CYBEHAVE · BASICS TO ADVANCED

Choice Architecture for Security

Course workbook

Designing the moments where people decide.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

The five security decisions I am working on

cybehave.com/training · © 2026 CyBehave. All rights reserved. For use alongside the Choice Architecture for Security video course.

BEFORE YOU START

How to use this workbook

Choice architecture is the design of the environment in which people make choices: the defaults, the options, the order, the wording, the timing and the feedback. This workbook holds the tools the videos refer to, from the decision inventory in module 1 to the ethics test in module 8, and it follows the ten videos in order. Each module section gives you the key ideas, the templates, the two worked examples, the five Reflect & Apply questions with room to write, and the six-question quiz. The answers, with explanations, are at the back.

Five ways to get the most from it

1. **Bring five decisions.** Five security choices your people face every week. Write them in the inventory now. Every module has a "Your five decisions" box where you redesign one of them.
2. **Look at real screens.** Open your own MFA prompt, report button and sharing dialog as you watch. The examples in the course are already sitting in your organisation.
3. **Take the quizzes.** They are scenarios, not definitions. Mark your answers here, then check the key. A wrong answer with a read explanation teaches more than a right guess.
4. **Change one thing per module.** A default, a sentence, a button position. Small, this week, with the baseline written down first.
5. **Do the defaults audit.** Module 8's audit sheet is the highest-leverage hour in the course. Book it before you finish the videos.

The course at a glance

Module	Title	Tools in this workbook
0	Welcome	Decision inventory; meet Tom.
1	Every Decision Has an Architecture	Architecture audit (five elements); two-systems check; intention-action gap sheet.
2	Defaults, Friction and Salience	Defaults register; friction count; salience and feedback map.
3	Framing, Anchoring and Loss Aversion	Three-way rewrite sheet; fear test; anchor and reference-point check.
4	Social Proof, Norms and Commitment	Norms message checker; messenger map; commitment design.
5	Timing, Context and Prompts	Moment map; fresh-start calendar; if-then plan builder; environment walk.
6	Designing a Nudge: The Method	EAST check; six-step sequence; the one-page nudge canvas.
7	Testing and Measuring What Changed	Test plan; the five enemies checklist; result reading sheet; honest report template.
8	Systems, Ethics and the Limits of Nudging	Defaults audit; nudge or boost; limits diagnosis; the ethics test.

Module	Title	Tools in this workbook
9	Close	Eight ideas; one nudge this week; glossary; further reading; quiz answers.

Three lines you will hear again

Make the secure choice the easy one. · Design the moment, not the message. · Test it. Then trust it.

WORKED EXAMPLE

Meet Tom

Tom is the Security Awareness Manager at Northgate Logistics: 3,000 people, a head office in Leeds, eleven depots, 1,900 people in warehouses and on the road and 1,100 in offices. He is a team of one, with a small budget and no authority over anyone's tools. After nine months of posters, emails and an annual module, MFA enrolment stands at 61% and 3% of simulated phishing emails are reported. His lever is the design of the choices people already face.

Decision	Baseline	Where the course takes it
MFA enrolment	61% after nine months of "Not now"	Module 2: default on, dated deadline, "Not now" limited: 97% in six weeks. Module 7: two prompt wordings tested.
Password manager	Installed by 23%, used weekly by 9%	Module 2: pre-installed, signed in, auto-save on, browser saving off: 64% weekly use.
Phishing reporting	3% of simulated phish reported, 14% clicked	Module 2: button in the ribbon, reply within the hour: 19%. Module 4: norms done wrong, then right: 31% reported, 6% clicked.
Shared warehouse terminals	7 in 10 left unlocked at shift change	Module 5: twenty minutes watching, then auto-lock, tap-out reader, handover line: 1 in 10.
Unknown USB devices	140 a month in the Doncaster depot	Module 6: the six steps end to end: 12 a month.
The platforms	11,000 anonymous sharing links; 90-day remembered devices	Module 8: the defaults audit, the request he refused, and twelve months on.

Use Tom as a mirror

Each time a Northgate card appears, ask: what is my equivalent? What is my "Not now" button, my printer 60 metres from the door, my league table that backfired?

Template: decision inventory

Five security choices your people face every week. Enrol or defer, report or delete, lock or walk, share or restrict, pay or pause are the usual families.

#	The decision, as the person meets it	Who, how often	What most people do today	How you know
1				
2				
3				
4				
5				

MODULE 1

Every Decision Has an Architecture

Key ideas from the video

- There is no neutral design. Every form, prompt, policy and screen pushes people somewhere; the only question is whether anyone chose the direction.
- Five elements of any choice: the default, the options and their order, the wording, the timing, the feedback.
- Security is designed for System 2 (slow, deliberate) and happens in System 1 (fast, automatic). Design for the system that is holding the mouse.
- The intention-action gap is not a character flaw. More information does not close it; design does.
- Five everyday security choices: enrol or defer, report or delete, lock or walk, share or restrict, pay or pause.

Template: architecture audit

Pick one prompt, form or process. Fill the five elements as they are today, then as they would be if someone had designed them for your outcome.

Element	As it is today	What it pushes people towards	As it could be
Default (what happens if they do nothing)			
Options and order (what is offered, first, biggest, grey)			
Wording			
Timing (when in their day it arrives)			
Feedback (what they see after choosing)			

Template: two-systems check

Security ask	What is the person doing when it arrives?	Fast or slow mode?	What would hand it to slow mode, briefly, only when needed?

Security ask	What is the person doing when it arrives?	Fast or slow mode?	What would hand it to slow mode, briefly, only when needed?

Template: intention-action gap

Behaviour	What people say (survey, conversation)	What people do (log, observation)	The moment where intention loses

Tom reads the MFA prompt

Appears at sign-in, first thing Monday, while the person is trying to reach email.

Two buttons, same size and colour; "Not now" on the right where the hand rests. Default if nothing is chosen: back in seven days, forever.

Wording: "Protect your account with multi-factor authentication." True, abstract, nobody's problem.

Feedback after enrolling: none. After "Not now": the inbox, instantly. The wrong choice is rewarded.

Sixty-one percent after nine months is not a people problem. It is this screen, working exactly as designed.

Three more prompts

"Remember this device for 30 days", pre-ticked: default to fewer checks on every device, including the shared ones.

"Save password in browser?" Save / Never: appears at the moment of success; the browser beats your password manager every time.

The fire door on the smoking route, propped open: a 90-second detour to the badge reader. Nobody chose insecurity; the route did.

Your five decisions

Take decision 1 from your inventory through the architecture audit. What is the single element doing most of the damage?

Reflect & apply

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

1. Pick one security prompt your people see this week. What is it pushing them towards, and did anyone choose that?

2. Which of your security asks arrive while people are in fast, automatic mode?

3. Where is the biggest gap between what your people say they will do and what they actually do?

4. Who are the choice architects in your organisation, and do they know they are?

5. Which one of your five decisions will you redesign first?

MODULE 2

Defaults, Friction and Salience

Key ideas from the video

- Defaults: what happens when people do nothing. Organ donation (Johnson and Goldstein 2003), pension auto-enrolment (Madrian and Shea 2001), Google's 2-step auto-enrolment. A fair default is the one most people would choose with time to think, easy to change, honest about what it does.
- Friction: every extra step loses people, and losses compound. Remove it from the secure path; spend it deliberately on the risky one. Sludge is friction that serves the organisation at the person's expense.
- Salience: people act on what they notice. Position, contrast, relevance, feedback. Find the fly, not the sign.
- Tom pulled all three in six weeks: MFA 61% to 97%, password manager 9% to 64% weekly use, reporting 3% to 19%. Budget: nothing.

Template: defaults register

Every default was set by someone. Start with identity, collaboration, mail, devices and finance systems; module 8 has the full audit.

Setting	Current default	Who set it, when	The fair default	Who has to agree
MFA enrolment				
Browser password saving				
Link sharing				
Auto-lock				

Template: friction count

Count the clicks, screens and waits from "I want to do the right thing" to "done". Then count the risky path. Be honest.

Behaviour	Secure path: steps	Risky path: steps	Sludge to delete	Friction to add (and where)
Report a phishing email				
Get a password manager				
Change a supplier's bank details				

Template: salience and feedback map

Secure option	Where it is now	Where attention already is at that moment	What the person sees after doing it	The fly

Secrets in code, a 400-person software company

Default: the template said "put your API key here". Friction: the secret manager needed a ticket and two days; pasting took four seconds. Salience: the scanner emailed a mailbox nobody read.

Fix: template wired to the secret manager, one-command self-service, a pre-commit check that says what to do instead, findings to the developer within a minute. Four months later: zero new keys. Nobody attended a session.

Your five decisions

Take decision 2 through the three levers. Which default would you flip, which friction would you move, and what would people see?

Reflect & apply

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

1. **List the security defaults in your organisation that were set by a vendor and never reviewed.**

2. **Which secure behaviour has the most friction in its path, and where exactly is the friction?**

3. **Which insecure behaviour is currently the frictionless one?**

4. **Where is the report button, and how many clicks is it from an open email?**

5. **What is one default you could flip this month, and who has to agree?**

MODULE 3

Framing, Anchoring and Loss Aversion

Key ideas from the video

- Losses loom larger than gains, roughly twice as large (Kahneman and Tversky, 1979). The same fact framed as a loss or a gain produces different behaviour.
- Loss frames for one-off protective actions; gain or identity frames for habits that must repeat. Never put a loss in the sentence that is not real.
- Anchors and reference points: say the small number first; decide whether the action is "extra work" or "part of standing up"; concrete beats abstract; the status quo feels free.
- Fear works only with efficacy: real threat, easy action, right now, said once. Apply the reporting test to every message.
- The method: write it three ways (gain, loss, norm), each under sixty words with one why, one action, one anchor; read them to someone in the target team before choosing.

Template: three-way rewrite

The behaviour and the audience:

Gain frame (for a repeated habit)	Loss frame (for a one-off protective action)	Norm frame (what people like them already do, action in the same sentence)

Read to (name, team)	Which one they picked, and the words they used

Template: fear test

Message	Real threat?	Easy action in the same sentence?	Right now?	Said once, not wallpaper?	Passes the reporting test?

Template: anchors and reference points

Security step	What it is anchored against today	The small number, said first	Reference point that makes it a cost	Reference point that makes it normal

Tom's payment-verification email, three ways

Gain: "Every bank change you verify keeps a supplier paid and a Friday calm. The known-number call takes four minutes."

Loss: "In March one unverified bank change sent £38,000 to a criminal. It took one email. Before any change: four minutes, the number on file, not the one in the email."

Norm: "Nine in ten bank changes in this team were verified last month. For the rest: the number on file, four minutes, before the payment."

Mo picked the loss version for the one-off email and the norm version for the payment form. The gain version "sounds like you".

The same simulation result, four ways

"14% clicked" shames the few and tells everyone clicking is common. "86% did not click" is calm and says nothing to do. "First report at 09:04, thanks to Dee" teaches the behaviour that stops a real attack. "One click is enough. Report before you delete: the button is in the ribbon" is loss plus efficacy. Lead with the third, close with the fourth, keep the first for the risk committee.

Your five decisions

Take decision 3 and write its message three ways. Read them to one person in the audience and record what they said.

Reflect & apply

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

1. Take your most-sent security message. Is it framed as a gain, a loss, or neither?

2. What reference point are your people using when they judge whether a security step is "a lot of effort"?

3. Where could a concrete, specific loss replace an abstract warning?

4. Where are you using fear, and does the message give an easy next action?

5. Rewrite one message three ways this week. Which one would you send, and to whom?

MODULE 4

Social Proof, Norms and Commitment

Key ideas from the video

- When unsure, people do what people like them do. Strongest when the situation is ambiguous, the behaviour is visible and the others are similar and local (HMRC letters, 2012).
- Descriptive norms (what people do) pull towards the average; injunctive norms (what people approve of) stop the good performers relaxing. Publish a bad descriptive norm and you make it worse.
- The boomerang (Schultz 2007): light energy users told they beat the average increased their use; a smiley face removed the effect. Every comparison needs the smiley face.
- The messenger: authority (rare), similarity, trust, consistency. Design the messenger as carefully as the message.
- Commitments: voluntary, specific, public, short. Identity ("we're the team that catches these") is a norm, a messenger and a commitment in one sentence.

Template: norms message checker

Statistic or comparison you want to publish	Descriptive or injunctive?	What does it say "most people" do?	Approval signal added (the smiley face)?	Who sees whose numbers?

Template: messenger map

Audience	Who they discount	Who they already go to with "does this look odd?"	Who has visibly done the behaviour	Messenger chosen

Audience	Who they discount	Who they already go to with "does this look odd?"	Who has visibly done the behaviour	Messenger chosen

Template: commitment design

Behaviour	The commitment, in their words	Voluntary?	Specific?	Public where?	Short (one line)?

Tom publishes the reporting rates, twice

First: a league table of 40 teams to every manager. Top team fell from 44% to 31% ("we're already top"); bottom team did not move; overall 19% to 18%.

Second: each team sees only its own number, the depot average and a green tick when it beats last month. Every report gets a reply within the hour. Every real catch is thanked by name at the huddle, by the shift lead. Three teams put "we catch these" on their own board. Three months later: 31% reported, 6% clicked.

The law firm's partners

96% enrolled; the 4% were 24 equity partners who ignore IT. The managing partner enrolled on camera and said: "Nineteen of us have done this. I'd like it to be all of us by Friday." A list with ticks went up in the partners' lounge. By Friday 23 of 24. The last needed help with his phone: a capability barrier, not a social one.

Your five decisions

Take decision 4. Who is the messenger, what is the true good norm you can quote, and what approval signal goes beside it?

Reflect & apply

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

1. **What do your people believe "everyone else" does about security, and is it true?**

2. **Where are you accidentally publishing a descriptive norm that says the risky behaviour is normal?**

3. **Who are the messengers your people actually trust, and are they the ones delivering security messages?**

4. **Where could a small, voluntary, public commitment replace a mandate?**

5. **How would you publish team reporting rates so that the low teams improve rather than relax?**

MODULE 5

Timing, Context and Prompts

Key ideas from the video

- Behaviour happens at a time and a place. Go and look: what are they doing, what is in their hands, what is pulling them away, what do they see?
- Just-in-time prompts belong at the point of action: one line and a button. If it needs a paragraph it is training in the wrong place.
- Fresh starts (Dai, Milkman and Riis 2014): onboarding, new device, new role, new system, after an incident. Day one is the biggest fresh start you own.
- Implementation intentions ("if X, then I will Y", Gollwitzer 1999) roughly double follow-through. Habit stacking borrows an existing habit as the cue. Ask teams to write their own line.
- The physical environment is architecture: if the secure behaviour needs a detour, it loses to the exit.

Template: moment map

Behaviour	What are they doing?	What is in their hands?	What is pulling them away?	What do they see?	The prompt, one line, placed where

Template: fresh-start calendar

Fresh start in your organisation	How many people a year	Secure default or habit to attach	Who owns that moment	Ready now?
Onboarding, day one				
Laptop or phone refresh				
New role or promotion				
System migration				
After an incident (prepared in advance)				

Template: if-then plan builder

Written by the team, in their words, where they work. Yours is a policy; theirs is a commitment.

If (the situation, as they would recognise it)	Then I will (one action)	The cue that makes it unmissable	Stacked on which existing habit?

Template: environment walk

- Where does the terminal face, and who can read it?
- How far is the printer from the door?
- Where is the bin for visitor badges?
- What is at eye level by the scanner, the kettle, the exit?
- Is the secure thing on the way out, or out of the way?

Tom at the Doncaster shift change

Watched: seven in ten terminals unlocked at 14:00; hands full of scanner, vest and phone; badge-out 40 metres away; bus at 14:10; a fifteen-minute vendor auto-lock.

Changed: auto-lock to ninety seconds and lock-on-walk-away from the lanyard badges; a tap-out reader on the exit path ("Tap your card on the way out and the desk locks"); one line on the handover sheet. Three weeks later: one in ten. No email was sent.

A retailer's day one

Before: MFA prompt with "Not now", password manager link in an email, 45-minute module due in 30 days. At 90 days: 58% MFA, 7% password manager.

After: both set up in the first ten minutes with the buddy; a signed if-then card in the welcome pack; the report button used once on a test email and thanked; three two-minute clips from week two. At 90 days: 99% and 81%.

Your five decisions

Take decision 5 and map its moment. Where would the one-line prompt go, and which fresh start could carry the behaviour?

Reflect & apply

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

1. For one secure behaviour, where exactly is the moment of choice: what is the person doing, where, with what in their hands?

2. Which of your security messages arrive hours or days away from the moment they are about?

3. What fresh starts happen in your organisation every month that you could attach a behaviour to?

4. Write one if-then plan for a behaviour you want: "If X, then I will Y."

5. What in the physical environment is quietly working against the behaviour?

MODULE 6

Designing a Nudge: The Method

Key ideas from the video

- EAST (Behavioural Insights Team, 2014): Easy, Attractive, Social, Timely. Easy is the letter that matters most. MINDSPACE is the longer checklist: use EAST to design and MINDSPACE to check.
- Six steps: define the behaviour (who, what, when, where, countable); map the decision journey as it really happens; find the moment; choose the lever (two, rarely three); prototype cheaply within a week; test against a baseline.
- The one-page nudge canvas: behaviour, baseline, moment, barrier, levers, EAST check, prototype, measure, ethics, owner.
- Design failures: wrong moment, too many levers, prompt fatigue, designed from a desk. Diagnosis failures: capability, structure, a rule was needed, trust.

Template: the one-page nudge canvas

Behaviour (who, what, when, where)	Baseline (how often now, and how you know)

Moment (what the person is doing and seeing)	Barrier (why the secure path loses at that moment)

Levers (which two, and the exact change)	EAST check (easy / attractive / social / timely, one honest word each)

Prototype (what, where, with whom, by when)	Measure (the number, the comparison, the date you will look)

Ethics (transparent, easy to avoid, in their interest, defensible in public)	Owner (who maintains it after you move on)

Template: the decision journey

Step (as it actually happens)	Where people drop off or go wrong	How many get here (if known)
Trigger		
Done		

MINDSPACE check

Messenger	Incentives	Norms	Defaults	Salience	Priming	Affect	Commitment	Ego

The Doncaster USB problem, end to end

Behaviour: plug only an issued, encrypted stick into a scanner. Baseline: 140 unknown devices a month. Journey: pick list needed; printer 60 metres away and often broken; stick in the pocket is faster; port right there; nothing happens.

Levers: friction and default. Issued sticks in a basket at the door ("take one, it's yours"), a drop box beside it, ports accepting issued sticks only with a one-line message, pick lists pushed to the scanners. Prototype: one shift, one week, 40 sticks. Measure: 140 to 12 after three months, other depots as the comparison.

Lost phone, reported within an hour

Median time to report was two days; nine phones a year never reported. The moment: an evening, no laptop, no asset tag, a sinking feeling. Fix: a number to text from any phone, printed on the lanyard; no tag needed; the reply says "it's wiped, nothing else to do, new one tomorrow". Median 35 minutes; never-reported zero.

Your five decisions

Fill the canvas for the decision you will actually change first. If a box is empty, that is the next piece of work.

Reflect & apply

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

1. **State one target behaviour in the form "who does what, when, where". Is it really one behaviour?**

2. **Draw the decision journey for it. Where is the first point someone can go wrong?**

3. **Which single lever from modules two to five fits that moment best, and why that one?**

4. **What is the cheapest prototype you could put in front of five real people this week?**

5. **Run your idea through EAST. Where is it weakest?**

MODULE 7

Testing and Measuring What Changed

Key ideas from the video

- Behavioural effects are real, often smaller than the headline studies, and context-dependent. Treat every nudge as a hypothesis until your own numbers say otherwise.
- Baseline: the behaviour counted the same way for at least as long as the test will run, written down with the date before the change. Comparison: somewhere alike you did not change. A before-and-after with no comparison is a story.
- Three designs: A/B (cleanest), stepped rollout (most practical), before-after with comparison (weakest, still better than nothing). One change per test.
- Five enemies: noise, seasonality, novelty, the Hawthorne effect, everything else that changed. Keep a diary.
- How big is real: under five points probably noise, over ten probably real, between run longer (groups of a few hundred). Measure at six weeks and six months. Report the number, the comparison, the period, what else changed, what you do not know.

Template: test plan

Nudge	Behaviour counted, and how	Baseline (value, period, date written)	Comparison group	Design (A/B, stepped, before-after)	The one change	Look at (six weeks) and again (six months)

Checklist: the five enemies

Enemy	How it could show up in this test	What I will do about it
Noise (small groups bounce)		
Seasonality (holidays, quarter-end, intakes, the news)		
Novelty (attention fades in a fortnight)		

Enemy	How it could show up in this test	What I will do about it
Hawthorne (people know they are watched)		
Everything else that changed (keep the diary)		

Template: the test diary

Date	What else happened (new manager, real incident, news, outage, campaign)	Which group it touched

Template: reading a result

Question	Answer for this result
Same test? (comparable difficulty, same measure)	
Same people, same season?	
Compared with what?	
How many people? (what is one person worth in points)	
What happened next? (six months)	

Template: the honest report

The number and the comparison, in one sentence	The period	What else changed	What we do not know	When we will look again

Tom's two MFA prompts

Two regions of about 400, matched on role mix, for a new field-service app without a default. A: "Protect your Northgate account. Set up MFA now (2 minutes)." B: "Without MFA one leaked password loses this account. 97% of Northgate is already set up. 2 minutes." Six weeks: 71% vs 83%.

What it proves: B wins here, this behaviour, this quarter; twelve points clears noise at that size. What it does not: whether the loss line or the norm did the work (two levers, one test), and the north region had a real incident in week three (diary). He will separate the lines next time and re-measure at six months. Both regions reached 97% once the default was on. The default was always the lever.

Your five decisions

Write the test plan for the nudge on your canvas. Which site or team is your comparison, and what will you leave alone there until the result is in?

Reflect & apply

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

1. **For your nudge, what is the baseline number, and over what period was it measured?**

2. **Where is your natural comparison group: a site, a team or a region you can leave unchanged for now?**

3. **What else is changing at the same time that could explain a result?**

4. **How long will you wait before you look, and when will you look again to check for decay?**

5. **If the result is a four-point improvement, what will you say about it, and to whom?**

MODULE 8

Systems, Ethics and the Limits of Nudging

Key ideas from the video

- Most of your choice architecture was designed by vendors for their support costs, not your risk. Changing one line in a console reaches everyone, forever, at no cost. Audit it.
- A nudge shapes the choice; a boost builds the chooser (Hertwig and Grüne-Yanoff 2017). Nudge the frequent everyday choices; boost people with two or three rules of thumb for the rare, clever attack.
- Four problems no nudge fixes: capability, structure, trust, deliberate misuse. Diagnose first with COM-B. A nudge on a trust problem is a sticking plaster on a broken bone.
- Dark patterns (Brignull 2010) are the same levers pointed the other way. Security must never use them: once people feel manipulated, every honest nudge is read as a trick.
- The ethics test: transparent, easy to avoid, in the person's interest, defensible in public (Sunstein's publicity principle). Nudge for good.

Template: the defaults audit

Open the console. For each row write the current setting, the fair default, and who has to agree. Book the hour before you finish the course.

Area	Setting	Current	Fair default	Owner / agree	Done
Identity	MFA enrolment default; "Not now" present?		On, dated deadline, limited		
Identity	Remembered-device length		14 days		
Identity	Self-service reset verification		Verified call-back / strong proof		
Collaboration	Link sharing default		People in the organisation		
Collaboration	External sharing and guest expiry		Guests expire (90 days)		
Collaboration	Who can create a public team / site		Request, not default		
Mail	External sender and first-contact banners		On		
Mail	Report button position		Ribbon, one click, reply sent		
Mail	Attachment / external send confirmation		On for sensitive labels		
Devices	Auto-lock		2 min desks, 90 s shared		
Devices	Browser password saving		Off; manager pre-installed		
Devices	USB policy and admin rights		Issued only; rights on request		

Area	Setting	Current	Fair default	Owner / agree	Done
Finance / HR	Supplier bank detail change		Second approver default, skips logged		

Template: nudge or boost?

Behaviour	Frequent or rare? High or low stakes?	Nudge (environment change)	Boost (the rule of thumb, one sentence)	Both?

Template: limits diagnosis

Behaviour that is not happening	Capability? (can they?)	Structure? (does the system allow it?)	Trust? (do they believe it is safe?)	Deliberate? (controls, not nudges)	Nudge appropriate?

The ethics test

The design:

Question	Yes / no	Evidence
Transparent: would I be happy for the person to see exactly how and why it was designed?		
Easy to avoid: is the other option visible, legible and one step away, never hidden or shamed?		
In their interest: does it serve the person and the organisation together, by the person's own standards?		
Defensible in public: if it appeared on the front page tomorrow, would I defend it or explain it away?		

Tom's audit, the refusal, and twelve months on

"Anyone with the link" was the default: 11,000 live anonymous links, 400 to folders with personal data. Changed to "People in Northgate", old links expired over 60 days, one-line explanation inside the sharing dialog. 31 tickets; no complaints after week two. Guest access 90-day expiry; remembered devices 90 to 14 days; second approver default on bank changes.

A product manager asked for a grey, small "decline" on a customer consent, "since you're good at this". Tom declined in writing with the four questions. The consent shipped with two equal buttons.

Twelve months: MFA 97%, password manager 71%, reporting 34%, clicks 5%, unlocked terminals under one in ten, USB 9 a month group-wide. Two real supplier frauds stopped by the second approver. Campaigns run: none. The annual module retired for three rules of thumb on day one.

The three rules of thumb

"The number on file, not the one in the message." "If the password manager goes quiet, stop." "Urgent and unusual together means report, not reply." Each works on a personal phone, at home, in a new job. Teach three. Never teach thirty.

Your five decisions

Run the nudge on your canvas through the ethics test, then write the request you would refuse and to whom you have said so.

Reflect & apply

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

1. List the three platforms where most of your organisation's sharing, access and sign-in choices are made. Who owns their defaults?

2. Which of your current nudges would you be comfortable explaining, in full, to the people it is aimed at?

3. Where are you nudging a problem that is really a capability or a system problem?

4. Where could a boost (a skill or a rule of thumb) do what a nudge cannot?

5. What is the request you would refuse, and have you said so before it arrives?

COURSE SUMMARY

Close

Eight ideas to carry forward

1. **There is no neutral design.** Someone shaped every security choice. Decide that it will be you.
2. **Defaults, friction, salience.** What happens by default, how many steps, what people see. Start here.
3. **Same fact, different frame.** Loss for the one-off action, gain for the habit, concrete over abstract, fear only with an easy action.
4. **Norms need the smiley face.** Show the good norm, add approval, choose the messenger, keep commitments voluntary.
5. **Design the moment.** Go and watch it. Prompt at the point of action. Use fresh starts and if-then plans.
6. **EAST and six steps.** Behaviour, journey, moment, lever, prototype, test. One page.
7. **Test it, then trust it.** Baseline, comparison, one change, six weeks and six months, the diary.
8. **Audit, boost, refuse.** Audit the vendor defaults, boost for the rare case, refuse the dark pattern.

The closing line

Make the secure choice the easy one. And never the only one.

One nudge this week

Flip one default. Move one button. Rewrite one message three ways. Stand at one shift change for twenty minutes. Write the baseline down first, with the date, look again in six weeks, and tell someone what you found.

Glossary

Term	Meaning
Choice architecture	The design of the environment in which people make choices: defaults, options and order, wording, timing, feedback (Thaler and Sunstein, 2008).
Nudge	A change to the architecture that alters behaviour predictably without forbidding options or significantly changing the economics; easy and cheap to avoid.
Default	What happens when the person does nothing. The most powerful single element.
Friction	Effort in the path: steps, clicks, waits, forms. Remove from the secure path; spend deliberately on the risky one.
Sludge	Friction that serves the organisation at the person's expense (Sunstein).
Salience	What people notice: position, contrast, relevance, feedback.
System 1 / System 2	Fast, automatic thinking and slow, deliberate thinking (Kahneman). Security happens in System 1.
Intention-action gap	The distance between what people mean to do and what they do. Closed by design, not information.
Framing	How the same facts are presented. Loss frames for one-off actions; gain frames for repeated habits.
Loss aversion	Losses weigh roughly twice as much as equivalent gains (prospect theory, 1979).
Anchor / reference point	The first number or norm against which a choice is judged. The status quo feels free.
Descriptive / injunctive norm	What most people do / what people approve of. Publishing a bad descriptive norm makes it worse.
Boomerang effect	Good performers told they beat the average relax (Schultz 2007). Fixed by an approval signal.
Messenger effect	The same words carry different weight from different people: authority, similarity, trust, consistency.
Commitment device	A voluntary, specific, public, short promise that people then keep.
Just-in-time prompt	One line and a button, at the point of action.
Fresh start effect	Openness to change at beginnings: onboarding, new device, new role, after an incident (Dai, Milkman and Riis 2014).
Implementation intention	"If X, then I will Y" (Gollwitzer 1999). Habit stacking ties the plan to an existing habit.
EAST / MINDSPACE	Easy, Attractive, Social, Timely (BIT 2014); Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitment, Ego (Dolan et al. 2010).
Baseline / comparison	The behaviour measured before the change; a similar group left unchanged. Together, evidence rather than a story.
Hawthorne effect	People behave differently when they know they are observed. Measure quietly, from logs.
Boost	A skill or rule of thumb that builds the chooser rather than shaping the choice (Hertwig and Grüne-Yanoff 2017).

Term	Meaning
Dark pattern	The levers pointed against the person's interest: hidden decline, pre-ticked box, confirmshaming, fake countdown (Brignull 2010).
Publicity principle	Sunstein: a nudge you would not defend in public should not be used.

Further reading

- Thaler, R. H. and Sunstein, C. R. (2008; final edition 2021). Nudge. Penguin.
- Kahneman, D. (2011). Thinking, Fast and Slow. Penguin.
- Sunstein, C. R. (2021). Sludge: What Stops Us from Getting Things Done and What to Do about It. MIT Press.
- Service, O. et al. (2014). EAST: Four Simple Ways to Apply Behavioural Insights. Behavioural Insights Team.
- Dolan, P. et al. (2010). MINDSPACE: Influencing Behaviour through Public Policy. Institute for Government and Cabinet Office.
- Johnson, E. J. and Goldstein, D. (2003). Do Defaults Save Lives? Science, 302.
- Schultz, P. W. et al. (2007). The Constructive, Destructive, and Reconstructive Power of Social Norms. Psychological Science, 18.
- Hertwig, R. and Grüne-Yanoff, T. (2017). Nudging and Boosting: Steering or Empowering Good Decisions. Perspectives on Psychological Science, 12.
- Dai, H., Milkman, K. L. and Riis, J. (2014). The Fresh Start Effect. Management Science, 60.
- Gollwitzer, P. M. (1999). Implementation Intentions: Strong Effects of Simple Plans. American Psychologist, 54.
- Michie, S., Atkins, L. and West, R. (2014). The Behaviour Change Wheel. Silverback. (For the COM-B diagnosis that tells you when a nudge is the right tool.)

Notes