BREACHROAD

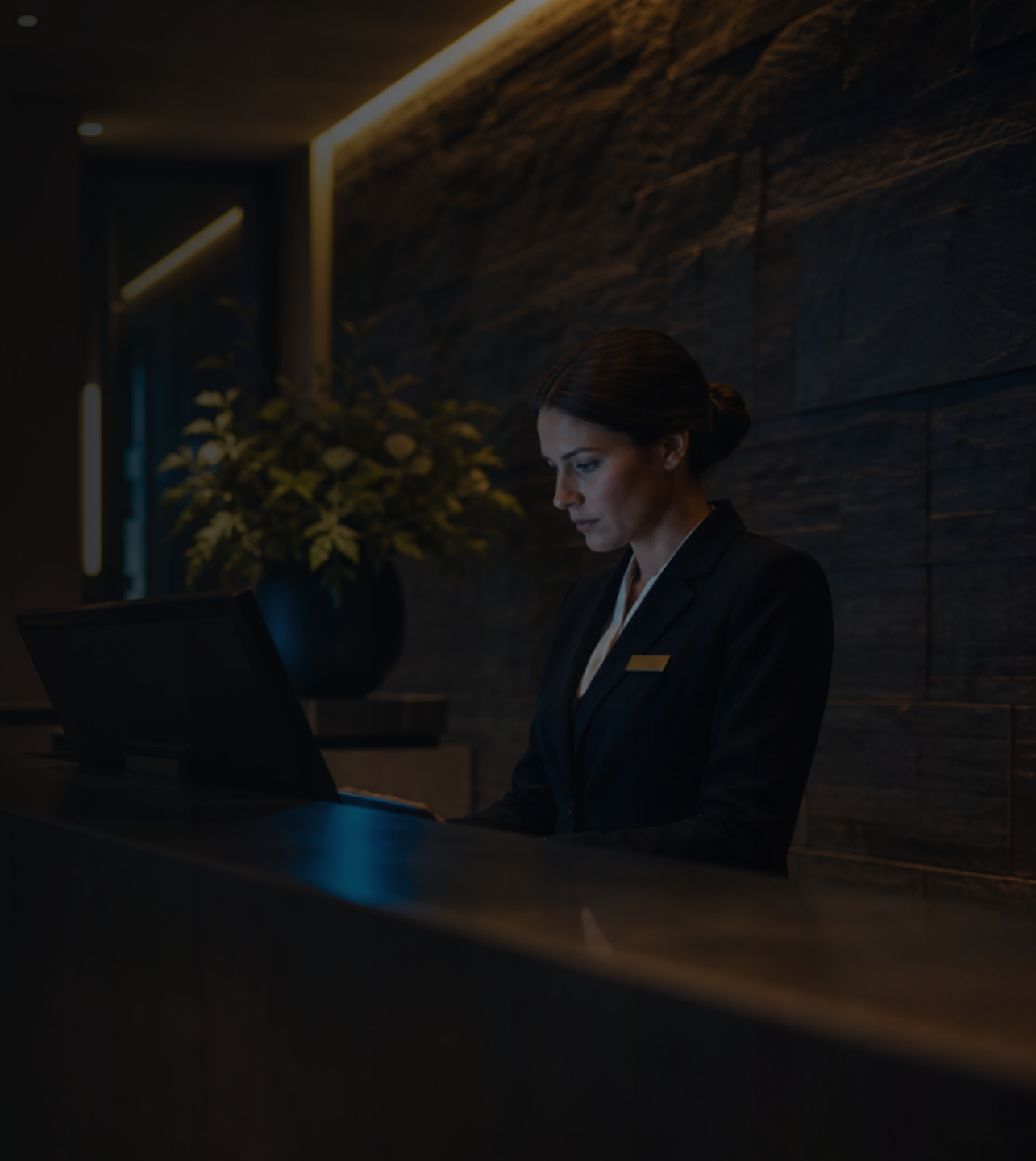
SAMPLE INDUSTRY TRAINING

Phishing in hospitality

When a message knows the booking, urgency becomes a vulnerability.

90 MIN

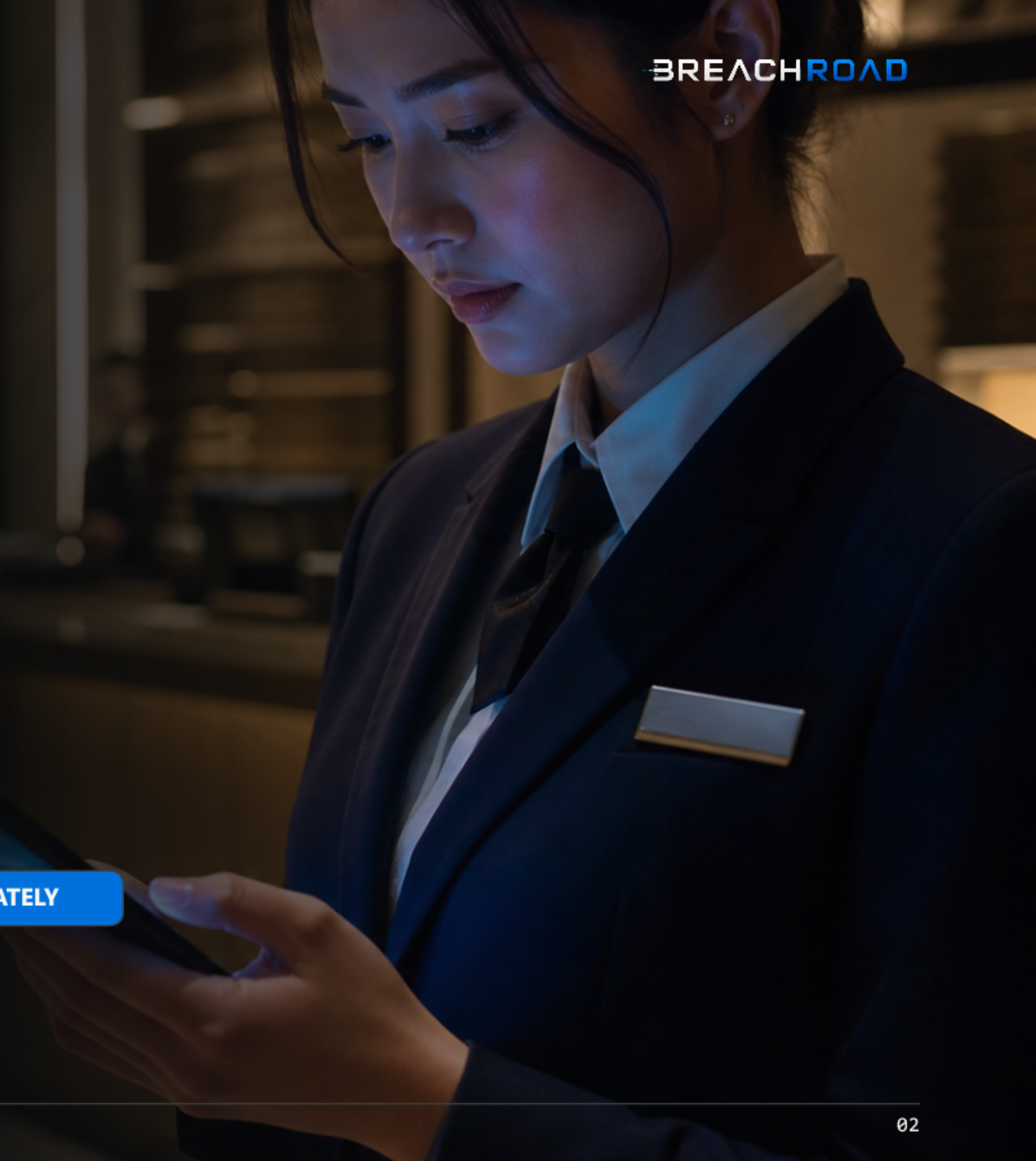
FRONT DESK • RESERVATIONS • FINANCE



BREACHROAD

17:46 • 120 CHECK-INS • WEDDING WEEKEND

“The guest’s payment has been declined.”



The message includes the guest’s name, booking number and arrival date.
It asks you to sign in again within 30 minutes.

What do you do first?

A • I CLICK

B • I CALL THE GUEST

C • I VERIFY SEPARATELY

BREACHROAD

After 90 minutes, you can make three moves without guessing

01

Pause

the action before pressure takes over.

02

Verify

the request outside the channel that delivered it.

03

Report

quickly — even after a click.

You do not need to become an analyst. You need to stop a risky action.

WHY HOSPITALITY?

Hotels work across many channels. So do attackers.

Bookings, email, OTAs, PMS, phone, messaging, payments, suppliers and shift handovers all converge in a single decision.

SERVICE SPEED

DISTRIBUTED TRUST

BREACHROAD

One booking moves through a chain of trust

E-MAIL

SMS / WHATSAPP

PHONE

PARTNER PORTAL

Every node may be legitimate. Every channel can be impersonated.

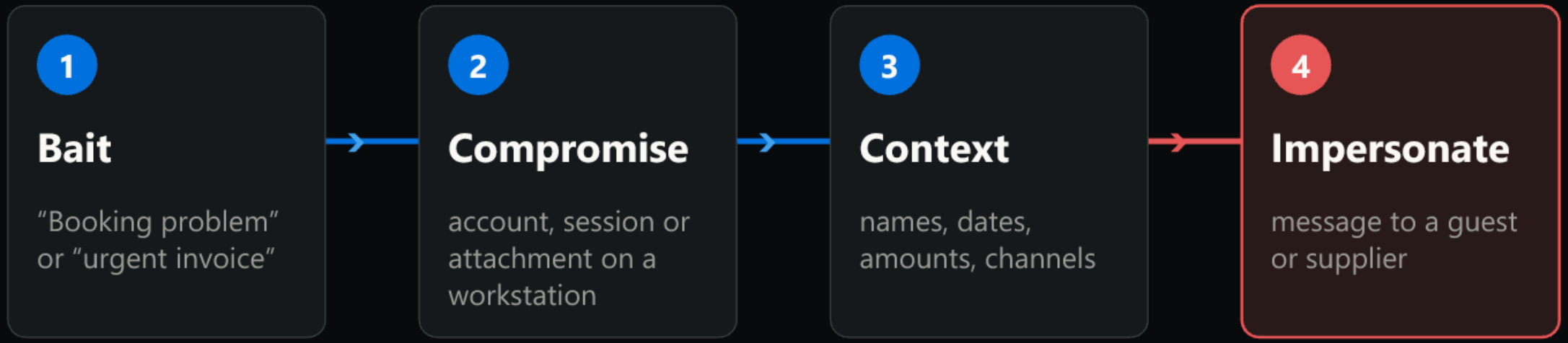
BREACHROAD

The attacker wants more than a password

01	**ACCESS**	mailbox • OTA portal • PMS
02	**MONEY**	extra charge • invoice • bank-detail change
03	**GUEST TRUST**	a message with genuine context
04	**TIME**	hidden rule • session • further impersonation

The most valuable account looks ordinary and understands the daily process.

One sign-in can trigger phishing against guests



Real data creates false confidence.

BREACHROAD

Channel and third-party context materially change risk

40%

higher median successful click rate in simulations that began on mobile or SMS rather than email

48%

of breaches in the 2026 DBIR involved a third party — a partner, supplier or another link in the chain

Global data does not describe every hotel. It shows where decision practice matters.

BREACHROAD

Do not hunt for typos. Look for a risky request.

Hello Marta,

we detected a payment discrepancy in booking 48172. To keep the room available, please reconfirm the account before 18:15.

Kind regards,
Partner Support Team

SOUNDS PROFESSIONAL

but asks you to:

- sign in urgently
- act from the message
- trust the booking number

The copy persuades. The context makes it feel authentic.

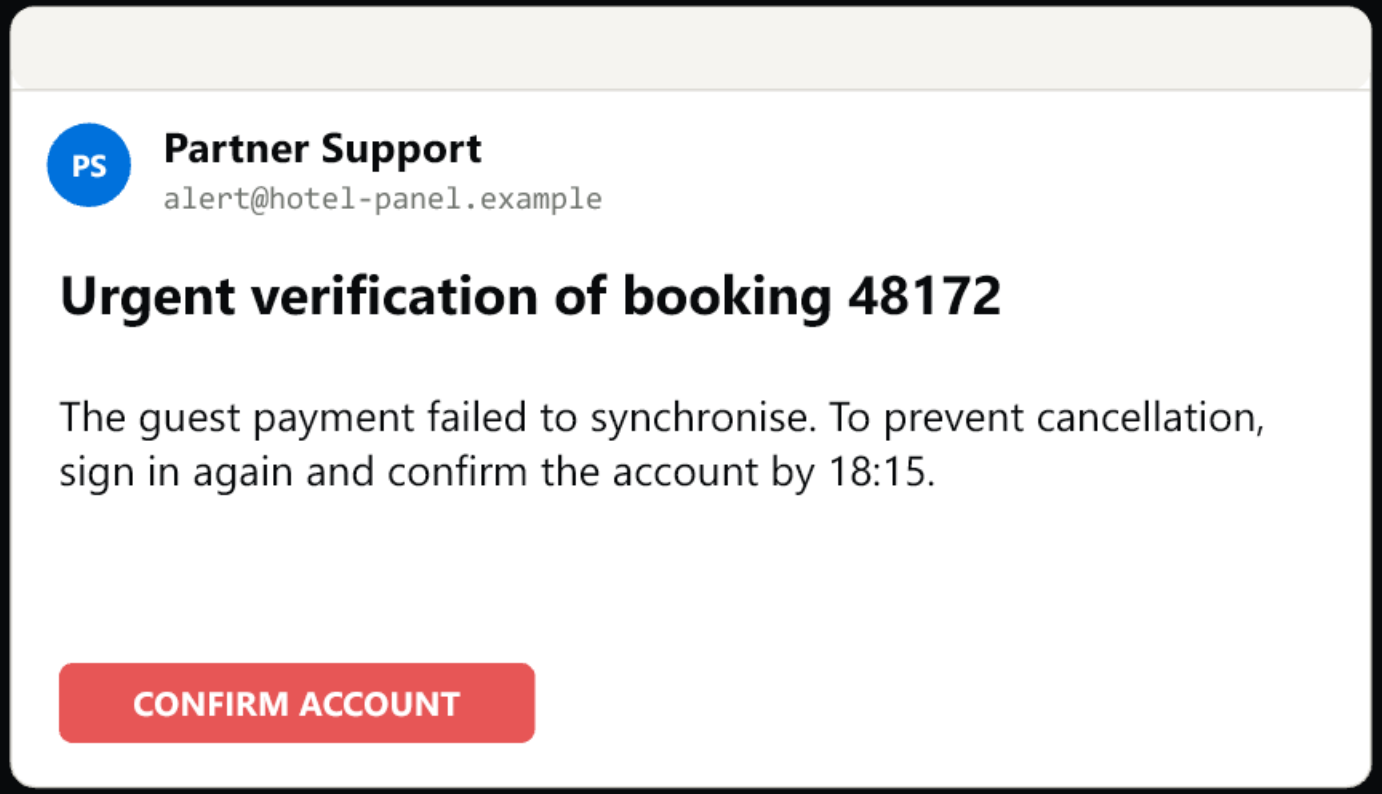
02

Context first.
Content second.

Four signals that should stop the action.

BREACHROAD

Four checkpoints reveal more than the entire message



1. **Full address and domain**
2. **Pressure of time or loss**
3. **Action: sign-in, file or payment**
4. **Can you verify it separately?**

BREACHROAD

The sender name is a label. The domain is a clue.

Partner Support

THE SAME NAME CAN APPEAR ABOVE TWO ADDRESSES

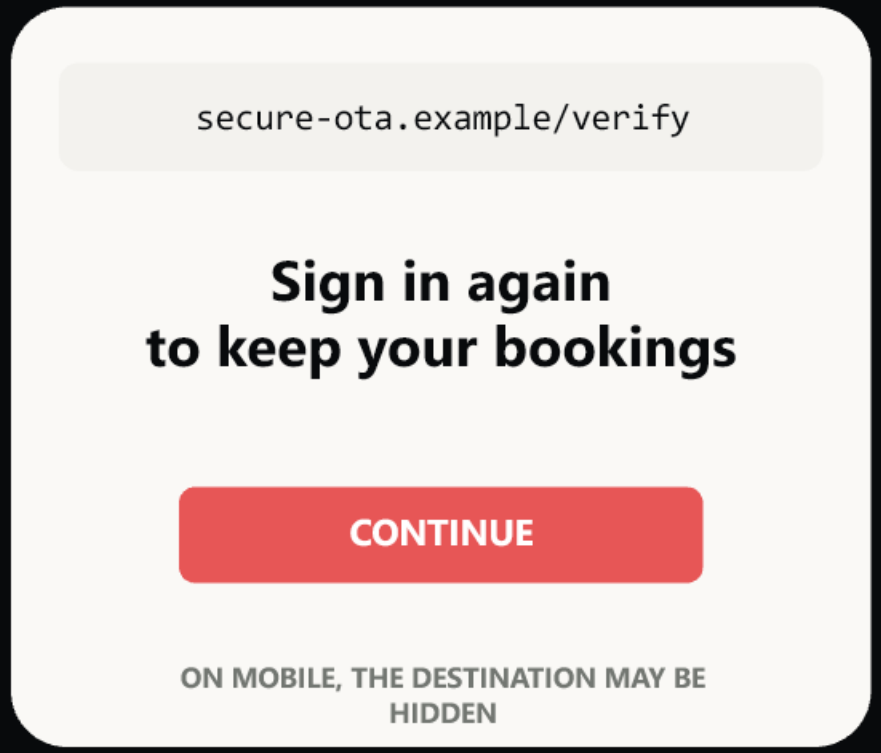
`support@panel.hotel.example`
address known from hotel procedure

`support@hotel-panel.example`
similar appearance ≠ known domain

A domain does not prove safety. A mismatch is enough to stop the action.

BREACHROAD

Links and QR codes shorten the path — including to a bad decision



1. Do not sign in from a message link
2. Open the portal from a saved bookmark
3. Treat a QR code as an invisible link

BREACHROAD

A bank-detail change is not information. It is a risk process.

1

HOLD

do not release payment

2

CALL BACK

using a saved number

3

CONFIRM

with a second person

The channel that delivered the change cannot verify it by itself.

EXERCISE 1

Three messages. One rule.

You have 20 seconds to decide:

PROCEED VERIFY ESCALATE

We are not asking, “Is this definitely phishing?” We are asking, “Is this action safe right now?”

BREACHROAD

A • A guest sends a “booking document”

AK

Anna Kowalska

anna.kowalska@example.com

Late arrival — booking 48172

Hello, I am sending the document required for a late check-in. The file is password-protected: 2026. Please confirm receipt.

reservation_details.html

DECISION

Do you open the attachment?

PROCEED

VERIFY

ESCALATE

BREACHROAD

You do not need to know whether the guest is genuine

1. Do not open an HTML file or a password-protected file from an unexpected message
2. Check the booking directly in the PMS
3. Contact the guest using the details stored in the booking

SAFE DECISION: VERIFY • ESCALATE IF THE ATTACHMENT WAS OPENED

BREACHROAD

B • “Partner Support” writes on WhatsApp

PS

Partner Support

WhatsApp • new number

Hello. Seven bookings failed to synchronise with your property. The account will be restricted in 30 minutes. Please scan the code and confirm your sign-in details.

DECISION

Do you scan the code?

PROCEED

VERIFY

ESCALATE

BREACHROAD

A real booking number does not authenticate the sender

DATA

“seven bookings”
“property account”

may be genuine

≠

IDENTITY

“this really is Partner Support”

requires separate verification

OPEN THE PORTAL FROM A BOOKMARK • CHECK ALERTS • REPORT THE MESSAGE

BREACHROAD

C • A supplier changes the bank details on an invoice

AN

Anna Nowak • LinenPro

anna.nowak@linenpro.example

New bank details from August

Due to a change of bank, please pay all future invoices to the new IBAN. Today's payment may already be sent to the new account.

INVOICE_07_2026.PDF

DECISION

Do you change the details?

PROCEED

VERIFY

ESCALATE

BREACHROAD

The most expensive message may be perfectly written

01

HOLD

payment and detail change

02

CALL BACK

using a previously saved number

03

APPROVE

with a second authorised person

SAFE DECISION: VERIFY • DO NOT USE THE NUMBER IN THIS MESSAGE

BREACHROAD

One procedure for email, SMS, WhatsApp and phone calls

S **Stop**
Do not click, reply or approve.

T **Origin**
Check the full address, domain, channel and context.

O **Open separately**
Use a saved bookmark or call a known number.

P **Promptly report**
Report quickly — even after a click.

STOP

Do not prove the message is fake.

Stop the risky action.

BREACHROAD

The front desk protects the guest before the mailbox

WHEN A MESSAGE CONCERNS A BOOKING

1. **Check the booking in the PMS** — not through a link in the message
2. **Do not disclose new details** — to a sender who already knows part of the story
3. **Use the contact stored in the booking** — not a number supplied in the message
4. **Report the impersonation attempt** — before a similar message reaches the next shift

PROFESSIONAL RESPONSE: “I’LL VERIFY THIS IN OUR SYSTEM AND GET BACK TO YOU THROUGH A KNOWN CHANNEL.”

BREACHROAD

A bank-detail change requires a second channel and a second person

MESSAGE

“New IBAN”

source of the request

›

CALL BACK

known number

not from the message

›

SECOND PERSON

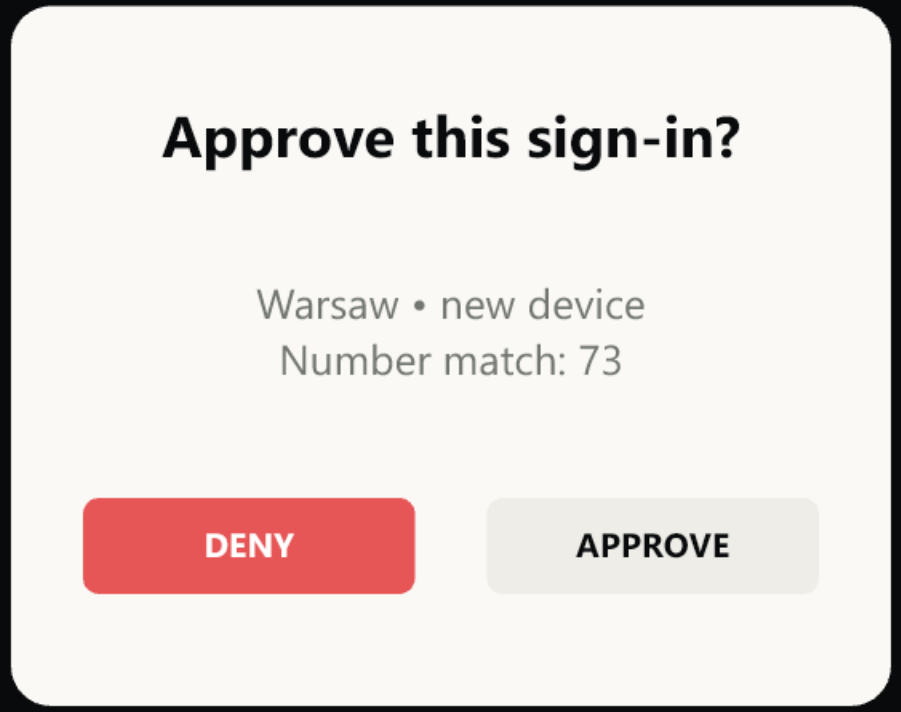
approves

after checking the evidence

Two people in the same email thread still use one channel.

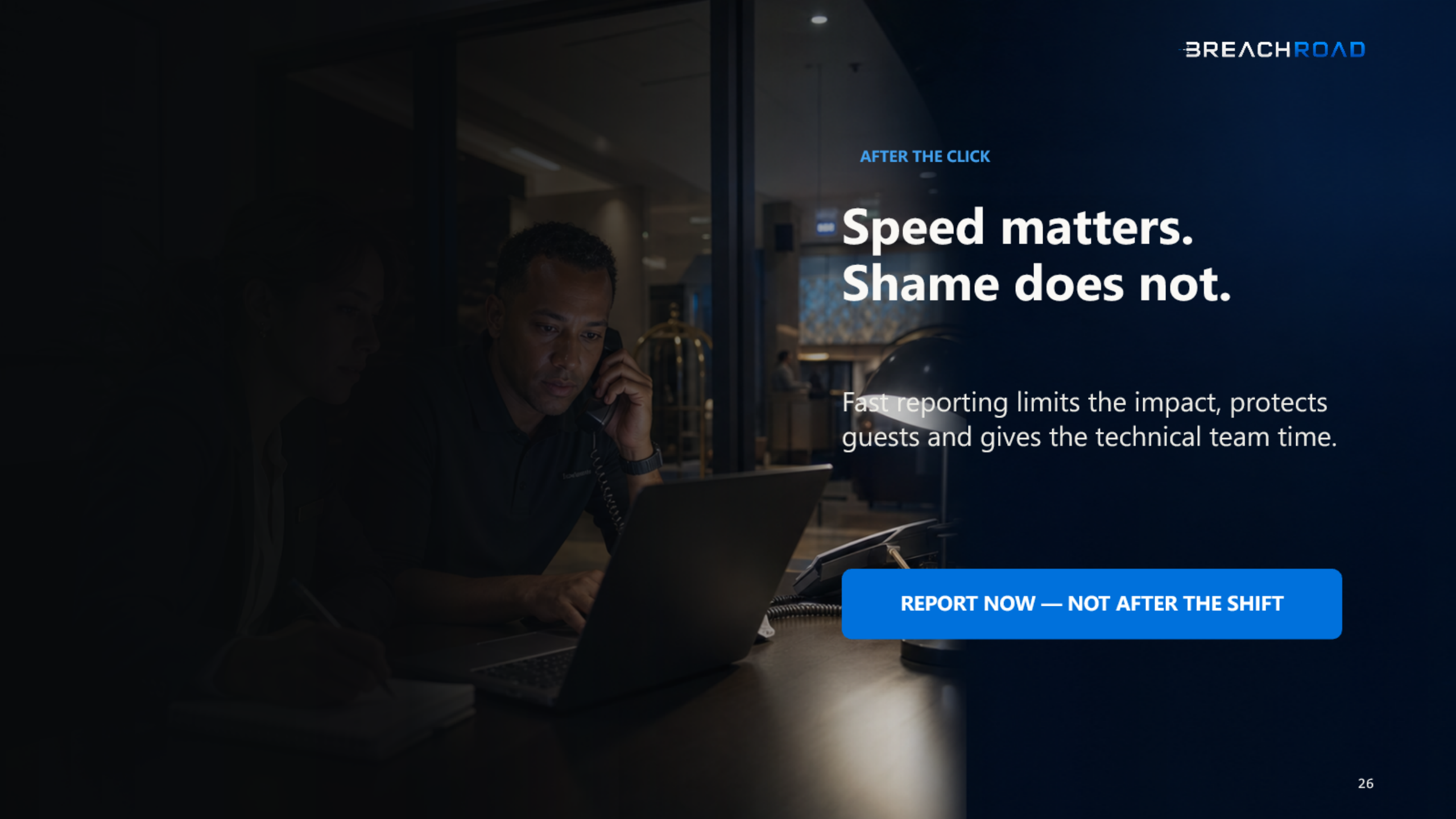
BREACHROAD

An unexpected MFA request is not a formality



1. Deny it if you did not start the sign-in
2. Never give the code to a caller or “support”
3. Report the attempt and review active sessions

For critical accounts: use passkeys or FIDO instead of phishable codes.



BREACHROAD

AFTER THE CLICK

Speed matters. Shame does not.

Fast reporting limits the impact, protects guests and gives the technical team time.

REPORT NOW — NOT AFTER THE SHIFT

BREACHROAD

The first minutes depend on what has already happened

CLICK ONLY

Close the page
Keep the message / address
Report the attempt

CREDENTIALS

Contact IT
Change the password through a trusted path
Revoke sessions and MFA

FILE / PAYMENT

Report immediately
Stop using the device
Call the bank and finance after a transfer

IN EVERY CASE: KEEP THE MESSAGE • DO NOT HIDE THE EVENT • REPORT THE TIME AND DEVICE

BREACHROAD

Three instincts that make an incident worse

01	**DO NOT DELETE**	the message, file or history
02	**DO NOT FIX IT QUIETLY**	without reporting and revoking sessions
03	**DO NOT WAIT**	until the end of the shift or the manager returns

The best report begins: “This happened a moment ago. Here is what I did.”

EXERCISE 2 • TABLETOP

17:46 before a wedding weekend

120
check-ins by 20:00

2
people at the front desk

7
allegedly “unsynchronised” bookings

30 min
until account restriction — according to the message

You are one shift. Decisions must be specific: who does what, through which channel.

BREACHROAD

Round 1 • The message reaches the front desk

PS

Partner Support
WhatsApp • new number

Seven bookings failed to synchronise. The property account will be restricted at 18:15. Please confirm the sign-in through the QR code.

90 SECONDS

Decide:

1. Who stops the action?
2. Where do you check bookings?
3. How do you contact the partner?
4. Who receives the report?

ANSWER = PERSON + ACTION + CHANNEL

BREACHROAD

Round 2 • A colleague entered a password and MFA code

17:51

“I thought it was the real portal. I entered my password and code. The page closed.”

The laptop still appears to work normally.

90 SECONDS

Your first three actions:

- who contacts IT?
- how are credentials changed?
- who revokes sessions?
- what evidence do you preserve?

BREACHROAD

Round 3 • A guest calls about an “urgent surcharge”

G **Guest • booking 48172**

“I received a text with the hotel name, stay dates and a link to pay an extra PLN 240. Is my booking at risk?”

The guest has not paid yet.

90 SECONDS

Decide:

1. What do you tell the guest?
2. How do you protect others?
3. Who secures the account?
4. What do you preserve for analysis?

BREACHROAD

A strong response runs on two tracks at once

TRACK 1 • GUEST SERVICE

Confirm the booking
Stop the fraudulent payment
Give the guest a known channel

TRACK 2 • INCIDENT

Secure the account and sessions
Check the reach of the messages
Preserve evidence and escalate

HOSPITALITY DOES NOT REQUIRE TRUSTING THE MESSAGE. IT REQUIRES A SAFE SERVICE PATH.

BREACHROAD

An employee cannot be the only line of defence

01	**Phishing-resistant MFA**	for critical and partner accounts
02	**Reporting button / channel**	visible on every shift
03	**Payment-change process**	second channel + second person
04	**Role-based access**	no shared accounts or excessive privileges
05	**Industry-specific exercises**	email, phone, WhatsApp, OTA

TRAINING WORKS BEST WHEN THE PROCEDURE MAKES THE SAFE DECISION POSSIBLE.

THE RULE FOR YOUR NEXT SHIFT

You do not need to prove the message is fake.

You need to stop the risky action.

STOP • ORIGIN • OPEN SEPARATELY • PROMPTLY REPORT