eviivo

UNA GUIDA PER PROTEGGERE LA TUA LIQUIDITÀ:

PAGAMENTI, RIMBORSI E PREVENZIONE DELLE FRODI

Per proteggere la tua liquidità, devi adottare strategie operative pensate per:

- Automatizzare i pagamenti e gli incassi (invece di affidarti a promemoria manuali)
- Evitare i chargeback
- Prevenire le frodi

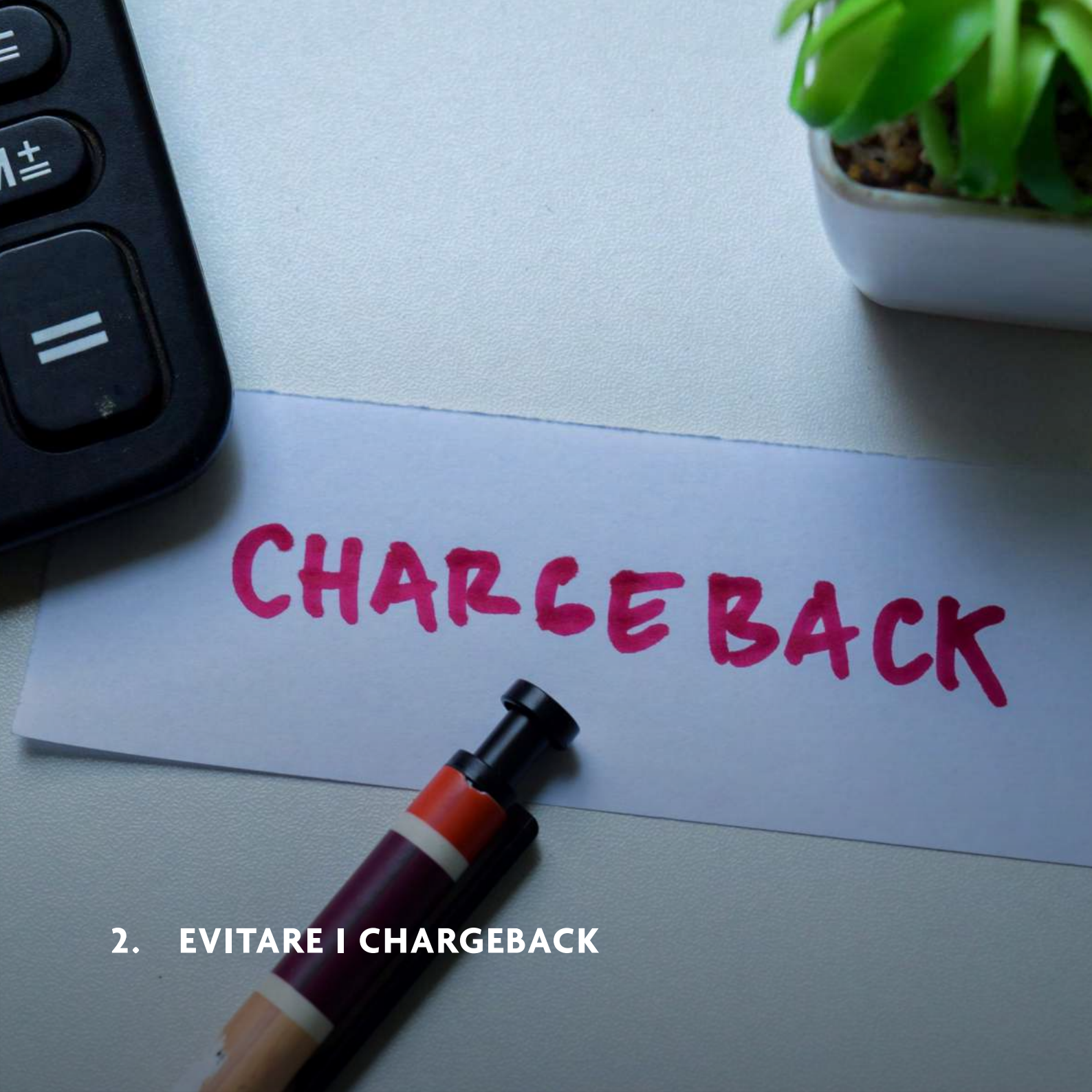
Questa guida offre consigli pratici da parte di esperti in tutte e tre le aree, pensati appositamente per albergatori, host e gestori di strutture. Continua a leggere per scoprire come iniziare a proteggere la tua liquidità.

1. AUTOMAZIONE DEI PAGAMENTI

Il modo migliore per ottimizzare la tua liquidità è utilizzare un PMS (sistema di gestione delle proprietà) che offra una piattaforma di pagamento completamente integrata.

Questo PMS deve essere in grado di:	eviivo Suite
Automatizzare l'addebito dei pagamenti in base a qualsiasi calendario definito dall'utente (tra la data di prenotazione e il check-out), senza intervento umano né errori.	✓
Confermare automaticamente qualsiasi pagamento.	✓
Inviare automaticamente un promemoria all'ospite prima della scadenza del pagamento..	✓
Determinare automaticamente se è dovuto un rimborso in caso di cancellazione della prenotazione.	✓
Elaborare automaticamente il rimborso corrispondente.	✓
Confermare automaticamente qualsiasi cancellazione e l'importo del rimborso.	✓
Bloccare automaticamente la consegna delle chiavi o dei codici di accesso se i pagamenti previsti non sono stati ricevuti.	✓
Pre-autorizzare automaticamente le carte (ad esempio, tramite comunicazione elettronica completa con la banca dell'ospite per [1] convalidare la carta e [2] verificare e autorizzare che ci siano fondi sufficienti sulla carta per coprire la prenotazione).	✓
Indicare automaticamente quale parte della prenotazione è stata addebitata tramite OTA, mostrandola all'host e sulla fattura dell'ospite, e indicando qualsiasi saldo residuo da riscuotere al check-in o successivamente.	✓

Questo PMS deve essere in grado di:	eviivo Suite
Indicare automaticamente se una carta di credito virtuale (VCC) fornita da un'OTA è disponibile e può essere addebitata.	✓
Fornire report semplici su depositi in sospeso; saldi di prenotazioni non pagate; pagamenti/transazioni in contanti per fonte di prenotazione e/o metodo di pagamento.	✓
Offrire una riconciliazione istantanea dei pagamenti OTA - tramite VCC o bonifico bancario diretto.	✓
Distinguere automaticamente tra una prenotazione OTA prepagata e un acconto, identificando quando un pagamento VCC può essere considerato come acconto e quando no.	✓
Generare o annullare automaticamente e con precisione le registrazioni contabili necessarie in base al momento dell'incasso o del rimborso (ad es. "contanti/clienti", "contanti/ricavi differiti", "contanti/ricavi e tasse").	✓



2. EVITARE I CHARGEBACK

Cosa sono i chargeback?

Un chargeback si verifica quando un cliente contesta un pagamento con carta e chiede alla propria banca di annullare la transazione. I clienti possono contattare la propria banca in qualsiasi momento e richiedere il rimborso dell'importo di una transazione effettuata con carta.
Normalmente, la banca dà ragione al cliente e gli restituisce l'importo. Il commerciante deve quindi dimostrare che:

1. L'addebito era giustificato.
2. L'ospite ha effettivamente autorizzato o firmato il pagamento con carta.

Quando ricevi un chargeback, puoi contestarlo, ma l'onere della prova ricade su di te.

- Se vinci la disputa, ti tieni il denaro.
- Se perdi, dovrai gestire il rimborso e probabilmente la banca ti addebiterà delle spese amministrative.

Buono a sapersi -> Nell'Unione Europea, i clienti possono richiedere un chargeback fino a 13 mesi dopo il primo addebito sulla loro carta. Al di fuori dell'UE, questo periodo si riduce a 70-120 giorni, a seconda della politica della banca.

Presenza del titolare della carta

Se il titolare della carta è presente durante l'elaborazione del pagamento, hai molte più possibilità di difenderti da eventuali chargeback. Si considera "presente" quando:

- Inserisce il proprio PIN segreto in un lettore di carte o in un bancomat.
- Paga online e gli viene richiesto di completare un'autenticazione di sicurezza 3DS (o Amex Safekey) in tempo reale. In questo caso, si richiede al cliente l'inserimento di una password OTP (one-time password), solitamente inviata via email o SMS.

Se il titolare non è presente, sei più esposto ai chargeback. Questo è spesso il caso quando i dati della carta ti vengono forniti da un'OTA, perché l'ospite non è più presente online quando elabori la carta nel PMS. Il pagamento potrebbe non fallire, ma sarà più a rischio di contestazioni.

Chargeback legittimi

Possono avvenire quando:

- L'ospite cancella per un motivo **reale, grave e imprevisto** (es. una "causa di forza maggiore" come il COVID-19, un disastro naturale, restrizioni di viaggio, ecc.) e non riceve alcun rimborso, specialmente se non ha un'assicurazione di viaggio.
- Gli ospiti temono che **l'alloggio o l'OTA non rimborsino la cancellazione**, soprattutto se il rimborso tarda troppo.

Chargeback fraudolenti possono verificarsi quando:

- Gli ospiti affermano di non aver soggiornato, anche se lo hanno fatto.
- Hai rimborsato l'ospite in contanti, ma questi chiede un secondo rimborso tramite chargeback.
- Gli ospiti decidono volontariamente di non soggiornare da te, ma vogliono evitare le penali da cancellazione tardiva.
- Un ospite soggiorna, ma la prenotazione è stata pagata con una carta rubata (e tu non hai preautorizzato/convalidato la carta).

Come posso evitare i chargeback?

Metti sempre in atto le seguenti raccomandazioni:

- **Chiedi agli ospiti di riconfermare il soggiorno** pochi giorni prima del check-in.

- **Registra correttamente l'ospite al suo arrivo**. Sempre:
  - Insisti perché l'ospite compili i dati di registrazione (via email/link).
  - Richiedi la carta nuovamente all'ospite e fai una verifica chip e PIN con un lettore di carte al momento della consegna delle chiavi (se offri un servizio di reception o accoglienza).
  - Clicca su "Check In" nel tuo PMS (es. eviivo Suite) per avere una traccia digitale.

- **Verifica che il titolare della carta e l'ospite siano la stessa persona**.
  - Se la carta è di un altro o il passaporto non corrisponde, chiedi una carta intestata all'ospite.
  - Se non può fornire un documento, addebita l'intero importo al check-in e/o chiedi al titolare della carta di confermare i dati e l'autorizzazione al pagamento via email.

- Se un ospite cancella telefonicamente, **annulla la prenotazione ed elabora subito il rimborso** o le penali (può essere automatizzato).

- **Rimborsa rapidamente se dovuto.** I ritardi spingono il cliente a rivolgersi alla banca.
- **Mantieni una traccia digitale.**
- **Addebita le penali di cancellazione appena scade il periodo gratuito,** idealmente prima del check-in.
- **Considera l'uso di un acconto non rimborsabile** (da pagare alla prenotazione o appena consentito dalla legge, ove previsto un periodo di riflessione di 24 ore). Assicurati di allineare le politiche di cancellazione e acconto.

Raccomandazioni sui pagamenti online

Se intendi addebitare i costi agli ospiti, anziché alle OTA, assicurati di **utilizzare un sistema di gestione delle prenotazioni e delle strutture ricettive con una funzione di automazione dei pagamenti completamente integrata e conforme alle norme PCI**. Si tratta di un sistema che consente di automatizzare l'intero processo di riscossione e rimborso dei pagamenti. Deve essere in grado di riscuotere un pagamento quando è dovuto e di elaborare un rimborso quando una prenotazione viene cancellata, senza alcun intervento manuale. Un sistema di questo tipo dovrebbe anche offrire:

- **Un'ampia scelta di processori di carte**, per evitare di essere vincolati a un'unica banca o processore di carte.
- **Diverse opzioni di configurazione**, come l'addebito tramite un link di pagamento, un sito web sicuro o un portale per gli ospiti; l'imposizione o la limitazione dei metodi di pagamento supportati; la selezione preventiva dei tipi di clienti che devono o non devono pagare con carta.

Il metodo migliore è quello di pre-autorizzare/elaborare una carta quando l'ospite è presente online, non appena si riceve una prenotazione. Pertanto, assicurati che il tuo sito web sia abilitato a 3DSecure/Safepay e che il tuo PMS sia in grado di inviare un link di pagamento all'ospite (via e-mail, SMS o WhatsApp), portandolo su una pagina sicura dove potrà elaborare la sua carta nel rispetto di tutti i requisiti 3DS. In entrambi i casi, la presenza online dell'ospite sulla pagina e il codice di sicurezza 3DS costituiscono una prova **inconfutabile della sua intenzione di pagare e della sua piena consapevolezza dei termini e delle condizioni al momento della prenotazione**.

Se decidi di elaborare la carta da solo, con un lettore di carte o direttamente in un PMS come eviivo Suite, e l'ospite non può più accettare di digitare un PIN segreto o di fornire un codice di sicurezza 3DS utilizzabile una sola volta, il rischio di chargeback è elevato. Anche se la carta viene elaborata con successo, il chargeback può avvenire giorni o settimane dopo e l'azienda può essere esposta a un rischio molto più elevato da parte di ospiti disonesti.

Come posso migliorare le mie possibilità di vincere una causa?

È necessario fornire una prova del soggiorno dell'ospite:

- **Fornire un report che mostri come e quando i pagamenti sono stati elaborati,** insieme a una copia di tutte le e-mail di pagamento/conferma della prenotazione inviate all'ospite che collegano il pagamento ai vostri termini e condizioni. (SUGGERIMENTO: rivedere i termini della propria politica di cancellazione/deposito. Assicurati che il tuo PMS includa automaticamente questi termini in tutte le e-mail di conferma della prenotazione, di pagamento o di cancellazione).

- **Conserva tutte le comunicazioni tra te e l'ospite.**

- **Allega una copia di qualsiasi estratto conto o fattura dell'ospite,** soprattutto se include un rimborso per il ritiro di contanti.

3. EVITA LE FRODI INFORMATICHE

Adotta misure preventive per evitare le frodi informatiche è essenziale per proteggere il tuo denaro.

Gli ultimi anni hanno portato con sé un aumento degli attacchi informatici di natura geopolitica, spingendo la maggior parte dei governi a incrementare le misure di sicurezza informatica e a spingere per requisiti di conformità più severi.

Il primo passo per proteggere la tua liquidità è quello di esaminare le misure di sicurezza messe in atto dai tuoi fornitori di software:	**eviivo Suite**
Quali controlli effettuano al momento dell'iscrizione di nuovi clienti? Effettuano controlli approfonditi sull'identità e sulle finanze per garantire che non permettano agli hacker di accedere alle loro piattaforme (se condividiate una piattaforma con altre aziende, vorrete che il vostro fornitore di piattaforme faccia tutto il possibile per garantire che siate in buona compagnia).	✓
Sono conformi agli standard PCI DSS (Payment Card Industry Data Security Standard), controllati e certificati in modo indipendente da Visa e Mastercard o da revisori designati, crittografano i dati delle carte ed eseguono scansioni regolari per impedirne la divulgazione?	✓
Forniscono solide funzioni di gestione degli utenti a un livello sufficientemente granulare (ad esempio, per funzione, per caratteristica, per attrezzatura e per gruppo di proprietà), consentendo agli utenti di visualizzare i dati di tutte le strutture consentite da un unico calendario di prenotazione?	✓
Forniscono firewall di base, rilevamento delle intrusioni, protezione anti-spam e anti-phishing, nonché funzionalità di backup e ripristino professionali?	✓
Dispongono di procedure per avvertirti quando uno dei tuoi clienti viene hackerato o subisce un attacco di phishing?	✓
Qual è la loro politica in materia di GDPR (General Data Protection Regulation) e/o DSA (Digital Services Act)?	✓

Il resto dipende da te. Devi orientare e formare il personale, implementare le migliori pratiche e, soprattutto, assicurarti che tutti siano all'erta. È anche una buona idea stipulare un'assicurazione contro gli attacchi informatici, se puoi permettertela.

Credenziali dei dipendenti

Uno dei modi più semplici ed efficaci per rafforzare le difese è garantire che ogni dipendente disponga di credenziali di accesso sicure e individuali. Ciascuna serie di credenziali dovrebbe includere quanto segue:

- Un indirizzo e-mail unico (il nome utente).
- Una password unica **che conosci solo tu** (più lunga è, meglio è: scegli un minimo di 12 caratteri, di cui almeno una lettera maiuscola, un numero e un carattere speciale).
- Una domanda di sicurezza unica di cui solo tu conosci la risposta (utilizzata se desideri resettare, recuperare o modificare le tue credenziali in futuro).
- Un secondo indirizzo e-mail o numero di cellulare di recupero (diverso dal primo), essenziale per contribuire a mitigare rapidamente eventuali danni nel caso in cui si sia vittima di un attacco informatico.
- Una seconda domanda e risposta di sicurezza, nota sia all'utente che al fornitore del software. Questa viene utilizzata da un fornitore come eviivo per verificare la tua identità quando ci contatti per telefono o in videoconferenza.
- Un identificativo univoco della struttura (eviivo lo chiama " shortname").

Scelta delle password

Le peggiori password (cioè quelle che hanno maggiori probabilità di essere compromesse) sono quelle che includono la parola “password”, le prime lettere di una tastiera (“Qwerty” o “Azerty”), serie numeriche di base (ad esempio ‘111111’ o “1234567”), o i nomi o le date di nascita dei vostri figli, del coniuge o del partner.

Le migliori password sono più lunghe di 12 caratteri e includono sempre una lettera maiuscola, un numero e un carattere speciale. Invece di una parola, usa una frase lunga e facile da ricordare. Includi uno o più numeri, una o più lettere maiuscole e uno o più caratteri speciali (ad esempio, *_-$£).

Se utilizzi eviivo e sei il titolare dell'account principale, puoi, a tua volta, concedere l'accesso ad altri utenti e dipendenti della tua organizzazione attraverso la schermata di gestione degli utenti di eviivo. È possibile accedervi facendo clic sull'icona dell'omino in alto a destra nella schermata di eviivo Suite.

Caselle postali pubbliche e condivise

Per evitare sorprese e violazioni della sicurezza informatica, ti consigliamo vivamente di prendere le seguenti precauzioni:

Evita assolutamente di condividere le credenziali. È sempre meglio assicurarsi che ogni dipendente abbia il proprio set di credenziali. Ignorare questo aspetto è la causa più frequente di frode informatica nel settore alberghiero. Tuttavia, la condivisione di dispositivi e login può essere comoda per le attività di reception o di housekeeping. Se proprio "devi" usare dispositivi e credenziali condivise, allora....

Assicurati che le credenziali utente condivise abbiano solo diritti di accesso minimi. Chiunque abbia a che fare con i pagamenti, l'elaborazione delle carte o le informazioni personali degli ospiti non dovrebbe poterlo fare utilizzando le credenziali condivise. Per la tua protezione, hai bisogno di una completa verificabilità. Cerca di avere il minor numero possibile di occhi su questo tipo di informazioni.

Non assegnare livelli massimi di autorizzazione alle caselle di posta elettronica pubbliche o condivise. Gli indirizzi pubblici condivisi (ad esempio "info@yourplace.com", "contact@yourplace.com", "reservations@yourplace.com", "bookings@yourplace.com" o "hello@yourplace.com") NON devono essere assegnati a ruoli di livello superiore come "Amministratore", titolare di un account primario o manager. Ignorare questo consiglio è la seconda ragione più comune di frode informatica nel settore dell'ospitalità.

Distingui sempre la tua e-mail/password professionale da qualsiasi e-mail personale utilizzata per comunicazioni private. Utilizza account di posta elettronica e password separati e usa indirizzi di posta elettronica e password diversi per le comunicazioni private.

Le caselle di posta elettronica pubbliche e condivise sono molto più facili da attaccare perché:

- Gli hacker utilizzano indirizzi e-mail pubblici per indurre gli ospiti a fornire dati o dettagli della carta.
- L'uso di caselle di posta elettronica o account condivisi aumenta le probabilità di attacco, poiché uno qualsiasi dei molteplici utenti può essere indotto a fornire le proprie credenziali.
- Le frodi interne possono essere commesse da lavoratori temporanei o a contratto, da nuovo personale o da appaltatori esterni che non conosci bene.

Sicurezza multiutente per team

Ad esempio, supponiamo che tre persone diverse abbiano bisogno dello stesso livello di sicurezza. Invece di creare una casella di posta condivisa, è possibile:

1. Assegnare a ogni persona le proprie credenziali di accesso.
2. Assegnare tutte e tre le persone a un “Team”.
3. Assegnare le autorizzazioni e i diritti di accesso alle proprietà desiderate al “Team” anziché a ciascun individuo.

Una configurazione basata sul team è molto più veloce e facile da gestire quando i dipendenti entrano o escono dall'azienda. Poiché ogni persona conserva le proprie credenziali, qualsiasi verifica delle transazioni collega ogni azione alla persona che l'ha eseguita. Pertanto, se le credenziali di una persona vengono rubate o violate, il resto del team può continuare a non essere coinvolto, mentre con le credenziali condivise tutti sono disabilitati.

Phishing: la forma di attacco più comune

Il phishing è l'atto illecito di tentare di ingannare gli utenti per indurli a rivelare le loro credenziali personali. Gli aggressori spesso inducono gli utenti a rivelare informazioni attraverso link dannosi, pagine web false o allegati di posta elettronica contenenti spyware o virus informatici come i trojan.

I criminali e i truffatori riproducono costantemente i loghi e le pagine di accesso di aziende affidabili. Sono molto abili nel riprodurre non solo i loghi, ma anche foto, video e persino voci.

I metodi più comuni per entrare negli account sono l'e-mail, le notifiche mobili, i social network e le telefonate. Gli aggressori possono impersonare uno dei fornitori della vostra azienda, la vostra banca, il vostro fornitore di telecomunicazioni o di software o varie autorità.

Un tentativo di phishing andato a buon fine può consentire a un aggressore:

- Raccogliere nomi utente e password o altre informazioni sensibili.
- Prendere il controllo della tua casella di posta elettronica per uso malevolo.
- Convincerti ad effettuare pagamenti per loro conto.
- Convincerti a depositare somme di denaro su un conto non autorizzato.
- Installare spyware o software dannosi che consentano di monitorare la tua attività online.
- Danneggiare il tuo computer o la rete dell'organizzazione, criptare i tuoi dati o chiedere un riscatto.
- Accedere a proprietà intellettuali, progetti o brevetti in corso di registrazione.

Il resto di questa guida illustra i modi intelligenti con cui i truffatori possono tentare di ingannarti e come mantenere la tua lucidità.

Spear phishing: false conferme di prenotazione

Lo spear phishing è una forma mirata di attacco di phishing. Gli autori spesso utilizzano informazioni pubblicamente disponibili su Internet, come gli indirizzi e-mail pubblici dei siti web, per creare messaggi falsi e incoraggiare il pubblico a cliccare su link dannosi.

Un esempio potrebbe essere la creazione di false conferme di prenotazione da inviare ai tuoi ospiti. I truffatori possono ottenere una conferma di prenotazione originale effettuando e poi annullando una prenotazione o un ordine presso di voi. Possono quindi utilizzarla per creare una conferma falsa che sembra provenire da te (o da eviivo, Airbnb, Booking.com, ecc.). Questi falsi messaggi di conferma inducono gli ignari ospiti a fornire informazioni personali, credenziali, dati di carte o conti bancari o addirittura a cliccare su un link per pagare sul conto bancario degli hacker.

Un metodo comune degli attacchi di phishing mirati consiste nel camuffare software dannosi in allegati e link apparentemente legittimi, che gli autori sperano vengano scaricati per infettare il computer o la rete di destinazione.

Inoltre, questi pulsanti e link spesso conducono gli utenti a pagine di login di siti web fasulli per acquisire informazioni sensibili o personali, che possono poi essere utilizzate per lanciare ulteriori attacchi o ottenere un accesso privilegiato all'account o alla rete organizzativa dell'obiettivo.

Per proteggerti, considera i seguenti punti per aiutarti a individuare i falsi e i trucchi di phishing online:

Fai clic sul nome del mittente nella casella "Da" dell'intestazione dell'e-mail per scoprire il suo indirizzo e-mail completo. Sembra un indirizzo legittimo? L'ortografia corrisponde al 100% all'e-mail ufficiale dell'azienda? In caso contrario, si tratta di un falso.

L'e-mail ti chiede di fare qualcosa di urgente e te lo aspettavi? La maggior parte dei truffatori crea un falso senso di urgenza, affermando di agire per conto di un'autorità superiore (ad esempio una banca, un'istituzione, un'azienda o un dirigente) e poi ti chiede di verificare i dati del tuo conto.

L'e-mail contiene errori ortografici o grammaticali insoliti? Molti criminali operano dall'estero. Poiché falsificano le notifiche ufficiali, spesso è possibile individuare errori grammaticali o di ortografia che un'azienda legittima eviterebbe.

Fai clic sul nome del sito web nella barra del browser e controlla la prima parte dell'indirizzo del sito. Ad esempio, gli indirizzi web legittimi di eviivo (nomi di dominio URL) iniziano sempre con https://eviivo.com/ o https://on.eviivo.com/ o https://via.eviivo.com/.

Controlla sempre con molta attenzione l'ortografia dell'indirizzo e-mail o della pagina web. Per reindirizzare l'utente a un sito web o a una pagina di login fasulli basta che un carattere sia diverso o che uno spazio sia al posto sbagliato. Esempio: un recente tentativo di phishing ha sostituito **"eviivo" con 'evlivo', mentre un altro diceva "eviivo. com" invece di "eviivo.com" - entrambi errori di ortografia appena percettibili!**

SUGGERIMENTO

Se sei un utente di eviivo, salva l'URL della pagina di login ufficiale di eviivo nel tuo browser e accedi sempre da lì. In questo modo si riduce il rischio di cliccare su link dubbi nelle e-mail o nelle pagine di login fasulle.

Whaling

Il whaling è un attacco di phishing che prende di mira gli utenti fingendo di essere persone di alto profilo, come dirigenti aziendali, senior manager, celebrità o personale con l'autorità di fornire accesso a sistemi o informazioni sensibili.

L'obiettivo è quello di indurre qualcuno a compiere un'azione o a rivelare informazioni che possono poi essere utilizzate per causare ulteriori violazioni della sicurezza.

Gli attacchi di whaling sono altamente personalizzati. Spesso incorporano il nome, il titolo di lavoro e altre informazioni rilevanti dell'obiettivo (ottenute da varie fonti, come i suoi profili sui social media o altri aspetti della sua impronta digitale).

Gli aggressori si spacciano per qualcuno con molta autorità o credibilità per:

Chiedendo ai loro obiettivi un favore o un aiuto urgente, gli utenti desiderosi di compiacere il loro capo finiscono per trasferire dati, credenziali o addirittura denaro! Per evitarlo, verifica tre volte ogni comunicazione ricevuta firmata dal direttore generale, dal vicepresidente o dall'amministratore delegato di un'azienda.

Minacciano gli utenti di chiudere il loro account o di infrangere alcune regole se non riconfermano immediatamente le loro credenziali. Gli utenti vengono quindi portati su un sito web falso dove gli hacker sono in attesa, pronti a catturare le loro credenziali.

Offrire una grossa ricompensa in denaro o fingere che l'utente abbia del denaro da reclamare (ad esempio, un premio della lotteria o un'eredità), per invogliarlo a fornire le proprie credenziali, i dati bancari o della carta.

Vishing

Vishing è l'abbreviazione di “voice phishing”. Significa semplicemente fare phishing tramite telefonate o messaggi vocali.

Potrebbe trattarsi di qualcuno che si spaccia per la tua banca, una società di telecomunicazioni o un provider come eviivo, e che ti chiede di confermare informazioni personali o account sensibili. L'aggressore potrebbe anche invitarti a condividere il tuo schermo per installare uno spyware che catturerà i tuoi tasti e le tue credenziali.

Per verificare se il chiamante proviene davvero dalla fonte che dichiara, è sufficiente porre domande che solo tu e quella fonte conoscete.

Ad esempio, se il chiamante afferma di provenire da eviivo, si possono fare domande su:
- Il numero di riferimento dell'ultima prenotazione effettuata.
- Il nome breve della proprietà.
- La (seconda) domanda e risposta di sicurezza che solo tu ed eviivo condividete.

eviivo - o qualsiasi altra organizzazione autentica - non ti contatterà mai nel modo descritto nello script sottostante:

Salve, sono Candice di eviivo,

La chiamiamo perché riteniamo che ci sia stata un'attività sospetta sul suo conto. È urgente verificare che tutto sia in ordine. Posso condividere il mio schermo con voi?

Ok, per poter accedere ai dettagli del suo account, devo chiederle di riconfermare la sua password, poiché dovremo reimpostarla durante la telefonata. Potrebbe riconfermare la sua domanda e risposta di sicurezza?

SUGGERIMENTO

Suggerimenti per stare all'erta:

- **eviivo, o qualsiasi altra azienda affidabile, non ti chiederà MAI di rivelare la tua password.** Anche se possono chiederti la risposta a una domanda di sicurezza, non ti chiederanno mai quale sia la domanda di sicurezza.

- Quando un fornitore ti chiede di condividere il tuo schermo, deve farlo dall'indirizzo ufficiale del sito web del fornitore (ad esempio, eviivo.com).

- Ricorda che qualsiasi dipendente del fornitore può vedere e accedere al tuo account; quindi, fai loro una domanda che solo loro potrebbero conoscere (ad esempio, il shortname della tua struttura, il riferimento della prenotazione più recente che è stata inserita nel tuo calendario). Un truffatore non conoscerà nessuna di queste risposte.

Smishing

Lo smishing è il phishing via SMS e messaggi di testo. I truffatori spesso inviano messaggi di testo con l'intento di:

- Rubare informazioni personali o riservate al destinatario, oppure
- infettare il dispositivo del destinatario con malware.

È altrettanto facile che i truffatori creino un account WhatsApp utilizzando una qualsiasi foto disponibile al pubblico di qualcuno che conoscono o la foto di una figura pubblica e/o di un'autorità.

Phishing sui social network

I criminali informatici utilizzano spesso i social network per effettuare attacchi finalizzati al furto di informazioni personali o alla diffusione di malware. Gli aggressori spesso si **fingono amici/colleghi/membri della famiglia** sui social network per indurvi a inviare loro del denaro. Alcuni attacchi tentano di dirottare il tuo account per lanciare attacchi successivi contro tutti i contatti, le connessioni, gli amici o i follower presenti nella tua rubrica.

Questo metodo si basa spesso su

- Annunci falsi che possono indurre l'utente a fare clic su un link che lo reindirizza a una pagina di accesso falsa che sembra legittima - ma non lo è - per acquisire le credenziali o i dettagli del conto.
- Ti chiedono di pagare una tassa, una penale o un costo illegittimo.

Le comunicazioni autentiche sui social media rimandano sempre all'URL del sito web ufficiale del venditore. Nel caso di eviivo, l'URL, visibile nella barra degli indirizzi, **inizia sempre con https://eviivo.com/ oppure https://on.eviivo.com/.**


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

eviivo

PER ULTERIORI INFORMAZIONI, CONTATTARE

SALES@EVIIVO.COM | +39 (0)694 801 487