SECURE CULTURE HUB
POWERED BY HOXHUNT

Built In A Day

Six Cybersecurity Awareness Month blueprints from the Secure Culture Hub

www.secureculture.com

June 2026

About this report

> ***No consultants. No pre-built templates. Just practitioners who know their organisations, a framework, and an afternoon to actually build something.***

Most Cybersecurity Awareness Month planning happens in meetings. Ideas get discussed, decks get built, and somewhere between the conversation and October the momentum dies. This report is different.

On 10 June 2026, a group of security awareness and human risk practitioners sat down and actually built their campaigns. Six topics. Six groups. One afternoon. What follows is what they made.

This report captures the work produced on the day. It is structured around the workshop framework that guided the afternoon session: the human problem, the core message, the delivery plan, and the hook. Each group's blueprint is documented in full so that anyone can pick it up and adapt it.

WHAT'S INSIDE

Six blueprints, each built around a real behaviour problem and a real October campaign. Every one covers the same four things: the human problem, the core message, the delivery plan, and the hook.

BLUEPRINT	TOPIC
01	**Physical Security**
02	**Cybersecurity at Home**
03	**Password Hygiene**
04	**AI Safe Use**
05	**Building the Security Brand**
06	**Advanced Social Engineering and Deepfakes**

Each blueprint is designed to be lifted and adapted. Take what works for your organisation and make it yours.

What Isn’t Landing?

The first exercise asked practitioners to think honestly about their own organisation. Not the programme, not the strategy. The people. Each person wrote down the one behaviour or risk that still isn't landing, no matter what they try. The responses were candid and consistent.

BEHAVIOURS THE ROOM IDENTIFIED

- Not reporting suspicious emails
- Clicking links and not reporting it
- Password / passphrase confidence and ability to generate secure ones
- Shadow IT and unapproved AI usage
- AI usage without reporting or deleting outputs
- Locking laptops
- Engagement from everyone, not just the already-engaged
- Third party due diligence and procurement risk
- Supply chain: new suppliers without prior security checks
- People mislabelling and missharing information
- Incident reporting
- The "it's not my issue, tech manages the risk" mindset
- Using work credentials on non-business websites
- Vibe coding and AI deployment without security checks
- No baseline in place to measure behaviour from

> ***"Not reporting" came up more than any other theme. People click. People see things. They just don't tell anyone.***

MORNING SESSION

Which Topics Matter Most This October?

Participants voted on which topics they wanted to tackle in the afternoon. The results shaped the six blueprints built after lunch.

TOPIC	VOTES
Cybersecurity at Home	**11**
Physical Security	**8**
Password Hygiene	**4**
Advanced Social Engineering: Deepfakes, Vishing, Teams...	**3**
Phishing: Reporting Suspicious Emails	**2**
AI Risks: Shadow AI (inc. non-dev vibe coding)	**1**
Data Protection (storing and sharing)	**1**
Culture Studies / Surveys	**1**
Vulnerability Management	**1**
Governance / Compliance	**1**
Business Continuity Plans, Drills	**1**
Building Brand	**1**

Cybersecurity at Home topped the poll with 11 votes. Physical Security came second with 8. The afternoon groups formed around these preferences, with each team picking a topic to build a full blueprint for.

MORNING SESSION

How Do We Measure Whether CAM Was a Success?

Before the afternoon build session, the group explored a question that does not get asked often enough: what would actually tell you it worked? The responses fell into three clear camps.

QUANTITATIVE MEASURES

- Engagement stats: attendance at events, article views, intranet hub page visits
- Click and fail rates vs reporting rates from phishing simulations
- Number of security champions recruited
- Feedback survey scores pre and post the month
- Baseline behaviour scans (e.g. password audits) repeated at month end
- Number of reports filed during the month vs baseline
- Participation in workshops, lunch and learns, competition entries
- Training completion rates

QUALITATIVE MEASURES

- Post-event surveys: how did it go, what was useful?
- Conversations had with colleagues after the month
- Understanding of whether the message landed as intended
- Pre/post culture survey to measure confidence and perception
- Manager feedback on team behaviour change
- Comments and questions raised via internal channels

THE CONSISTENT PRINCIPLE

Across all the responses, one theme kept coming back: decide what behaviour you are trying to change before you start, get a baseline, and track against that baseline over the month. Engagement metrics are useful as a proxy but they are not the same as behaviour change. The room agreed that quantitative and qualitative data need to be used together, with risk aligned to the numbers.

The blueprints that follow were each built with this question in mind.

How the Blueprints Were Built

Each group worked through the same four-part framework. The discipline of the framework is what makes the outputs usable: every blueprint has a human problem, a single message, a delivery plan, and a hook. Pick one up and you can run with it.

#	ELEMENT	WHAT IT MEANS
01	**The Human Problem**	What do your people currently believe or do that creates risk? Why do they do it? What would success actually look like? Groups started here to avoid jumping straight to tactics.
02	**The Core Message**	One sentence. This October, we want our people to understand that… If someone remembered only this, would it change their behaviour?
03	**The Delivery Plan**	What format works for this message? What channel reaches the right people? What week of October and why? How do you reinforce it? Who else needs to be involved?
04	**The Hook**	One piece of copy that proves the message works in the real world. A subject line. A manager question. A story. An opening line. The actual words, not a description of them.

Every blueprint that follows was built using this framework. The structure is the same across all six. What differs is the topic, the audience, and the thinking each group brought to the room.

BLUEPRINT 01

Physical Security

BLUEPRINT 01	PHYSICAL SECURITY
CORE MESSAGE	You never know who is sitting next to you.
DELIVERY PLAN	Short video content showing the attacker's perspective. Deployed on digital screens at office entrances, intranet, and email. Optional entrance table game during awareness week.
HOOK	See it. Steal it. Sink it.

THE HUMAN PROBLEM

Physical security is hard to measure and even harder to make people care about. The dominant attitude in the room was "it's not that big a deal", combined with over-reliance on technical controls. People minimise their own role. The group focused specifically on the risk of working on the move, because telling people not to work on trains does not work. People are going to work. The question is whether they do it consciously.

Risks identified: Tailgating, shoulder surfing, sensitive documents on desks or at shared printers, technology left unattended, QR codes in public spaces, lanyards worn in public, OT and R&D areas left accessible.

Success looks like: People politely challenging tailgating attempts, people knowing how to report a physical security incident, a visible increase in reports.

THE CORE MESSAGE

> ***You never know who is sitting next to you.***

The group built a character: the comedian. The person on the train you would never suspect. Attackers do not look like attackers. The old lady on the 8:15 could be the one reading your screen.

THE DELIVERY PLAN

- Short video: puts the viewer in the mindset of someone working on the move
- Digital screens at office entrances: short clips, no sound required
- Email and intranet: same content adapted for each channel
- Optional entrance table activity during awareness week
- Strapline runs across all assets throughout October

THE HOOK

> ***See it. Steal it. Sink it.***

Reworked from the Transport for London slogan "See it. Say it. Sorted." – flipped to the attacker's perspective. Works as a standalone anchor with a rotating sub-message underneath: "Attackers could be anyone" / "Be careful about tailgating" / "Who are you sharing your screen with?"

BONUS IDEA: THE ENTRANCE GAME

Flash an image of a person or an email for five seconds, then hide it. Ask: what colour was their jacket? What did the subject line say? The exercise makes the point that it only takes seconds to read something sensitive, faster than most people think.

BLUEPRINT 02

Cybersecurity at Home

BLUEPRINT 02	CYBERSECURITY AT HOME
CORE MESSAGE	From screen to front door, stay secure.
DELIVERY PLAN	Four-week themed structure through October. Videos, workshops, newsletters, screen takeovers, merch, Teams/Slack reinforcement. Campaign mascot: Homer.
HOOK	From screen to front door, stay secure.

THE HUMAN PROBLEM

Security does not stop at the office door, but most programmes treat it as if it does. Employees' home habits directly affect organisational risk. The challenge is relevance: making people feel this applies to their actual life, not an abstract risk scenario.

THE CORE MESSAGE

> ***From screen to front door, stay secure.***

The group created Homer, a mascot for the campaign (flexible enough to be any gender). Homer carries the messaging across four weeks, each with a distinct theme.

THE FOUR WEEK STRUCTURE

WEEK	THEME	FOCUS AREAS
WEEK 1	**Secure Your Device**	Device updates, patch management, locking screens
WEEK 2	**Secure Yourself**	Social media, QR codes, scam messages, public Wi-Fi, VPN
WEEK 3	**Secure Your Family**	Protecting kids online, parental controls, shared accounts
WEEK 4	**Secure Your Home**	Smart speakers, default passwords, home network security

ACTIVITIES ACROSS THE MONTH

- Videos, workshops, newsletters, in-person events, talks
- Screen takeovers with the campaign strapline
- Posters, merch, Teams and Slack messages
- Preferred VPN supplier recommendation: CAM is the moment to surface it

THE HOOK

> ***From screen to front door, stay secure.***

Secondary options from the group: "One password away from a bad day" / "Lock, Check, Protect" / "No just a 9-5 responsibility"

BLUEPRINT 03

Password Hygiene

BLUEPRINT 03	PASSWORD HYGIENE
CORE MESSAGE	You are strong, unique and special... unlike your password.
DELIVERY PLAN	Education on the new password vault tool. Passphrase tombola. Memes. Pen tester as external speaker. Live social engineering demo. Power Apps word game.
HOOK	Pa55w0rd_ Hygi3n3*

THE HUMAN PROBLEM

The group found a real baseline to work from: employees were storing passwords in Excel and Word documents. The reason was not laziness. There was no password manager available. Long password policies left people with no practical alternative. This is a COM-B diagnosis: the problem is one of Opportunity, not Motivation or Capability. The environment created the behaviour.

FUD is also at play: Fear, Uncertainty and Doubt. People who will not adopt a new tool are usually not obstinate. They are scared they will do it wrong and do not want to admit it.

TARGET BEHAVIOUR

Adoption of a password vault being implemented, and elimination of saved passwords in Excel and Word by the end of the month.

KEY MESSAGES TO LAND

- This is the new tool. It's easy and convenient. Here is how to use it.
- Did you know? Excel is not a secure place to store passwords, even if the file is password protected.
- If in doubt, here is who to talk to.
- Tricks and tips for remembering and generating strong passphrases.

FORMAT IDEAS

- Passphrase tombola: spin a wheel to generate a random passphrase, run as a competition
- Memes: quick, shareable, emotionally resonant. Expectation vs reality works well for password behaviour.
- Animations that visualise how an attacker exploits passwords stored in Excel
- Pen tester as external speaker: how they find and leverage passwords across an estate
- Live social engineering demo to make the abstract concrete
- Power Apps word game (Family Fortunes format) to build engagement
- Passphrase generation competition: invite employees to submit creative methods

THE HOOK

Pa55w0rd_ Hygi3n3*

The campaign header is written in the style people actually use: substitutions that feel clever but are not. It is the visual proof of the problem.

You are strong, unique and special... unlike your password.

BLUEPRINT 04

AI Safe Use

BLUEPRINT 04	AI SAFE USE
CORE MESSAGE	Curiosity killed the network.
DELIVERY PLAN	Internal campaign tapping existing visible channels. Multi-team collaboration. AI Champions. "Spot the Hallucination" competition. Role-based foundational training. Bitesize, multi-format, not bombarding.
HOOK	Subject line: Curiosity Killed the Network. Story: Samsung employee posts confidential info into ChatGPT. CTA: Spot the Hallucination Challenge.

THE HUMAN PROBLEM

AI was released into organisations like a wild animal. Policies are being written retrospectively while people are already using tools, sharing sensitive data, and accepting outputs without verification. Three structural problems were identified:

- **People:** Data classification failures, unapproved tools, cognitive biases toward preferred tools
- **Process:** Policies too difficult to understand, too slow to keep pace with how the business uses AI
- **Tooling:** Either a wild west with no oversight, too restrictive with workarounds emerging, or no visibility at all

A critical cultural point: pausing to verify AI outputs must be accepted and understood as legitimate behaviour. If senior leaders penalise people for slowing down to check, the message will not land.

ONE-LINER OPTIONS

- Curiosity killed the network.
- AI Assisted. Human Approved.
- Don't outsource your judgement.
- Powerful. But not foolproof.
- Smart tools. Smarter risks.
- Prompt. Pause. Protect.

THE DELIVERY PLAN

- Tap into existing visible channels: all-hands, intranet, existing comms. Stop creating new ones.
- Mixed media: no single channel, bitesize nudges across the business
- Role-based foundational knowledge for both general users and developers
- Multi-team collaboration: InfoSec does not own this alone
- Relevant scenarios and table-top exercises
- AI Champions: trusted peers who support colleagues with low-friction questions
- Identify high-risk areas first (execs, developers, finance) and target those specifically
- Celebrate success publicly when people use AI safely and deliver business outcomes
- "Spot the Hallucination" competition as the engagement mechanic

THE HOOK

Subject line: Curiosity Killed the Network
Manager question: How can I manage the opportunities of AI alongside the risks?
Story: A Samsung employee posted confidential information into ChatGPT. That information was later accessed by a malicious actor. Just because a tool looks intelligent does not mean it is safe. 54% of IT security professionals have now faced an AI-related security incident.

Don't forget to take part in the Spot the Hallucination Challenge. Could your team win the prize?

BLUEPRINT 05

Building the Security Brand

BLUEPRINT 05	BUILDING THE SECURITY BRAND
CORE MESSAGE	Your secure decisions enable innovation.
DELIVERY PLAN	Phased approach: September teaser, October rebrand launch, ongoing integration. New logo, motto, tone of voice. "You Said / We Did" narrative. Competition to launch.
HOOK	Security enables innovation.

THE HUMAN PROBLEM

Security is seen as the team that says no. More passwords, more access restrictions, more friction. That perception directly reduces engagement: fewer people click, fewer people watch, fewer people care, because they have already categorised security comms as something that makes their life harder. The challenge is not just a campaign. It is a rebrand.

THE CORE MESSAGE

> ***Your secure decisions enable innovation.***

The group also developed a "You Said / We Did" approach to reframe the narrative: "You said we added another password. What we did was protect the company from thousands of attacks this week."

THE DELIVERY PLAN

- **September (pre-October):** Teaser campaign. "Something is coming." Build anticipation before the rebrand lands.
- **October launch:** Reveal the new brand identity: logo, strapline, tone of voice. Use the full channel mix.
- High-footfall physical placements: screens, pop-ups, town halls. Go where people already are.
- Competition to launch the rebrand: invite the business to engage, not just observe.
- For international organisations: keep it digital to reach all offices without overcomplicating delivery.
- **Measurement:** Feedback surveys, focus groups, intranet page traffic, engagement with insight pages month on month.

The rebrand is not a one-month effort. CAM is the launch. The new brand then gets built into the strategy and roadmap as regular nudges going forward.

THE HOOK

> ***Security enables innovation.***

Key identifiers for the new brand: a unique logo, a motto or strapline, a consistent tone of voice that positions security as part of how the organisation moves forward, not what slows it down.

BLUEPRINT 06

Advanced Social Engineering and Deepfakes

BLUEPRINT 06	ADVANCED SOCIAL ENGINEERING AND DEEPFAKES
CORE MESSAGE	Get free cake and find out about deepfakes.
DELIVERY PLAN	Immersive in-person event with a virtual option. Three interactive stations (deepfakes, vishing, Teams/Slack). Live talk delivered as a deepfake. Bingo mechanic. Badge on completion. Security champions run virtual version in other regions.
HOOK	Get free cake and find out about deepfakes. Exit message: Are you faking it?

THE HUMAN PROBLEM

Criminals are no longer just sending poorly written emails. They are using deepfakes, vishing, and Teams and Slack messages to exploit cognitive biases and psychological pressure. In high-stress situations, people default to automatic thinking: something feels urgent, they act. The sophistication of the attack is outpacing the awareness of most employees.

Objectives: improve the ability and confidence of colleagues to spot and report advanced social engineering, and improve the overall perception of cybersecurity in the organisation.

THE EVENT: HOW IT WORKS

AT THE ENTRANCE

Baseline test on arrival. Exit test at the end. Handout covering cognitive bias and principles of persuasion. Bingo card to collect stamps from each station.

STATION 1: DEEPFAKES

Attendees record their own voice and send a deepfake message to a colleague or friend, then discuss what the risks are and how someone might have spotted it was fake.

STATION 2: VISHING (PHONE A COLLEAGUE)

Actors from the security team are on the other end of the phone. Attendees receive a pretext script and make a social engineering call live. People who have tested this were visibly nervous. Put it on loudspeaker and the whole room feels the pressure.

STATION 3: TEAMS / SLACK

Examples of real-looking platform messages. Is it fake or not? No guidance. Just the message and a decision.

THE TALK: ARE YOU THINKING DEEP?

The talk itself can be delivered as a deepfake. The speaker is a deepfake of a real person, who then walks on stage or reveals themselves at the end. Budget dependent, but the live moment makes the point better than any slide ever could.

VIRTUAL OPTION

- Week 1: recorded talk released
- Week 2: deepfake recording activity
- Weeks 3 and 4: vishing and Teams/Slack exercises
- Digital or physical badge on completion
- Security champions run the virtual version in their own regions

THE HOOK

> ***Get free cake and find out about deepfakes.***

Pre-event: "Think you can spot a deepfake? Come and find out." Exit message: "Are you faking it?" Badge awarded on completion.

CLOSING

What to Take Away

Six blueprints. Six topics. October is closer than it looks.

October is the one month of the year where the entire organisation is primed to pay attention to security. That is a rare window. The difference between programmes that use it well and those that do not usually comes down to one thing: going in with a plan that was built around a specific behaviour, not a topic.

The blueprints in this report were not handed to a room and discussed. They were built by practitioners, in an afternoon, using nothing but their own experience of what their organisations need. That is what makes them usable. They are not theoretical. They reflect the real problems that real security awareness professionals are trying to solve right now.

THREE THINGS THAT CAME UP IN EVERY SESSION

Start with the behaviour, not the topic. The topic is the vehicle. The behaviour you want to change is the destination. Every group that produced something useful on the day started here.

Get a baseline before October. Deciding what you want to change is only half the job. If you do not know where you are starting from, you cannot demonstrate that anything moved.

Not reporting is the hardest problem in the room. Every group touched it across the day. None of them have fully solved it. That in itself is worth sitting with.

HOW TO USE THESE BLUEPRINTS

Each blueprint in this report is designed to be lifted and adapted. Take the core message and make it yours. Take the delivery plan and pressure-test it against your channels and your audience. Take the hook and rewrite it in your organisation's voice. None of this needs to be built from scratch.

If your topic is not covered here, the framework still applies. Define the human problem. Write one core message. Plan the delivery. Write the actual words. That process works for any topic, any audience, any organisation.

ABOUT THE SECURE CULTURE HUB

The Secure Culture Hub is a practitioner community for security awareness and human risk professionals, powered by Hoxhunt. It exists for the people doing this work day to day: building programmes, making the case internally, trying to move the needle on behaviour, and doing it without always having the budget, the headcount, or the senior buy-in they need.

The Hub brings practitioners together to share what is working, challenge what is not, and build things that are actually useful. Events like this one are part of that. So are the resources, the peer connections, and the ongoing conversation about what good looks like in security awareness.

www.secureculture.com

SECURE CULTURE HUB
POWERED BY HOXHUNT