CYBEHAVE ACADEMY · SPECIALIST

The Psychology of Social Engineering

Course workbook

Why the lure works, how to read it, and how to design the counter.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

The first real lure I will autopsy, in one line

cybehave.com/training · © 2026 CyBehave. All rights reserved. For use alongside The Psychology of Social Engineering video course.

BEFORE YOU START

How to use this workbook

This is the specialist course on the human side of the attack: why a well-made lure works on an ordinary, careful person, how to read one back to the mechanism that made it work, and how to choose a counter that defeats the mechanism rather than the symptom. The workbook follows the ten videos in order, holds every sheet the videos refer to, and ends with the eight quizzes and their answers. By the end you will have a lure library started, three autopsies written, a never-asks list drafted, two risk maps drawn and a twelve-month programme on one page.

Five ways to get the most from it

1. **Bring three real lures.** Reported ones, not templates. Every section has a "Your next lure" box; the autopsy in module 7 uses all three.
2. **Fill the diagnostic card every time.** Seven fields, the same order, the ask as a verb. The card is what makes two readers agree and the library comparable.
3. **Never write a name.** The card has no field for the person. If you catch yourself describing character, go back to the moment.
4. **Take the quizzes.** Scenarios, not definitions. Check the key and read the explanation for anything you missed.
5. **Do one thing per module.** Fill a card. Tag the levers. Name the mechanism. Map the emotion. Draft the never-asks list. Draw the two maps. Run the autopsy. Pick the counter.

The course at a glance

Module	Title	Tools in this workbook
0	Welcome	The lifecycle of an attack; meet Ola.
1	The Attack as a Designed Decision	The lifecycle sheet; the diagnostic card, blank and worked.
2	Six Principles, Read Backwards	Principles vocabulary; lever tagging sheet; counter-by-principle starter.
3	Scam Mechanics	Stajano and Wilson sheet; mechanism and lever side by side.
4	Emotion and the Narrowing of Attention	The emotion map; the first-report experience audit.
5	Pretext, Identity and Trust	Pretext library; never-asks lists by role; independent-channel sheet.
6	Who, When and Where	Role risk map; moment map; the no-blame rule as written.
7	The Lure Autopsy	Three blank cards; the ten-minute procedure; the lure library sheet; the four-sentence autopsy.
8	Designing the Defence	Counter-by-mechanism table; simulation-as-diagnostic sheet; twelve months on one page; HEROES map.
9	Close	Eight ideas; Monday list; glossary; further reading; quiz answers.

Three lines you will hear again

Diagnose the lure, not the person. · The counter must match the mechanism. · Nobody is disciplined for being caught by a lure.

WORKED EXAMPLE

Meet Ola

Ola Adeyemi is the security awareness lead at Calder and Voss, a law firm of 2,100 people across London, Manchester, Leeds and Edinburgh, with a finance team of 40, a helpdesk of 9 and around 60 trainees a year. Before this job she spent eight years as a fraud investigator at a bank, where she learned to read a scam backwards. The course follows one year in which she builds a lure library of 42 entries, runs an autopsy clinic with the firm's Champions, and replaces an awareness programme with a diagnostic one.

The five lures the course returns to
The completion-day email (modules 1, 7): a conveyancing client paid £312,000 to the wrong account at 10:50 on completion morning, after an email from a look-alike domain built from their own compromised mailbox. The client rang the number in the email to check. Levers: authority, time, consistency.
The MFA reset call (modules 3, 6, 7): a trainee four weeks in took a call at 17:40 from "IT", who was patient, kind and apologetic, and read out a code after five small steps. Levers: social compliance, kindness, consistency.
The vendor who moved banks (modules 2, 3, 8): a letter on day one, a call on day six, an email on day twelve, each referring to the last. A callback to the number on file saved £48,000. The supplier's own mailbox had been compromised in September. Lead lever: consistency.
The LinkedIn recruiter (modules 4, 6): a second-year associate opened a "pre-interview brief" that was a credential stealer and did not report it for nine days. Levers: curiosity, liking. Counter: the report route redesigned; latency from 4h 10m to 22 minutes by year end.
The partner on video (modules 5, 7, 8): a finance manager was asked on a short video call, from "an airport", to release £184,000. She rang the partner's PA, Maria. The partner was in Leeds. The partner then recorded a 30-second video for the firm on what he will never ask.

Use Ola as a mirror

Each time a Calder and Voss card appears, ask: what is my equivalent? Which of my roles can pay, admit or reset? Which lever is winning in my own lures, and does any control I have address it?

MODULE 1

The Attack as a Designed Decision

Key ideas from the video

- A social engineering attack is a designed decision: the attacker chooses the channel, pretext, lever, emotion, timing, target and ask so that the easiest thing to do is the thing they want. Every one of those is a choice, and choices can be read back.
- The lifecycle: research (public sources, a compromised mailbox, a previous breach), pretext, approach, pressure, the ask, and the exit. Most controls watch the approach. The decision is made at the pressure stage.
- The diagnostic card has seven fields and no field for character. The ask is a verb: pay, read out, click, admit, change. The verb tells you where the brace goes.
- Around six in ten breaches involve a human element (Verizon DBIR 2025); business email compromise alone cost $2.77 billion across 21,442 complaints to the FBI's IC3 in 2024. The decision is the attack surface.
- Diagnosing the lure produces a counter that protects the next person in the role. Diagnosing the person produces blame and a lost report.

Template: the lifecycle sheet

Stage	What the attacker did (or must have done)	What we saw of it	What could have seen it
Research			
Pretext			
Approach			
Pressure			
The ask			
Exit			

Template: the diagnostic card (blank)

Field	Entry
Channel	
Pretext	
Lever (lead, closer, quiet one)	
Emotion	
Timing	
Target (role, tenure)	

Field	Entry
The ask (a verb)	

Worked: the completion-day email

Field	Entry
Channel	Email, then the attacker's phone number
Pretext	The firm; details taken from the client's own mailbox
Lever (lead, closer, quiet one)	Authority (lead), time (closer), consistency (quiet)
Emotion	Anxiety
Timing	10:50 on completion morning
Target (role, tenure)	A conveyancing client, first house purchase
The ask (a verb)	Pay £312,000 to a new account

What Ola wrote under the card

"This worked because the firm's authority, the client's own expectation of a payment that morning, and a check routed through the attacker's number made the wrong account the easiest thing to do." Counter: the firm's bank details printed at engagement with the line "these will never change by email; if you are told they have, ring the number on this letter", and a client-facing never-asks card.

Your next lure

Fill the seven fields for your most recent real lure. Which field was hardest, and why?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take your most recent real lure. Walk it through the lifecycle: where did the research come from, what was the pretext, where was the pressure applied?

2. What channels reach your people that your controls never see: phone, chat, letter, visitor, video, text?

3. Fill in the seven fields of the diagnostic card for that lure. Which field was hardest to answer, and why?

4. What did the attacker need the person to do, in one plain verb?

5. Who else in your organisation reads lures, and do they use the same seven fields as you?

Module 1 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. The course describes a social engineering attack as "a designed decision". What does that mean in practice?

A The attacker decides which technical control to bypass

B The victim designs their own downfall through carelessness

C The decision is random and cannot be analysed

D The attacker chooses the channel, pretext, lever, emotion, timing, target and ask so that the easiest thing for the person to do is the thing the attacker wants

2. Which of these is NOT one of the seven fields on the diagnostic card?

A The emotion

B The ask

C The target's personality type

D The channel

3. Why does the course insist that "the ask is a verb"?

A Because the quiz software needs it

B Because the counter is designed around the action the attacker needs, and a verb (pay, read out, click, admit) points straight at where a brace or a verification goes

C Because verbs are easier to translate

D Because the ask is always to send money

4. In Ola's completion-day case, the client paid £312,000 to the wrong account after ringing the number in the email. What does the course take from the phone call?

A That verification through a channel the attacker supplied is not verification, so the counter is a known channel, not "ring to check"

B That clients should never phone law firms

C That the client was unusually careless

D That phone calls are always safer than email

5. What is the difference between diagnosing the lure and diagnosing the person?

A There is no difference; both find the cause

B Diagnosing the person is faster and therefore preferable

C Diagnosing the lure requires forensic tooling

D Diagnosing the lure produces a counter that protects the next person in that role; diagnosing the person produces blame and a lost report

6. According to the 2025 Verizon DBIR cited in the module, roughly what share of breaches involve a human element?

- **A** Exactly half
- **B** Almost all, around 98%
- **C** About six in ten
- **D** Under one in ten

MODULE 2

Six Principles, Read Backwards

Key ideas from the video

- Cialdini's principles (reciprocity, commitment and consistency, social proof, authority, liking, scarcity; unity added in 2021) are a vocabulary for diagnosis. Read them backwards: from the lure in front of you to the lever doing the work, never from the list to an example.
- Authority and scarcity of time are the commonest pair. Authority borrows a role's permissions; a deadline forecloses the check. In Ola's library: authority 31, time 27.
- Consistency is the quiet one under almost every multi-step attack: having agreed to four small things, refusing the fifth feels like going back on yourself. The vendor who moved banks was a letter, a call and an email, each referring to the last.
- Social proof and liking are levers for the attacker as well as defences for you. "Everyone has already confirmed" is a pretext line. A visible norm of reporting is the same mechanism pointed the other way.
- The vocabulary becomes useful when it becomes a tally. Tag every lure; count the levers quarterly; let the counts choose the first counter.

Template: the principles vocabulary

Principle	What it looks like in a lure	A line from a real lure of ours	The counter that works
Authority	A senior name, a role, a regulator, a client		Verified channel; never-asks list
Scarcity (time)	A deadline that forecloses checking		The brace; a delay nobody justifies
Social proof	"Everyone else has done this"		A visible norm of reporting
Liking	Warmth, shared interest, flattery		Permission to refuse, scripted
Reciprocity	A favour first, then the ask		The stop rule at the step that matters
Consistency	Small steps, each referring to the last		A stop rule that ignores what came before
Unity	"We", the same firm, the same team		Known-contact check

Template: lever tagging sheet

Lure (date, one line)	Lead lever	Closer	Quiet one	Ask (verb)

Lure (date, one line)	Lead lever	Closer	Quiet one	Ask (verb)

The vendor who moved banks

Day 1, a letter on the supplier's paper: "we are changing banks next month". Day 6, a call: "did you get our letter?" Day 12, an email from the supplier's real, compromised mailbox with the new details, "as discussed". Each contact referred to the last; by the third, the change felt established. The accounts assistant followed the callback rule and rang the number already on file. The supplier knew nothing about it. £48,000 stayed where it was.

Ola's tag: consistency (lead), authority (the supplier's own paper), time (the month end). Counter: the callback rule on any change of details, which does not care how many contacts came before it.

Your next lure

Tag three real lures. Which principle carried the weight in each, and which counter do you already have for it?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take three real lures from your organisation. Which principles does each pull, and which one carried the weight?

2. Where does your organisation make authority easy to fake: titles in signatures, org charts on the website, a culture that does not question seniors?

3. What small first step do your people routinely take for a stranger (a form, a survey, a confirmation) that an attacker could build consistency on?

4. Which norms messages in your programme could an attacker borrow? "Everyone has completed the update" works both ways.

5. For each principle, which counter do you already have, and which is missing?

Module 2 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does "read backwards" mean when applied to Cialdini's principles?

A Apply the principles to persuade colleagues to be more careful

B Memorise the six and recite them

C Start from the lure in front of you and work out which principle is doing the work, rather than starting from the list and looking for examples

D Read the principles in reverse alphabetical order

2. A message from "the managing partner" asks for a payment "before the auditors arrive at 3". Which two principles are leading?

A Liking and reciprocity

B Authority and scarcity (of time)

C Reciprocity and liking

D Social proof and consistency

3. Which principle most often appears as the "quiet one" underneath multi-step attacks?

A Consistency: each small step makes the next feel like the natural continuation of what has already been agreed

B Scarcity

C Social proof

D Reciprocity

4. In the vendor-who-moved-banks case, what order did the attacker use the channels, and why does the order matter?

A Email first because it is fastest

B Call only, because voice is most convincing

C All three on the same day to overwhelm the target

D Letter, then call, then email, each referring to the last, so that by the third contact the change felt established rather than new

5. Why does the course treat "social proof" as a lever rather than only a defence?

A Because it only appears in marketing

B Because it is the strongest of the six

C Because "everyone else has already done this" is a pretext line, and a lure that claims the whole team has complied borrows the herd

D Because social proof cannot be used defensively

6. What was the first thing Ola did with the principles vocabulary at Calder and Voss?

A Tested whether staff could recite the six

B Used it to tag every lure in the library with its levers, so that the counts, not opinions, decided which counter to build first

C Ran a lunchtime talk on persuasion

D Rewrote the phishing policy

MODULE 3

Scam Mechanics

Key ideas from the video

- Stajano and Wilson (2011) studied real confidence tricks and found seven recurring principles: distraction, social compliance, the herd, dishonesty, kindness, need and greed, and time. Security should be designed around how people actually behave, which is what the scams exploit.
- Cialdini names why a person is inclined to comply; Stajano and Wilson name how the scam is staged. A full autopsy usually needs both layers, and the card has room for both.
- Social compliance plus kindness is the signature of the fake IT call: the role carries compliance, the patient, apologetic caller invites help. Neither is a flaw in the trainee.
- Dishonesty predicts under-reporting: a person drawn into something slightly irregular is less likely to report, because reporting feels like confession. No-blame is an operational control, not a kindness.
- Time, in reverse, is the defence: a process that gives people time to think has defeated the commonest closer before it arrives.

Template: the scam-mechanics sheet

Principle (Stajano and Wilson)	How it is staged	Where it lands in our organisation	Our control, if any
Distraction	Something urgent occupies attention while the ask passes		
Social compliance	A role we are trained to obey asks		
The herd	"Everyone is doing it"; a crowd of confederates		
Dishonesty	The target is drawn into something they cannot report		
Kindness	The target's wish to help is the lever		
Need and greed	What the target wants is offered		
Time	The clock forecloses the check		

Template: mechanism and lever side by side

Lure	Cialdini lever(s)	Stajano and Wilson mechanism(s)	Where the two readings disagree

Lure	Cialdini lever(s)	Stajano and Wilson mechanism(s)	Where the two readings disagree

The MFA reset call

17:40, a Thursday. A trainee four weeks in. The caller says he is from IT, apologises for the hour, explains a sync problem, asks her to confirm her username, then her device, then whether she can see a prompt, then to approve it, then to read the six digits back "so I can close the ticket and let you go home". Five small steps. She read the code out. She reported it the next morning, and the account had already been locked by a Champion who saw the login from Lagos.

Ola's reading: social compliance (lead), kindness (closer), consistency (quiet); Cialdini authority and liking underneath. Counter: "IT will never ask you to read out a code", in week one of induction, with the helpdesk callback number on the same card.

Your next lure

Take one real lure and name both a Cialdini principle and a Stajano and Wilson principle in it.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Which of the seven scam principles does your awareness programme never mention? Why not?

2. Where does kindness get exploited in your organisation: reception, the helpdesk, the new starter who wants to help?

3. Where is distraction built into the working day: the busiest hour, the busiest screen, the task people do while on the phone?

4. Which of your processes relies on "the time principle" in reverse, giving people time to think, and which does not?

5. Take one real lure and name both a Cialdini principle and a Stajano and Wilson principle in it. Where do the two vocabularies disagree?

Module 3 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. Stajano and Wilson derived their principles from studying what?

A Interviews with convicted hackers

B Real confidence tricks, including those filmed for a television series, to find the mechanisms that recur regardless of the scam

C Phishing emails collected by a bank

D Laboratory experiments on students

2. Which mechanism describes a caller who is patient, friendly and apologetic, and asks a new starter to "just read the code back so I can close the ticket"?

A Social compliance combined with kindness: the role of IT carries compliance and the person wants to help someone who seems to be struggling

B Dishonesty

C Need and greed

D The herd

3. What does the "dishonesty" principle predict about reporting?

A Dishonest people are more often targeted

B Attackers never lie outright

C Reporting rates are unaffected by the lure

D A person who was drawn into something slightly irregular is less likely to report, because reporting means admitting the irregularity

4. Which of these is the "distraction" mechanism in the course's terms?

A Background music on a phone call

B A long email that nobody reads

C Something urgent and legitimate-looking occupies attention while the real ask passes unexamined

D A pop-up advert

5. Why does the course pair Stajano and Wilson's principles with Cialdini's rather than replacing one with the other?

A Stajano and Wilson only apply to in-person fraud

B Cialdini names why a person is inclined to comply; Stajano and Wilson name how a scam is staged. A full autopsy usually needs both

C The two lists are identical

D Cialdini is out of date

6. In the module's case, what single control stopped the vendor payment, and which mechanism did it defeat?

A A callback to the number already on file, defeating the time pressure and the manufactured consistency of three contacts

B A spam filter, defeating distraction

C A password change, defeating dishonesty

D A warning banner, defeating the herd

MODULE 4

Emotion and the Narrowing of Attention

Key ideas from the video

- Under a strong emotion, attention narrows to the source of the feeling and the fastest way to relieve it. The checks that would normally run do not run. The lure offers relief one click away.
- Two systems (Kahneman): the fast one acts, the slow one checks. Every element of a lure is designed to keep the slow one off. Loewenstein's "visceral factors" (1996) describe how hot states crowd out longer-term considerations: the cost of skipping a check is discounted to nothing.
- Ola's library by emotion: anxiety 23, helpfulness 14, curiosity 9. Greed barely featured. The programme had been built around greed.
- "Don't rush" only feels like a counter, because the emotion that makes a person rush also makes them certain they are not rushing. A brace built into the process does not depend on the person noticing. Design for the Friday brain.
- Measure report latency, not just rate: a report after four hours is an attack that ran for four hours. Latency is where the shame lives, and shame is the attacker's second lever.

Template: the emotion map

Emotion the lure aimed for	How the lure produced it	What relief it offered	Where that emotion is built into our own processes	The pause we could design in
Anxiety				
Helpfulness				
Curiosity				
Fear of blame				
Other				

Template: the first-report experience audit

Question	Honest answer	Change
How many clicks or calls to report, and does the person know the route without looking?		
Who sees the report first, and is their manager copied?		
What is the first reply, in what tone, how fast?		
Does anyone ever ask what the lure was about (the job advert, the parcel)?		
What happens to a person who reports that they clicked, paid or read out a code?		

Question	Honest answer	Change
Median latency last quarter, real lures		

The LinkedIn recruiter and the nine days

A second-year associate received a warm message from a recruiter with a real agency's name about a confidential role at a rival firm, then a "pre-interview brief". Curiosity and liking. The brief was a credential stealer. She did not report it for nine days, because the only route she knew ran through her supervising partner, and reporting would mean admitting she had been looking at a job. Ola's reading: the lure was designed so that the report would feel like a confession.

Counter: a report route with no manager in the loop; a line from the top, "we never ask what the lure was about"; the stories of people who reported, told with permission and no names. Median latency on real lures: 4 hours 10 minutes in the first quarter, 22 minutes in the last.

Your next lure

Sort your last ten lures by the emotion they aimed for. Which dominates, and does your programme ever name it?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Sort your last ten lures by the emotion they aimed for. Which one dominates, and does your programme ever name it?

2. Where in your processes is a strong emotion built in by design (a deadline, a disciplinary, a bonus letter)? That is where the attacker's version will land.

3. What does your first-report experience feel like for someone who is embarrassed? Would you report, in their place?

4. Which of your processes has a pause designed into it, and which relies on the person inventing one under pressure?

5. What is the one sentence your programme gives people to name a feeling in the moment?

Module 4 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does the course mean by "the narrowing of attention"?

A Under a strong emotion, attention focuses on the source of the feeling and the fastest way to relieve it, so the checks that would normally run are not run

B People become unable to read

C Only one person can be attacked at a time

D Attention narrows only in people with anxiety disorders

2. Which three emotions led Ola's lure library, in order?

A Anger, fear, greed

B Curiosity, boredom, pride

C Greed, anxiety, loneliness

D Anxiety, helpfulness, curiosity

3. Why does the course call "don't rush" a counter that only feels like one?

A Because rushing is sometimes correct

B Because posters are expensive

C Because the emotion that makes a person rush also makes them certain they are not rushing; a brace built into the process does not depend on the person noticing

D Because everyone already knows not to rush

4. Loewenstein's work on "visceral factors", cited in the module, supports which claim?

A That people can switch emotions off at will

B That strong immediate states crowd out longer-term considerations, so a person under acute anxiety discounts the cost of skipping a check

C That emotions make people more careful

D That only hunger affects decisions

5. The LinkedIn recruiter lure at Calder and Voss went unreported for nine days. What did the course identify as the reason, and the counter?

A Shame that the curiosity had been about a new job; the counter was a report route with no manager in the loop and a public statement that the content of a lure is never asked about

B The trainee did not know the IT number; the counter was a poster

C Nine days is normal; no counter was needed

D The firm had no email; the counter was to buy one

6. Why does the course insist on measuring report latency and not only report rate?

A Because rate is impossible to measure

B Because latency is what the regulator asks for

C Because latency is always zero

D Because a report after four hours is an attack that ran for four hours; latency measures the damage window and shows whether shame is still in the system

MODULE 5

Pretext, Identity and Trust

Key ideas from the video

- A pretext is a borrowed identity or role that brings its own permissions. IT may ask for codes; the partner may ask for payments; the client may demand urgency. The lure borrows the permission with the role.
- An hour of open-source research (OSINT) gives an attacker names, roles, projects, travel, suppliers and systems. The pretext is built from what you publish. The Arup case (reported by CNN, May 2024): about $25 million released after a video call on which the CFO and colleagues were deepfakes.
- The never-asks list is the strongest cheap counter: by role, by channel, what that role will never ask for. "IT will never ask you to read out a code" is a rule, not a judgement, so it works in a fast-system moment.
- For a voice, a video or a document that looks exactly right, the only counter is an independent channel the attacker does not control: a known number, a known person, a known process.
- Authority is a lever for the attacker only while the real authority is silent. The most impersonated person in the firm saying out loud what they will never ask turns the lever into a defence.

Template: the pretext library

Pretext (sender and story)	Permission it borrows	Channel it would use	Who it would target	What would give it away (if anything)
IT / helpdesk				
Senior leader				
Client / customer				
Supplier / vendor				
Recruiter / HR				
Regulator / auditor / bank				
Colleague / new starter				

Template: never-asks lists by role

Role	Will never ask you to…	By this channel	If you get that request, do this
IT / helpdesk			
Finance			
Senior leaders			
HR			

Role	Will never ask you to…	By this channel	If you get that request, do this
The firm, to clients			

Template: the independent channel

Process that moves money, access or data	Channel the request usually arrives by	The independent channel we verify on	Who owns the known numbers / list

The partner on video

15:10 on a Thursday. A finance manager accepted a short video call from a partner "between flights", picture breaking up, asking her to release £184,000 to complete a client matter before the counterparty's deadline. The partner's travel was on LinkedIn. She said she would do it straight away, hung up, and rang the partner's PA, Maria, on the internal number. The partner was in the Leeds office. Nothing was paid.

The partner then recorded a 30-second video for the whole firm: "I will never ask you to move money by message or video. If you get that request, ring Maria." Ola filed it as the cheapest counter of the year.

Your next lure

Write the five pretexts that would work best against your people, as a sender and a story.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. What could an attacker learn about your organisation in an hour from public sources: names, roles, projects, travel, suppliers, systems?

2. Which five pretexts would work best against your people? Write them as a sender and a story.

3. What does your IT team never ask for? What does your finance team never do by phone? Are those lists written down and taught?

4. For a voice, a video call or a document that looks exactly right, what is the independent channel in each of your main processes?

5. Who in your organisation is most impersonated, and have they said out loud what they will never ask?

Module 5 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. **What is a pretext, in the course's definition?**

   A A fake email address

   B The excuse a victim gives afterwards

   C A password reset link

   D A borrowed identity or role that brings its own permissions, so that the ask seems to be the role asking rather than a stranger

2. **What is a "never-asks list"?**

   A A blocklist of email domains

   B A list of forbidden passwords

   C A published statement, by role, of what that role will never ask for by that channel, so a request that breaks it is recognisable without judgement

   D A list of people who never ask questions

3. **In the Arup case cited in the module, roughly how much was lost, and through what?**

   A About $250 million, through ransomware

   B About $25 million, after a finance employee joined a video call on which the CFO and colleagues were deepfakes

   C About $25,000, through a phishing email

   D Nothing; the attack was stopped

4. **The partner-on-video lure at Calder and Voss asked for £184,000. What stopped it?**

   A The finance manager rang the partner's PA, Maria, on a known number; the partner was in Leeds, not an airport

   B The video quality was poor

   C The bank blocked the transfer

   D The partner happened to walk past

5. **Why does the course say "check the sender address" only feels like a counter to familiarity?**

   A Because sender addresses are hidden by most mail clients

   B Because it takes too long

   C Because attackers always use the real address

   D Because a look-alike domain is designed to pass a glance, a compromised real mailbox passes any inspection, and a phone call has no address to check

6. The partner recorded a 30-second video for the firm after the attempt. What was the point, in the course's terms?

A To warn that staff would be disciplined

B To demonstrate deepfake technology

C The most senior voice setting the norm: "I will never ask you to move money by message or video; if you get that request, ring Maria", which turns authority into a defence

D To apologise for being impersonated

MODULE 6

Who, When and Where: Susceptibility Without Blame

Key ideas from the video

- Traits predict susceptibility weakly and inconsistently: personality, age, gender, intelligence, education and security knowledge all come and go across studies. Situations predict strongly and repeatably: workload, expectation, sender familiarity, role, channel, tenure (Williams, Hinds and Joinson, 2018).
- Experts are caught in their own domain because expertise sets the template the attacker copies, and routine makes the hundred-and-first payee change look like the other hundred.
- Two maps: the role map (who can pay, approve, admit, reset or move data, and what reaches them) and the moment map (Friday afternoon, month end, the first four weeks, the day after a breach in the news, alone on a shift). Lay the lure library over both.
- The "gullible user" model costs reports, latency, trust and produces the wrong fix. No-blame is a control with a measurable return: more reports, sooner, from the roles that matter.
- Simulations report by lever, role, channel and moment, never by name, never to a line manager. A simulation that teaches fear of the security team has built the attacker a lever.

Template: the role risk map

Role	Can pay / approve / admit / reset / move data	What reaches them, by which channels	How often they are asked	Lures in our library targeting this role	Rank (access × exposure)
Finance and payments					
PAs and executive assistants					
Reception and facilities					
Helpdesk					
HR					
New starters (first six weeks)					
Other					

Template: the moment map

Moment	When it falls for us	Lures in our library landing here	Who is most alone or newest then	Control that assumes this moment
End of day / Friday afternoon				

Moment	When it falls for us	Lures in our library landing here	Who is most alone or newest then	Control that assumes this moment
Month end, quarter end, completion, payroll				
First four weeks in a job				
Day after a breach in the news				
Alone: night, home, single cover				
During a real change: new system, merger, move				

Template: the no-blame rule, as written

Line	Our wording	Said by whom, where, when
Nobody is disciplined for being caught by a lure		
Everyone is thanked for reporting one, including the ones they fell for		
We never ask what the lure was about		
Simulation results are never reported by name		
When a manager asks for a name, the answer is no, because…		

Ola lays the library over the maps

By target role: finance and conveyancing 17; trainees and new starters 9; PAs 6; reception and facilities 4; helpdesk 3; everyone else 3. Partners were the pretext in 14 and the target in 1. By moment: 11 after 16:00; 9 in the last three days of a month; 7 in the first six weeks of tenure; 5 in the week a breach was in the news; 4 on the one person covering a desk. The twelve people caught or nearly caught were ordinary; two were among the most experienced in the firm.

What changed: the never-asks card and callback rule in week one of induction; the payee brace and a four-eyes rule on first payments; a quarterly PA session built from the partner-impersonation lures; "no pass, no entry, however nice" at reception with the partners' backing. Disciplinaries: zero. Managers who asked for a name: three. Names given: none.

Your next lure

Which of your controls assume a careful person, and which assume a Friday afternoon?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Draw your role risk map: which five roles can pay, approve, admit, reset or move data, and what reaches them?

2. Draw your moment map: when are your people busiest, newest, most expected to comply, and most alone?

3. What does your programme currently say or imply about the kind of person who gets caught? Would you say it to their face?

4. Which of your controls assume a careful person, and which assume a Friday afternoon?

5. Who was caught last year, and what was true of the moment rather than the person?

Module 6 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. Williams, Hinds and Joinson (2018) studied phishing susceptibility in real workplaces. What did they find predicted it?

A Age over fifty

B Lack of security training

C Situational factors: workload and pressure, whether the message was expected, and familiarity with the apparent sender, rather than stable personal traits

D Low intelligence

2. Why are finance teams among the most caught, according to the module?

A Attackers dislike accountants

B They have the access and the routine: a hundred genuine payee changes a year make the hundred-and-first look ordinary

C Finance staff are less careful than others

D They receive less training

3. What are the two maps the module asks you to draw?

A A role map (who can pay, approve, admit, reset or move data) and a moment map (when people are busiest, newest, most expected to comply, and most alone)

B A network diagram and a floor plan

C A map of attackers and a map of victims

D An org chart and a holiday calendar

4. Which of these is a cost of the "gullible user" model, as the course lists them?

A Higher software licence fees

B More spam

C Fewer phishing emails sent

D Longer report latency, because shame delays the report

5. How did Ola redesign simulations to fit the no-blame rule?

A Results were published with names to motivate staff

B Only partners were simulated

C Results reported by lever, role, channel and moment, never by name and never to a line manager

D Simulations were stopped entirely

6. Why does the course describe no-blame as "a control with a measurable return" rather than a value statement?

A Because auditors require it

B Because it produces more reports, sooner, from the roles that matter, which shows up as a falling latency line and a rising report rate

C Because values are not allowed in security policy

D Because it reduces the cost of training licences

MODULE 7

The Lure Autopsy

Key ideas from the video

- The ten-minute autopsy has six steps, the same every time: collect; read as the target; fill the seven fields; order the levers (lead, closer, quiet one); write the "this worked because" sentence; choose the counter.
- Collect at report time: the lure, headers or call notes, the time, the role and tenure, what else was happening, what the person did and when they reported. A week later it is gone.
- Read as the target first, once, at their pace. The first feeling is the emotion field, and it is lost the moment you start analysing.
- The lure library is one row per lure: the seven fields plus source, outcome, latency and counter. Useful at ten entries, persuasive at forty. It shows which mechanism is winning, whether voice is rising, and whether your counter moved the latency. A click rate shows none of that.
- The autopsy clinic: forty-five minutes a month with Champions, three anonymised lures, the card on a whiteboard, an argument about the lead lever, a sentence the target could read without flinching. The four-sentence autopsy (what arrived, why it worked, the moment, the counter) is what the board and the incident report get. No name.

The ten-minute procedure

Step	What to do	Minutes	Done
1 Collect	Lure, headers or notes, time, role, tenure, context, action, report time	2	
2 Read as the target	Once, at their pace, on their device if you can; note the first feeling	1	
3 Fill the seven fields	One line each; the ask is a verb	3	
4 Order the levers	Lead, closer, quiet one; multi-step lures always have consistency	1	
5 Write the sentence	"This worked because…", a mechanism, words the target could read	2	
6 Choose the counter	From the mechanism, not the symptom: brace, control, channel, message, norm	1	

Autopsy one

Field	Entry
Channel	
Pretext	
Lever (lead, closer, quiet one)	
Emotion	

Field	Entry
Timing	
Target (role, tenure)	
The ask (a verb)	

This worked because…

Counter chosen

Autopsy two

Field	Entry
Channel	
Pretext	
Lever (lead, closer, quiet one)	
Emotion	
Timing	
Target (role, tenure)	
The ask (a verb)	

This worked because…

Counter chosen

Autopsy three

Field	Entry
Channel	
Pretext	
Lever (lead, closer, quiet one)	
Emotion	
Timing	
Target (role, tenure)	
The ask (a verb)	

This worked because…

Counter chosen

Template: the lure library sheet

#	Date	Channel	Pretext	Levers	Emotion	Timing	Target role	Ask	Source (R/S)	Outcome	Latency	Counter

#	Date	Channel	Pretext	Levers	Emotion	Timing	Target role	Ask	Source (R/S)	Outcome	Latency	Counter

Source: R reported, S simulation. Outcome: reported before harm, stopped by brace or callback, reached the ask. Aggregate before it goes anywhere; names stay in the incident system.

Template: the four-sentence autopsy

Sentence	Yours
1 What arrived: channel, pretext and ask, in plain words	
2 Why it worked: the levers and the emotion	
3 The moment: time, tenure, what else was happening, which control was not yet in place	
4 The counter: what changes, and the library entry number	

Template: the autopsy clinic agenda (45 minutes)

Minutes	Item
0 to 5	Three anonymised lures from the month on the table; real ones beat simulations
5 to 10	Everyone reads the first one as the target, silently, and writes their first feeling
10 to 25	Fill the card together on a whiteboard; argue about the lead lever
25 to 35	Write the sentence as a group; test it: would the target read it without flinching?
35 to 40	Choose the counter; record the library entry
40 to 45	Each Champion names what they will take to their team's huddle

Ola's library at forty-two

Levers: authority 31, time 27, familiarity 24, consistency 11, social proof 9, kindness 8, liking 7, scarcity 6, reciprocity 5. Emotions: anxiety 23, helpfulness 14, curiosity 9. Channels: email 26, voice 8, chat 4, letter 2, video 2. Sources: 29 reported, 13 from simulations. Outcomes: 30 reported before harm, 8 near misses stopped by a brace or callback, 4 reached the ask. Thirteen entries came from the clinic, brought by Champions.

What the library said that a click rate never had: authority and time were the problem, not "awareness"; voice was rising and produced the closest calls; consistency sat under every multi-step attack with no control addressing it. The board paper was one page. The managing partner asked: "Why didn't we have this before?"

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Autopsy your three real lures now, on the card, in ten minutes each. Write the "this worked because" sentence for each.

2. Which fields were you guessing at? What would you need to collect at report time to stop guessing?

3. Compare your reading of one lure with a colleague's. Where do you disagree, and which of you has the evidence?

4. What does your lure library tell you after ten entries that a click rate never could?

5. Who should be in your first autopsy clinic, and which lure will you open with?

Module 7 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What are the six steps of the ten-minute autopsy, in order?

A Read the headers; check the domain; run antivirus; reset the password; notify the bank; file a report

B Collect; read as the target; fill the seven fields; order the levers; write the "this worked because" sentence; choose the counter

C Block; delete; report; train; test; repeat

D Identify the victim; interview them; assign training; close the ticket; record the click; report to HR

2. Why does the procedure insist on "read as the target" before analysis?

A Because the first feeling is the emotion field, and it is lost the moment you start analysing; it is also what tells you what the lure was designed to do

B Because it is polite to the victim

C Because analysis is unnecessary

D Because it makes the autopsy longer

3. What makes a "this worked because" sentence a good one?

A It names the person and what they should have noticed

B It is at least a paragraph long

C It recommends more training

D It names a mechanism, in words the target could read without flinching, and nothing about the person

4. What is the quality check on an autopsy?

A The victim agrees with it

B It matches the vendor's threat report

C Two readers fill the card for the same lure independently and compare; disagreement is a conversation about the vocabulary, not a failure

D A manager signs it off

5. What did Ola's library show at forty-two entries that a click rate never had?

A That the spam filter needed upgrading

B That authority and time were the programme's real problem, that voice lures were rising and producing the closest calls, and that consistency sat under every multi-step attack with no control addressing it

C That the firm had a 12% click rate

D That trainees were the weakest link

6. What is the four-sentence autopsy for, and what does it leave out?

A For incident reports and the board: what arrived, why it worked, the moment, and the counter; it leaves out the name

B For the victim's HR file: what they did wrong

C For the attacker: a warning letter

D For the regulator: a legal defence

MODULE 8

Designing the Defence from the Diagnosis

Key ideas from the video

- The counter must match the mechanism. Authority: a verified channel and a never-asks list. Time: the brace. Familiarity: the callback rule and the known-contact check. Consistency: a stop rule that ignores what came before. Social proof and liking: a visible norm of reporting. Kindness and compliance: scripted permission to refuse.
- Recognition training is the weakest counter: it trains the symptom of the lure you showed, assumes the slow system is running, and decays in weeks. It keeps a place as vocabulary, so people can name and report. The order of preference: remove the decision, brace it, verify it, then teach it.
- A simulation is an experiment. Hypothesis first, one lever, matched roles and moments from the two maps, outcomes as report rate and latency, results by lever and never by name. Every simulated lure goes in the library on the same card. (See Running Behavioural Experiments for the design of a fair comparison.)
- The course produces four behaviours: verify by a known channel; report fast, including the ones you fell for; refuse the unverified ask politely; pause at the brace. In HEROES they are priority behaviours, each counter an intervention with its COM-B driver, two Team Pulse items, and report rate and latency as outcome measures.
- Twelve months on one page: a lever per quarter, a control per lever, a measure per control, a clinic a month. Nothing on the page says "awareness".

Template: counter by mechanism

Lever / mechanism	Count in our library	The counter that works	The one that only feels like one (what we do now?)	Build this quarter?
Authority		Verified channel; never-asks list	"Be suspicious of senior requests"	
Time		The brace; a delay nobody justifies	"Don't rush"	
Familiarity		Callback rule; known-contact check	"Check the sender address"	
Consistency		Stop rule at the step that matters	"Trust your instincts"	
Social proof / liking		Visible norm of reporting; stories told	A poster	
Kindness / compliance		Scripted permission to refuse	"It's OK to say no"	
Curiosity / fear		Report route with no shame; latency measured	"Think before you click"	

Template: the simulation as a diagnostic

Line	Entry
Hypothesis (which role, which lever, which moment)	
The one lever this simulation isolates	
Roles and moments matched, from the two maps	
Outcome measures: report rate, report latency (and click rate, last)	
Reported by lever, role, channel, moment; never by name; never to a line manager	
Library entry number and counter it tests	
What we will do if it shows no change	

Template: twelve months on one page

Quarter	Lever	Control built	Measure	Clinic lures
Q1				
Q2				
Q3				
Q4				

Template: the HEROES map

This course	In HEROES	Ours
Verify by a known channel before acting on any instruction that moves money, access or data	Priority behaviour from the catalogue	
Report suspected lures fast, including the ones you fell for	Priority behaviour; report rate and latency as reporting measures	
Refuse the unverified ask, politely and without apology	Priority behaviour; refusal scripts as an intervention	
Pause at the brace	Priority behaviour; each brace an intervention with its COM-B driver and APEASE pass	
"I know how to check a request is genuine" / "I would report a mistake"	Team Pulse quarterly items	
The lure library and simulations	Not in HEROES: they stay with you; the movement shows on the programme overview	

Ola's year, by the numbers she chose

Three counters: the payment brace with a four-eyes rule on first payments; the callback rule on any change of details; the never-asks card and refusal scripts in week one of induction. Simulations redesigned: one lever each, matched roles, reported by lever and moment; simulated report rate 12% in the first quarter, 34% in the last. Report latency: median 4h 10m to 22 minutes. Eight near misses stopped by a brace or callback, including £48,000 and £184,000. Disciplinaries: zero.

In HEROES: four priority behaviours ranked; three interventions with their COM-B drivers; the two Team Pulse items up eleven and nine points; report rate and latency on the programme overview as the lines the board now asks for. Next year: voice. Eight calls produced three of the four closest calls, and no control yet assumes the phone can lie.

Your next lure

Take your top lever from the library. Which row of the counter table does it point to, and what is the one control you would build this quarter?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take your top lever from the lure library. Which row of the counter table does it point to, and what is the one control you would build this quarter?

2. Which of your processes has a brace today, and which one that moves money, access or data has none?

3. What does your simulation programme report, and to whom? Would it survive the "no names" rule?

4. Which behaviours from this course are already in your HEROES catalogue, and which measures will show they moved?

5. Write your twelve-month programme on one page: a lever per quarter, a control per lever, a measure per control.

Module 8 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. **What is the rule the module says most programmes break?**

   A The counter must match the mechanism: an authority lure needs a verified channel, not a spelling lesson

   B Never run simulations

   C Always train everyone annually

   D Block all external email

2. **What is the counter to the "time" lever that works, and the one that only feels like it works?**

   A Works: faster payment systems. Feels like it: slower ones

   B Works: a poster about deadlines. Feels like it: a brace

   C Works: removing all deadlines. Feels like it: a callback rule

   D Works: a brace built into the process, a pause nobody has to justify. Feels like it: telling people not to rush

3. **Why does the course rank recognition training as the weakest counter?**

   A Because staff dislike it

   B Because attackers attend the same training

   C It trains the symptom of the lure you showed, assumes the slow system is running when the attack is designed to keep it off, and decays within weeks

   D Because training is expensive

4. **What is the order of preference for counters that the module gives?**

   A Brace, teach, remove, verify

   B Remove the decision, then brace it, then verify it, and only then teach it

   C Teach first, then test, then punish

   D Verify everything, then train, then remove email

5. **What makes a simulation a diagnostic rather than a test?**

   A A hypothesis first, one lever per simulation, matched roles and moments from the two maps, outcome measured as report rate and latency, and results by lever not by name

   B Sending it to everyone at once

   C Using the vendor's most popular template

   D Publishing a league table

6. How do the course's four behaviours sit in HEROES?

A HEROES runs the simulations and stores the lure library

B HEROES replaces the need for a lure library

C They do not; HEROES is only for Champions

D As priority behaviours from the catalogue, with each counter as an intervention, two Team Pulse items, and report rate and latency as outcome measures on the programme overview

CLOSE

Close: What to Do on Monday

The course in eight lines

1. **The attack is a designed decision.** Seven fields on the card: channel, pretext, lever, emotion, timing, target, the ask.
2. **Six principles, read backwards.** From the lure to the lever, not the other way.
3. **Scam mechanics.** Distraction, social compliance, the herd, dishonesty, kindness, need and greed, time.
4. **Emotion narrows attention.** Design for the Friday brain; measure latency.
5. **Pretext, identity and trust.** The borrowed role carries its permissions; the never-asks list and the verified channel take them back.
6. **Who, when and where.** Situation beats trait; two maps; no blame.
7. **The lure autopsy.** Ten minutes, six steps, one sentence, a library.
8. **The defence from the diagnosis.** Counter matched to mechanism; simulations as diagnostics; the behaviours in HEROES.

Monday

Done	This week
☐	Collect three real lures from the last quarter, with the time, the role and what happened
☐	Run three ten-minute autopsies on the card and write the "this worked because" sentence for each
☐	Start the library: a spreadsheet, seven fields plus source, outcome, latency and counter
☐	Draft the never-asks list and find the senior voice to publish it
☐	Book the first autopsy clinic with your Champions, forty-five minutes, next month
☐	Write down, and say out loud, that nobody is disciplined for being caught by a lure

Glossary

Term	Meaning in this course
Lure	Any contact designed to produce a decision the attacker wants: email, call, chat, letter, video, visit.
Pretext	A borrowed identity or role that brings its own permissions.
Lever	The persuasion principle doing the work: authority, scarcity, social proof, liking, reciprocity, consistency, unity.
Lead, closer, quiet one	The lever that opens, the lever that forces the decision, the lever underneath that nobody notices.

Term	Meaning in this course
Mechanism	How the scam is staged (Stajano and Wilson): distraction, social compliance, the herd, dishonesty, kindness, need and greed, time.
Narrowing of attention	Under a strong emotion, attention focuses on relief and the normal checks do not run.
The brace	A pause built into a process so that it does not depend on the person noticing they are being rushed.
Never-asks list	By role and channel, what that role will never ask for; a rule, not a judgement.
Independent channel	A way to verify that the attacker does not control: a known number, a known person, a known process.
Role map / moment map	Who can pay, approve, admit, reset or move data; when people are busiest, newest, most compliant and most alone.
Autopsy	The ten-minute, six-step reading of a lure onto the diagnostic card, ending in a sentence and a counter.
Lure library	One row per lure, seven fields plus source, outcome, latency, counter; tallied quarterly.
Report latency	Time from the lure landing to the report; the damage window, and where shame shows.
Simulation as diagnostic	A simulated lure run as an experiment: hypothesis, one lever, matched roles, results by lever not by name.

Further reading

- Cialdini, R. B. (2021). Influence, New and Expanded: The Psychology of Persuasion. Harper Business.
- Stajano, F. and Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3).
- Ferreira, A., Coventry, L. and Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. Human Aspects of Information Security, Privacy and Trust, LNCS 9190.
- Gragg, D. (2003). A Multi-Level Defense Against Social Engineering. SANS Institute.
- Kahneman, D. (2011). Thinking, Fast and Slow. Penguin.
- Loewenstein, G. (1996). Out of control: visceral influences on behavior. Organizational Behavior and Human Decision Processes, 65(3).
- Williams, E. J., Hinds, J. and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120.
- Verizon (2025). Data Breach Investigations Report. FBI Internet Crime Complaint Center (2025). 2024 Internet Crime Report.
- National Cyber Security Centre. Phishing attacks: defending your organisation. ncsc.gov.uk.
- CyBehave Academy: Running Behavioural Experiments; Being a Security Champion; Thinking Clearly Under Pressure; Behavioural Risk Foundations.

Notes

ANSWER KEY

Quiz answers

Four of six is a pass. Read the explanation for every question you missed, then go back to the card it points at.

Module 1: The Attack as a Designed Decision

#	Answer	Why
1	D The attacker chooses the channel, pretext, lever, emotion, timing, target and ask so that the easiest thing for the person to do is the thing the attacker wants	Every field on the diagnostic card is a choice the attacker made. Reading those choices back is the whole method.
2	C The target's personality type	The card has no field for character. Channel, pretext, lever, emotion, timing, target and ask describe the attack, not the person.
3	B Because the counter is designed around the action the attacker needs, and a verb (pay, read out, click, admit) points straight at where a brace or a verification goes	A vague ask ("gain access") hides the control point. "Read out a code" tells you exactly which moment to protect.
4	A That verification through a channel the attacker supplied is not verification, so the counter is a known channel, not "ring to check"	The client did what most guidance says: they checked. The attacker had designed the check into the lure.
5	D Diagnosing the lure produces a counter that protects the next person in that role; diagnosing the person produces blame and a lost report	The method is deliberately about the attack. The person is the witness, not the fault.
6	C About six in ten	The figure is around 60%, and the course uses it to argue that the human decision is the main attack surface, not a side issue.

Module 2: Six Principles, Read Backwards

#	Answer	Why
1	C Start from the lure in front of you and work out which principle is doing the work, rather than starting from the list and looking for examples	The principles are a vocabulary for diagnosis. The direction matters: lure to lever, never lever to lure.
2	B Authority and scarcity (of time)	A senior name is authority; a deadline that forecloses checking is scarcity. Together they are the commonest pair in Ola's library.
3	A Consistency: each small step makes the next feel like the natural continuation of what has already been agreed	Having said yes to the first four small things, saying no to the fifth feels like going back on yourself. That is the lever.
4	D Letter, then call, then email, each referring to the last, so that by the third contact the change felt established rather than new	The sequence manufactures consistency. The callback to a known number broke it and saved £48,000.

#	Answer	Why
5	C Because "everyone else has already done this" is a pretext line, and a lure that claims the whole team has complied borrows the herd	The same mechanism that makes a visible reporting norm work for you makes "your colleagues have all confirmed" work for the attacker.
6	B Used it to tag every lure in the library with its levers, so that the counts, not opinions, decided which counter to build first	The vocabulary becomes useful when it becomes a tally. Authority 31 and time 27 set the first quarter's programme.

Module 3: Scam Mechanics

#	Answer	Why
1	B Real confidence tricks, including those filmed for a television series, to find the mechanisms that recur regardless of the scam	Their 2011 paper argues that security systems should be designed around how people actually behave, which is what the scams exploit.
2	A Social compliance combined with kindness: the role of IT carries compliance and the person wants to help someone who seems to be struggling	The MFA reset call in Ola's library leads with compliance to a role and closes with kindness. Neither is a flaw in the trainee.
3	D A person who was drawn into something slightly irregular is less likely to report, because reporting means admitting the irregularity	This is why no-blame matters operationally: the lure may have been designed to make the report feel like a confession.
4	C Something urgent and legitimate-looking occupies attention while the real ask passes unexamined	Attention is finite. Attacks place the ask where the attention is not.
5	B Cialdini names why a person is inclined to comply; Stajano and Wilson name how a scam is staged. A full autopsy usually needs both	Lever and mechanism are different layers of the same attack. The card has room for both.
6	A A callback to the number already on file, defeating the time pressure and the manufactured consistency of three contacts	A verified channel does not care how many contacts came before it. That is why it beats a multi-step attack.

Module 4: Emotion and the Narrowing of Attention

#	Answer	Why
1	A Under a strong emotion, attention focuses on the source of the feeling and the fastest way to relieve it, so the checks that would normally run are not run	Anxiety wants relief, curiosity wants the answer, helpfulness wants to help. The lure offers exactly that, one click away.
2	D Anxiety, helpfulness, curiosity	Anxiety 23, helpfulness 14, curiosity 9. Greed barely featured, which surprised the partners.
3	C Because the emotion that makes a person rush also makes them certain they are not rushing; a brace built into the process does not depend on the person noticing	Advice aimed at the slow system does not work in a fast-system moment. Design for the Friday brain.
4	B That strong immediate states crowd out longer-term considerations, so a person under acute anxiety discounts the cost of skipping a check	The paper is about how hot states override cold reasoning. The lure manufactures the hot state.

#	Answer	Why
5	A Shame that the curiosity had been about a new job; the counter was a report route with no manager in the loop and a public statement that the content of a lure is never asked about	Latency fell from over four hours to 22 minutes once reporting stopped feeling like a confession.
6	D Because a report after four hours is an attack that ran for four hours; latency measures the damage window and shows whether shame is still in the system	Rate says whether people report. Latency says how long they hesitate, and hesitation is where the emotion and the blame live.

Module 5: Pretext, Identity and Trust

#	Answer	Why
1	D A borrowed identity or role that brings its own permissions, so that the ask seems to be the role asking rather than a stranger	IT may ask for codes; the partner may ask for payments; the client may ask for urgency. The pretext borrows that permission.
2	C A published statement, by role, of what that role will never ask for by that channel, so a request that breaks it is recognisable without judgement	"IT will never ask you to read out a code" is worth more than an hour of recognition training, because it is a rule not a judgement.
3	B About $25 million, after a finance employee joined a video call on which the CFO and colleagues were deepfakes	Reported by CNN in May 2024. The course uses it to show that a familiar face on video is now a pretext, not a verification.
4	A The finance manager rang the partner's PA, Maria, on a known number; the partner was in Leeds, not an airport	A verified channel, independent of the one the attacker controls, is the counter to every pretext including a convincing face.
5	D Because a look-alike domain is designed to pass a glance, a compromised real mailbox passes any inspection, and a phone call has no address to check	The supplier mailbox compromise in September came from the genuine address. The callback rule still caught it.
6	C The most senior voice setting the norm: "I will never ask you to move money by message or video; if you get that request, ring Maria", which turns authority into a defence	Authority is a lever for the attacker only while the real authority is silent. Thirty seconds took it back.

Module 6: Who, When and Where: Susceptibility Without Blame

#	Answer	Why
1	C Situational factors: workload and pressure, whether the message was expected, and familiarity with the apparent sender, rather than stable personal traits	The research is consistent: traits are weak and inconsistent predictors; situations are strong and repeatable.
2	B They have the access and the routine: a hundred genuine payee changes a year make the hundred-and-first look ordinary	Expertise sets the template the attacker copies. Role and routine, not character, explain the pattern.
3	A A role map (who can pay, approve, admit, reset or move data) and a moment map (when people are busiest, newest, most expected to comply, and most alone)	Lay the lure library over both. Where the lures cluster is where the next control goes.

#	Answer	Why
4	D Longer report latency, because shame delays the report	Blame costs reports, latency, trust, and produces the wrong fix: training a person instead of bracing a process.
5	C Results reported by lever, role, channel and moment, never by name and never to a line manager	A simulation that teaches fear of the security team has built a lever for the attacker. Fear narrows attention.
6	B Because it produces more reports, sooner, from the roles that matter, which shows up as a falling latency line and a rising report rate	At Calder and Voss: zero disciplinaries, three managers refused a name, latency from 4h 10m to 22 minutes.

Module 7: The Lure Autopsy

#	Answer	Why
1	B Collect; read as the target; fill the seven fields; order the levers; write the "this worked because" sentence; choose the counter	The same six steps every time, so that two readers reach the same card and the library stays comparable.
2	A Because the first feeling is the emotion field, and it is lost the moment you start analysing; it is also what tells you what the lure was designed to do	Analysts read lures as puzzles. Targets read them as a Friday afternoon. The card needs the second reading first.
3	D It names a mechanism, in words the target could read without flinching, and nothing about the person	A sentence the target cannot read is a sentence that will cost the next report.
4	C Two readers fill the card for the same lure independently and compare; disagreement is a conversation about the vocabulary, not a failure	Agreement between readers is what makes the library's tallies mean something.
5	B That authority and time were the programme's real problem, that voice lures were rising and producing the closest calls, and that consistency sat under every multi-step attack with no control addressing it	A click rate says how many. The library says which mechanism, in which role, at which moment.
6	A For incident reports and the board: what arrived, why it worked, the moment, and the counter; it leaves out the name	Mechanism, moment, counter. The managing partner's only question was "why didn't we have this before?"

Module 8: Designing the Defence from the Diagnosis

#	Answer	Why
1	A The counter must match the mechanism: an authority lure needs a verified channel, not a spelling lesson	The whole course is diagnosis so that the treatment fits. A counter aimed at the wrong lever feels like action and changes nothing.
2	D Works: a brace built into the process, a pause nobody has to justify. Feels like it: telling people not to rush	The brace is there on Friday afternoon in month eleven. The advice decayed in week three.
3	C It trains the symptom of the lure you showed, assumes the slow system is running when the attack is designed to keep it off, and decays within weeks	It still has a place as vocabulary, so people can name and report. It is not the control.
4	B Remove the decision, then brace it, then verify it, and only then teach it	A decision that no longer exists cannot be exploited. Teaching is the last resort, not the first.

#	Answer	Why
5	A A hypothesis first, one lever per simulation, matched roles and moments from the two maps, outcome measured as report rate and latency, and results by lever not by name	A test produces a number. A diagnostic produces a decision about which counter to build next.
6	D As priority behaviours from the catalogue, with each counter as an intervention, two Team Pulse items, and report rate and latency as outcome measures on the programme overview	HEROES holds the behaviours and the evidence they moved. The library stays with you; the movement shows in the platform.