



eviivo

A GUIDE TO PROTECTING YOUR CASH:
PAYMENTS, CHARGEBACKS, AND FRAUD PREVENTION

To protect your cash, you need to adopt operational strategies designed to:

1. Automate payment and collection (instead of relying on human reminders)
2. Avoid chargebacks
3. Avoid fraud

This guide offers expert advice in all three areas, tailored for hoteliers, hosts and property managers. Read on to start safeguarding your cash flow.





1. PAYMENT AUTOMATION

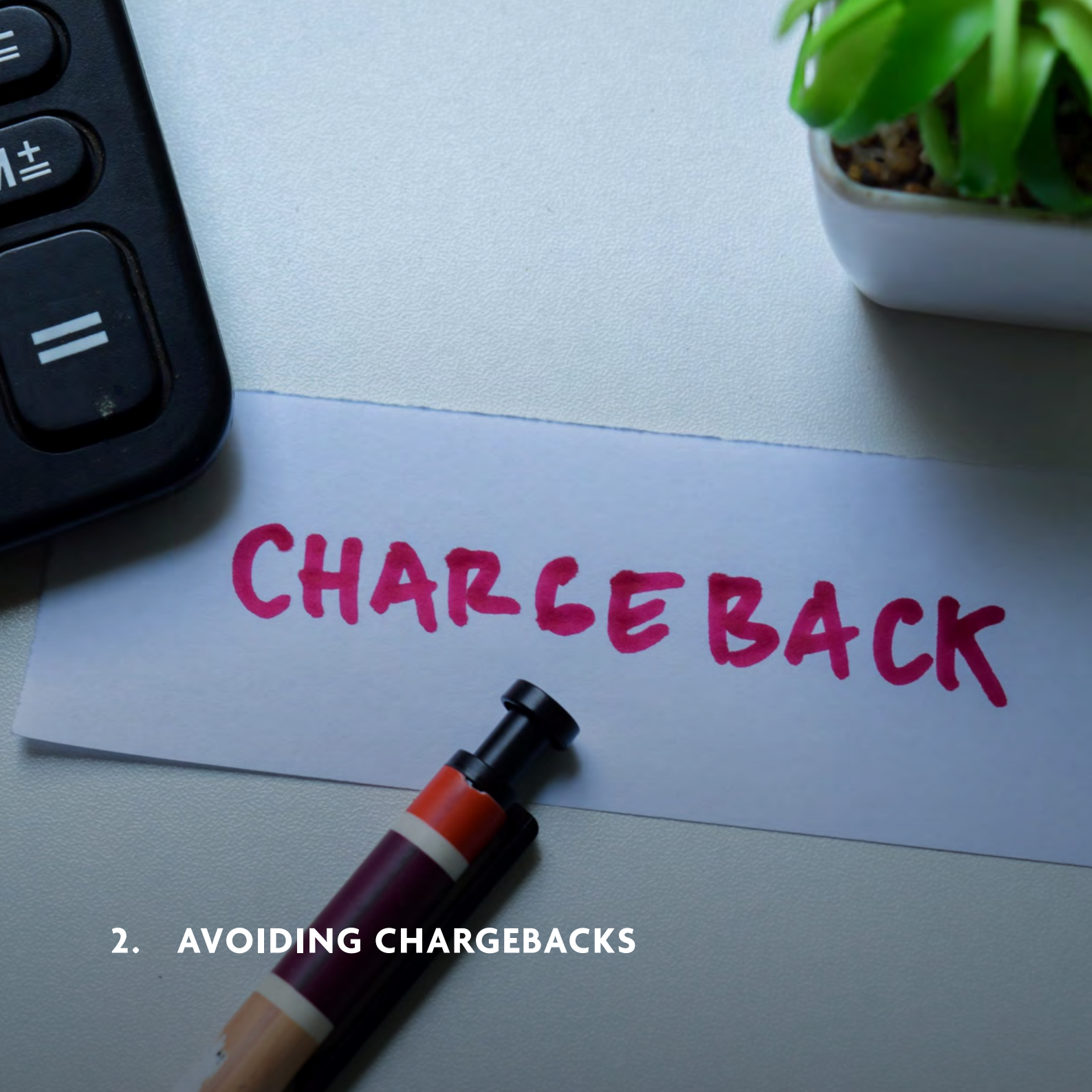
The best way to optimise your cash flow is by using a Property Management System (PMS) that provides a fully integrated payment engine.

This PMS must include the ability to:	eviivo Suite
Automate the collection of payments based on any user-defined schedule (between booking date and check-out), without human intervention or error.	✓
Automatically confirm any payment.	✓
Automatically issue a gentle reminder to the guest ahead of an upcoming due date.	✓
Automatically determine whether or not a refund is due when a booking is cancelled.	✓
Automatically process the appropriate refund.	✓
Automatically confirm any cancellation and the value of any refund.	✓
Automatically control the release of keys and access codes if the expected payments have not been collected.	✓
Automatically preauthorise cards (e.g. via a full electronic call to the guest's bank to [1] validate the card and [2] verify and authorise that there are enough funds on the card for the booking).	✓
Automatically indicate which part of the booking was collected via an OTA, then show it to the host and on the guest invoice, displaying any remaining balance to be collected on or after check-in.	✓





This PMS must include the ability to:	eviivo Suite
Automatically indicate whether/when a Virtual Credit Card (VCC) provided by an OTA is released and chargeable.	✓
Provide easy reporting for deposits due; outstanding booking balances; and payment/cash transaction by booking source and/or payment method.	✓
Provide instant reconciliation of OTA payouts – by VCC or direct bank transfer.	✓
Automatically distinguish between a prepaid OTA booking and an advanced deposit, and identify when a VCC payment qualifies as an advanced deposit and when it does not.	✓
Automatically and accurately generate or reverse the necessary accounting entries based on the timing of any collection or refund (e.g. “cash/receivable”, “cash/deferred revenue”, “cash/revenue & tax”).	✓



CHARGEBACK

2. AVOIDING CHARGEBACKS

What are chargebacks?

A chargeback is when a guest disputes a card payment and asks their bank to reverse the transaction. Guests can call their bank at any time and ask that a card transaction be refunded. The bank will usually take the guest's side and refund their card. It is then up to you, the merchant, to prove:

1. The payment was justified.
2. The card payment was genuinely authorised or signed by the guest.

When you receive a chargeback, you can dispute it – but the burden of proof is on you.

- If you win the dispute, you get to keep the money.
- If you lose the dispute, you need to process a refund, and you are also likely to be charged administrative costs by the bank.

Good to know -> The timeframe within which guests can request a chargeback after their card is first debited is generally governed by the applicable card-scheme rules, the reason for the dispute, and any applicable local laws or regulations. It is **typically around 120 days**, although the timeframe and the date from which it is calculated can vary depending on the circumstances: options may include from the transaction date, expected service date, or cancellation date.

Cardholder presence

If the cardholder is present when the payment is processed, you have a very good chance of being able to defend against any chargebacks. A cardholder is deemed “present” when:

- They enter their secret PIN code into a card reader or ATM machine.
- They pay online and are asked to answer a 3DS security challenge (or the Amex Safekey challenge) in real-time. This is where guests are asked to enter a one-time password (OTP) as part of the check-out process, which their bank usually sends via email or SMS.

If the cardholder is not present when you process the card, you are far more likely to be exposed to chargebacks. This will often be the case when card details are passed on to you by an OTA, because the guest is no longer present online when you process the card in your PMS. The payment will not necessarily fail, but it is far more likely to be exposed to chargebacks. Read on for recommendations on how to avoid this.

Legitimate chargebacks

Legitimate chargebacks may occur when:

- The guest cancels for a **genuine, serious and unexpected reason** (For example, a ‘force majeure’ such as the COVID-19 pandemic, a natural catastrophe, travel bans, etc.) and obtains no sympathy from the accommodation, especially if their trip was not insured.
- Guests are nervous that **the accommodation or OTA will not refund them for a legitimate full or partial cancellation**, especially if the accommodation takes too long to do so.

Fraudulent chargebacks can happen when:

- Guests claim they never stayed – when they did.
- You refunded the guest in cash, but they claim a second refund via card chargeback.
- Guests deliberately decide NOT to stay with you, but want to avoid paying late cancellation fees, and avoid any contact with you or the OTA.
- A guest stays, but the stay was prepaid by another person using a stolen card (and you did not preauthorise/revalidate the card).

How can I avoid chargebacks?

You should always implement the following recommendations to avoid chargebacks:

- **Ask guests to reconfirm** their stay a few days before check-in.
- **Register and verify the guest appropriately on arrival**
 - **Require guests to provide the registration information required by applicable local law and your property's procedures.** Where appropriate, this can be completed electronically (e.g., via email or message link) before check-in.
 - **Verify the guest's identity where required by law or where warranted by your property.** Use an appropriate ID document or a secure identity-verification process. Ensure any personal data collected is handled securely and retained only as necessary.
 - **For higher-risk or card-not-present bookings, consider additional payment verification at check-in.** A card-present transaction or verification can provide an additional fraud-control measure if you operate a reception or meet and greet service.
 - If you use eviivo as your PMS, **click the Check In button in eviivo Suite** to leave a digital trace.
- **Confirm that the cardholder and the person staying with you are the same person.**
 - If the card shows a different person's name, or the passport does not match, ask the guest to provide a card in their own name.
 - If the guest cannot provide an ID, then charge the card for the full stay at check-in (do not wait until check-out) and/or ask the cardholder to confirm their details and agreement to pay via email.

Many top hotels insist on receiving a written, signed third-party payment form along with a scanned photo of both sides of the card, with the photo dated and signed by the cardholder.





- **If a guest cancels over the phone**, cancel the booking and process the applicable cancellation fee/refund right away. This can be fully automated with the right technology.
- **If the guest is due a full or partial refund, process it promptly.** Delays may lead the guest to request a chargeback via their bank, which could end up costing you more than the refund!
- **Keep a digital trace.**
- **Charge your cancellation fee** (if applicable) **as soon as the cancellation deadline has passed**, ideally before check-in.
- Consider using a **non-refundable deposit** (i.e. a down payment due at the time of booking, or as soon as legally permissible in areas where a 24h grace period is imposed by law). This requires harmonising your cancellation and deposit policies.

Recommendations related to the payment of online bookings

If you are collecting payments from the guests, rather than the OTA, make sure you **use a booking and property management system with a fully embedded, PCI-compliant payment automation feature**. This is a system that allows you to automate the entire collection/refund process. It should be able to collect a payment the minute it is due and process a refund the minute a booking is cancelled, without any manual intervention. Such a system should also give you:

- A wide choice of supported card processors, to prevent you being locked in to a single bank or card processor.
- Different configuration options such as collecting payment via a payment link, a secure webpage or a guest portal; imposing or restricting the supported payment method; and targeting the customer types who should or should not pay by card in advance.

The best method is to preauthorise/process a card when the guest is present online, as soon as you receive a booking. So, make sure your website has 3D Secure enabled, and that your PMS is able to send a payment link to the guest (via email, SMS or WhatsApp), taking them to a secure page where they can process their card in full 3DS compliance. In both cases, the online presence of the guest on the page and the 3DS security code serve as **irrefutable proof that they intended to pay and were fully aware of your terms and conditions when they made their booking.**





If you choose to process the card yourself – with a card reader or directly in a PMS like eviivo Suite – and the guest can no longer be challenged to type in a secret PIN or provide a 3DS one-time passcode, then the risk of chargeback is high. Even if the card processes successfully, the chargeback can still hit you days or weeks later, and you remain exposed to a much higher risk from disingenuous guests.

How can I improve my chances of winning a dispute?

You need to **provide evidence of the guest's stay**:

- Provide appropriate evidence of the guest's identity and check-in. This may include the guest registration record, details of the ID verification performed, or other appropriate evidence.
- Provide a **report showing how/when the payments were processed**, along with a copy of any payment/booking confirmation email sent to the guest that links the payment to your T&Cs. (TOP TIP: Spend time reviewing the terms of your cancellation/deposit policy. Make sure your PMS includes these terms automatically in any booking, payment or cancellation confirmation email.)
- **Retain any communications between you and the guest.**
- **Provide a copy of any guest statement or invoice**, especially if it includes an existing over-the-counter refund.



3. AVOIDING CYBER FRAUD

Taking proactive measures to avoid cyber fraud is critical to protecting your cash.

With the last few years bringing mounting geopolitical cyber-attacks, most governments have increased cybersecurity measures and driven stronger security compliance requirements.

The first step in protecting your cash is to review the security measures built-in by your software providers:	eviivo Suite
Do they perform thorough identity and financial checks when onboarding new customers to ensure they don't allow hackers onto their platforms? (If you share a platform with other businesses, you want your platform vendor to ensure you are in good company!)	
Are they natively compliant with the PCI DSS (Payment Card Industry Data Security Standard)? Are they audited and certified independently by Visa and Mastercard or appointed auditors? Do they encrypt card details and run regular scans to prevent disclosures?	
Do they provide strong user management features at a sufficiently granular level (i.e. by role, by feature, by teams, and by property set) while still allowing users to view data for all permitted properties from a single booking calendar?	
Do they provide basic firewall, intrusion detection, anti-spam and anti-phishing protection, as well as professional backup and recovery capabilities?	
Do they have procedures in place to alert you when any of their customers is hacked or subject to a phishing attack?	
Do they have a robust GDPR (Global Data Protection Regulation) and/or DSA (Digital Services Act) policy?	

The rest is in your hands. You are expected to provide guidance and training to staff, implement best practices, and – above all – ensure that everyone remains vigilant! It's also a good idea to take out cyber-attack insurance if you can afford it.

Employee credentials

One of the simplest — and most effective — ways to strengthen your defences is by ensuring each employee has secure, individual login credentials. Each set of credentials should comprise the following:

- A unique email (your username).
- A unique password **known only to you**. The longer, the better: opt for 12 characters minimum, including at least one capital, one number + one special character.
- A unique security question that only you know the answer to (used if you wish to reset, recover or change your credentials in the future).
- A second recovery email or mobile number, essential to help mitigate any damage quickly should you fall victim to a cyber-attack.
- A second security question and answer, known to BOTH you and the software vendor. This is used by a vendor like eviivo to verify your identity when you contact us by phone or video conference.
- A unique property ID (eviivo calls it a shortname).

Choosing passwords

The worst (i.e. most commonly compromised) passwords are those which include the word “password”, the first letters on a keyboard (“Qwerty” or “Azerty”), basic number series (e.g. “111111” or “1234567”), or the names or birthdates of your children, spouse or partner.

The best passwords are more than 12 characters long and always include one or more capital letters, one or more numbers, and one or more special characters (e.g. *_-\$£).

If you use eviivo and are the main account holder, you can in turn provide access to other users and employees within your organisation via eviivo’s user management screen. This is accessible when you click on the little man icon in the top right of your screen in eviivo Suite.

Public and shared mailboxes

To avoid surprises and cybersecurity breaches, we strongly recommend you adopt the following precautions:

Avoid sharing credentials at all costs. It is always best to ensure that each employee has their own set of credentials. Ignoring this is the most prevalent cause of cyber fraud in the hospitality space. However, sharing devices and logins can be convenient for front-desk or housekeeping activities. If you really must use shared devices and credentials, then ...

Make sure any shared user credentials are only given minimal access rights. Prohibit any employee dealing with payments, card processing, or personal guest information from doing so using shared credentials. For your own protection, you should aim to enforce full auditability here and keep as few eyes as possible on any sensitive information.

Do not give top permission levels to public or shared mailboxes. Public shared addresses (e.g. “info@yourplace.com”, “contact@yourplace.com”, “reservations@yourplace.com”, “bookings@yourplace.com” or “hello@yourplace.com”) should NOT be given to top-level roles such as the ‘Administrator’, main account holder, or manager. Ignoring this advice is the second most prevalent reason for cyber fraud in the hospitality industry.

Always differentiate your business email/password from any personal email used for private communications. Use separate email accounts and passwords – and instruct your employees to do the same.





Public and shared mailboxes are much easier to breach because:

- Hackers use published email addresses to lure guests into providing data or card details.
- Using shared mailboxes or accounts increases the odds of an attack since any one of multiple users can be tricked into giving away their credentials.
- Internal fraud can be committed by temporary or contracted workers, new staff, or outsourced contractors you don't know well.

Team-based, multi-user security

A team-based security configuration should help you manage a multiplicity of roles easily.

For example, let's say three different people require the same security level. Rather than create a shared mailbox, you can:

- a. Give each person their own distinct unique login credentials.
- b. Assign all three people to one "Team".
- c. Assign the desired permissions and property access rights to the "Team" rather than to each individual.

A team-based configuration is much quicker and easier to manage as employees join or leave your business. Because each individual retains their own credentials, any transaction audit matches each action to the person who took it. Therefore, if one person's credentials were to be stolen or broken into, the rest of the team can continue unaffected – whereas with shared credentials, everyone is out of action.

Phishing: the most common form of attack

Phishing is the malicious act of attempting to trick users into revealing their personal credentials. Attackers often induce users to reveal information via malicious links, fake webpages, or email attachments that contain spyware or computer viruses such as trojans.

Bad actors and fraudsters constantly fake the logos and login pages of reputable companies. They have become extremely clever at reproducing not only logos, but photos, videos, and even voices!

The most common methods of breaking into accounts are via email, mobile notifications, social media, and phone calls. Attackers may pretend to be one of your business suppliers, your bank, your telecommunications or software provider, or various authorities.

A successful phishing attempt can allow an attacker to:

- Collect usernames and passwords or other sensitive information.
- Take control of your email inbox for malicious use.
- Convince you to make payments for their benefit.
- Convince you to pay sums of money into an unauthorised account.
- Install spyware or malware enabling them to monitor your online activity.
- Damage your computer or the organisation's network, encrypt your data, or hold it to ransom.
- Gain access to intellectual property, designs, or pending patents.

The rest of this guide examines the clever ways in which fraudsters may attempt to trick you – and how to stay vigilant.

Spear phishing: fake booking confirmations

Spear phishing is a targeted form of phishing attack. Perpetrators often use information publicly available on the internet, such as public email addresses on websites, to create fake messages and encourage their audience to click on malicious links.

One example of spear phishing could involve creating fake booking confirmations to send to your guests. Fraudsters can obtain an original booking confirmation by placing, then cancelling, a booking or an order with you. They can then use it to create a fake confirmation that looks like it comes from you (or from eviivo, or Airbnb, or Booking.com, etc.). These fake confirmation messages trick unsuspecting guests into providing personal information, credentials, or card/bank account details, or even into clicking on a link to pay into the hackers' bank account.

A common approach to spear phishing attacks is to disguise malicious software in seemingly legitimate attachments and links, which perpetrators hope will be downloaded to infect the target computer or network.

Furthermore, these buttons and links will often drive users to fake website login pages to capture sensitive or personal information, which can be used later to launch further attacks or gain privileged access into the target's account or organisational network.





To protect yourself, consider the points below to help you spot fakes and online phishing tricks:

Click on the sender's name in the “From” box of the email header to unveil their full email address. Does it look like a legitimate address? Does the spelling match the official company email 100%? If not, it's a fake.

Does the email ask you do something urgently? Did you expect such a request? Most fraudsters **create a false sense of urgency**, claiming that they are acting on behalf of a higher authority, (e.g. a bank, an institution, a company, or a senior executive) then telling you that you must verify your account details.

Does the email contain **unusual spelling or grammatical mistakes**? Many bad actors operate out of foreign countries. As they fake official notices, you can often spot grammatical or spelling errors that a legitimate business would usually catch.

Click on the website name in your browser bar and check the very first part of the website address. For example, legitimate eviivo webpage addresses (URL domain names) always start with <https://eviivo.com/> or <https://on.eviivo.com/> or <https://via.eviivo.com/>

Always check the spelling of the email address or webpage address extremely carefully. All it takes is to redirect you to a fake website or login page is one incorrect character or extra space. Example: A recent phishing attempt replaced “eviivo” with “evlivo”, while another said “eviivo.com” rather than “eviivo.com” – both barely noticeable misspellings!



TOP TIP

If you're an eviivo user, bookmark the URL web address of eviivo's official login page in your browser and always login from there. This reduces the risk of clicking on dubious links in faked emails or login pages.

Whaling

Whaling is a phishing attack that targets users by faking high-profile individuals such as corporate executives, senior management, celebrities, or staff with the authority to provide access to systems or sensitive information.

The goal is to trick the targeted individual into carrying out an action or disclosing information that can then be used to drive further security breaches.

Whaling attacks are highly customised and personalised. They often incorporate the target's name, job title, and other relevant information (gleaned from various sources, such as their social media profiles or other aspects of their digital footprint).





Whaling attackers impersonate someone with high authority or credibility in order to:

Ask their targets for a favour or urgent assistance, so that users eager to please their boss end up transferring data, credentials, or even money! **To prevent this**, triple check any communication you receive that is signed by the CEO, Vice President, or Managing Director of a company.

Threaten users that their account will be shut down or fall afoul of certain regulations if they do not reconfirm their credentials immediately. Users are then driven to a fake webpage where the hackers lie in wait, ready to capture their credentials.

Offer a big cash reward or pretend that a user has some money they need to claim (e.g. a lottery win, an inheritance) as a way of enticing them to provide their credentials and/or bank or card details.

Vishing

Vishing is short for “voice phishing”. It simply means phishing via phone calls or voice messages.

This could be someone pretending to be your bank, a telecom company, or a vendor like eviivo, asking you to confirm confidential personal or account information. The attacker may also invite you to share your screen, so they can install spyware that will capture your keystrokes and credentials.

To check whether the person calling you is genuinely from the source they claim, simply ask them questions that only you and that source would know.

For example, if the person claims to be from eviivo, you could ask for:

- The reference number of the last booking you took.
- The shortname code of your property.
- The (second) security question and answer shared only by you and eviivo.

eviivo – or any other genuine organisation – would never contact you in the way described by the script below:

Hi, this is Candice at eviivo,

We are calling you because we believe that there has been suspicious activity on your account. It is urgent that we verify that everything is in good order. Can I share my screen with you?

Ok, in order to access your account details, I need to ask you to reconfirm your password, as we will need to reset it during the call. Could you reconfirm your security question and answer?





TOP TIP

Top tips to stay vigilant:

- **eviivo, or any other reputable company, will NEVER ask you to disclose your password.** While they may ask you the answer to a security question, they will never ask you what the security question is.
- When a vendor asks you to share your screen, they should do so from the vendor's official website address (for example, eviivo.com).
- Remember that any vendor staff can see and access your account, so just ask them a question that only they would know (e.g. your property short name, the reference of the most recent booking that came into your calendar). A fraudster will not know any of these answers.

Smishing

Smishing is phishing via SMS and text messages. Fraudsters often send text messages in an attempt to either:

- Steal personal or confidential information from the recipient, or
- Infect the recipient's device with malware.

Fraudsters will just as easily fake a WhatsApp account, using any publicly available photo of someone you know or the photo of a public and/or authoritative figure.

Social media phishing

Cyber criminals often use social media to carry out attacks aimed at stealing personal information or spreading malware. Perpetrators typically **impersonate a friend/colleague/family member** on social media to trick you into sending them money. Some attackers attempt to hijack your account in order to launch follow-on attacks against your address book contacts, connections, friends or followers.

This method often relies on:

- Spoof ads which can trick you into clicking on a link that redirects you to a fake login page that looks legitimate – but is not – to capture your credentials or account details.
- Asking you to pay a premium, a penalty, or an illegitimate fee.

Genuine social media communications will always send you back to the vendor's official website URL. In the case of eviivo, the URL address, visible in your address bar, would always start with either **<https://eviivo.com/>** or **<https://on.eviivo.com/>**



eviivo

FOR MORE INFORMATION, CONTACT

SALES@EVIIVO.COM | +44 (0)20 3103 3500