com base no momento de qualquer cobrança ou reembolso (por exemplo, “caixa/recebimento”, “caixa/receitas diferidas”, “caixa/receitas e impostos”).	✓



2. EVITAR CHARGEBACKS

O que são chargebacks?

Um chargeback ocorre quando um cliente contesta um pagamento com cartão e pede ao seu banco para reverter a transação. Os clientes podem telefonar para o seu banco em qualquer altura e pedir o reembolso de uma transação com cartão. Normalmente, o banco toma o partido do cliente e reembolsa o montante do cartão. O comerciante terá então de provar esse facto:

1. A cobrança era justificada.
2. O hóspede autorizou ou assinou efetivamente o pagamento com cartão.

Quando recebe um estorno, pode contestá-lo, mas o ónus da prova recai sobre si.

- Se ganhar o litígio, fica com o dinheiro.
- Se perder a ação judicial, terá de processar o reembolso e o banco cobrar-lhe-á provavelmente custos administrativos.

É bom saber -> Na União Europeia, os clientes podem solicitar um estorno (reembolso) até 13 meses após o primeiro débito no seu cartão. Fora da UE, este período é reduzido para 70-120 dias, consoante a política do banco.

Presença do titular do cartão

Se o titular do cartão estiver presente quando o pagamento for processado, tem boas hipóteses de se defender contra qualquer estorno. Considera-se que um titular do cartão está "presente" quando:

- Introduzem o seu código PIN secreto num leitor de cartões ou numa caixa multibanco
- Pagam online e é-lhes pedido que respondam a um sistema de segurança 3DS (ou Amex Safekey) em tempo real. Neste caso, os clientes são solicitados a introduzir uma palavra-passe de uso único (OTP) como parte do processo de pagamento, que o seu banco normalmente envia por correio eletrónico ou SMS

Se o titular do cartão não estiver presente quando o cartão é processado, é muito mais provável que fique exposto a estornos. Isto acontece frequentemente quando os dados do cartão lhe são transmitidos por uma OTA, porque o hóspede já não está presente online quando processa o cartão no seu PMS. O pagamento não falhará necessariamente, mas é muito mais provável que fique exposto a estornos. Continue a ler para obter recomendações sobre como evitar esta situação.

Chargebacks legítimos

Podem ocorrer **chargebacks legítimos** quando:

- O hóspede cancela por um motivo **real, grave e inesperado** (por exemplo, um "caso de força maior" como a pandemia de COVID-19, uma catástrofe natural, proibições de viagem, etc.) e não recebe qualquer indemnização do alojamento, especialmente se a sua viagem não estava segurada
- Os hóspedes receiam que o **alojamento ou a OTA não os reembolse por um cancelamento total ou parcial legítimo**, especialmente se o alojamento demorar demasiado tempo a fazê-lo

Os chargebacks fraudulentos podem ocorrer quando:

- Os hóspedes afirmam que nunca ficaram alojados, quando na verdade ficaram
- O cliente é reembolsado em dinheiro, mas reclama um segundo reembolso através de um débito no seu cartão
- O hóspede opta deliberadamente por NÃO ficar na sua propriedade, mas quer evitar o pagamento de taxas de cancelamento tardio e evitar qualquer contacto consigo ou com a OTA
- Um hóspede efectua o check-in, mas a estadia foi pré-paga por outra pessoa utilizando um cartão roubado (e você não pré-autorizou/revalidou o cartão)

Como posso evitar chargebacks?

Para evitar chargebacks, deve aplicar sempre as seguintes recomendações:

- **Pedir aos hóspedes que reconfirmem** a sua estadia alguns dias antes do check-in.
- **Efetuar corretamente o check-in dos hóspedes à chegada**. Sempre:
  - Insistir para que o hóspede envie os dados de registo (isto pode ser feito por correio eletrónico/via ligação)
  - Peça ao hóspede que lhe entregue novamente o seu cartão e efectue uma verificação do chip e do pin com um leitor de cartões quando lhe entregar as chaves (se tiver um serviço de receção ou de "meet & greet")
  - Clique no botão "Check In" no eviivo Suite para deixar um rasto digital (se utilizar o eviivo como PMS).

- **Confirme que o titular do cartão e a pessoa que fica consigo são a mesma pessoa**.
  - Se o cartão pertencer a outra pessoa ou se o passaporte não corresponder, pedir ao hóspede que apresente um cartão em seu nome.
  - Se o hóspede não puder apresentar um documento de identidade, debitar a totalidade da estadia no cartão no momento do check-in (não esperar pelo check-out) e/ou pedir ao titular do cartão que confirme os seus dados e o acordo de pagamento por correio eletrónico.

- **Se um hóspede cancelar por telefone**, cancele a reserva e processe imediatamente um reembolso ou uma taxa de cancelamento (isto pode ser totalmente automatizado).

- **Se o cliente tiver direito a um reembolso total ou parcial, processe-o imediatamente**. Os atrasos podem levar o cliente a solicitar um reembolso através do seu banco, o que pode acabar por custar-lhe mais do que o reembolso.

- **Mantenha um registo digital**.

- **Cobrar as taxas de cancelamento (se aplicável) assim que o prazo de cancelamento tiver passado**, idealmente antes do check-in.

- Considerar a utilização de um **depósito não reembolsável** (ou seja, um depósito devido no momento da reserva, ou logo que permitido por lei em áreas onde a lei impõe um período de carência de 24 horas). Isto requer a harmonização das políticas de cancelamento e de depósito.

Recomendações relativas ao pagamento de reservas em linha

Se vai cobrar aos hóspedes, em vez de cobrar à OTA, certifique-se de que **utiliza um sistema de gestão de reservas e propriedades com uma função de automatização de pagamentos totalmente integrada e compatível com PCI**. Este é um sistema que permite automatizar todo o processo de cobrança e reembolso de pagamentos. Deve ser capaz de cobrar um pagamento quando este é devido e processar um reembolso quando uma reserva é cancelada, sem qualquer intervenção manual. Um sistema deste tipo deve também oferecer-lhe:

- **Una amplia selección de procesadores de tarjetas**, para evitar que te quedes bloqueado con un único banco o procesador de tarjetas.
- **Diferentes opciones de configuración**, como cobrar a través de un enlace de pago, una página web segura o un portal de huéspedes; imponer o restringir el método de pago admitido; y seleccionar por adelantado los tipos de clientes que deben o no pagar con tarjeta.
- **Uma vasta seleção de processadores de cartões**, para evitar ficar preso a um único banco ou processador de cartões.
- **Diferentes opções de configuração**, como a cobrança através de uma ligação de pagamento, de um sítio Web seguro ou de um portal para hóspedes; a imposição ou restrição do método de pagamento suportado; e a seleção prévia dos tipos de clientes que devem ou não pagar com cartão.

O melhor método é pré-autorizar/processar um cartão quando o hóspede estiver presente online, assim que receber uma reserva. Por conseguinte, certifique-se de que o seu sítio Web está habilitado para o 3DSecure/Safepay e que o seu PMS pode enviar uma ligação de pagamento ao hóspede (por correio eletrónico, SMS ou WhatsApp), conduzindo-o a uma página segura onde poderá processar o seu cartão em conformidade com todos os requisitos 3DS. Em ambos os casos, a presença online do hóspede na página e o código de segurança 3DS servem como **prova irrefutável de que ele pretendia pagar e estava totalmente ciente dos seus termos e condições quando efectuou a reserva**.

Se decidir processar o cartão você mesmo - com um leitor de cartões ou diretamente num PMS como o eviivo Suite - e o hóspede já não concordar em digitar um PIN secreto ou fornecer um código de segurança 3DS de utilização única, então o risco de estorno é elevado. Mesmo que o cartão seja processado com sucesso, o estorno pode ocorrer dias ou semanas mais tarde, e pode ficar exposto a um risco muito maior de hóspedes desonestos.

Como posso aumentar as minhas hipóteses de ganhar um recurso?

É necessário apresentar **um comprovativo da estadia do hóspede**:

- Forneça um **relatório que mostre como e quando os pagamentos foram processados**, juntamente com uma cópia de todos os e-mails de confirmação de pagamento/reserva enviados ao hóspede que associam o pagamento aos seus termos e condições (DICA: reveja os termos da sua política de cancelamento/depósito. Certifique-se de que o seu PMS inclui automaticamente estes termos em qualquer confirmação de reserva, pagamento ou e-mails de cancelamento).
- **Guarde todas as comunicações entre si e o hóspede**.
- **Anexe uma cópia de qualquer extrato ou fatura do hóspede**, especialmente se incluir um reembolso por levantamento de dinheiro.

3. EVITAR A FRAUDE CIBERNÉTICA

Tomar medidas preventivas para evitar a fraude cibernética é essencial para proteger o seu dinheiro.

Nos últimos anos, registou-se um aumento dos ciberataques geopolíticos e a maioria dos governos aumentou as medidas de cibersegurança e impôs requisitos de conformidade de segurança mais rigorosos.

O primeiro passo para proteger a sua liquidez é rever as medidas de segurança implementadas pelos seus fornecedores de software:	eviivo Suite
Que controlos efectuam quando inscrevem novos clientes? Efectuam controlos financeiros e de identidade minuciosos para garantir que não permitem a entrada de piratas informáticos nas suas plataformas? (Se partilhar uma plataforma com outras empresas, quererá que o seu fornecedor de plataformas faça tudo o que estiver ao seu alcance para garantir que está em boa companhia).	✓
São nativamente compatíveis com a norma PCI DSS (Payment Card Industry Data Security Standard), auditadas e certificadas de forma independente pela Visa e pela Mastercard ou por auditores designados, encriptam os dados dos cartões e efectuam análises regulares para evitar a sua divulgação?	✓
Fornecem funções robustas de gestão de utilizadores a um nível suficientemente granular (ou seja, por função, por caraterística, por equipamento e por conjunto de propriedades), permitindo simultaneamente aos utilizadores visualizar os dados de todas as propriedades autorizadas a partir de um único calendário de reservas?	✓
Fornecem firewalls básicas, deteção de intrusões, proteção anti-spam e anti-phishing, bem como capacidades profissionais de cópia de segurança e recuperação?	✓
Dispõem de procedimentos para o alertar quando algum dos seus clientes é pirateado ou sofre um ataque de phishing?	✓
Qual é a vossa política em matéria de RGPD (Regulamento Geral sobre a Proteção de Dados) e/ou **DSA** (Lei dos Serviços Digitais)?	✓

O resto é consigo. É necessário orientar e formar o pessoal, implementar as melhores práticas e, acima de tudo, garantir que todos estão atentos. É também uma boa ideia subscrever um seguro contra ciberataques, se o puder pagar.

Credenciais dos empregados

Uma das formas mais simples e eficazes de reforçar as suas defesas é garantir que cada funcionário possui credenciais de acesso seguras e individuais. Cada conjunto de credenciais deve incluir o seguinte:

- Um endereço de correio eletrónico único (o seu nome de utilizador).
- Uma palavra-passe única que **só o utilizador conhece** (quanto mais longa, melhor: escolha um mínimo de 12 caracteres, incluindo pelo menos uma letra maiúscula, um número + um carácter especial).
- Uma pergunta de segurança única para a qual só o utilizador sabe a resposta (utilizada se pretender repor, recuperar ou alterar as suas credenciais no futuro).
- Um segundo e-mail ou número de telemóvel de recuperação (diferente do primeiro), essencial para ajudar a mitigar rapidamente quaisquer danos caso seja vítima de um ciberataque.
- Uma segunda pergunta e resposta de segurança, conhecida por si e pelo fornecedor do software. Esta é utilizada por um fornecedor como a eviivo para verificar a sua identidade quando nos contacta por telefone ou videoconferência.
- Um identificador de propriedade único (a eviivo chama-lhe shortname).

Escolha de palavras-passe

As piores palavras-passe (ou seja, as que têm maior probabilidade de serem comprometidas) são as que incluem a palavra "password", as primeiras letras de um teclado ("Qwerty" ou "Azerty"), séries numéricas básicas (por exemplo, '111111' ou "1234567") ou os nomes ou datas de nascimento dos seus filhos, cônjuge ou parceiro.

As melhores palavras-passe têm mais de 12 caracteres e incluem sempre uma letra maiúscula, um número e um carácter especial. Em vez de uma palavra, utilize uma frase longa e fácil de memorizar. Inclua um ou mais números, uma ou mais letras maiúsculas e um ou mais caracteres especiais (por exemplo, *_-$£).

Se utilizar o eviivo e for o titular da conta principal, pode, por sua vez, dar acesso a outros utilizadores e funcionários da sua organização através do ecrã de gestão de utilizadores do eviivo. Pode aceder-lhe clicando no ícone do homenzinho no canto superior direito do ecrã do eviivo Suite.

Caixas de correio públicas e partilhadas

Para evitar surpresas e violações da cibersegurança, recomendamos vivamente que tome as seguintes precauções:

Evite a todo o custo a partilha de credenciais. É sempre melhor garantir que cada funcionário tenha o seu próprio conjunto de credenciais. Ignorar isto é a causa mais frequente de fraude cibernética no sector hoteleiro. No entanto, a partilha de dispositivos e de logins pode ser conveniente para actividades de receção ou de limpeza. Se "tiver" mesmo de utilizar dispositivos e credenciais partilhados, então....

Certifique-se de que as credenciais de utilizador partilhadas têm apenas direitos de acesso mínimos. Qualquer pessoa que lide com pagamentos, processamento de cartões ou informações pessoais dos hóspedes não deve poder fazê-lo utilizando credenciais partilhadas. Para sua própria proteção, é necessária uma auditabilidade total. Tente manter o menor número possível de olhos neste tipo de informação.

Não dê níveis máximos de permissão a caixas de correio públicas ou partilhadas. Os endereços públicos partilhados (por exemplo, "info@yourplace.com", "contact@yourplace.com", "reservations@yourplace.com", "bookings@yourplace.com" ou "hello@yourplace.com") NÃO devem ser atribuídos a funções de nível superior, como "Administrador", titular da conta principal ou gestor. Ignorar este conselho é a segunda razão mais comum para a fraude cibernética no sector da hotelaria e restauração.

Diferencie sempre o seu e-mail/palavra-passe profissional de qualquer e-mail pessoal utilizado para comunicações privadas. Utilize contas de correio eletrónico e palavras-passe separadas e dê instruções aos seus empregados para fazerem o mesmo.

- **As caixas de correio públicas e partilhadas são muito mais fáceis de violar porque:**

- Os piratas informáticos utilizam endereços de correio eletrónico públicos para induzir os hóspedes a fornecer dados ou detalhes de cartões.
- A utilização de caixas de correio ou contas partilhadas aumenta a probabilidade de ataque, uma vez que qualquer um dos vários utilizadores pode ser induzido a fornecer as suas credenciais.
- As fraudes internas podem ser cometidas por trabalhadores temporários ou contratados, novos funcionários ou prestadores de serviços externos que não conhece bem.

Segurança multi-utilizador baseada em equipas

Uma configuração de segurança baseada em equipas deve ajudá-lo a gerir facilmente uma multiplicidade de funções.

Por exemplo, suponha que três pessoas diferentes necessitam do mesmo nível de segurança. Em vez de criar uma caixa de correio partilhada, pode:

- Atribuir a cada pessoa as suas próprias credenciais de início de sessão.
- Atribuir as três pessoas a uma "Equipa".
- Atribuir as permissões pretendidas e os direitos de acesso às propriedades à "Equipa" em vez de a cada indivíduo.

Uma configuração baseada em equipas é muito mais rápida e fácil de gerir quando os funcionários entram ou saem da empresa. Como cada pessoa mantém as suas próprias credenciais, qualquer auditoria de transação associa cada ação à pessoa que a executou. Assim, se as credenciais de uma pessoa forem roubadas ou violadas, o resto da equipa pode continuar sem ser afetada, ao passo que com credenciais partilhadas, todos ficam desactivados.

Phishing: a forma mais comum de ataque

Phishing é o ato malicioso de tentar enganar os utilizadores para que revelem as suas credenciais pessoais. Os atacantes enganam frequentemente os utilizadores para que revelem informações através de ligações maliciosas, páginas Web falsas ou anexos de correio eletrónico que contêm spyware ou vírus informáticos, como os Trojans.

Os criminosos e os autores de fraudes falsificam constantemente os logótipos e as páginas de início de sessão de empresas respeitáveis. São muito hábeis a reproduzir não só logótipos, mas também fotografias, vídeos e até vozes.

Os métodos mais comuns de invasão de contas são o correio eletrónico, as notificações móveis, as redes sociais e as chamadas telefónicas. Os atacantes podem fazer-se passar por um dos fornecedores da sua empresa, pelo seu banco, pelo seu fornecedor de telecomunicações ou de software, ou por várias autoridades.

Uma tentativa de phishing bem sucedida pode permitir a um atacante:

- Recolher nomes de utilizador e palavras-passe ou outras informações sensíveis.
- Assumir o controlo da sua caixa de correio eletrónico para uso malicioso.
- Convencer o utilizador a efetuar pagamentos em seu nome.
- Convencer o utilizador a depositar somas de dinheiro numa conta não autorizada.
- Instalar spyware ou software malicioso que lhes permita monitorizar a sua atividade online.
- Danificar o seu computador ou a rede da organização, encriptar os seus dados ou exigir um resgate pelos mesmos.
- Obter acesso a propriedade intelectual, desenhos ou patentes pendentes.

O resto deste guia analisa as formas inteligentes como os burlões o podem tentar enganar e como se manter alerta.

Spear phishing: confirmações de reserva falsas

O spear phishing é uma forma direcionada de ataque de phishing. Os perpetradores utilizam frequentemente informações publicamente disponíveis na Internet, como endereços de correio eletrónico públicos em sítios Web, para criar mensagens falsas e incentivar o seu público a clicar em ligações maliciosas.

Um exemplo pode ser a criação de confirmações de reserva falsas para enviar aos seus hóspedes. Os autores de fraudes podem obter uma confirmação de reserva original ao efetuar e depois cancelar uma reserva ou encomenda consigo. Em seguida, podem utilizá-la para criar uma confirmação falsa que parece vir de si (ou da eviivo, Airbnb, Booking.com, etc.). Estas falsas mensagens de confirmação induzem os hóspedes a fornecerem informações pessoais, credenciais ou detalhes de cartões ou contas bancárias, ou mesmo a clicarem numa hiperligação para pagar a conta bancária dos piratas informáticos.

Um método comum de ataques de phishing direcionados consiste em disfarçar software malicioso em anexos e ligações aparentemente legítimos, que os criminosos esperam que sejam descarregados para infetar o computador ou a rede alvo.

Além disso, estes botões e ligações conduzem frequentemente os utilizadores a páginas falsas de início de sessão em sítios Web para recolher informações sensíveis ou pessoais, que podem depois ser utilizadas para lançar outros ataques ou obter acesso privilegiado à conta ou rede organizacional do alvo.

Para se proteger, considere os seguintes pontos para o ajudar a detetar falsificações e truques de phishing em linha:

Clique no nome do remetente na caixa "De" do cabeçalho da mensagem de correio eletrónico para descobrir o endereço de correio eletrónico completo. Parece um endereço legítimo? A ortografia corresponde a 100% à do correio eletrónico oficial da empresa? Se não corresponder, é falso.

O e-mail pede-lhe que faça algo com urgência e estava à espera? A maioria dos burlões cria um falso sentido de urgência, alegando estar a agir em nome de uma autoridade superior (por exemplo, um banco, uma instituição, uma empresa ou um executivo sénior) e depois diz-lhe para verificar os detalhes da sua conta.

A mensagem contém erros ortográficos ou gramaticais invulgares? Muitos criminosos operam a partir do estrangeiro. Como falsificam notificações oficiais, é frequente detetar erros gramaticais ou ortográficos que uma empresa legítima evitaria.

Clique no nome do sítio Web na barra do navegador e verifique a primeira parte do endereço do sítio Web. Por exemplo, os endereços Web eviivo legítimos (nomes de domínio URL) começam sempre por https://eviivo.com/ ou https://on.eviivo.com/ ou https://via.eviivo.com/.

Verifique sempre com muito cuidado a ortografia do endereço de correio eletrónico ou do endereço da página Web. Para o redirecionar para um sítio Web falso ou para uma página de início de sessão, basta que um carácter seja diferente ou que um espaço esteja no sítio errado. Exemplo: Uma tentativa recente de phishing substituiu "eviivo" por 'evlivo', enquanto outra dizia "eviivo.com" em vez de "eviivo.com" - ambos os erros ortográficos quase imperceptíveis!

DICA

Se for um utilizador eviivo, guarde o URL da página de início de sessão oficial do eviivo no seu browser e inicie sempre sessão a partir daí. Isto reduz o risco de clicar em ligações duvidosas em mensagens de correio eletrónico ou páginas de início de sessão falsas.

Whaling

O whaling é um ataque de phishing que visa os utilizadores fingindo ser indivíduos de alto nível, tais como executivos de empresas, gestores de topo, celebridades ou pessoal com autoridade para fornecer acesso a sistemas ou informações sensíveis.

O objetivo é enganar alguém para que tome uma ação ou revele informações que possam depois ser utilizadas para causar mais violações de segurança.

Os ataques whaling são altamente personalizados. Incorporam frequentemente o nome do alvo, o seu cargo e outras informações relevantes (obtidas de várias fontes, como os seus perfis nas redes sociais ou outros aspectos da sua pegada digital).

Os atacantes fazem-se passar por alguém com muita autoridade ou credibilidade para:

Pedem aos seus alvos um favor ou ajuda urgente, de modo que os utilizadores ansiosos por agradar ao seu chefe acabam por transferir dados, credenciais ou mesmo dinheiro! Para evitar isto, verifique três vezes qualquer comunicação que receba assinada pelo diretor-geral, vice-presidente ou CEO de uma empresa.

Ameaçam os utilizadores de encerrar a sua conta ou de quebrar certas regras se não reconfirmarem imediatamente as suas credenciais. Os utilizadores são então levados para um site falso onde os hackers estão à espera, prontos para capturar as suas credenciais.

Oferecer uma grande recompensa em dinheiro ou fingir que o utilizador tem dinheiro para reclamar (por exemplo, um prémio de lotaria ou uma herança), a fim de o levar a fornecer as suas credenciais, dados bancários ou dados do cartão.

Vishing

Vishing é a abreviatura de “voice phishing”. Significa simplesmente phishing através de chamadas telefónicas ou mensagens de voz.

Pode tratar-se de alguém que se faz passar pelo seu banco, por uma empresa de telecomunicações ou por um fornecedor como a eviivo, e que lhe pede para confirmar informações pessoais ou de conta sensíveis. O atacante pode também convidá-lo a partilhar o seu ecrã para instalar spyware que captará as suas teclas e credenciais.

Para verificar se o autor da chamada é realmente da fonte que afirma, basta fazer-lhe perguntas que só você e essa fonte saberiam.

Por exemplo, se o autor da chamada afirma ser da eviivo, pode fazer-lhe perguntas sobre:
- O número de referência da última reserva efectuada.
- O nome abreviado da sua propriedade.
- A (segunda) pergunta e resposta de segurança que só você e a eviivo partilham.

A eviivo - ou qualquer outra organização genuína - nunca o contactaria da forma descrita no guião abaixo:

Olá, fala a Candice da eviivo,

Estamos a ligar porque acreditamos que houve uma atividade suspeita na sua conta. É urgente verificarmos se está tudo em ordem. Posso partilhar o meu ecrã consigo?

Muito bem, para aceder aos detalhes da sua conta, tenho de lhe pedir que reconfirme a sua palavra-passe, uma vez que teremos de a redefinir durante a chamada. Pode reconfirmar a sua pergunta e resposta de segurança?

DICA

Conselhos para se manter alerta:

- **A eviivo, ou qualquer outra empresa de renome, NUNCA lhe pedirá para revelar a sua palavra-passe.** Embora possam pedir-lhe a resposta a uma pergunta de segurança, nunca lhe perguntarão qual é a pergunta de segurança.

- Quando um fornecedor lhe pede para partilhar o seu ecrã, deve fazê-lo a partir do endereço oficial do sítio Web do fornecedor (por exemplo, eviivo.com).

- Lembre-se de que qualquer funcionário do fornecedor pode ver e aceder à sua conta, por isso faça-lhe uma pergunta que só ele saberia (por exemplo, o nome abreviado da sua propriedade, a referência da reserva mais recente que entrou no seu calendário). Um burlão não saberá nenhuma destas respostas.

Smishing

Smishing é o phishing através de SMS e mensagens de texto. Os autores de fraudes enviam frequentemente mensagens de texto com a intenção de:

- Roubar informações pessoais ou confidenciais do destinatário; ou
- infetar o dispositivo do destinatário com malware

Os burlões podem facilmente falsificar uma conta WhatsApp, utilizando qualquer fotografia disponível publicamente de alguém que conheçam, ou a fotografia de uma figura pública e/ou de autoridade.

Phishing nas redes sociais

Os cibercriminosos utilizam frequentemente as redes sociais para levar a cabo ataques com o objetivo de roubar informações pessoais ou espalhar malware. Os atacantes fazem-se muitas vezes **passar por um amigo/colega/familiar** nas redes sociais para o levar a enviar-lhes dinheiro. Alguns ataques tentam sequestrar a sua conta para lançar ataques posteriores contra todos os contactos, ligações, amigos ou seguidores do seu livro de endereços.

Este método baseia-se frequentemente em

- Anúncios falsos que podem induzir o utilizador a clicar numa ligação que o redirecciona para uma página de início de sessão falsa que parece legítima - mas não é - para capturar as suas credenciais ou detalhes da conta.
- Pedir-lhe que pague uma taxa, uma penalização ou uma taxa ilegítima.

As comunicações autênticas nas redes sociais remetem sempre para o URL do sítio Web oficial do vendedor. No caso do eviivo, o URL, visível na barra de endereço, começa sempre por **https://eviivo.com/ ou https://on.eviivo.com/**.


evilivo
Search
Help
Thu, 09 Dec
Fri, 10 Dec
Sat, 11 Dec
Sun, 12 Dec
Mon, 13 Dec
Book

eviivo

PARA MAIS INFORMAÇÕES, CONTACTAR

SALES@EVIIVO.COM | +35 1308 807 980