operto

1. Security incident email

Send as soon as you know personal information may be at risk. Fill in the brackets, remove what does not apply, and send from your official company email.

Subject: Important security notice from [Company Name]

Hi [First Name],
We are writing to let you know about a security incident that [may have] affected information we hold about you. We want you to hear it from us, with clear steps you can take.

What happened
[One or two plain sentences: what occurred and the date it was found.]

What information was involved
[For example: name, email address, phone number, booking dates. State clearly if payment details or access codes were NOT involved.]

What we have done
[For example: secured the affected systems, reset affected access codes, notified the relevant authorities where required.]

What we will never do
- Ask for your password or PIN, or ask you to share a verification code by reply, chat or phone. Codes are only ever entered on [official site].
- Send a link demanding urgent payment, or say a booking will be cancelled unless you act within hours.
- Ask you to pay or re-pay for a stay outside our official booking channel.
- Send you door or lock codes through any channel other than [official guest channel, for example our guest messaging].

Steps to take now
1. Turn on multi-factor authentication (MFA) on your account with us and on your email and other key accounts.
2. If you reuse your password anywhere, change it to a strong, unique one. A password manager helps.
3. Be careful with unexpected messages about a booking, payment or check-in, even if they look like ours. Do not click the link. Contact us using the details below.
4. Check your bank or card statements for charges you do not recognize.

How to reach us
Our only official channels are [website], [support email] and [phone]. We will not contact you from any other address or number.

We are sorry for the worry this causes. If you have questions, our team is ready to help.
[Name] | [Company Name]

operto

2. Trust card

Add to booking confirmations, guest portals or your property guidebook.

What we do	What we never do	If in doubt
Email only from @[yourcompany.com]	Email from free accounts or lookalike domains	Do not reply or click
Send payment links only through [official booking site]	Ask for payment by gift card, wire transfer or crypto	Open your booking from the official site or app
Share door codes only through [official channel]	Send codes outside [official channel]	Call us on [official phone]
Answer questions in [official support channel]	Ask for passwords or card numbers, or for a code by reply or phone	Forward the message to [security email]

Not sure about a message? Contact us at [phone] or [support email] before you act. We are always happy to confirm.

operto

3. SMS and WhatsApp alerts

Short messages that do not look like phishing, for SMS and WhatsApp. Only link to [official domain], never ask guests to reply with a code, and keep each to about 160 plain characters.

Use	Message
General alert	[Company]: We saw unusual activity. Our links only go to [official domain]. Never share a code by reply or call. If unsure, open our website or app directly.
Password reset	[Company]: A password reset was requested. Not you? Ignore this text. Enter your code only at [official domain] and never share it with anyone, including our team.
Check-in details	[Company]: Your check-in details and door code will be sent to you through [official channel] before your stay. Questions? Call [phone].
Payment warning	[Company]: We never ask for payment by text or outside your booking. Unsure? Call [phone] before you pay.
WhatsApp warning	[Company]: We only message from [official WhatsApp number]. We never ask for payment or a code in this chat. Unsure? Call [phone] before you act.

operto

4. Support script

For staff who handle calls and messages from worried guests and owners.

Step	What to say
1. Reassure	"I understand why this is worrying, and thank you for checking with us. I will help you with next steps."
2. State the rule	"I will never ask for your password, card number or verification codes, and nobody from [Company] will."
3. Verify safely	"Please do not use any link in that message. Open your booking on [official site or app] and tell me what it shows."
4. Direct to safety	"To change any details, please go to [URL] yourself and sign in there. I can stay on the line while you do."

Never ask for or accept passwords, card numbers or verification codes, and never send a door code to a new email or number given on a call. If a caller has already paid, shared a code or lost account access, escalate to [security contact] right away.

operto

5. Prevention checklist

Most problems start with a stolen login, a lookalike message or a shared code. Review this checklist every quarter.

Accounts

- [ ] Turn on multi-factor authentication for email, booking and operations tools
- [ ] Give every team member their own login, with a unique password
- [ ] Give people only the access their role needs
- [ ] Remove access the same day someone leaves

Door codes

- [ ] Use a different code for every stay, set to expire at checkout
- [ ] Do not use a guest's phone number digits, such as the last four, to create codes
- [ ] Send codes only through your official guest channel
- [ ] Change codes after any suspected incident

Guests, owners and team

- [ ] Tell guests which channels you use, and share the trust card in your welcome message
- [ ] Confirm any change to bank or payout details by calling a number you already have
- [ ] Give staff one place to report suspicious messages, and refresh training every few months