eviivo

PROTÉGER VOTRE TRÉSORERIE :

Paiements, Oppositions et Prévention de la fraude

Pour sécuriser votre argent et votre trésorerie, vous devez adopter des stratégies opérationnelles capables de :

- Automatiser l'encaissement et le suivi des paiements (au lieu de relancer manuellement)
- Prévenir et éviter les oppositions
- Lutter efficacement contre la fraude.

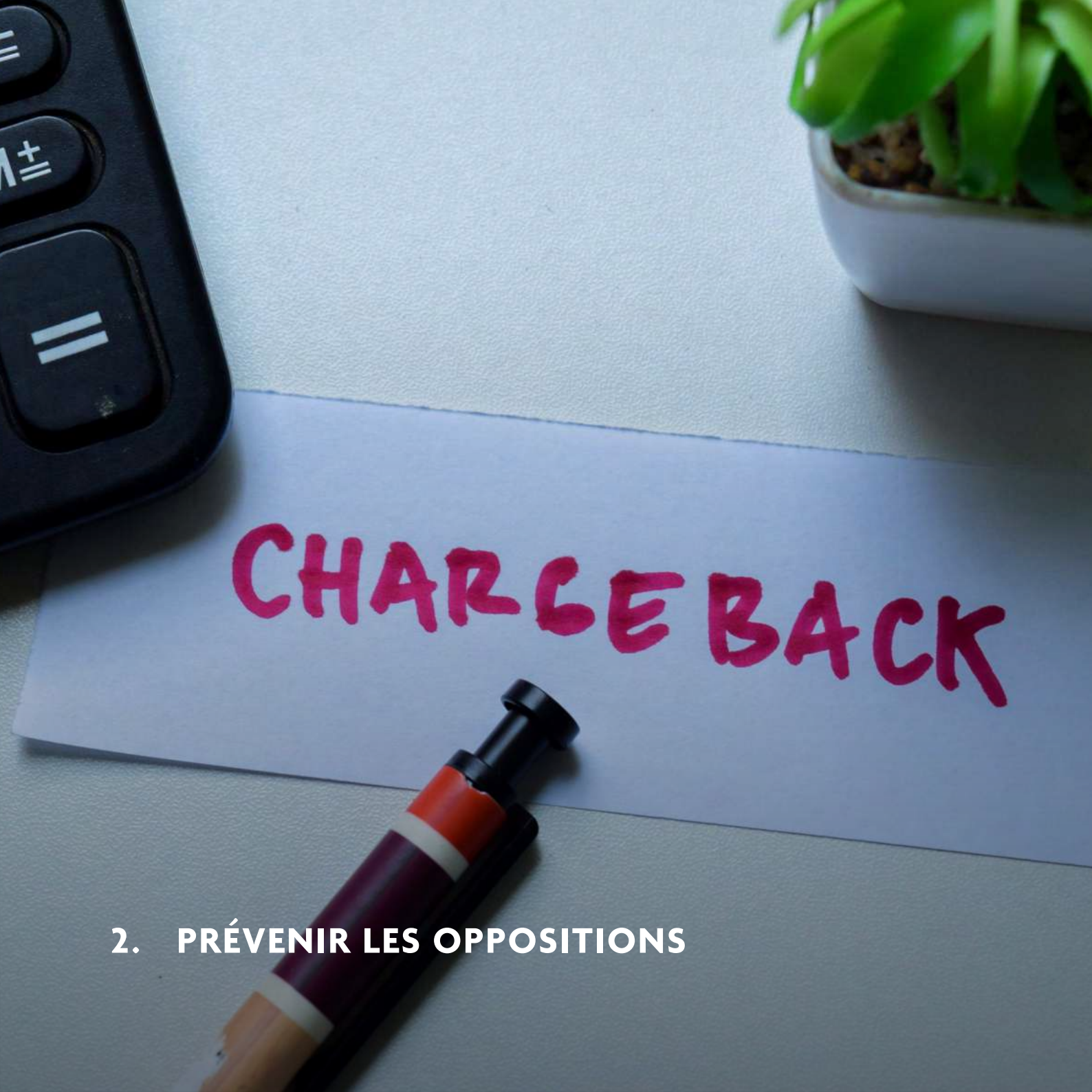
Ce guide fournit des conseils concrets et avisés, spécialement conçus pour les hôteliers, gérants de locations saisonnières et gestionnaires de biens immobiliers pour apprendre à protéger vos revenus et travailler l'esprit tranquille.

1. L'AUTOMATISATION DES PAIEMENTS

Vous avez tout à gagner à choisir un logiciel de gestion des réservations PMS qui comprend un système de paiement entièrement intégré et conforme aux normes sécuritaires PCI, au plus haut-niveau.

Votre système PMS est-il capable de... ?	eviivo Suite
Automatiser les paiements en fonction d'échéances définies par vous – de la réservation au check-out – sans besoin d'intervention manuelle.	✓
Confirmer tous vos paiements automatiquement.	✓
Relancer automatiquement vos clients pour les paiements tardifs, et les prévenir gentiment à l'avance de toute collecte à venir.	✓
Déterminer automatiquement si un remboursement est nécessaire en cas d'annulation.	✓
Confirmer, traiter et déterminer la valeur de tout remboursement automatiquement.	✓
Empêcher l'émission automatique de codes d'accès en cas d'impayé ou de caution non prélevée.	✓
Assurer la préautorisation automatique des réservations ou des cautions (appel direct à la banque du client pour valider la carte et la disponibilité réelle de fonds)	✓
Signaler si le paiement a été collecté par une OTA et indiquer s'il reste un montant à collecter clairement – à l'hébergeur et au client.	✓

Votre système PMS est-il capable de... ?	eviivo Suite
Indiquer la date précise à partir de laquelle il vous est possible de débiter une carte virtuelle transmise par un OTA.	✓
Fournir un tableau qui liste les acomptes ou les paiements à collecter, de même que les soldes impayés, pour toutes vos réservations, quelle qu'en soit la source et quelle que soit la méthode de paiement utilisée.	✓
Permettre la réconciliation et le rapprochement instantané des montants reversés par les OTAs – par carte virtuelle VCC ou par transfert bancaire.	✓
Savoir distinguer et traiter – automatiquement – les paiements qui peuvent de suite être enregistrés en chiffre d'affaires de ceux qui doivent être imputés en « produits constatés d'avance » jusqu'à à la date d'arrivée.	✓
Générer ou annuler automatiquement les écritures comptables associées aux encaissements ou remboursements, en fonction de leur nature (ex. : "encaissé / à recevoir", "encaissé / revenus différés", « encaissé / Taxes.).	✓



2. PRÉVENIR LES OPPOSITIONS

Comprendre les oppositions

Le droit d'opposition est un droit de protection des consommateurs. Un client peut faire opposition à un paiement par carte s'il pense que le paiement est frauduleux, non autorisé ou abusif. Un client peut contacter sa banque à tout moment pour faire opposition et obtenir le remboursement d'un paiement par carte.
Les banques qui ont un devoir de protection, prennent en général le parti du client qui fait opposition.
Il vous appartient alors de prouver que :

1. Le paiement était justifié et légitime.
2. La carte a bien été signée et autorisée par le client et sa banque.

Lorsqu'un client fait opposition, vous pouvez la contester, mais c'est à vous de prouver que le paiement était légitime, et il faut bien savoir que :

- Si vous gagnez le litige, vous conservez l'argent.
- Sinon, le client est remboursé, vous perdez la somme initialement versée et serez possiblement facturé de frais administratifs par votre banque ou prestataire de paiement.

Bon à savoir -> Dans l'Union Européenne, un client peut faie opposition jusqu'à 13 mois après le paiement initial. Hors UE, ce délai varie entre 70 et 120 jours, selon les conditions de la banque. Il est donc impératif d'adopter les mesures de sécurité nécessaires.

Présence du titulaire de carte

Lorsque le titulaire d'une carte est présent en ligne au moment du paiement, il est très rare que le client puisse faire opposition et s'il le fait, vous avez toutes les chances de votre côté pour. Un titulaire de carte est considéré "présent" quand :

- Il saisit un code secret ou PIN dans un lecteur de carte ou une billetterie.
- Il paye en ligne et fournit un code de sécurité à usage unique en temps réel (le code 3DS pour Visa et Mastercard et le code Safekey pour Amex). Pendant la session de paiement en ligne, le client est renvoyé vers sa banque qui lui demande un mot de passe et lui envoie en retour, par SMS ou email, un numéro de validation à usage unique que le client doit saisir pour confirmer son paiement par carte. Vérifiez que votre site internet soit bien capable de traiter les codes 3DS.

Lorsque le titulaire d'une carte n'est pas présent en ligne au moment où sa carte est imputée, le risque d'opposition est beaucoup plus élevé. C'est bien le cas lorsqu'une OTA vous transmet les coordonnées de carte bancaire du client : même si le client était présent au moment de réserver sur le site de l'agence OTA, il n'est plus considéré comme « présent » quelques instants plus tard lorsque vous essayez de débiter sa carte. Ce paiement ne va pas forcément être rejeté, il peut même être accepté par la banque, mais comme le client conserve un droit d'opposition pendant des semaines voire des mois, la banque peut encore en demander l'annulation. Pour vous protéger, implémentez nos recommandations au chapitre « Comment minimiser les oppositions »

Oppositions légitimes

- **Le client annule sa réservation pour une raison de force majeure sérieuse** (accident grave, décès, catastrophe naturelle) mais n'obtient aucune sympathie ni compréhension de la part de l'établissement, qui n'a aucune obligation de rembourser le client qui devrait plutôt avoir recours à son assurance voyage. Dans un soucis de maintenir une bonne réputation et contrer toute éventuelle fausse raison d'annulation, l'établissement préférera offrir un bon cadeau plutôt qu'un remboursement.
- **Le client a peur que l'OTA ou l'hébergeur ne le rembourse pas** ou prenne bien trop longtemps à effectuer un remboursement tout à fait légitime.

Certaines oppositions sont légitimes, d'autres ne le sont pas du tout :

Oppositions frauduleuses

- Le client affirme ne jamais avoir séjourné chez vous — alors qu'il est bel et bien venu.
- Vous avez remboursé le client en espèces plutôt que par carte. Il réclame un second remboursement via une opposition dans l'espoir d'être remboursé une seconde fois.
- Le client s'y prend trop tard pour annuler une réservation et fait
- Le client séjourne dans votre établissement, mais le séjour avait été prépayé par une autre personne à l'aide d'une carte bancaire volée ou périmée — que vous n'avez pas pré-autorisée ou revalidée à l'arrivée
- Le client conteste la qualité du service mais ne vous a jamais rien signalé pendant son séjour.

Comment prévenir les oppositions ?

Vous devriez toujours mettre en œuvre les recommandations suivantes pour éviter les oppositions :

- **Demander au client de reconfirmer l'heure d'arrivée** quelques jours avant le check-in.
- **Enregistrer le client à son arrivée.** Veillez à toujours :
  - Insister à ce que client remplisse un formulaire le jour même avant de lui donner les clés. (Même si cela est fait par SMS ou email.)
  - Exiger une pièce d'identité ou une copie/photo de celle-ci. (Elle peut être envoyée par e-mail ou message, mais pour plus de sécurité, demandez un appel vidéo où le client montre sa pièce d'identité à la caméra, ou utilisez un logiciel de reconnaissance faciale.)
  - Faire une deuxième validation ou préautorisation de la carte du client à l'arrivée avant de leur remettre la clé (si vous avez une réception).
  - Changer le statut de la réservation dans votre logiciel dès l'arrivée et la remise des clés pour garder une trace digitale du check-in dans votre PMS.
- **Confirmer que le titulaire de la carte est bien la personne qui séjourne chez vous.**
  - Si la carte enregistrée est émise au nom d'une autre personne ou que le passeport ne correspond pas, exigez une carte et une pièce d'identité au nom du client qui séjourne chez vous.
  - Si le client n'est pas capable de vous fournir une carte et une pièce d'identité, débitez la totalité du séjour sur la carte en votre possession dès que le client arrive (N'attendez pas le dernier jour !) et/ou assurez-vous que 100% de la réservation devienne non-remboursable à partir du jour d'arrivée.

Les meilleurs hôtels exigent un formulaire de paiement tiers signé, accompagné d'une photo scannée recto-verso de la carte bancaire, datée et signée par le titulaire.

- **Si un client annule par téléphone,** annulez la réservation et **traitez immédiatement les frais ou le remboursement** applicable (cette procédure peut être entièrement automatisée).

- **Si un client a droit à un remboursement total ou partiel, traitez-le sans délai.** Tout retard pourrait inciter le client à engager une opposition via sa banque, ce qui pourrait entrainer tout un tas de complications et vous coûter plus cher que le remboursement lui-même !

- **Gardez toujours une trace électronique de toutes vos actions et communications client**

- **Prélevez les frais d'annulation dès que ceux-ci deviennent non remboursables** mais si vous le faites avant le check-in, assurez-vous bien de prévenir le client en harmonisant vos conditions de paiement et vos conditions d'annulation et envoyez un petit rappel poli au client juste avant.

- **Envisagez d'appliquer un acompte non remboursable** (c'est-à-dire un montant dû au moment de la réservation, ou dès que légalement possible si un délai de rétractation de 24h vous est imposé). Cela nécessite d'harmoniser vos politiques d'annulation et de dépôt.

- **Demandez directement un feedback sur la qualité du séjour avant le départ**.

Recommandations propres aux paiements effectués en ligne

Si vous prenez des paiements en ligne directement sur votre propre site internet, plutôt que via les sites de réservation des agences OTA, il faut un **moteur de réservation totalement intégré et conforme aux normes PCI-DSS** (Payment Card Industry Data Security Standard / Standard de Sécurisation de l'Industrie des paiements par carte) et 3DS (3 Dimensional Security / Sécurité sur 3 Dimensions).

Un bon moteur de réservation doit être entièrement intégré à votre PMS et à votre Channel Manager. Jamais séparé. Il doit être capable d'automatiser la totalité du processus de collecte/remboursement dans tous les cas de figure – à savoir :

- Prendre le paiement dès qu'une réservation est prise ou qu'un acompte est dû et effectuer un remboursement dès l'instant où une réservation est annulée – sans intervention humaine et sans erreur.
- Offrir un grand choix de connexion à des banques et prestataires de services de paiement pour éviter que vous soyez pris au piège et vous donner l'option de pouvoir changer de fournisseur aisément.
- Offrir plusieurs options de traitement : liens de paiement sécurisés envoyés per email automatiquement ou au besoin, portail de paiement sécurisé sur votre site, la capacité d'imposer ou de réduire les options de paiement par type de client.

Il est toujours préférable d'assurer que le client soit présent en ligne au moment du paiement. Votre PMS doit de ce fait être capable d'inviter automatiquement vos clients à revenir sur votre propre site internet afin de visualiser, reconfirmer et solder leur réservation, quelle qu'en soit la source (même s'ils ont réservé via une OTA) et donc de soumettre, préautoriser ou débiter leur carte en mode sécurisé 3DS - **preuve irréfutable qu'ils avaient bien l'intention de payer et avaient connaissance de vos conditions générales au moment de la réservation.**

Si vous choisissez de traiter une carte lorsque le client n'est pas présent en ligne – par le biais d'un lecteur de carte ou d'un logiciel comme eviivo Suite – le client ne sera pas invité à fournir mot de passe secret et un code unique 3DS. Vous vous exposez alors à un risque plus élevé. Même si la transaction est acceptée quand vous traitez la carte, le client a encore des semaines pour faire opposition et obtenir un remboursement. Les clients abusifs ou malveillants utilisent cette loi de protection des consommateurs pour déclencher des oppositions illégitimes. Plutôt que de traiter la carte vous-même, il est toujours préférable **d'envoyer un lien de paiement 3DS à ces clients pour les forcer à traiter la carte en ligne et donc à être présent et accepter vos conditions.**

Mettre tous les atouts de votre côté pour contester une opposition

Pour contester une opposition vous devez **fournir des preuves** que le client a bien séjourné dans votre établissement ou qu'il a bel et bien accepté vos conditions d'annulation. Voici ce que vous devez présenter:

- Une **copie du passeport, de la pièce d'identité ou de la carte bancaire** (recto et verso).
- **Un rapport détaillant comment et quand les paiements ont été traités**, accompagné d'une copie de l'email de confirmation de paiement ou de réservation envoyé au client, liant clairement le paiement à vos conditions générales. (ASTUCE : Prenez le temps de revoir les termes de votre politique d'annulation et de dépôt. Assurez-vous que votre PMS les insère automatiquement dans tous les e-mails de confirmation de réservation, de paiement ou d'annulation).
- **Une copie de toute facture ou relevé de compte, l'imprimer et la faire contresigner par le client au check-out (même électroniquement avant de rembourser une caution par exemple).**

3. PRÉVENIR LA FRAUDE EN LIGNE

Protéger votre activité contre la fraude en ligne.

Alors que les gouvernements amplifient la lutte contre la fraude et exigent de plus en plus de conformité aux standards de sécurité – l'IA n'a fait qu'accroître la capacité des acteurs malveillants à créer des « faux ». **Il faut donc rester vigilant !**

Commencez par choisir un logiciel professionnel conforme aux normes de sécurité plutôt qu'une solution jeune, non établie et poreuse :	**eviivo Suite**
Quelles sont les procédures suivies par votre éditeur de logiciel? Vérifie-t-il **l'identité des hébergeurs** qui partagent leur plateforme avec vous – y compris pièces d'identité et contrôle d'identité bancaire pour s'assurer qu'il n'y ai pas d'acteurs malveillants partageant le système avec vous ?	✓
Est-il nativement conforme à la norme PCI DSS (Payment Card Industry Data Security Standard) ? Est-il audité et certifié de manière indépendante par Visa, Mastercard ou des auditeurs agréés ? Chiffre-t-il les données de carte et effectue-t-il des scans réguliers pour prévenir toute fuite ?	✓
Vous offre-t-il un **système avancé de contrôle des accès** utilisateurs et permissions avec un niveau de granularité suffisant – par utilisateur, par rôle, par équipe, par hébergement) tout en permettant la gestion de multiples propriétés sur un seul calendrier ?	✓
A-t-il mis en place un pare-feu, un détecteur d'intrusions, un anti-spam et anti-phishing ainsi qu'un dispositif de sauvegarde et rétablissement opérationnel ?	✓
A-t-il mis en place un **système d'alerte** pour prévenir tous les utilisateurs dès que l'un d'entre eux est soumis à une invitation malicieuse ?	✓
Quelle est sa politique en matière de RGPD (Règlement général sur la protection des données) et/ou de DSA (Digital Services Act) ?	✓

C'est une conversation qu'il faut absolument avoir avec votre éditeur.
Pour le reste, tout dépend de vous. En tant que propriétaire ou chef d'entreprise, veillez à ce que vos équipes restent vigilantes et averties ! Et par prudence, souscrivez aux options cybersécurité proposées par votre assureur.

Les identifiants utilisateurs

La grande majorité des brèches et sinistres informatiques sont causés par un manque de prudence de la part des utilisateurs.
La plus simple — et la plus efficace — des méthodes de protection consiste à renforcer vos pratiques internes concernant la gestion des identifiants et des mots de passe. Voici la liste des consignes à suivre :

- Chaque utilisateur reçoit une adresse email et un identifiant qui lui sont unique
- Un mot de passe n'est connu que de l'utilisateur qui l'a créé (il n'est jamais partagé et plus il est long, mieux c'est)
- Une question de sécurité dont la réponse n'est connue que de l'utilisateur qui l'a spécifiée (utilisée pour recouvrir un mot de passe)
- Une adresse email de secours ou un numéro de mobile secondaire (différent de l'email principal), est essentiel pour réagir rapidement en cas de cyberattaque
- Une deuxième question de sécurité (différente de la première) doit être partagée avec votre prestataire de service (bancaire ou logiciel) pour leur permettre de vérifier votre identité en ligne lorsque vous les contactez par téléphone ou visioconférence
- Un identifiant de propriété unique (appelé shortname chez eviivo)

Choisir un mot de passe

Les pires (et donc les plus facilement piratables) mots de passe sont ceux qui contiennent le mot "password", les premières lettres d'un clavier ("Qwerty" ou "Azerty"), des séries de chiffres simples ("111111", "1234567"), ou encore les noms ou dates de naissance de vos enfants, conjoint(e) ou partenaire.

Les meilleurs mots de passe font plus de **12 caractères,** incluent **au moins une majuscule, un chiffre, et un caractère spécial,** et ne sont **pas des mots,** mais plutôt **des phrases mémorables.** Par exemple, une **phrase longue et facile à retenir,** contenant un ou plusieurs chiffres, majuscules et caractères spéciaux **(comme *_-$£),** offre une sécurité bien supérieure.

Si vous êtes le titulaire principal ou l'administrateur de votre compte, vous pouvez dès lors assigner un profil utilisateur à chacun des membres de votre équipe. Choisissez un logiciel qui permet de définir les permissions nécessaires avec beaucoup de granularité, en particulier au niveau de :

- Vos utilisateurs (internes ou externes)
- Des rôles exacts dont vous avez besoin
- La gestion des permissions par équipe pour gagner du temps
- La gestion des permissions par portefeuille

Boîtes mail publiques et partagées

Pour éviter les mauvaises surprises et les brèches, considérez sérieusement les précautions suivantes :

Évitez à tout prix de partager des identifiants. Il est toujours préférable que chaque employé dispose de ses propres identifiants. Ne pas respecter cette règle est la cause la plus fréquente de fraude informatique dans le secteur de l'hôtellerie. Cependant, le partage de dispositifs ou de connexions peut être pratique à la réception ou pour le personnel d'entretien. Si vous devez absolument utiliser des appareils ou des identifiants partagés, alors...

Assurez-vous que ces identifiants partagés n'aient que des droits d'accès minimaux. Toute personne traitant des paiements, des cartes bancaires ou des données personnelles de clients ne doit jamais utiliser d'identifiants partagés. Pour votre propre protection, vous devez pouvoir auditer chaque action, et limiter au maximum l'accès à ces informations sensibles.

Ne donnez pas de permissions stratégiques et majeures aux boites de réception publiques ou partagées. Réduisez au maximum les accès et permissions données à des identifiants basés sur des adresses publiques de type : info@... Reservations@... Hello@ Contact@ etc. La deuxième cause de brèche informatique la plus prévalente passe par des adresses publiques ou partagées nanties de permissions d'administrateur de compte ou de gestion des paiements.

Différenciez toujours les identifiants utilisés pour votre activité professionnelle de ceux qui sont utilisés à titre personnel ! Toute communication privée ou personnelle doit se faire avec un identifiant personnel. Un grand nombre d'employés utilisent internet pour les réseaux sociaux – interdisez clairement l'utilisation des identifiants professionnels que vous leur donnez dans ces contextes !

Les boites de réception publiques et partagées sont bien plus faciles à pirater :

- Les acteurs malveillants vont les utiliser pour créer des « faux » et falsifier des messages en votre nom pour collecter les cartes bancaires de clients inavertis
- Si un des utilisateurs qui partagent le même identifiant se fait berner par un acteur malveillant, ce sont tous les utilisateurs qui sont affectés
- Si une fraude est commise en interne par un employé temporaire, vous n'avez aucune trace d'audit individuelle et donc aucun recours.

Sécurité multi-utilisateurs

Si votre logiciel permet de gérer les accès par équipe vous gagnerez du temps tout en renforçant votre sécurité en ligne.

Imaginez trois collègues qui ont le même type de travail et ont besoin du même niveau de permissions. Plutôt que de créer un identifiant partagé, il est préférable de :

a. Assigner un identifiant unique à chaque personne
b. Les assigner tous les 3 à une équipe
c. Définir les permissions une fois seulement, au niveau de l'équipe

Cette approche est beaucoup plus rapide et facile à gérer lorsque des employés rejoignent ou quittent votre entreprise. Les actions de chaque employé sont toujours auditées, vous savez qui est responsable de quelle transaction à tout moment. Et si l'une de ces personnes perd son identifiant ou se fait piéger par un acteur malveillant, le reste l'équipe n'est pas du tout affecté. Un employé arrive, un autre part, retirer le ou ajouter le à l'équipe, pas besoin de changer tous vos mots de passe et identifiants.

Hameçonnage (phishing) : la forme d'attaque la plus courante

Le phishing, ou hameçonnage, est un acte malveillant visant à tromper les utilisateurs pour leur faire révéler leurs identifiants personnels. Les attaquants incitent souvent les utilisateurs à transmettre des informations via des liens frauduleux, de fausses pages web ou des pièces jointes à des e-mails contenant des logiciels espions ou des virus informatiques.

Les fraudeurs imitent constamment les logos et pages de connexion d'entreprises réputées. Ils sont devenus extrêmement habiles à reproduire non seulement des logos, mais aussi des photos, vidéos, voire des voix . Les méthodes et tentatives les plus courantes prennent la forme de notification officielle par email vous demandant de confirmer vos identifiants sous peine de fermeture de compte ou « pour votre sécurité ». Une société ou institution réputée ne vous demandera jamais de confirmer votre identifiant et mot de passe par email.

Une attaque "phishing" réussie permet à un acteur malveillant de :

- Collecter votre identifiant et mot de passe ou autres données personnelles
- Prendre le contrôle de votre boite aux lettres ou de votre ordinateur
- Vous convaincre de faire un paiement sur un compte frauduleux ou non autorisé
- Installer un programme espion (spyware) ou malicieux (malware) qui leur permet d'enregistrer tout ce que vous faites ou saisissez sur votre ordinateur ou smartphone
- Entraver le fonctionnement de votre ordinateur ou du réseau de votre société et/ou de rendre toutes vos données inutilisables sous peine du paiement d'une rançon
- Gagnez accès à vos secrets, et votre propriété intellectuelle

Le reste de ce guide vous donne des exemples plus détaillés du type d'attaque auxquelles vous pouvez vous attendre et explique comment les éviter.

Hameçonnage ciblé (spear phishing) : fausses confirmations de réservation

Le spear phishing est une forme ciblée d'attaque par hameçonnage. Les fraudeurs utilisent souvent des informations accessibles publiquement sur Internet (comme des adresses e-mail présentes sur les sites web) pour créer **de faux messages** et inciter leurs cibles à cliquer sur des **liens malveillants**.

Un exemple courant consiste à créer **de fausses confirmations de réservation** envoyées à vos clients. Les fraudeurs peuvent obtenir un véritable email de confirmation en effectuant, puis annulant, une réservation ou commande auprès de vous. Ils utilisent ensuite ce modèle pour fabriquer une fausse confirmation qui semble provenir de vous (ou d'eviivo, Airbnb, Booking.com, etc.).

Ces faux messages peuvent **tromper vos clients**, les incitant à fournir des informations personnelles, leurs identifiants de connexion, des coordonnées bancaires ou de carte ou même à cliquer sur un **lien de paiement** menant au compte du pirate.

Une méthode fréquente consiste à **dissimuler un logiciel malveillant dans une pièce jointe ou un lien légitime en apparence**, dans l'espoir que la victime télécharge le fichier ou visite le site, infectant ainsi son ordinateur ou le réseau.
De plus, **ces liens redirigent souvent vers de fausses pages de connexion**, dans le but de capturer des informations sensibles. Celles-ci peuvent ensuite servir à d'autres attaques ou à obtenir un accès privilégié à un compte ou au réseau de l'entreprise.

Que faire pour vous protéger ?

Cliquez toujours sur le nom de l'expéditeur (Le boitier "De" dans l'en-tête du courriel) pour révéler l'adresse exacte de l'expéditeur. S'agit-il d'une adresse légitime ? Est-elle épelée correctement, caractère par caractère ? Sinon, c'est un faux !

Urgence : Est-ce que cet email vous **invite à cliquer, ou d'agir en urgence**? Avez-vous une raison d'attendre ce type de demande ou est-ce une surprise ? La plupart des communications malveillantes créent un faux sentiment d'urgence, alors que les sociétés réputées vous donnent plusieurs rappels polis et le temps de prendre action. Au moindre doute, appelez votre banque ou la société pour vérifier.

Orthographe. Est-ce que le message contient des fautes d'orthographe ou de style ? De nombreux fraudeurs opèrent depuis l'étranger, et leurs traductions trahissent souvent leur origine. Quant aux adresses email et internet, **les « faux » contiennent toujours un caractère erroné dans l'adresse mail ou dans l'adresse du site internet.**

Domaine internet. Cliquez sur l'adresse du site dans la barre de votre navigateur. Le mot qui apparait après https:// ou après www doit toujours être épelé correctement – comparez le au site de votre banque ou fournisseur. Exemple : eviivo utilisent 3 adresses officielles, toujours **https://eviivo.com/ ou https://on.eviivo.com/ ou https://via.eviivo.com/**

Vérifiez toujours l'adresse de l'expéditeur ou de la page internet caractère par caractère. Si vous ne la reconnaissez pas ne cliquez pas. Il suffit d'une seule différence de caractère pour vous tromper. Une tentative récente utilisait « evlivo.com » au lieu de « eviivo.com », ou encore « eviivo. com » avec un espace en trop — des différences très discrètes mais dangereuses.

TOP TIP

Si vous êtes utilisateur d'eviivo, enregistrez l'adresse web officielle de la page de connexion dans vos favoris. Connectez-vous uniquement depuis ce lien. Cela réduit considérablement les risques de cliquer sur des liens frauduleux reçus par e-mail.

Harponnage (Whaling)

Le whaling est une forme d'hameçonnage qui cible spécifiquement des personnes en prétendant venir de quelqu'un de célèbre ou d'important (d'où le mot Whaling qui veut dire baleine en Anglais) – tel qu'un cadre supérieur d'une société prestataire avec laquelle vous travaillez – ou en se faisant passer pour des personnes ayant l'autorité de discuter votre compte ou vos droits d'accès à un réseau ou à des informations sensibles.

Leur but est de vous piéger pour vous faire divulguer vos identifiants, vos données personnelles ou vos coordonnées bancaires afin de pouvoir les utiliser par la suite à des fins malveillantes, ou bien tout simplement de vous faire prendre action (par exemple faire un virement d'urgence).

Les attaques de type whaling sont hautement personnalisées et adaptées à leur cible. Elles incluent souvent le nom de la cible, son poste ainsi que d'autres données collectées sur ses profils sociaux ou sa présence numérique.

Les attaques “baleines” prétendent venir d’une personne célèbre ou importante. Que faire pour vous protéger ?

Il s’agit d’un abus de confiance qui joue sur le fait que la personne ciblée par l’arnaqueur fera tout pour faire plaisir à son patron ou répondre aux demandes d’une personne célèbre qu’elle admire. Ces demandes consistent à faire un virement de secours pour les dépanner, ou d’aller acheter des cartes de jeux ou bons cadeaux. Pour vous protéger vérifiez caractère par caractère l’adresse de l’expéditeur ou appelez la personne impliquée avant de cliquer.

Les menaces de fermeture de compte, de pénalité ou de répercussions juridiques sont un moyen souvent utilisé pour encourager le partage de données ou un paiement frauduleux. N'agissez jamais sous la panique, vérifiez caractère par caractère l’adresse de l’expéditeur ou l’adresse du site internet ou contactez l’autorité concernée pour vérifier.

Une autre tactique consiste à prétendre que vous avez gagné un prix ou une récompense ou que vous avez hérité d’un parent lointain. On vous demande alors des données personnelles et coordonnées bancaires afin de pouvoir vous payer. Une fois de plus, ne cliquez jamais sans contrôler l’origine de la demande et l’adresse exacte de l’expéditeur ou de la page internet.

Vishing – par la voix

Vishing est l'abréviation de « voice phishing », autrement dit hameçonnage vocal. Cela désigne les tentatives de fraude par appels téléphoniques ou messages vocaux.

Vous recevez un appel téléphonique d'une personne se faisant passer pour votre banque, votre opérateur téléphonique, ou un fournisseur comme eviivo, vous demandant de confirmer des informations personnelles ou confidentielles. L'attaquant peut aussi vous inviter à partager votre écran, afin d'installer un logiciel espion capable de capturer vos frappes au clavier et vos identifiants.

Ne vous y trompez pas. En général, lorsqu'un prestataire vous appelle c'est en réponse à une demande de votre part – vous vous y attendez, il s'agit rarement d'un appel inopiné. Dans tous les cas de figure, c'est au prestataire de vous démontrer qu'il s'agit bien d'eux, ce qui est facile à établir si c'est vous qui leur posez des questions sur l'activité de votre compte et non pas l'inverse. Par exemple :

- La référence de la dernière réservation ou du dernier paiement que vous avez traité.
- L'identifiant de votre compte (numéro unique) et non pas votre identifiant personnel
  Exemple d'appel frauduleux qui ne viendrait jamais d'un vrai prestataire :

> *Bonjour, je vous appelle de la part du service financier de eviivo,*
>
> *Nous pensons qu'il y a une activité suspicieuse sur votre compte et j'ai besoin de vérifier certains détails de toute urgence. Pouvez-vous reconfirmer votre identifiant et mot de passe ?*
>
> *Etes-vous en ligne et pouvez-vous me donner accès à votre compte pour vérifier que tout est en ordre ?*

TOP TIP

Comment rester vigilant :

- **eviivo, comme toute autre entreprise sérieuse, NE vous demandera JAMAIS de divulguer votre mot de passe**. On peut vous demander de répondre à une question de sécurité pour vérifier votre identité mais on ne vous demandera jamais de confirmer quelle est la question convenue. Un prestataire peut vous envoyer un code à usage unique pour valider un accès, mais il ne vous demandera jamais de dévoiler votre mot de passe.

- Lorsqu'un fournisseur vous demande de partager votre écran, fermez toutes les fenêtres qui contiennent des coordonnées bancaires, mots de passe ou données confidentielles et ne leur permettez jamais de prendre le contrôle de votre souris ou de votre clavier ou de votre machine. Un partage d'écran permet à un prestataire de vous assister ou de vous montrer comment faire quelque chose mais il ne permet en aucun cas au prestataire de contrôler votre ordinateur sans que vous le permettiez. Ne cliquez donc jamais pour concéder le contrôle de votre ordinateur ou de votre souris à un tiers.

- Seuls vous et votre prestataire sont à même de voir l'activité sur votre compte. Donc, une façon simple de différencier un prestataire légitime d'un acteur malveillant est de demander au prestataire (une fois qu'il a établi votre identité) de confirmer les dernières transactions passées sur votre compte. Un acteur malveillant ne saura pas répondre à cette question.

Smishing – par SMS

Le Smishing, c'est le phishing par SMS ou « textos ». Le but de ces attaques consiste à:

- Obtenir des informations personnelles ou confidentielles sur vous (souvent pour préparer une autre attaque plus tard)
- Infecter votre PC, tablette ou portable avec un virus ou un programme de rançon ou d'enregistrement d'activité (souvent pour préparer une autre attaque plus tard).

Les fraudeurs peuvent tout aussi bien usurper un compte WhatsApp, en utilisant n'importe quelle photo publique d'une personne que vous connaissez, ou la photo d'une personnalité publique ou faisant autorité.

Ne vous laissez pas piéger et vérifiez – il y a toujours au moins un caractère de différence sur l'adresse email, l'adresse de la page internet ou une différence sur le numéro utilisé pour l'envoi d'un message SMS ou WhatsApp

Phishing sur les réseaux sociaux

Les cybercriminels utilisent souvent les réseaux sociaux pour mener des attaques visant à voler des informations personnelles ou à diffuser des logiciels malveillants. Les auteurs se font généralement passer pour un ami, un collègue ou un membre de la famille sur les réseaux sociaux afin de vous tromper pour leur envoyer de l'argent. Certaines attaques visent à pirater votre compte pour lancer des attaques contre tous vos contacts, amis, connexions ou abonnés.

Les attaques sur réseaux sociaux se reposent en général sur :

- Des publicités trompe-l'œil et artificielles qui vous incitent à cliquer sur une page d'accès falsifiée afin de capturer votre identifiant et mot de passe.
- Des demandes urgentes pour le paiement d'une pénalité, d'une contribution, d'un prêt ou de frais non-légitimes ou de faux frais d'annulation.

Lorsqu'un prestataire vous envoie une communication sur un réseau social, il vous redirige toujours sur son site officiel. Une fois de plus, soyez prudent en vérifiant bien l'adresse de toute page internet avant de cliquer !
Sauvegardez l'adresse internet officielle de votre prestataire dans votre navigateur ainsi que l'adresse officielle de leur page d'accès et de login, et n'utilisez que celles-ci.


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

eviivo

POUR PLUS D'INFORMATION, CONTACTEZ-NOUS

SALES@EVIIVO.COM | +33 (0)1 82 88 79 17