FULL SCRIPT • READABLE WITHOUT JAVASCRIPT

Who is on the line? The full script

Every simulation screen, the branching map and all five endings with their summaries.

Play the interactive simulation

INTERACTIVE SIMULATION • FICTIONAL LEARNING SCENARIO

Who is on the line?

One evening, one call from "the bank", and a decision at every stage. About 4-6 minutes, with five possible endings.

A fictional learning scenario. The characters and conversation are invented. They are not based on a real case or workplace. There is no single correct answer. You can go back and choose differently at any stage.

What this is

One evening with Yael, the owner of a small plant shop, and a call from "the bank" that sounds professional and calm. You decide what happens at each stage. About 4-6 minutes, one screen at a time, with no time limit or artificial pressure.

Learn how a scammer can sound like the bank, why "I will not ask for a code" lowers suspicion, and where to stop: hang up and dial the number on the back of your card yourself.

Six chances to stop before the money moves. Five endings. Three characters: Yael, Daniel and Orna.

Branching map

- This call could cost you NIS 38,000. Can you spot why?: Start → Tuesday, 18:40
- Tuesday, 18:40: Answer the call → The call
- Tuesday, 18:40: Do not answer. Check the banking app → Ending 1 of 5 • Stopped early
- The call: "I did not make that purchase." → Two perspectives: the first minute
- The call: "Wait, how do I know you really work for the bank?" → Two perspectives: the first minute
- Two perspectives: the first minute → The message
- Two perspectives: the first minute → The call
- The call: Hang up and dial the number on the back of the card → Ending • Stopped at the first check
- The call: "All right, send a message." → The message
- The message: Approve in the app. The message is real, and he did not even ask for a code. → Two perspectives: the message
- The message: "The message says not to approve if I did not request this. You are telling me to approve." → The question about the message
- The message: Hang up and dial the number on the back of the card. → Ending • Stopped at the message
- The question about the message: Accept the explanation and approve. → Two perspectives: the message
- The question about the message: "I would rather hang up and call myself." → Ending • Stopped at the message
- Two perspectives: the message → The second voice
- Two perspectives: the message → The second voice

- The second voice: Transfer through the app. I am making the transfer myself, so it is safe. → Two perspectives: the transfer
- The second voice: "That is a large amount. I will ask at the branch tomorrow first." → "I will ask at the branch tomorrow"
- The second voice: Hang up and dial the number on the back of the card. → Ending • Close call: stopped before the transfer
- "I will ask at the branch tomorrow": "All right, I will transfer it." → Two perspectives: the transfer
- "I will ask at the branch tomorrow": "I am hanging up and calling the bank." → Ending • Close call: stopped before the transfer
- Two perspectives: the transfer → Ending • Transfer completed
- Two perspectives: the transfer → Ending • Transfer completed
- Ending 1 of 5 • Stopped early: Show me → The call
- Ending 1 of 5 • Stopped early: Summary → Summary below the ending
- Ending • Stopped at the first check: Summary → Summary below the ending
- Ending • Stopped at the first check: What if I had continued? → The message
- Ending • Stopped at the message: Summary → Summary below the ending
- Ending • Stopped at the message: What if I had continued? → The second voice
- Ending • Close call: stopped before the transfer: Summary → Summary below the ending
- Ending • Transfer completed: Summary → Summary below the ending

S0

This call could cost you NIS 38,000. Can you spot why?

Step into one evening in Yael's life.

Start

S1

Tuesday, 18:40

Yael, 42, runs a small plant shop. She is making dinner when her phone rings. The screen says "The bank", and the number looks like her bank's number.

Answer the call

Do not answer. Check the banking app

S2

The call

> **Daniel**
>
> Good evening, am I speaking to Yael? This is Daniel from the bank's credit card security team.

> **Daniel**
>
> We have received a request to charge the card ending in 4417. NIS 3,890, at an electronics website overseas. The charge is still pending.

> **Daniel**
>
> One more thing before we continue. I will not ask you for a code or password, now or later. If anyone does, hang up.

"I did not make that purchase."

"Wait, how do I know you really work for the bank?"

V1A

Two perspectives: the first minute

What Yael knew

The number looks like the bank's. He knows her name and the last digits of her card. He sounds calm and polite, and he has warned her not to share a code.

The fraudsters' aim

Lower her guard before making the first request. A number can be spoofed and details obtained elsewhere. A warning that says "I am on your side" makes her question him less.

The mechanism

The Chameleon and the Professional: speaking the bank's language and preparing an answer to every suspicion.

V1B

Two perspectives: the first minute

What Yael knew

The number looks like the bank's. He knows her name and the last digits of her card. He sounds calm and polite, and he has warned her not to share a code.

The fraudsters' aim

Lower her guard before making the first request. A number can be spoofed and details obtained elsewhere. A warning that says "I am on your side" makes her question him less.

The mechanism

The Chameleon and the Professional: speaking the bank's language and preparing an answer to every suspicion.

S2V

The call

> **Daniel**
>
> Good question. I am glad you asked. You do not have to take my word for it.

> **Daniel**
>
> Hang up, dial the number on the back of your card and ask about a pending charge on card 4417. Or, if you prefer, I can send a bank message to your phone now so you can see I am genuine.

Hang up and dial the number on the back of the card

"All right, send a message."

S3

The message

> **Daniel**
>
> Good. We will cancel the charge and block the card. It will take two minutes. I am sending you a message from the bank now. Read it.

> **Message from "Bank"**
>
> A request has been received to add a new payee to your account. Open the app to approve. Did not request this? Do not approve it. Call the number on the back of your card.

> **Daniel**
>
> Got it? Good. That means the system has identified you. Do not worry about the wording. It is a standard message the system sends for every action. Open the app and approve the request waiting there. That will cancel the charge.

Approve in the app. The message is real, and he did not even ask for a code.

"The message says not to approve if I did not request this. You are telling me to approve."

Hang up and dial the number on the back of the card.

S3Q

The question about the message

> **Daniel**
>
> Yes, and you are right to read it. It is standard wording attached to every request. This is the cancellation request, which is why you need to approve it.

Accept the explanation and approve.

"I would rather hang up and call myself."

V3A

Two perspectives: the message

What Yael knew

An official message arrived just when he said it would, under the bank's name. He did not ask her for a code. Everything seems to match his promise.

The fraudsters' aim

He initiated the request himself. In this scenario, he had Yael's account access details from another source, not from the bank. He used them to request a new payee, and the bank sent a genuine notification. He turned it into proof that he was genuine.

The mechanism

The Chameleon: details in a criminal's hands do not prove that he is an insider. A real safeguard became his cover.

V3B

Two perspectives: the message

What Yael knew

An official message arrived just when he said it would, under the bank's name. He did not ask her for a code. Everything seems to match his promise.

The fraudsters' aim

He initiated the request himself. In this scenario, he had Yael's account access details from another source, not from the bank. He used them to request a new payee, and the bank sent a genuine notification. He turned it into proof that he was genuine.

The mechanism

The Chameleon: details in a criminal's hands do not prove that he is an insider. A real safeguard became his cover.

S5

The second voice

Yael approves in the app. It says: "New payee added: Temporary security account".

> **Daniel**
>
> Excellent, thank you. I am putting you through to the shift manager, who will close the case with you.

> **Orna**
>
> Good evening, Yael. I am Orna, the shift manager. Daniel said you were precise and helpful. There is one step left.

> **Orna**
>
> To keep the pending charge from affecting the money in your account, you need to move it temporarily to the security account you approved. NIS 38,000. It will come back when we close the case.

Transfer through the app. I am making the transfer myself, so it is safe.

"That is a large amount. I will ask at the branch tomorrow first."

Hang up and dial the number on the back of the card.

S6

"I will ask at the branch tomorrow"

> **Orna**
>
> I understand. But the charge could go through tonight, and then it becomes harder to deal with. It is in your hands.

"All right, I will transfer it."

"I am hanging up and calling the bank."

V4A

Two perspectives: the transfer

What Yael knew

Daniel and Orna sound like the bank. The message and the app look like the bank. And she is the one pressing the button, in her own account, in her own app.

The fraudsters' aim

Get her to make the transfer herself. They do not need to break into anything, just get her to act. Technically, she carried out the transaction herself.

The mechanism

The Operator and the Chameleon: several voices switch roles, all speaking the bank's language, until the action looks like something Yael did herself.

V4B

Two perspectives: the transfer

What Yael knew

Daniel and Orna sound like the bank. The message and the app look like the bank. And she is the one pressing the button, in her own account, in her own app.

The fraudsters' aim

Get her to make the transfer herself. They do not need to break into anything, just get her to act. Technically, she carried out the transaction herself.

The mechanism

The Operator and the Chameleon: several voices switch roles, all speaking the bank's language, until the action looks like something Yael did herself.

E1

Ending 1 of 5 • Stopped early

You stopped early. What would have happened if Yael had answered?

Yael lets the phone ring and opens her banking app. There is no alert, no pending charge and no message. The ringing stops. A minute later she dials the number on the back of her card and asks whether they tried to contact her. The answer is no.

Show me

Summary

E1 summary



Summary 1 of 3 • The key decision

The key decision was not answering the call and checking through a channel you chose yourself, without relying on the caller's claims.

What you did right. You did not rely on the caller's claims. You checked through a channel you chose yourself.



Summary 2 of 3 • Warning signs along the way

- The call came to her. She did not initiate it.
- A number that looks like the bank's is not proof. The caller display can be spoofed.
- The app check showed no pending charge and no message.

On caller ID spoofing: FCC, United States.



Summary 3 of 3 • What you could do differently

- Hang up and dial the number on the back of the card yourself, at any stage. The caller can wait.

- Open the app independently, without instructions from the caller.
- Ask a question the script did not anticipate.
- Tell someone close to you before taking action.

Sources: Bank of Israel public warning (the bank will not ask for secret details or verification codes; call back only using a number you found independently). This is general advice, not a particular bank's procedure.

E2

Ending • Stopped at the first check

Yael hangs up and dials the number on the back of her card. The representative checks: there is no pending charge. She offers to block the card in case its details have leaked and records the suspicious call. Daniel does not call again.

Summary

What if I had continued?

E2 summary



Summary 1 of 3 • The key decision

The key decision was ending the call and contacting the bank through a channel you chose yourself.

Notice this. "I will not ask for a code" sounds protective, but it also lowers suspicion. It was said to make you check less.



Summary 2 of 3 • Warning signs along the way

- The call came to her. She did not initiate it.
- A number that looks like the bank's is not proof. The caller display can be spoofed.
- He knew her name and the last digits of her card. Those details do not prove that he works for the bank.
- "I will not ask for a code" lowered suspicion. It is still worth checking.
- Politeness and calm are not evidence.

On caller ID spoofing: FCC, United States.



Summary 3 of 3 • What you could do differently

- Hang up and dial the number on the back of the card yourself, at any stage. The caller can wait.
- Open the app independently, without instructions from the caller.
- Ask a question the script did not anticipate.
- Tell someone close to you before taking action.

Sources: Bank of Israel public warning (the bank will not ask for secret details or verification codes; call back only using a number you found independently). This is general advice, not a particular bank's procedure.

E3

Ending • Stopped at the message

Yael hangs up. The bank sees an unapproved request to add a new payee that Yael did not initiate. The representative cancels it, changes the account access credentials and records Yael's report.

Summary

What if I had continued?

E3 summary



Summary 1 of 3 • The key decision

The key decision was ending the call and contacting the bank through a channel you chose yourself.

The revealing moment. "I will not ask for a code" sounds protective. And the real bank message, the one saying "Do not approve if you did not request this", arrived just when he promised it would. Those two details seemed to prove he was on her side. In fact, he knew she would look for exactly those signs and fitted them to his story. The genuine message was there to protect her. Instead, it became part of his script.



Summary 2 of 3 • Warning signs along the way

- The call came to her. She did not initiate it.
- A number that looks like the bank's is not proof. The caller display can be spoofed.
- He knew her name and the last digits of her card. Those details do not prove that he works for the bank.
- "I will not ask for a code" lowered suspicion. The real request was different: that she approve it herself.
- The bank message said not to approve if she had not requested it. The caller told her to approve.

- Politeness and calm are not evidence.

On caller ID spoofing: FCC, United States.



Summary 3 of 3 • What you could do differently

- Hang up and dial the number on the back of the card yourself, at any stage. The caller can wait.
- Open the app independently, without instructions from the caller.
- Ask a question the script did not anticipate.
- Tell someone close to you before taking action.

Sources: Bank of Israel public warning (the bank will not ask for secret details or verification codes; call back only using a number you found independently). This is general advice, not a particular bank's procedure.

E4

Ending • Close call: stopped before the transfer

Yael hangs up and calls. The bank representative sees that the payee was added a few minutes earlier, but no transfer has been made. She removes it and blocks account access pending renewed verification. The money stays where it is.

Summary

E4 summary



Summary 1 of 3 • The key decision

You stopped after approving a payee but before the money moved. The key decision was not making the transfer and returning to a channel you chose yourself.

The revealing moment. "I will not ask for a code" sounds protective. And the real bank message, the one saying "Do not approve if you did not request this", arrived just when he promised it would. Those two details seemed to prove he was on her side. In fact, he knew she would look for exactly those signs and fitted them to his story. The genuine message was there to protect her. Instead, it became part of his script.



Summary 2 of 3 • Warning signs along the way

- The call came to her. She did not initiate it.
- A number that looks like the bank's is not proof. The caller display can be spoofed.
- He knew her name and the last digits of her card. Those details do not prove that he works for the bank.
- "I will not ask for a code" lowered suspicion. The real request was different: that she approve it herself.

- The bank message said not to approve if she had not requested it. The caller told her to approve.
- A second voice, the "shift manager", moved the call toward a transfer.
- A request to move money "temporarily" to a security account.
- Politeness and calm are not evidence.

On caller ID spoofing: FCC, United States.



Summary 3 of 3 • What you could do differently

- Hang up and dial the number on the back of the card yourself, at any stage. The caller can wait.
- Open the app independently, without instructions from the caller.
- Ask a question the script did not anticipate.
- Do not transfer money to an account someone else designated, or approve a request you did not initiate.
- Tell someone close to you before taking action.

Sources: Bank of Israel public warning (the bank will not ask for secret details or verification codes; call back only using a number you found independently). On moving money "to protect it": FTC, United States. This is general advice, not a particular bank's procedure.

E5

Ending • Transfer completed

Ten minutes later Yael dials the number on the back of her card herself. The representative asks one question: who asked you to transfer money? The money is already gone.

What to do now: report immediately to the bank and the police, and preserve the call and message details.

> **Orna**
>
> The case is closed. Thank you, Yael. Good evening.

Summary

E5 summary



Summary 1 of 3 • The key decision

The key decision was when Yael approved the new payee on the caller's instructions. From then on, everything led to one step: a transfer. But there were still two chances to stop before transferring: with Orna, and at "I will ask at the branch".

The revealing moment. "I will not ask for a code" sounds protective. And the real bank message, the one saying "Do not approve if you did not request this", arrived just when he promised it would. Those two details seemed to prove he was on her side. In fact, he knew she would look for exactly those signs and fitted them to his story. The genuine message was there to protect her. Instead, it became part of his script.



Summary 2 of 3 • Warning signs along the way

- The call came to her. She did not initiate it.
- A number that looks like the bank's is not proof. The caller display can be spoofed.
- He knew her name and the last digits of her card. Those details do not prove that he works for the bank.
- "I will not ask for a code" lowered suspicion. The real request was different: that she approve it herself.

- The bank message said not to approve if she had not requested it. The caller told her to approve.
- A second voice, the "shift manager", moved the call toward a transfer.
- A request to move money "temporarily" to a security account.
- Politeness and calm are not evidence.

On caller ID spoofing: FCC, United States.



Summary 3 of 3 • What you could do differently

- Hang up and dial the number on the back of the card yourself, at any stage. The caller can wait.
- Open the app independently, without instructions from the caller.
- Ask a question the script did not anticipate.
- Do not transfer money to an account someone else designated, or approve a request you did not initiate.
- Tell someone close to you before taking action.

Sources: Bank of Israel public warning (the bank will not ask for secret details or verification codes; call back only using a number you found independently). On moving money "to protect it": FTC, United States. This is general advice, not a particular bank's procedure.

All characters and events are fictional. There is no connection to a real case, bank or workplace. English translation: 27 October 2026.

The patterns behind the scenario

The Chameleon • The Professional • The Operator

Download the full English script (PDF)