Between the Lines

Issue 01 | October 2026

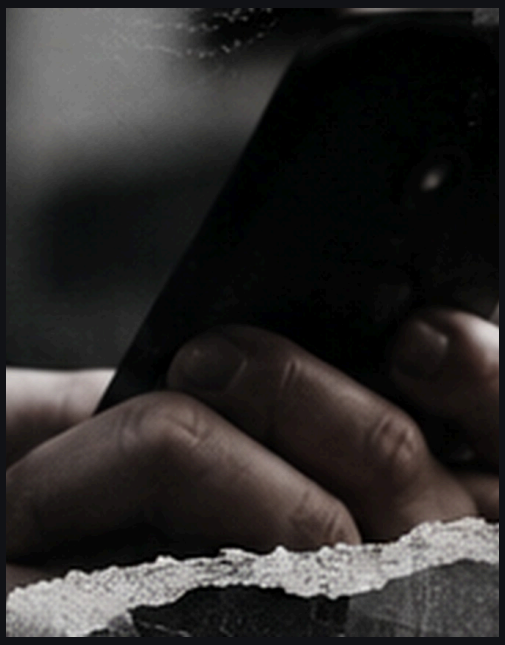
SHAHAR PAYNE

Fraud investigations · Behavioural analysis · Risk management

A monthly magazine about fraud, people
and the gap between what is said and what is happening

How do scammers build trust?

The psychology behind a call that sounds credible



Anatomy of impersonation

Authority, urgency and isolation

A scam scenario, step by step

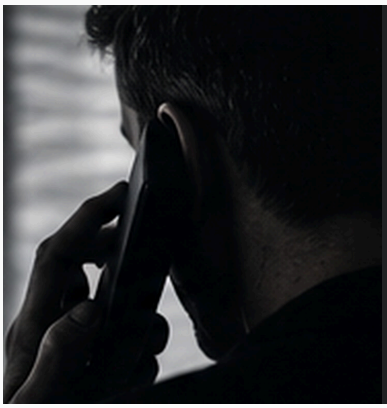
Five minutes leading to a dangerous decision

The toolbox

Questions to help you stay in control

Editor's note

The problem is not a call that sounds suspicious. The problem is a call that makes sense.



Someone trying to scam us does not have to convince us they are a good person. Sometimes it is enough to convince us they are the right person, at the right moment.

In this first issue, we examine a familiar method: someone impersonates a trusted authority, creates a sense of emergency and leads us to act before doubt has time to emerge.

$3.5B

Impersonation losses reported in the United States in 2025.
According to an analysis published by the US Federal Trade Commission (FTC) in June 2026. This figure concerns US reports only, not the scale of fraud in Israel. [1]

In this issue

03 · The three main manipulations

04 · Five minutes inside a scam call

05 · What the FTC figures really tell us

06 · Five questions an investigator asks

07 · What to do in the moment

08 · Sources, principles and further reading

> **The aim is not to fear every call. It is to recognise the moment someone asks us to give up independent verification.**

Anatomy of impersonation

Three pressure tactics. One decision.

In most calls described in official warnings, the questionable request does not appear at the start. First, the caller creates a situation in which the instruction sounds reasonable. These are three methods worth recognising. [2][3]



01

Authority

The caller claims a role, uses professional terms and sometimes supplies real information about you. The aim: reduce your need to verify who is on the other end.

Warning sign: a claimed identity is presented as proof.



02

Urgency

"If we do not act now, the money will disappear." The story leaves little time to think, consult someone or check the facts independently.

Warning sign: someone decides for you that there is no time.



03

Isolation

"Do not hang up", "Do not speak to anyone", "I will handle it personally". These instructions try to keep other sources of information out of the conversation.

Warning sign: outside verification is framed as a risk.

A successful scammer does not have to lie in every sentence.

Sometimes it is the combination of correct details, familiar language and one wrong instruction that makes the story believable.

This classification of three pressure tactics is the author's analytical framework, not an official taxonomy used by the authorities. The principles of impersonation, pressure and requests for information are supported by sources [2] and [3].

Illustrative scenario · A minute-by-minute view

Five minutes. Five steps. One suspicion.

Fictional scenario based on publicly described patterns. Not an account of a real case.

This is not "how a scammer lies". It is how an ordinary person is moved, gradually, from checking to carrying out instructions.

09:41

The first message: "Unusual activity detected"

A short message that appears to come from a financial institution. There is no request for payment, just a vague threat that creates a need to understand.

What is being created? A sense of concern.

09:42

The call: "I am from the security department"

The caller uses the name of a familiar institution, a professional tone and a few correct details. He does not prove his identity. He asks us to accept it.

What is being created? A sense of authority.

09:44

The clock: "We need to stop the transaction immediately"

The call shifts from an explanation to handling an "incident". The recipient is asked to stay on the line and not use another channel.

What is being created? Pressure and isolation.

09:45

The request: "Tell me the code we sent"

Now comes an action that seems relevant to a security process, but breaks a basic rule: do not give a verification code in a call you did not initiate.

The critical moment: moving from checking a story to taking a dangerous action.

09:46

The choice: hang up and verify independently

The recipient ends the call, opens the financial institution's app or calls its official number, and checks whether the incident really exists.

What changed? The recipient has taken back control.

> **The question is not "Does the caller sound credible?" It is "Do I have an independent way to check the claim before I act?"**
>
> **Source: Bank of Israel and FTC warnings. [2][3]**

Research and data · What the reports show

Impersonation is widespread. The reports show its scale.

In June 2026, the US Federal Trade Commission published a review of impersonation reports for 2025. The figures show the seriousness of the problem, but they also require careful interpretation. [1]

$3.5B

Reported losses · United States · 2025

The amount people reported losing to impersonation scams in the US. These are reported losses, not sums verified by a court in every case or a measure of all fraud that occurred.

Source: FTC press release, 15 June 2026. [1]

~1/3

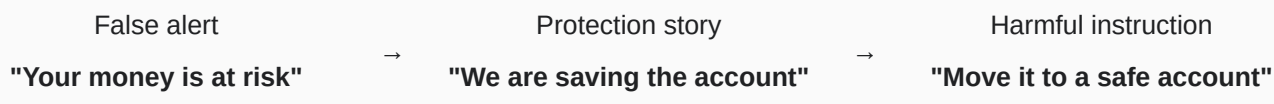
Almost one in three fraud complaints submitted to the FTC in 2025 concerned impersonation.

~$1B

About one billion dollars in reported losses from business impersonation, with bank impersonation prominent in this category.

$920M

About 920 million dollars in reported losses from impersonation of US government bodies.



The diagram illustrates a pattern described in the official publication, not an individual case. The reports do not establish prevalence rates in Israel or the total unreported harm.

The investigator's lens · Questions before conclusions

Before I believe a story, I check its structure.

A conversation can sound natural, well organised and even helpful. But an impression is not evidence. A useful way to examine a story is to separate what was said, what was verified and what is still unknown.



01 **Who initiated contact, and who is trying to choose the channel?**

Am I allowed to end the call and return through an official source I chose myself?

02 **Which facts have been verified independently?**

A name, address or four digits do not prove the caller's identity.

03 **Why does action have to happen right now?**

Real urgency can be checked. Urgency that prevents checking is a warning sign.

04 **Who gains control through this action?**

Does money, a code, device access or sensitive information pass to the other side?

05 **What answer would change my conclusion?**

If nothing could change it, we have probably stopped testing the story.

> **Working principle: suspicion justifies checking, not a premature finding of guilt. Even when signs cause concern, distinguish facts from interpretations and consider other explanations.**

Practical steps · Save and share

What should you do when someone "only wants to help"?

According to Bank of Israel and FTC recommendations, the simplest defence against impersonation is to change channels: stop the contact initiated by the caller and verify independently. [2][3]

Before taking action

01 Stop the call.

You may say "I will check and get back to you" and hang up.

02 Check through an independent channel.

Open an official app or call a number you found yourself.

03 Do not share a verification code.

Especially in a call or message you did not initiate.

04 Do not make a "rescue" transfer.

A demand to move money to a safe account is a serious warning sign.

05 Consult another person.

A request to keep the incident secret should raise a red flag.

If you already shared details

01 Contact your bank or card company immediately.

Use an official number and report what you shared.

02 Ask how to block further access or payments.

Secure accounts, payment methods and digital access as the relevant institution directs.

03 Preserve records.

Messages, phone numbers, references, receipts and screenshots.

04 Report to the appropriate bodies.

Contact the bank, police or other reporting service appropriate to the incident.

05 Check whether passwords need changing.

Revoke remote access if it was granted.

A phrase worth remembering

"I do not approve or share anything on an incoming call. I will contact you through the official channel."

This is general guidance, not a substitute for instructions specific to your case from the bank or authorities. If you fear a financial loss, contact the financial institution without delay.

Professional transparency · Public sources

You do not need to suspect everyone. You need to know what to check.

A good investigator is not measured by how quickly they decide they have spotted a scammer, but by the quality of the questions they ask on the way to a conclusion. This issue aims to encourage careful checking, not fear. Pause, check and separate the impression someone creates from facts you can verify.

> **If the other side resists independent verification, that itself is information worth considering.**

What is this issue based on?

[1] US Federal Trade Commission, 15 June 2026.
FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025
Financial figures and reporting volumes on pages 2 and 5.

[2] Bank of Israel, Banking Supervision Department, public warning.
Warning to the public: impersonating the Bank of Israel or commercial banks
Impersonation methods, the risk of sharing codes and recommended actions.

[3] FTC Consumer Advice, January 2026.
How to handle unexpected calls that claim your money is at risk
Independent verification, avoiding disclosure and consulting someone.

[4] Bank of Israel, Banking System Annual Survey 2024.
Israel's Banking System: Annual Survey 2024
Israeli background on impersonation and social engineering, not a source for US figures.

The investigation continues on the site.

Public-source case analyses, behavioural patterns and an interactive simulation:

shahar-payne.pages.dev/en/
Shahar Payne · Fraud investigations, behavioural analysis and risk management

© Shahar Payne, 2026. Educational publication based on public sources. The scenario on page 4 is fictional and contains no material from a workplace. The images are adaptations of AI-generated work made for this issue, not photographs of a real event. This is not legal or financial advice. Source links are active in the digital edition. English translation: 27 October 2026. Source dates and figures are those of the Hebrew edition.