ONLINE SCAM EMERGENCY GUIDE

Phishing, WhatsApp & bank-transfer first aid in the Netherlands

A calm checklist for the first hour

01/15

COULD THIS BE A SCAM?

Check the red flags

- [ ] Unexpected contact or a “new number”
- [ ] Pressure to act now
- [ ] Told to keep it secret
- [ ] Asked to click, scan or leave the platform
- [ ] Asked for PIN, one-time code, DigiD or full card details
- [ ] Asked to raise a limit or move money to a “safe account”
- [ ] Asked to share your screen or install a remote-access app
- [ ] Someone will collect your card, cash or jewellery

HARD STOP

Any of the last four?
Stop and contact the bank or organisation independently.

60-SECOND SCAM CHECK

Should you trust this?

1	Was this contact expected?
2	Can you hang up and verify via the official number?
3	Do they resist a callback, video call or independent check?
4	https:// — Did the link, IBAN or phone number suddenly change?
5	Are they demanding urgent payment, secrecy or a higher limit?
6	Would waiting 10 minutes really cause the claimed consequence?

YOUR RESULT

0 signs	Still verify independently
1–2 signs	Pause. Don't pay or click.
3+ signs	Highly suspicious. Stop.
HARD STOP	PIN, code, "safe account", remote access or card collection

Already entered details, authorised or sent money? Go to the **emergency steps**.

THE FIRST 15 MINUTES

Act quickly, stay calm

1. Save screenshots and note the time
2. Call your bank using the official app or number on your card
3. Freeze the card or lower payment limits
4. Change key passwords on a trusted device
5. Check for unknown payments or logins

FAKE BANK CALLS

There is no "safe account"

A bank will never ask you to:

- ✕ Move money to a "safe account"
- ✕ Share your PIN, codes or passwords
- ✕ Hand your card to a courier
- ✕ Install AnyDesk or TeamViewer

Move money to a "safe account"

Share your PIN, codes or passwords

Hand your card to a courier

Install AnyDesk or TeamViewer

REMEMBER

Caller ID can be spoofed.

Hang up. Call the official bank number yourself.

PHISHING, SMS & QR CODES

Pause before links and scans

RED FLAGS

- Urgent payment or "re-verification" threats
- Fake DigiD, bank, CJIB, parcel or tax messages
- One extra letter can mean a fake domain
- A QR code can hide its destination

SAFER MOVE

Type the official address yourself.

If you entered details, contact the affected organisation immediately.

Whatsapp Help-Request Fraud

“New number — can you pay this?”

BEFORE YOU PAY

1 Call the old saved number

2 Ask something only your family knows

3 Remember: a photo or voice note is not proof

IF YOU PAID

Contact your bank, Fraudehelpdesk and the police.
Save screenshots before reporting.

MARKETPLACES & FAKE SHOPS

Fake links can look convincing

WATCH FOR

- Pressure to move the chat off-platform
- A request to “verify your receiving account”
- A very low price plus urgency
- A payment link sent by the other person

SAVE AS EVIDENCE

The ad, product photos, IBAN, phone number and full chat

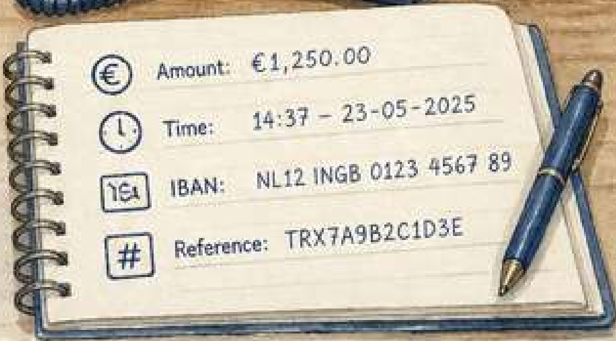
REPORT

Dutch Police offers online reporting routes for fraud.

ALREADY PAID?

Don't wait

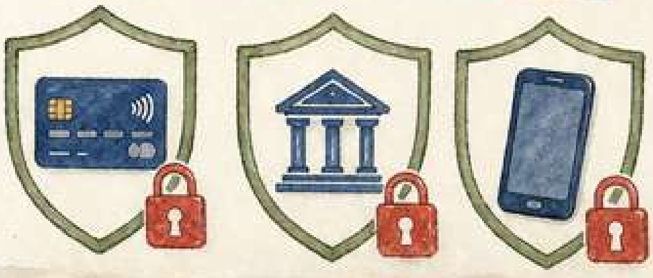
1. Call your bank immediately



2. Give the amount, time, IBAN and transaction reference

3. Say: "suspected fraud"

4. Ask whether cards, accounts or devices need blocking



5. Then report to the police by fraud type

IMPORTANT
Your bank may try to help, but recovery is not guaranteed.

DIGID COMPROMISED?

Check your login history

1. Change your DigiD password
2. Open Mijn DigiD → Gebruiksgeschiedenis
3. Check unknown organisations, dates and times
4. Contact DigiD and the organisation accessed
5. Deactivate the app on a stolen phone

USE A TRUSTED DEVICE

Act immediately if you see activity you do not recognise.

ID COPY LEAKED?

Protect your identity

1. 
Record who received it, when and why

2. 
Suspected identity misuse: contact CMI

3. 

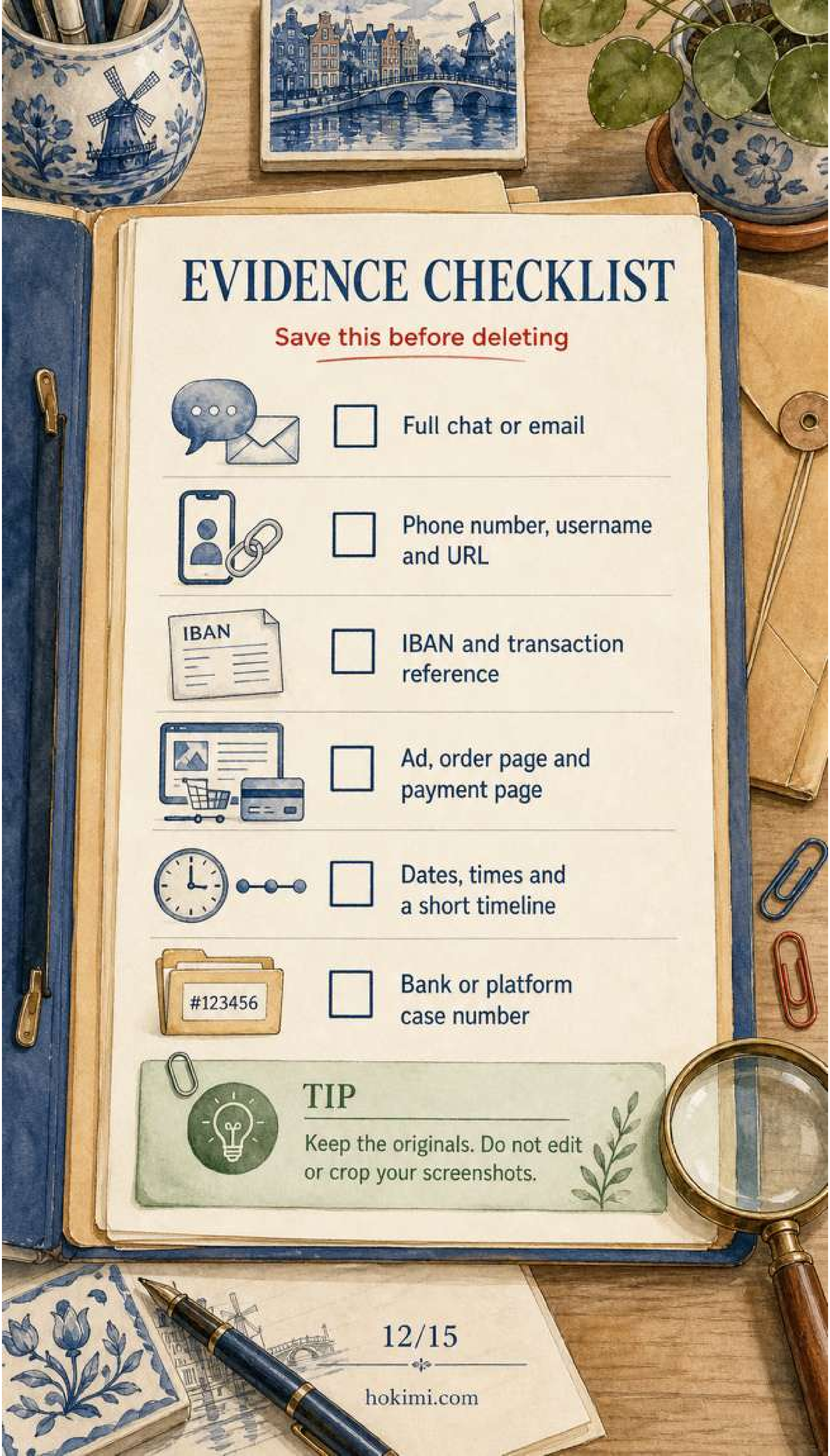
Actual fraud: report it to the police

4. 

Check MijnOverheid, your bank and unknown contracts

5. 

For future copies, use the KopieID app


EVIDENCE CHECKLIST
Save this before deleting
Full chat or email
Phone number, username and URL
IBAN
IBAN and transaction reference
Ad, order page and payment page
Dates, times and a short timeline
#123456
Bank or platform case number
TIP
Keep the originals. Do not edit or crop your screenshots.
12/15
hokimi.com

WHO TO CONTACT

Choose the right first call

BANK

Cards, accounts and payments

POLICE

Report and investigation

FRAUDEHELPDESK

Identify the scam, report it and plan next steps

DIGID OR THE AGENCY

Account misuse and unauthorised access

CMI

Identity theft and registration problems

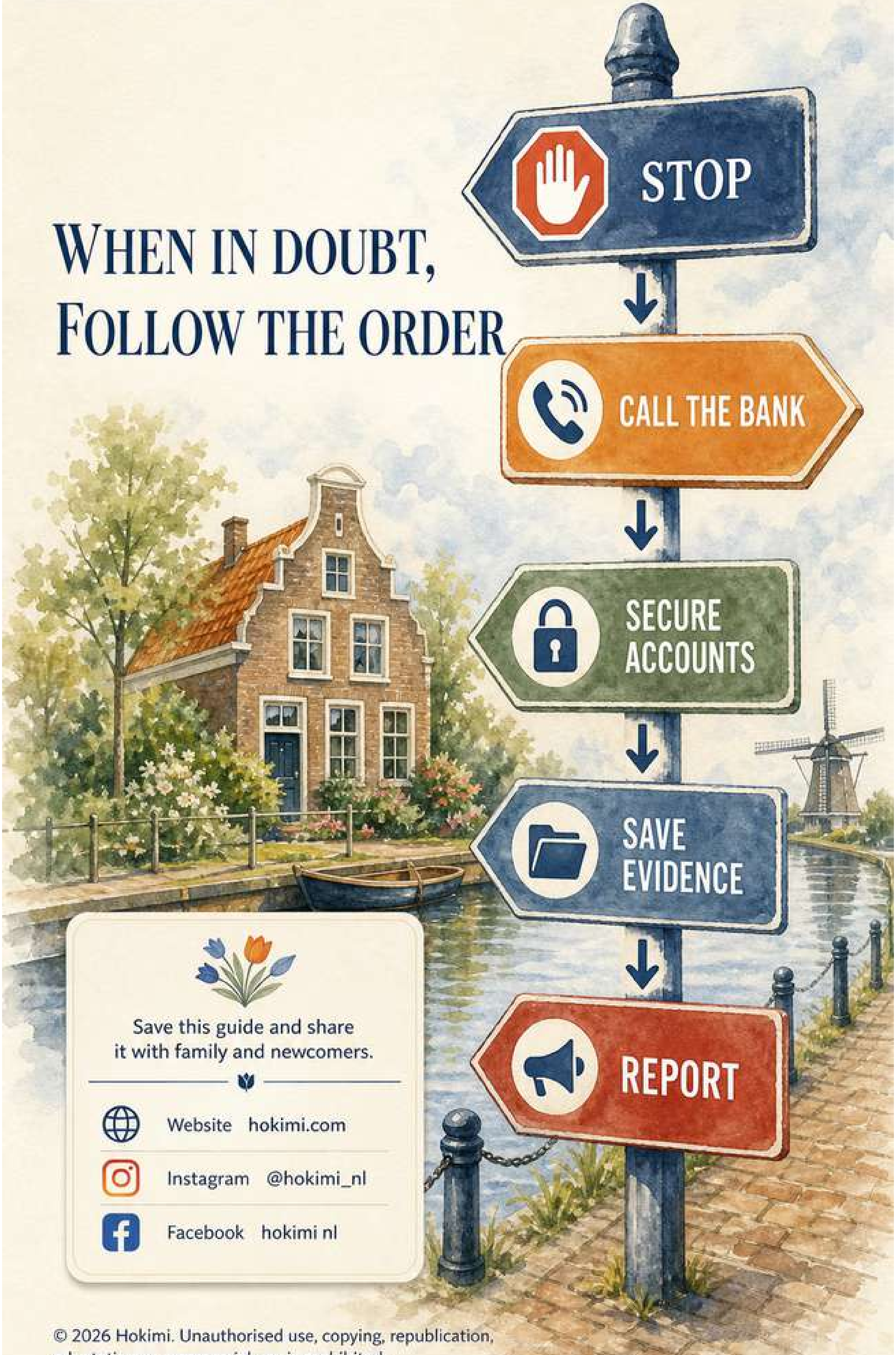
Build a Safer Routine

Small habits, stronger protection

THE GOLDEN RULE

Urgency is a signal to slow down.

When in doubt, Follow the order



Save this guide and share it with family and newcomers.

Website hokimi.com

Instagram @hokimi_nl

Facebook hokimi nl

General information only. Follow the latest guidance from your bank, Dutch Police, DigiD, Fraudehelpdesk and CMI.