

Vorsicht Falle! So erkennen Sie
Fakebuchungen & Betrugsversuche

Die Psychologie des Betrugs: Warum fallen wir darauf rein?

- **Zeitdruck:** Wenn Sie mir die Anzahlung nicht sofort (außerhalb der Plattform) zurückerstatten, obwohl ich erst vor 5 Minuten storniert habe, werde ich Sie überall schlecht bewerten.“
- **Autorität:** Gefälschte E-Mails von Geschäftsführern (CEO-Fraud) oder bekannten Buchungsportalen.
- **Emotionen:** Extreme Hilfsbereitschaft oder die Angst, einen lukrativen Kunden zu verlieren.

Typische Warnsignale

Sprachliche Auffälligkeiten

- offensichtliche Übersetzungsfehler
- ungewöhnlich förmliche/distanzierte Sprache -> oft durch Übersetzung durch KI

Unplausible Anforderungen

- Scheckzahlung
- Wirre/komische Links

Übermäßige Freundlichkeit & "Storytelling"

- lange, emotionale Romane (z. B. über eine Erbschaft, eine kirchliche Mission oder ein schwerkrankes Kind) um Vertrauen aufzubauen

Die "Offline-Buchung"

- Gast versucht massiv, Kommunikation wegzulocken: *"Mein Internet ist schlecht, schreiben Sie mir bitte direkt an meine private E-Mail-Adresse oder per WhatsApp."*

Warnsignale bei der Bezahlung

Splitting

Gast fragt, ob er den Betrag verschiedene Kreditkarten aufteilen kann. Das ist ein klassisches Zeichen für gestohlene Kreditkartendaten mit geringem Restlimit.

Zahlung per Scheck:

Im digitalen Zeitalter ist ein Scheck (besonders aus dem Ausland) fast immer ein Betrugsversuch. Er wird erst gutgeschrieben, platzt aber oft erst nach 2–4 Wochen ("Eingang vorbehalten").

„Wir zahlen per Scheck über den doppelten Betrag, bitte überweisen Sie den Rest an unseren Reiseleiter zurück.“
(Klassischer Überzahlungsbetrug)

Kreditkarten-Validierung per Link:

Man erhält eine Nachricht dass man die Kontodaten oder Kreditkartendaten "bestätigen" muss, damit die Auszahlung des Gastes erfolgen kann.
Vorsicht: Phishing!

Kreditkartendetails

Sie erhalten einen Link wo Sie angeblich die Kreditkartendetails des Gastes finden

Die "Storno-Masche"

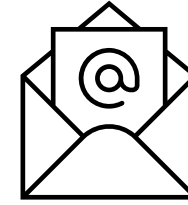


Sofortige Stornierung nach Zahlung:

Der Gast zahlt (oft mit gestohlenen Daten) und storniert 24 Stunden später. Er bittet aber darum, die Rückerstattung auf ein **anderes Konto** oder per PayPal zu senden, da sein "altes Konto gerade gesperrt" sei.

So wäscht er das Geld über dein Konto.

Der Check für den Ernstfall - E-Mails



- **E-Mail-Header** prüfen: Ist die E-Mail-Adresse komisch?
-> viele Zahlen in der E-Mail-Adresse, Name passt nicht überein zu Signatur, Tippfehler
- **Links in der E-Mail checken:** Mit der Maus über den Link fahren (Hover), ohne zu klicken, um die wahre Ziel-URL zu sehen.
- **Anhänge:** Seriös: meist PDF // Fake bzw. Phishing: .zip, .html, .exe
- **Verträge/Abos:** Fragen Sie sich ob Sie überhaupt ein Abo oder einen Vertrag zum Absender haben oder dies z.B. von OBS abgewickelt wird
- **Druck:** übt der Absender Druck auf Sie auf oder werden Sie zur Zahlung aufgefordert?
- **Identitätsprüfung:** Firmennamen oder Gastnamen in den bekannten Suchmaschinen prüfen

-> zwei Augen Prinzip

Der Check für den Ernstfall - Buchungen



- **Unvollständige oder unglaubwürdige Gästeinformationen**

-> Name nur aus komischen Zeichen, offensichtliche falsche Adresse

- **Verdächtige Kommunikation**

-> Sehr schlechte oder automatisierte Antworten, weicht Fragen aus, Gast möchte Kommunikation auf WhatsApp / via E-Mail umleiten, Gast sendet Link wo Informationen zur Person oder KK-Details hinterlegt sein sollen, überdramatische Nachricht

- **Zahlungen**

-> Gast behauptet er habe zu viel bezahlt, Gast möchte nicht vorab überweisen sondern nur Bar vor Ort obwohl das gegen die hinterlegten Einstellungen verstößt (oft dann Fakebuchungen)

- **Ungewöhnliche Sonderwünsche**

-> Gast möchte sich Pakete in die Unterkunft liefern, Gast möchte nicht übernachten sondern nur Unterkunft für ein paar Stunden nutzen

- **Links**

-> Anweisung auf Links zu klicken

Wie kann ich mich gegen Fakebuchungen schützen?

Vorauszahlung
verlangen
mit Frist

Bezahlungsmethode über
Portale nutzen
Wie Booking.com
Payments

kurze Verifizierung durch
Kommunikation

Auf typische
Warnsignale achten



- Klicken Sie auf keine unbekanntem Anhänge und Links
- Arbeiten Sie mit dem zwei Augen Prinzip
- Werden Sie hellhörig



+49 941 46374849 oder +43 720 881639



info@obsg.de



online-buchung-service.de



obs_onlinebuchungservice



OBS OnlineBuchungService



OBS Online Buchung Service