eviivo

EIN LEITFADEN ZUM SCHUTZ IHRES BARGELDES:

ZAHLUNGEN, RÜCKLASTSCHRIFTVERLETZUNGEN UND BETRUGSVERHÜTUNG

Um Ihr Bargeld zu schützen, müssen Sie Betriebsstrategien anwenden, die darauf ausgerichtet sind:

1. Automatisieren Sie Zahlung und Einzug (anstatt sich auf menschliche Mahnungen zu verlassen)
2. Vermeiden Sie Rückbuchungen
3. Betrug vermeiden

Dieser Leitfaden bietet Expertenratschläge in allen drei Bereichen, zugeschnitten auf Hoteliers, Gastgeber und Immobilienverwalter. Lesen Sie weiter, um Ihren Cashflow zu sichern.

1. ZAHLUNGSAUTOMATISIERUNG

Die beste Möglichkeit zur Optimierung Ihres Cashflows ist die Verwendung eines Property Management Systems (PMS), das über eine vollständig integrierte Zahlungsmaschine verfügt.

Dieses PMS muss die Fähigkeit umfassen:	eviivo Suite
Automatisieren Sie die Zahlungseinziehung basierend auf einem benutzerdefinierten Zeitplan (zwischen Buchungsdatum und Check-out), ohne menschliches Eingreifen oder Fehler.	✓
Bestätigen Sie jede Zahlung automatisch.	✓
Senden Sie dem Gast vor einem bevorstehenden Fälligkeitstermin automatisch eine freundliche Erinnerung.	✓
Bestimmen Sie automatisch, ob bei Stornierung einer Buchung eine Rückerstattung fällig ist oder nicht.	✓
Verarbeiten Sie automatisch die entsprechende Rückerstattung.	✓
Bestätigen Sie automatisch jede Stornierung und den Wert einer Rückerstattung.	✓
Steuern Sie automatisch die Ausgabe von Schlüsseln und Zugangscodes, wenn die erwarteten Zahlungen nicht eingegangen sind.	✓
Automatische Vorautorisierung von Karten (z. B. über einen vollständigen elektronischen Anruf bei der Bank des Gastes, um [1] die Karte zu validieren und [2] zu überprüfen und zu autorisieren, dass auf der Karte genügend Guthaben für die Buchung vorhanden ist).	✓
Geben Sie automatisch an, welcher Teil der Buchung über ein OTA eingezogen wurde, und zeigen Sie ihn dann dem Gastgeber und auf der Gästerechnung an. Geben Sie dabei an, ob beim oder nach dem Check-in ein Restbetrag eingezogen werden muss.	✓

This PMS must include the ability to:	eviivo Suite
Automatische Anzeige, ob/wann eine von OTA bereitgestellte virtuelle Kreditkarte (VCC) freigegeben und belastet werden kann.	✓
Ermöglichen Sie eine einfache Berichterstattung über fällige Anzahlungen, ausstehende Buchungssalden, Zahlungs-/Bargeldtransaktionen nach Buchungsquelle und/oder Zahlungsmethode.	✓
Sorgen Sie für eine sofortige Abstimmung der OTA-Auszahlungen – per VCC oder direkter Banküberweisung.	✓
Unterscheiden Sie automatisch zwischen einer im Voraus bezahlten OTA-Buchung und einer Anzahlung und erkennen Sie, wann eine VCC-Zahlung als Anzahlung gilt und wann nicht.	✓
Erstellen oder stornieren Sie automatisch und präzise die erforderlichen Buchhaltungseinträge basierend auf dem Zeitpunkt einer Einziehung oder Rückerstattung (z. B. „Bargeld/Forderungen“, „Bargeld/abgegrenzter Umsatz“, „Bargeld/Umsatz und Steuern“).	✓

2. Vermeidung von Rückbuchungen

Was sind Rückbuchungen?

Bei einer Rückbuchung beanstandet ein Gast eine Kartenzahlung und bittet seine Bank, die Transaktion rückgängig zu machen. Gäste können jederzeit ihre Bank anrufen und eine Rückerstattung der Kartenzahlung verlangen. Die Bank wird in der Regel dem Gast Recht geben und den Kartenbetrag erstatten. Sie als Händler müssen dann Folgendes nachweisen:

1. Die Zahlung war gerechtfertigt.
2. Die Kartenzahlung wurde vom Gast echt autorisiert bzw. unterschrieben.

Wenn Sie eine Rückbuchung erhalten, können Sie diese anfechten – die Beweislast liegt jedoch bei Ihnen.

- Wenn Sie den Streit gewinnen, dürfen Sie das Geld behalten.
- Wenn Sie den Streitfall verlieren, müssen Sie eine Rückerstattung beantragen und es kann sein, dass Ihnen von der Bank Verwaltungskosten in Rechnung gestellt werden.

Gut zu wissen -> Innerhalb der Europäischen Union können Gäste bis zu 13 Monate nach der ersten Belastung ihrer Karte eine Rückbuchung (Rückerstattung) beantragen. Außerhalb der Europäischen Union verkürzt sich diese Frist je nach Bankrichtlinie auf 70–120 Tage.

Karteninhaberpräsenz

Wenn der Karteninhaber bei der Zahlungsabwicklung anwesend ist, haben Sie sehr gute Chancen, sich gegen etwaige Rückbuchungen wehren zu können. Ein Karteninhaber gilt als anwesend, wenn:

- Sie geben ihren geheimen PIN-Code in ein Kartenlesegerät oder einen Geldautomaten ein.
- Sie bezahlen online und werden aufgefordert, in Echtzeit eine 3DS-Sicherheitsherausforderung (oder die Amex Safekey-Herausforderung) zu beantworten. Dabei werden die Gäste im Rahmen des Check-out-Prozesses aufgefordert, ein Einmalkennwort (OTP) einzugeben, das ihre Bank normalerweise per E-Mail oder SMS sendet.

Wenn der Karteninhaber bei der Kartenzahlung nicht anwesend ist, erhöht sich das Risiko von Rückbuchungen deutlich. Dies ist häufig der Fall, wenn Ihnen Kartendaten von einem Online-Reisebüro übermittelt werden, da der Gast bei der Kartenzahlung in Ihrem PMS nicht mehr online ist. Die Zahlung schlägt zwar nicht unbedingt fehl, aber es besteht ein deutlich höheres Risiko von Rückbuchungen. Lesen Sie weiter, um Empfehlungen zur Vermeidung dieser Situation zu erhalten.

Legitime Rückbuchungen

LeZu legitimen Rückbuchungen kann es kommen, wenn:

- Der Gast storniert aus einem **echten, schwerwiegenden und unerwarteten Grund** (z. B. „höhere Gewalt“ wie die COVID-19-Pandemie, eine Naturkatastrophe, Reiseverbote usw.) und erhält kein Verständnis von der Unterkunft, insbesondere wenn seine Reise nicht versichert war.
- Gäste befürchten, dass **ihnen die Unterkunft oder das Online-Reisebüro bei einer berechtigten vollständigen oder teilweisen Stornierung den Betrag nicht zurückerstattet**, insbesondere, wenn die Unterkunft dafür zu lange braucht.

Betrügerische Rückbuchungen können in folgenden Fällen erfolgen:

- Gäste behaupten, sie hätten nie übernachtet – obwohl sie es taten.
- Sie haben dem Gast den Betrag in bar erstattet, er fordert jedoch eine zweite Rückerstattung per Kartenrückbuchung.
- Gäste entscheiden sich bewusst, NICHT bei Ihnen zu übernachten, möchten aber die Zahlung einer Gebühr für eine kurzfristige Stornierung vermeiden und jeglichen Kontakt mit Ihnen oder dem OTA vermeiden.
- Ein Gast übernachtet, aber der Aufenthalt wurde von einer anderen Person mit einer gestohlenen Karte im Voraus bezahlt (und Sie haben die Karte nicht vorab autorisiert/erneut validiert).

Wie kann ich Rückbuchungen vermeiden?

Um Rückbuchungen zu vermeiden, sollten Sie die folgenden Empfehlungen stets umsetzen:

- Ihren Aufenthalt einige Tage vor dem Check-in **erneut zu bestätigen** .
- **Melden Sie den Gast bei der Ankunft ordnungsgemäß an** . Immer:
  - Bestehen Sie darauf, dass der Gast seine Registrierungsdaten übermittelt. (Dies kann per E-Mail/Nachrichtenlink erfolgen.)
  - Bestehen Sie darauf, dass der Gast einen Ausweis oder eine Fotokopie/ein Foto seines Ausweises vorlegt. (Dies kann per E-Mail/Nachricht übermittelt werden. Wenn Sie jedoch auf Nummer sicher gehen möchten, bestehen Sie auf einem Videoanruf, bei dem der Ausweis vor der Kamera gezeigt wird, oder verwenden Sie alternativ eine Gesichtserkennungssoftware.)
  - Bitten Sie den Gast, Ihnen seine Karte erneut zu geben , und führen Sie bei der Schlüsselübergabe eine Chip- und PIN-Prüfung mit einem Kartenleser durch (sofern Sie über eine Rezeption oder einen Meet-and-Greet-Service verfügen).
  - Klicken Sie in der eviivo Suite auf die Schaltfläche „Check-in“, um eine digitale Spur zu hinterlassen (wenn Sie eviivo als Ihr PMS verwenden).
- **Vergewissern Sie sich, dass der Karteninhaber und die Person, die bei Ihnen übernachtet, dieselbe Person sind** .
  - Wenn die Karte für eine andere Person ist oder der Reisepass nicht übereinstimmt, bitten Sie den Gast, eine Karte auf seinen eigenen Namen vorzulegen.
  - Wenn der Gast keinen Ausweis vorlegen kann, belasten Sie die Karte beim Check-in mit dem vollen Betrag Ihres Aufenthalts (warten Sie nicht bis zum Check-out) und/oder bitten Sie den Karteninhaber, seine Daten und seine Zahlungszusage per E-Mail zu bestätigen.

Top-Hotels bestehen auf der Vorlage eines schriftlich unterzeichneten Drittzahlerformulars sowie eines gescannten Fotos beider Kartenseiten, wobei das Foto vom Karteninhaber datiert und unterschrieben sein muss.

- **Wenn ein Gast telefonisch storniert** , stornieren Sie die Buchung und veranlassen Sie umgehend die entsprechende Stornierungsgebühr/Rückerstattung. (Dies kann vollständig automatisiert werden.)
- **Wenn dem Gast eine vollständige oder teilweise Rückerstattung zusteht, bearbeiten Sie diese umgehend**. Verzögerungen können dazu führen, dass der Gast eine Rückbuchung über seine Bank veranlasst, was Sie letztendlich mehr kosten kann als die Rückerstattung!
- **Behalten Sie eine digitale Spur.**
- **Belasten Sie Ihre Stornierungsgebühr** (sofern zutreffend) **unmittelbar nach Ablauf der Stornierungsfrist**, idealerweise vor dem Check-in.
- Erwägen Sie die Verwendung einer **nicht rückzahlbaren Anzahlung** (d. h. eine Anzahlung, die zum Zeitpunkt der Buchung fällig wird oder sobald dies gesetzlich zulässig ist, in Gebieten, in denen eine 24-stündige Zahlungsfrist gesetzlich vorgeschrieben ist). Dies erfordert die Harmonisierung Ihrer Stornierungs- und Anzahlungsrichtlinien.

Empfehlungen zur Bezahlung von Online-Buchungen

Wenn Sie Zahlungen direkt von Ihren Gästen und nicht von der Online-Reiseagentur einziehen, **verwenden Sie unbedingt ein Buchungs- und Property-Management-System mit einer vollständig integrierten, PCI-konformen Zahlungsautomatisierungsfunktion**. Mit diesem System können Sie den gesamten Inkasso- und Rückerstattungsprozess automatisieren. Es sollte in der Lage sein, Zahlungen sofort nach Fälligkeit einzuziehen und eine Rückerstattung sofort nach Stornierung der Buchung zu veranlassen – ohne manuelle Eingriffe. Ein solches System bietet Ihnen außerdem:

- **Eine große Auswahl an Kartenprozessoren**, damit Sie nicht an eine einzige Bank oder einen einzigen Kartenprozessor gebunden sind.
- **Verschiedene Konfigurationsoptionen**, wie etwa das Einziehen der Zahlung über einen Zahlungslink, eine sichere Webseite oder ein Gästeportal, das Vorschreiben oder Einschränken der unterstützten Zahlungsmethode und die gezielte Ansprache der Kundentypen, die im Voraus mit Karte bezahlen sollten oder nicht.

Die beste Methode ist die Vorautorisierung/Verarbeitung einer Karte, sobald der Gast online ist und eine Buchung eingeht. Stellen Sie daher sicher, dass Ihre Website für 3DSecure/ Safepay aktiviert ist und Ihr PMS dem Gast einen Zahlungslink (per E-Mail, SMS oder WhatsApp) senden kann, der ihn auf eine sichere Seite führt, auf der er seine Karte 3DS-konform verarbeiten kann. In beiden Fällen dienen die Online-Präsenz des Gastes auf der Seite und der 3DS-Sicherheitscode als **unwiderlegbarer Beweis dafür, dass er bei der Buchung die Zahlungsabsicht hatte und Ihre Geschäftsbedingungen vollständig kannte.**

Wenn Sie die Kartenzahlung selbst durchführen – mit einem Kartenlesegerät oder direkt in einem PMS wie der eviivo Suite – und der Gast nicht mehr zur Eingabe einer geheimen PIN oder eines 3DS-Einmalpassworts aufgefordert werden kann, ist das Risiko einer Rückbuchung hoch. Selbst bei erfolgreicher Kartenverarbeitung kann die Rückbuchung Sie noch Tage oder Wochen später treffen, und Sie sind weiterhin einem deutlich höheren Risiko durch unehrliche Gäste ausgesetzt.

Wie kann ich meine Chancen verbessern, einen Streit zu gewinnen?

Sie müssen den Aufenthalt des Gastes nachweisen:

- Legen Sie Ihre Kopie des **Pass-/Personalausweisfotos oder Kreditkartenfotos** (beide Seiten) vor.
- Legen Sie einen **Bericht vor, der zeigt, wie und wann die Zahlungen verarbeitet wurden**, zusammen mit einer Kopie der an den Gast gesendeten Zahlungs-/Buchungsbestätigungs-E-Mail, die die Zahlung mit Ihren AGB verknüpft. (TIPP: Lesen Sie Ihre Stornierungs-/Anzahlungsbedingungen sorgfältig durch. Stellen Sie sicher, dass Ihr PMS diese Bedingungen automatisch in jede Buchungs-, Zahlungs- oder Stornierungsbestätigungs-E-Mail einfügt.)
- **Bewahren Sie die gesamte Kommunikation zwischen Ihnen und dem Gast auf**.
- **Legen Sie eine Kopie aller Gästeabrechnungen oder Rechnungen** vor, insbesondere wenn diese eine bestehende Rückerstattung am Schalter enthalten.

3. Cyber-Betrug vermeiden

Um Ihr Bargeld zu schützen, sind proaktive Maßnahmen zur Vermeidung von Cyberbetrug von entscheidender Bedeutung!

Angesichts der zunehmenden geopolitischen Cyberangriffe der letzten Jahre haben die meisten Regierungen ihre Cybersicherheitsmaßnahmen verstärkt und strengere Anforderungen an die Einhaltung der Sicherheitsvorschriften eingeführt.

Der erste Schritt zum Schutz Ihres Bargeldes besteht darin, die von Ihren Softwareanbietern integrierten Sicherheitsmaßnahmen zu überprüfen:	**eviivo Suite**
Welche Kontrollen werden bei der Aufnahme neuer Kunden durchgeführt? Werden gründliche Identitäts- und Finanzprüfungen durchgeführt, um sicherzustellen, dass Hacker keinen Zugriff auf ihre Plattformen erhalten? (Wenn Sie eine Plattform mit anderen Unternehmen teilen, möchten Sie, dass Ihr Plattformanbieter alles tut, um sicherzustellen, dass Sie in guter Gesellschaft sind!)	✓
Sind sie Sind sie PCI DSS-konform (Payment Card Industry Data Security Standard)? Werden sie unabhängig von Visa und Mastercard oder beauftragten Prüfern geprüft und zertifiziert? Verschlüsseln sie die Kartendaten und führen sie regelmäßige Scans durch, um Offenlegungen zu verhindern?	✓
Bieten sie leistungsstarke Benutzerverwaltungsfunktionen auf ausreichend detaillierter Ebene (z. B. nach Rolle, nach Funktion, nach Teams und nach Eigenschaftssatz), während sie es Benutzern dennoch ermöglichen, Daten für alle zulässigen Eigenschaften aus einem einzigen Buchungskalender anzuzeigen?	✓
Bieten sie eine grundlegende Firewall, Angriffserkennung, Antispam- und Antiphishing-Schutz sowie professionelle Backup- und Wiederherstellungsfunktionen?	✓
Verfügen sie über Verfahren, die Sie benachrichtigen, wenn einer ihrer Kunden gehackt wird oder einem Phishing-Angriff ausgesetzt ist?	✓
Was ist ihre DSGVO-Richtlinie (Datenschutz-Grundverordnung) und/oder DSA-Richtlinie (Digital Services Act)?	✓

Der Rest liegt in Ihren Händen. Sie müssen Ihre Mitarbeiter anleiten und schulen, Best Practices implementieren und vor allem dafür sorgen, dass alle wachsam bleiben! Es ist außerdem ratsam, eine Cyber-Versicherung abzuschließen, sofern Sie es sich leisten können.

Mitarbeiter-Anmeldeinformationen

Eine der einfachsten und effektivsten Möglichkeiten zur Stärkung Ihrer Abwehrmaßnahmen besteht darin, jedem Mitarbeiter sichere, individuelle Anmeldedaten zuzuweisen. Jeder Satz dieser Anmeldedaten sollte Folgendes umfassen:

- Eine eindeutige E-Mail (Ihr Benutzername).
- Ein einzigartiges Passwort, **das nur Sie kennen** (je länger, desto besser: Wählen Sie mindestens 12 Zeichen, darunter mindestens ein Großbuchstabe, eine Zahl und ein Sonderzeichen).
- Eine einzigartige Sicherheitsfrage, deren Antwort nur Sie kennen (wird verwendet, wenn Sie Ihre Anmeldeinformationen in Zukunft zurücksetzen, wiederherstellen oder ändern möchten).
- Eine zweite Wiederherstellungs-E-Mail oder Mobiltelefonnummer (unterschiedliche zur ersten E-Mail), die wichtig ist, um den Schaden schnell zu begrenzen, falls Sie Opfer eines Cyberangriffs werden.
- Eine zweite Sicherheitsfrage und -antwort, die sowohl Ihnen als auch dem Softwareanbieter bekannt ist. Diese wird von einem Anbieter wie eviivo verwendet, um Ihre Identität zu überprüfen, wenn Sie uns per Telefon oder Videokonferenz kontaktieren.
- Eine eindeutige Eigenschafts-ID (eviivo nennt sie Kurzname).

Passwörter auswählen

Die schlimmsten (d. h. am häufigsten kompromittierten) Passwörter sind jene, die das Wort „Passwort“, die Anfangsbuchstaben einer Tastatur („Qwerty“ oder „Azerty“), einfache Zahlenreihen (z. B. „111111“ oder „1234567“) oder die Namen oder Geburtsdaten Ihrer Kinder, Ihres Ehepartners oder Lebensgefährten enthalten.

Die besten Passwörter sind mehr als 12 Zeichen lang und enthalten immer einen Großbuchstaben, eine Zahl und ein Sonderzeichen . Verwenden Sie anstelle eines Wortes einen **langen, einprägsamen Satz** . Verwenden Sie eine oder mehrere Zahlen, einen oder mehrere Großbuchstaben und ein oder mehrere Sonderzeichen (z. B. *_-$£).

Wenn Sie eviivo nutzen und der Hauptkontoinhaber sind, können Sie über die Benutzerverwaltung von eviivo anderen Benutzern und Mitarbeitern innerhalb Ihrer Organisation Zugriff gewähren. Klicken Sie dazu in der eviivo Suite oben rechts auf das Männchen-Symbol.

Öffentliche und freigegebene Postfächer

Um Überraschungen und Verstöße gegen die Cybersicherheit zu vermeiden, empfehlen wir Ihnen dringend, die folgenden Vorsichtsmaßnahmen zu treffen:

Vermeiden Sie unbedingt die Weitergabe von Anmeldedaten . Es ist immer ratsam, sicherzustellen, dass jeder Mitarbeiter über eigene Anmeldedaten verfügt. Die Nichtbeachtung dieser Daten ist die häufigste Ursache für Cyberbetrug im Gastgewerbe. Die gemeinsame Nutzung von Geräten und Anmeldedaten kann jedoch für die Rezeption oder das Housekeeping praktisch sein. Wenn Sie unbedingt gemeinsam genutzte Geräte und Anmeldedaten verwenden müssen, dann ...

Stellen Sie sicher, dass Gemeinsam genutzte Benutzeranmeldeinformationen erhalten nur minimale Zugriffsrechte . Personen, die Zahlungen, Kartenzahlungen oder persönliche Gästeinformationen bearbeiten, sollten dies nicht mit gemeinsam genutzten Anmeldeinformationen tun dürfen. Zu Ihrem eigenen Schutz benötigen Sie hier vollständige Nachvollziehbarkeit. Versuchen Sie, diese Informationen so wenig wie möglich im Blick zu behalten.

Geben Sie öffentlichen oder freigegebenen Postfächern keine höchsten Berechtigungsstufen. Öffentliche freigegebene Adressen (z. B. „info@yourplace.com“, „contact@yourplace.com“, „reservations@yourplace.com“, „bookings@yourplace.com“ oder „hallo@yourplace.com“) sollten NICHT an hochrangige Rollen wie Administratoren, Hauptkontoinhaber oder Manager vergeben werden. Die Missachtung dieses Hinweises ist der zweithäufigste Grund für Cyberbetrug im Gastgewerbe.

Trennen Sie Ihre geschäftliche E-Mail-Adresse und Ihr Passwort stets von privaten E-Mails für die private Kommunikation. Verwenden Sie separate E-Mail-Konten und Passwörter – und weisen Sie Ihre Mitarbeiter an, dies ebenfalls zu tun.

Öffentliche und gemeinsam genutzte Postfächer können aus folgenden Gründen viel leichter gehackt werden:

- Hacker nutzen veröffentlichte E-Mail-Adressen, um Gäste zur Herausgabe von Daten oder Kartendetails zu verleiten.
- Die Verwendung gemeinsam genutzter Postfächer oder Konten erhöht die Wahrscheinlichkeit eines Angriffs, da jeder einzelne Benutzer dazu verleitet werden kann, seine Anmeldeinformationen preiszugeben.
- Interner Betrug kann von Zeitarbeitern, Vertragsarbeitern, neuen Mitarbeitern oder externen Auftragnehmern begangen werden, die Sie nicht gut kennen

Teambasierte Mehrbenutzersicherheit

Eine teambasierte Sicherheitskonfiguration sollte Ihnen dabei helfen, eine Vielzahl von Rollen problemlos zu verwalten.

Nehmen wir beispielsweise an, dass drei verschiedene Personen dieselbe Sicherheitsstufe benötigen. Anstatt ein freigegebenes Postfach zu erstellen, können Sie Folgendes tun:

- Geben Sie jeder Person ihre eigenen, eindeutigen Anmeldedaten.
- Ordnen Sie alle drei Personen einem „Team“ zu.
- Weisen Sie die gewünschten Berechtigungen und Zugriffsrechte auf Immobilien dem „Team “ und nicht jedem Einzelnen zu.

Eine teambasierte Konfiguration lässt sich deutlich schneller und einfacher verwalten, wenn Mitarbeiter neu ins Unternehmen eintreten oder es verlassen. Da jeder Mitarbeiter seine eigenen Zugangsdaten behält, kann jede Transaktionsprüfung jede Aktion der Person zuordnen, die sie ausgeführt hat. Sollten die Zugangsdaten einer Person gestohlen oder kompromittiert werden, kann das restliche Team unbeeinträchtigt weiterarbeiten – während bei gemeinsam genutzten Zugangsdaten alle außer Gefecht gesetzt sind.

Phishing: die häufigste Angriffsform

Phishing ist der böswillige Versuch, Benutzer dazu zu bringen, ihre persönlichen Daten preiszugeben. Angreifer verleiten Benutzer häufig über schädliche Links, gefälschte Webseiten oder E-Mail-Anhänge, die Spyware oder Computerviren wie Trojaner enthalten, zur Preisgabe von Informationen.

Betrüger fälschen ständig die Logos und Anmeldeseiten seriöser Unternehmen. Sie sind äußerst geschickt darin geworden, nicht nur Logos, sondern auch Fotos, Videos und sogar Stimmen zu reproduzieren!

Die häufigsten Methoden, sich Zugang zu Konten zu verschaffen, sind E-Mails, mobile Benachrichtigungen, soziale Medien und Telefonanrufe. Angreifer geben sich möglicherweise als einer Ihrer Lieferanten, Ihre Bank, Ihr Telekommunikations- oder Softwareanbieter oder verschiedene Behörden aus.

Ein erfolgreicher Phishing-Versuch kann einem Angreifer Folgendes ermöglichen:

- Sammeln Sie Benutzernamen und Passwörter oder andere vertrauliche Informationen.
- Übernehmen Sie die Kontrolle über Ihren E-Mail-Posteingang, um ihn für böswillige Zwecke zu nutzen.
- Überzeugen Sie sich, Zahlungen zu ihrem Vorteil zu leisten.
- Sie dazu zu bringen, Geldbeträge auf ein nicht autorisiertes Konto einzuzahlen.
- Installieren Sie Spyware oder Malware, die es ihnen ermöglicht, Ihre Online-Aktivitäten zu überwachen.
- Beschädigen Sie Ihren Computer oder das Netzwerk Ihrer Organisation, verschlüsseln Sie Ihre Daten oder erpressen Sie Lösegeld.
- Erhalten Sie Zugriff auf geistiges Eigentum, Designs oder angemeldete Patente.

Der Rest dieses Handbuchs untersucht die raffinierten Methoden, mit denen Betrüger versuchen könnten, Sie auszutricksen – und wie Sie wachsam bleiben.

Spear-Phishing: Gefälschte Buchungsbestätigungen

Spear-Phishing ist eine gezielte Form des Phishing-Angriffs. Täter nutzen häufig öffentlich zugängliche Informationen im Internet, wie beispielsweise öffentliche E-Mail-Adressen auf Websites, um gefälschte Nachrichten zu erstellen und ihre Zielgruppe zum Klicken auf schädliche Links zu bewegen.

Ein Beispiel hierfür wäre die Erstellung gefälschter Buchungsbestätigungen, die Sie an Ihre Gäste senden. Betrüger können eine Original-Buchungsbestätigung erhalten, indem sie eine Buchung oder Bestellung bei Ihnen aufgeben und anschließend stornieren. Diese können sie dann verwenden, um eine gefälschte Bestätigung zu erstellen, die aussieht, als stamme sie von Ihnen (oder von eviivo, Airbnb, Booking.com usw.). Diese gefälschten Bestätigungsnachrichten verleiten ahnungslose Gäste dazu, persönliche Informationen, Anmeldeinformationen oder Karten-/Bankkontodaten preiszugeben oder sogar auf einen Link zu klicken, um auf das Bankkonto der Hacker einzuzahlen.

Eine gängige Methode bei Spear-Phishing-Angriffen besteht darin, Schadsoftware in scheinbar legitimen Anhängen und Links zu verstecken. Die Täter hoffen, dass diese heruntergeladen werden und so den Zielcomputer oder das Zielnetzwerk infizieren.

Darüber hinaus führen diese Schaltflächen und Links die Benutzer häufig auf gefälschte Anmeldeseiten von Websites, um vertrauliche oder persönliche Informationen abzufangen, die später für weitere Angriffe oder zum Erhalt privilegierten Zugriffs auf das Konto oder das Unternehmensnetzwerk des Ziels verwendet werden können.

Um sich zu schützen, **beachten Sie die folgenden Punkte, die Ihnen helfen, Fälschungen und Online-Phishing-Tricks zu erkennen:**

Klicken Sie im Feld „Von“ auf den Namen des Absenders des E-Mail-Headers, um die vollständige E-Mail-Adresse anzuzeigen. Sieht es aus wie eine legitime Adresse? Stimmt die Schreibweise hundertprozentig mit der offiziellen Firmen-E-Mail überein? Wenn nicht, handelt es sich um eine Fälschung.

Werden Sie in der E-Mail zu einer dringenden Handlung aufgefordert? Haben Sie mit einer solchen Aufforderung gerechnet? Die meisten Betrüger erzeugen ein falsches Gefühl der Dringlichkeit, indem sie behaupten, im Auftrag einer höheren Behörde (z. B. einer Bank, einer Institution, eines Unternehmens oder einer Führungskraft) zu handeln, und Ihnen dann mitteilen, dass Sie Ihre Kontodaten bestätigen müssen.

Enthält die E-Mail ungewöhnliche Rechtschreib- oder Grammatikfehler? Viele Betrüger agieren vom Ausland aus. Da sie offizielle Mitteilungen fälschen, fallen oft Grammatik- oder Rechtschreibfehler auf, die ein seriöses Unternehmen vermeiden würde.

Klicken Sie in Ihrer Browserleiste auf den Websitenamen und überprüfen Sie den ersten Teil der Websiteadresse. Beispielsweise beginnen legitime eviivo-Webseitenadressen (URL-Domänennamen) immer mit https://eviivo.com/ oder https://on.eviivo.com/ oder https://via.eviivo.com/

Überprüfen Sie die Schreibweise Ihrer E-Mail-Adresse oder Webseite stets sorgfältig . Schon ein falscher Buchstabe oder ein falsch platziertes Leerzeichen genügt, um Sie auf eine gefälschte Website oder Anmeldeseite umzuleiten. Beispiel: Bei einem kürzlichen Phishing-Versuch wurde „ **eviivo** “ durch „ **evlivo** “ ersetzt, während bei einem anderen Versuch „ **eviivo.com**“ statt „ eviivo.com“ stand – beides kaum erkennbare Rechtschreibfehler!

TOP TIPP

Wenn Sie eviivo nutzen, speichern Sie die URL der offiziellen eviivo-Anmeldeseite in Ihrem Browser und melden Sie sich immer von dort aus an. Dies verringert das Risiko, auf zweifelhafte Links in gefälschten E-Mails oder Anmeldeseiten zu klicken.

Walfang

Whaling ist ein Phishing-Angriff, der auf Benutzer abzielt, indem er sich als prominente Personen ausgibt – etwa als Unternehmensleiter, Führungskräfte, Prominente oder Mitarbeiter mit der Befugnis, Zugriff auf Systeme oder vertrauliche Informationen zu gewähren.

Das Ziel besteht darin, jemanden dazu zu verleiten, eine Aktion auszuführen oder Informationen preiszugeben, die dann für weitere Sicherheitsverletzungen verwendet werden können.

Whaling-Angriffe sind stark individualisiert und personalisiert. Sie enthalten häufig den Namen, die Berufsbezeichnung und andere relevante Informationen des Ziels (aus verschiedenen Quellen, wie etwa Social-Media-Profilen oder anderen Aspekten seines digitalen Fußabdrucks).

Whaling-Angreifer geben sich als jemand mit hoher Autorität oder Glaubwürdigkeit aus, um:

Bitten Sie Ihre Opfer um einen Gefallen oder dringende Hilfe. So können Nutzer, die ihrem Chef einen Gefallen tun wollen, am Ende Daten, Anmeldeinformationen oder sogar Geld weitergeben! Um dies zu verhindern, überprüfen Sie jede vom CEO, Vizepräsidenten oder Geschäftsführer eines Unternehmens unterzeichnete Korrespondenz dreifach.

Drohen Sie Nutzern, dass ihr Konto gesperrt wird oder gegen bestimmte Vorschriften verstößt, wenn sie ihre Anmeldedaten nicht umgehend erneut bestätigen. Nutzer werden dann auf eine gefälschte Webseite weitergeleitet, auf der Hacker lauern und ihre Anmeldedaten abgreifen.

Bieten Sie eine große Geldprämie an oder geben Sie vor, ein Benutzer habe Geld, das er einfordern müsse (z. B. einen Lottogewinn oder eine Erbschaft), um ihn dazu zu bewegen, seine Anmeldeinformationen und/oder Bank- oder Kartendaten preiszugeben.

Vishing

Vishing ist die Abkürzung für „Voice Phishing“. Es bedeutet schlicht Phishing über Telefonanrufe oder Sprachnachrichten.

Es könnte sich um jemanden handeln, der sich als Ihre Bank, ein Telekommunikationsunternehmen oder ein Anbieter wie eviivo ausgibt und Sie auffordert, vertrauliche persönliche oder Kontoinformationen zu bestätigen. Der Angreifer kann Sie auch auffordern, Ihren Bildschirm freizugeben, um Spyware zu installieren, die Ihre Tastatureingaben und Anmeldeinformationen erfasst.

Um zu überprüfen, ob die Person, die Sie anruft, wirklich von der Quelle ist, die sie vorgibt zu sein, stellen Sie ihr einfach Fragen, die nur Sie und die Quelle kennen. Wenn die Person beispielsweise behauptet, von eviivo zu sein, könnten Sie Folgendes verlangen:

- Die Referenznummer Ihrer letzten Buchung.
- Der Kurznamencode Ihrer Immobilie.
- Die (zweite) Sicherheitsfrage und -antwort, die nur Sie und eviivo teilen.

eviivo – oder jede andere seriöse Organisation – würde Sie niemals auf die im folgenden Skript beschriebene Weise kontaktieren:

Hallo, hier ist Candice von eviivo.

Wir rufen Sie an, weil wir vermuten, dass es auf Ihrem Konto verdächtige Aktivitäten gab. Wir müssen dringend überprüfen, ob alles in Ordnung ist. Kann ich Ihnen meinen Bildschirm zeigen?
Um auf Ihre Kontodaten zugreifen zu können, muss ich Sie bitten, Ihr Passwort erneut zu bestätigen, da wir es während des Anrufs zurücksetzen müssen. Könnten Sie Ihre Sicherheitsfrage und -antwort erneut bestätigen?

TOP TIPP

Tipps, um wachsam zu bleiben:

- **eviivo oder ein anderes seriöses Unternehmen wird Sie NIEMALS nach Ihrem Passwort fragen.** Sie werden zwar nach der Antwort auf eine Sicherheitsfrage gefragt, aber niemals nach der Sicherheitsfrage selbst.

- Wenn ein Anbieter Sie auffordert, Ihren Bildschirm freizugeben, sollte er dies über die offizielle Website-Adresse des Anbieters tun (z. B. eviivo.com).

- Bedenken Sie, dass alle Mitarbeiter Ihres Anbieters Ihr Konto einsehen und darauf zugreifen können. Stellen Sie ihnen daher nur eine Frage, die nur sie kennen (z. B. den Kurznamen Ihrer Unterkunft oder die Referenznummer Ihrer letzten Buchung in Ihrem Kalender). Ein Betrüger kennt diese Antworten nicht

Smishing

Smishing ist Phishing per SMS und Textnachrichten. Betrüger versenden Textnachrichten häufig mit dem Ziel,

- Persönliche oder vertrauliche Informationen vom Empfänger stehlen oder
- Infizieren Sie das Gerät des Empfängers mit Malware.

Betrüger können ebenso einfach ein WhatsApp-Konto fälschen, indem sie ein öffentlich verfügbares Foto einer Ihnen bekannten Person oder das Foto einer öffentlichen und/oder einflussreichen Person verwenden.

Social-Media-Phishing

Cyberkriminelle nutzen soziale Medien häufig für Angriffe, die auf den Diebstahl persönlicher Daten oder die Verbreitung von Malware abzielen. Täter geben sich in sozialen Medien typischerweise **als Freund, Kollege oder Familienmitglied aus**, um Sie zu Geldzahlungen zu verleiten. Manche Angriffe zielen darauf ab, Ihr Konto zu kapern, um anschließend alle Ihre Adressbuchkontakte, Verbindungen, Freunde oder Follower anzugreifen.

Diese Methode basiert häufig auf:

- Gefälschte Anzeigen, die Sie dazu verleiten können, auf einen Link zu klicken, der Sie auf eine gefälschte Anmeldeseite weiterleitet, die legitim aussieht – es aber nicht ist –, um Ihre Anmeldeinformationen oder Kontodetails abzufangen.
- Sie werden aufgefordert, eine Prämie, eine Strafe oder eine unrechtmäßige Gebühr zu zahlen.

Bei seriöser Social-Media-Kommunikation werden Sie immer zur offiziellen Website des Anbieters zurückgeleitet. Bei eviivo beginnt die in Ihrer Adressleiste angezeigte URL immer mit **https://eviivo.com/** oder **https://on.eviivo.com/**.


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

eviivo

FÜR WEITERE INFORMATIONEN KONTAKTIEREN SIE

SALES@EVIIVO.COM | +49 (0)32 221 094 701