

ANTES DE RESERVAR

A viagem começa na verificação.



Fotos bonitas e uma boa oferta não bastam.

1 Confira quem está oferecendo.

Cruze nome, endereço, telefone e avaliações em fontes diferentes. Busque o perfil ligado ao site oficial. Fotos, seguidores e a posição no Google, sozinhos, não provam autenticidade.

2 Confirme antes de pagar.

Compare preços e desconfie de pressa para fechar. Confirme datas, regras de cancelamento e recebedor do Pix ou boleto. Se o nome não corresponder ao combinado, pare e esclareça.

3 Guarde o que foi combinado.

Peça a confirmação por escrito e salve anúncio, valores e comprovantes. Consulte o Cadastur quando aplicável; o cadastro não autentica quem manda uma cobrança em nome da hospedagem.

Uma oferta boa pode esperar uma confirmação.

ANTES DE CLICAR

O link chegou. Você precisa abrir?



Vale para e-mail, SMS, WhatsApp e outros apps.

1 Olhe além do nome e da foto.

Confira o endereço completo do remetente e o destino do link. No computador, passe o cursor sem clicar. No celular, se não conseguir ver o destino sem abrir, não prossiga.

2 Prefira chegar por conta própria.

Abra o aplicativo oficial ou digite o endereço já conhecido. Não use o link da mensagem para confirmar a própria mensagem. Encurtadores e QR Codes pedem o mesmo cuidado.

3 HTTPS não confirma a identidade.

Uma conexão criptografada também pode levar a um site falso. Confira o domínio, letras trocadas e terminações estranhas. Não ignore alertas de site perigoso ou conexão não particular.

Na dúvida, vá pelo caminho que você conhece.

LINKS, ARQUIVOS E MALWARE

Não transforme a reserva em acesso.



Malware é um programa malicioso que pode roubar seus dados.

1 Atualize suas defesas.

Mantenha celular, computador, navegador e proteção antimalware atualizados. Não desative alertas para abrir uma página. Atualizações corrigem falhas que podem ser exploradas.

2 Não instale para “validar” a estadia.

Recuse apps, arquivos de instalação e ferramentas de acesso remoto enviados por mensagem. Baixe aplicativos somente de lojas oficiais e confira o desenvolvedor. Uma logo não é garantia.

3 Anexo inesperado? Confirme antes.

Comprovantes e vouchers também podem servir de isca. Confirme a origem por um contato conhecido antes de baixar ou abrir. Não habilite macros nem permissões extras para ler um documento.

Confirmar uma reserva não exige controlar seu aparelho.

SUSPEITA DE GOLPE

Conhecem sua reserva. Isso não prova a origem.



Nome, datas e hotel correto não legitimam uma cobrança.

1 Pare antes de agir.

Uma taxa inesperada ou ameaça de cancelamento urgente merece verificação. Não pague, não envie documentos nem converse para “testar” o contato. Não forneça senhas ou códigos de acesso.

2 Confirme por outro caminho.

Retome o telefone da confirmação original ou abra a plataforma da reserva por conta própria. Pergunte se o pedido existe e qual é o procedimento combinado. Não ligue só para o número recebido.

3 Preserve e avise.

Salve mensagem, número, endereço do site e horário. Avise a hospedagem real e a plataforma, se houver. Depois, denuncie e bloqueie o contato no aplicativo. Não exponha seus dados em posts públicos.

A urgência do remetente não precisa virar a sua.

SE VOCÊ JÁ CLICOU

Agora, cuide do que foi exposto.



Clicar não comprova uma infecção. O que aconteceu depois?

1 Só abriu a página?

Feche o site. Não preencha dados, baixe arquivos ou aceite permissões. Confira se houve download; não abra o arquivo suspeito. Mantenha as proteções ativas e faça uma verificação de segurança.

2 Digitou senha ou passou um código?

De outro aparelho confiável, troque a senha e todas as iguais usadas em outras contas. Encerre sessões desconhecidas e ative a verificação em duas etapas. Revise seu e-mail de recuperação.

3 Instalou algo ou liberou acesso?

Suspenda acessos bancários nesse aparelho. Busque ajuda técnica de confiança para avaliar e remover a ameaça. Não restaure tudo por impulso: preserve evidências e proteja os dados antes.

Se houve acesso a dados bancários, avise seu banco.

SE HOUVE PAGAMENTO

Aja rápido. Não pague de novo.



Procure ajuda pelos canais oficiais, não pelos recebidos.

1 Fale com seu banco imediatamente.

Se foi Pix, conteste e peça o MED (Mecanismo Especial de Devolução). Se foi cartão, conteste a cobrança e peça o bloqueio quando necessário. A devolução depende da análise; não é garantida.

2 Organize as provas.

Guarde conversas, perfis, links, comprovantes, datas e protocolos. Registre boletim de ocorrência e denuncie na plataforma. Avise a hospedagem real para que confirme sua reserva e oriente outros hóspedes.

3 Cuidado com o “resgate” pago.

Não faça outra transferência para liberar estorno ou recuperar o dinheiro. Acompanhe pelo banco e pela plataforma oficial. Não entregue senha, código ou controle do aparelho a quem promete resolver.

Você não precisa lidar com isso sozinho.

FONTES E CONFIRMAÇÃO

Orientações que você pode conferir.



No PDF, toque no nome da fonte para abrir.

Ministério do Turismo

Antes de reservar >

CERT.br | Evite fraudes

Links, perfis e pagamentos >

CERT.br | Não se deixe enganar

Pressão, urgência e falsa identidade >

CERT.br | Computadores

Atualizações e programas maliciosos >

CERT.br | Caiu? Veja o que fazer

Contas, provas e reação ao golpe >

Google Chrome

Conexão segura e alertas do navegador >

Banco Central | MED do Pix

Pedido de devolução em caso de fraude >

Salve. Compartilhe. Confirme pelo canal oficial.

BOOKING HACKER | CUIDADO COM QUEM VAI VIAJAR

Orientações educativas. Nenhum cuidado elimina todos os riscos.