



CISO Summit

Thursday 9 July 2026

Chair

Professor Andy Clark
Content Advisor, The SASIG

Host

Simon Turner
Chief Security Officer, Which?

House rules



Respect others

The Chatham House Rule must be universally respected – please do not attribute anything shared today. Phones should also be turned to silent, though you are free to leave the room for calls if needed.

Take part

We welcome questions or comments – don't forget to introduce yourself when you join the conversation. Be sure to make five new friends throughout the day, too!

Get involved

Fancy taking to the stage yourself? Speak to the team or drop us an email. Don't forget to follow us on LinkedIn and share SASIG with your colleagues, too.

Upcoming webinars



The Next Insider Threat: Securing AI Agents, Machine Identities, and Hybrid Environments Using Behaviour Analytics

11am, Friday 10 July

Agentic SOC's in the age of Mythos - What it means for Vulnerability Management

11am, Friday 17 July

Fighting Financial Fraud (F3): Insight into a Collaborative Framework

11am, Tuesday 21 July

What's Hiding in Your Microsoft 365 Tenant Could Derail Your AI Plans

11am, Wednesday 22 July

View the full calendar at www.thesasig.com/events

Upcoming in-person events



An Evening with... Petra Velzeboer

Tuesday 14 July, London

ISACA Central & SASIG Leadership Conference

Thursday 16 July, Birmingham

Scotland SASIG

Tuesday 22 September, Edinburgh

Cybersecurity Awareness SASIG

Thursday 8 October, London

View the full calendar at www.thesasig.com/events



Where will cyber leaders
be this September?

bigsasig

The flagship conference from SASIG Events

Wednesday 9 September, Central London

Apply to attend
today to avoid
disappointment...

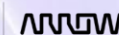


bigsasig.com

Our Supporters and Contributors



A special thanks to our
Supporters, Contributors and
all the speakers who share
their expertise with us.



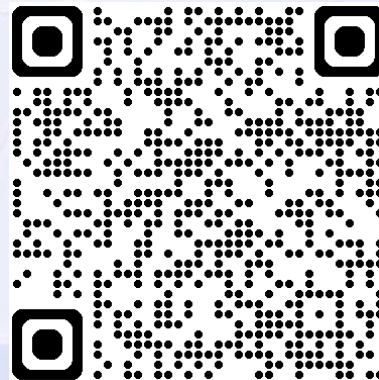
Have you got a minute?



We'd appreciate your feedback

Let us know what you thought of today's event as well as any ideas you have for future SASIG events, using our short survey or commenting on our LinkedIn post.

We'll display the below QR code on screen throughout the day which will be live at 11.30am – we'd be very grateful if you would share your views.





CISO Summit

Thursday 9 July 2026

Chair

Professor Andy Clark
Content Advisor, The SASIG

Host

Simon Turner
Chief Security Officer, Which?



Keynote presentation

Rocio Concha

Director of Advocacy, Which?



Panel session: Conscious Uncoupling for resilience?

Facilitator

Liz Murray Chief of Staff, The SASIG

Panellists

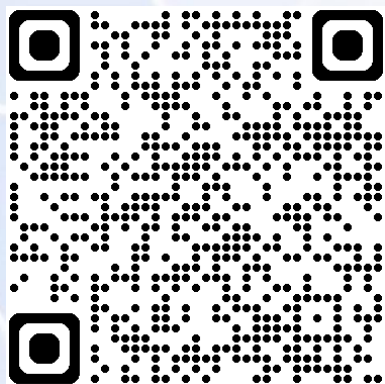
Gary Osborn Head of Information Security, Amnesty International

Ade Clewlow MBE Senior Advisor, NCC Group

Adam Boynton Enterprise Strategy Manager, Jamf

Tea, coffee & networking break

We'll be back at 11.30am



PLEASE SCAN HERE to share your
thoughts on today's event so far...



When AI Gets Personal: Fraud Visibility, Nudges, and Compliance Together

Tim Ward
CEO & Founder, Redflags

When AI Gets Personal

Bringing Visibility, Nudges, and Compliance Together.



Tim Ward

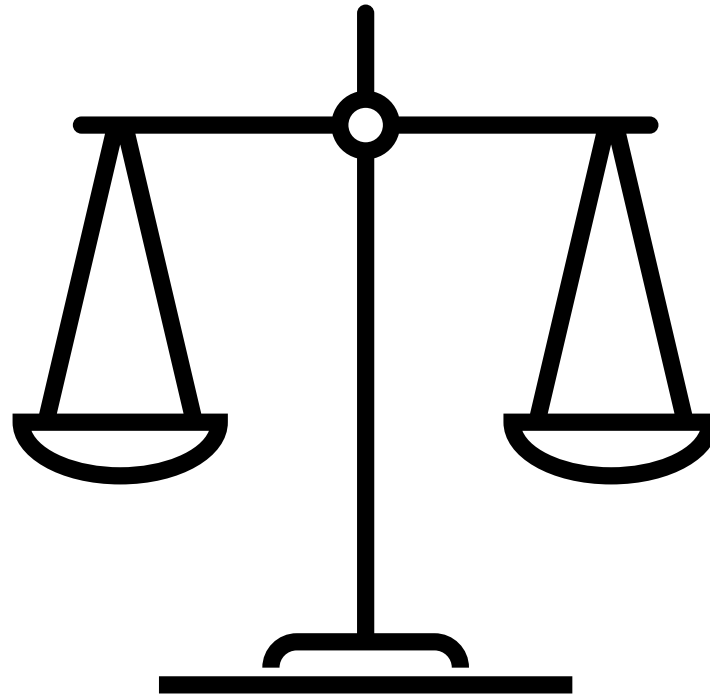
CEO and Co-Founder



AI, AI everywhere

The double-edged sword

AI:
The enabler



AI:
The
Information
Security Risk

What's the risk?

The old risks – on steroids

- Better phishing
- Better social engineering

The new risks

- Data leakage into AI
- Shadow AI
- Unmanaged local AI
- Over-trust

“The meeting of rapid technological change driven by developments in AI ... is giving rise to a period of tumultuous uncertainty.”

Richard Horne, CEO, UK
NCSC, CYBERUK 2026

The security team challenges ?

AI Visibility.... and then **Governance.**

AI governance is evolving...

2023-2004: “Keep an eye on it.”

- Focus on “visits to AI”
- Larger organisations mainly
- Block or free reign?
- Limited number of sites being nudged on

Most popular AI sites visited:

#1	 OpenAI	93%
#2	 Gemini	5%
#3	 Copilot	> 1%
#4	 perplexity	> 1%
#5	 Claude	> 1%
#6	 deepseek	> 1%

2025: “Better focus on this.”

- Nearly double the interest in visibility
- More sites being nudged on
- Initial shaping of policy
- Approved tools – nudging towards and away
- Emergence of “power” users



+91%

increase in organisations tracking AI usage year over year



+43%

average increase in visits to AI sites



3%

18%

Outliers (3% of users) make up 18% of events

2026: Pandora's box

- Hyper-speed developments
(Claude Mythos & vulnerability exploits)
- Governance, ethics & data protection headaches intensify with agents
- Rapid development of new AI trackers and nudges as behaviours evolve: 100+ sites being tracked
- Block or allow? debate still ongoing
- Redflags trends showing mix of both

Version of AI tool 'too powerful for public' released to public



Anthropic suspends new AI tools over US government security concerns

And into the future?

- Agents as extension of attack
- Hyper-efficient social engineering
- Attacker-controlled agents – long, quiet recon campaigns
- Widening gap between out-dated businesses
- Will it be the same but faster?
- Or more novel attacks?

NEWS

UK critical systems at increased risk from 'digital divide' created by AI threats

New report warns that organisations unable to defend AI-enabled threats are exposed to greater cyber risk.



mustafaU via Getty Images

Where should we focus?

- Good **security fundamentals** are still key
- Attackers still **need context** to be perfect
- Attackers still need you or your employees to **step outside processes**
- Human behaviour has **not** evolved as rapidly as AI!

*“Amid all this change, one message stays the same: The threat landscape will keep evolving, but the **fundamentals still matter most.**”*

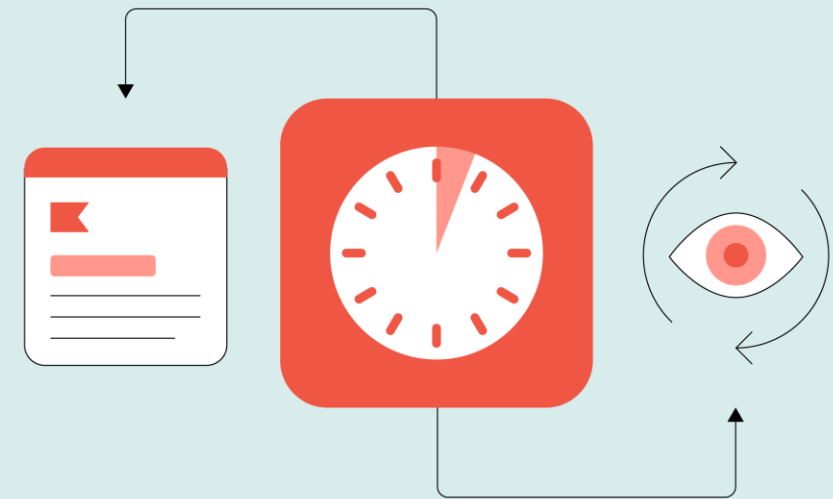
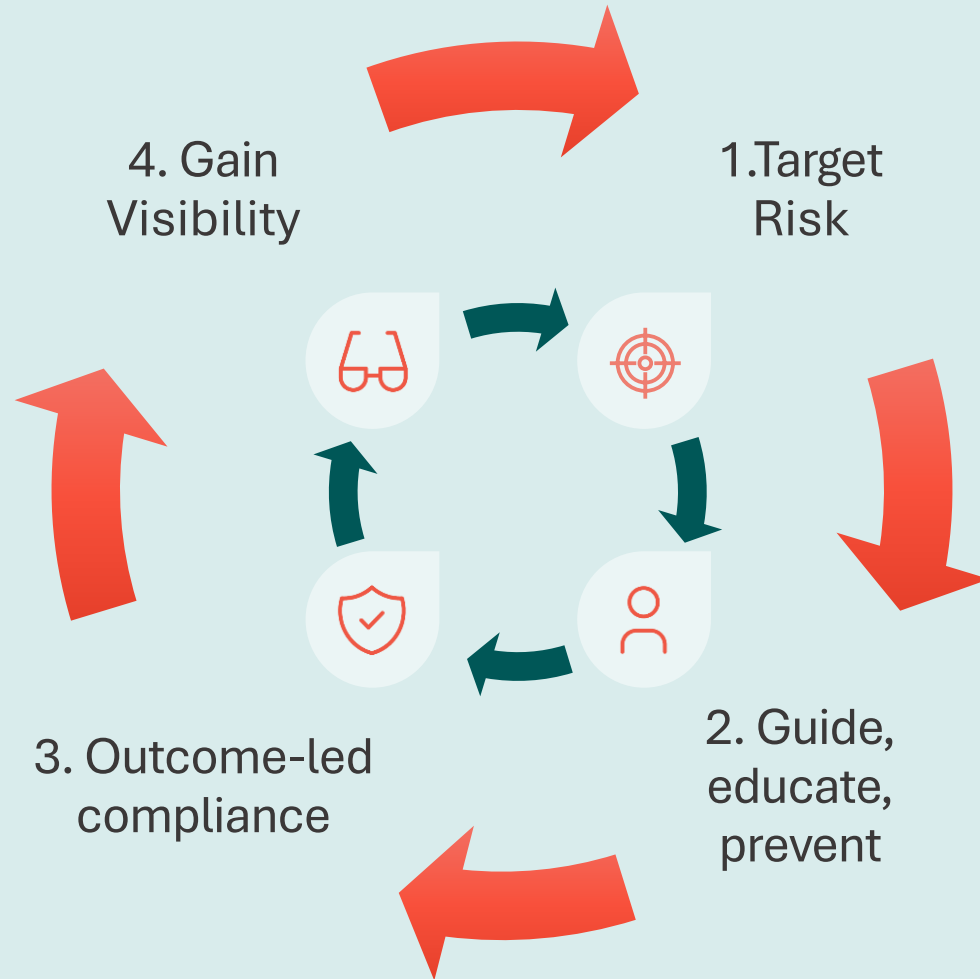
(Verizon DBIR 2026)

How can we do this?

- **Ongoing visibility is key** – focus your efforts with judicious trackers aligned to your behavioural risks
- **Inventive use of existing tools** – Redflags for visibility, inform your policy, AI teams activity, combat shadow AI
- **Human nature is unchanged** – nudge towards and reward good behaviour, nudge away from undesired
- Clear **AI usage boundaries** – enable, but safely
- Making the ***secure** choice the **easy** choice*

**Behaviour change at the point
of risk remains fundamental**

Target Risk where it lies



Visibility and targeting risk



Search portal

Refresh portal

User name

ORGANISATION
Super Bank

Dashboard

Download

Dashboard

Campaign
Manager

User
Management

Nudge
Library

Campaign
Library

Studio

Reports

Content
Report

Behaviour
Report

Risk Report

Intelligence
Pack

Updates

Risk Snapshot

254
USERS

5
BEHAVIOURS

94
HIGH-RISK USERS



TOP RISK USERS

da9d82373f88d6...	5H 0M 0L HH
73ed4592260119...	5H 0M 0L HH
4d0643cbcb1534...	5H 0M 0L HH
9c5b3e49869975...	5H 0M 0L HH
c7800b44bbf6bd...	5H 0M 0L HH

[View full report →](#)

Content Highlights

20
CONTENT ITEMS

90%
AVG ENGAGEMENT

3817
INTERACTIONS

TOP PERFORMERS

- Password Change Reminder 99%
- Policy Update Notice 99%
- Phishing Refresher Reminder 97%

NEEDS ATTENTION

- Corporate Login Warning 78%
- Incident Response Quiz 79%

[View full report →](#)

Campaign Activity

2
ACTIVE

0
DRAFTS

2
COMPLETED

RUNNING NOW

- Phishing Awareness ends 1 Jun 2026
- Sensitive Content Upload Protection ends 1 Jun 2026

[Manage campaigns →](#)



ORGANISATION
Super Bank

Dashboard

Campaign
Manager

User
Management

Nudge
Library

Campaign
Library

Studio

Reports

Content
Report

Behaviour
Report

Risk Report

Intelligence
Pack

Updates

Each user is categorised by their **ceiling** (highest per-behaviour level) and **floor** (lowest per-behaviour level) across 5 selected behaviours.

248

TOTAL USERS

9

ACTIVE CATEGORIES

132

HIGH CEILING

8

CONSISTENT HIGH (HH)

Selected Behaviours

CheckTheSender - clicked link in Outlook tracker

CheckTheSender - hovered link in Outlook cursor decorator

Clicked link in Outlook followed by password entry form decorator

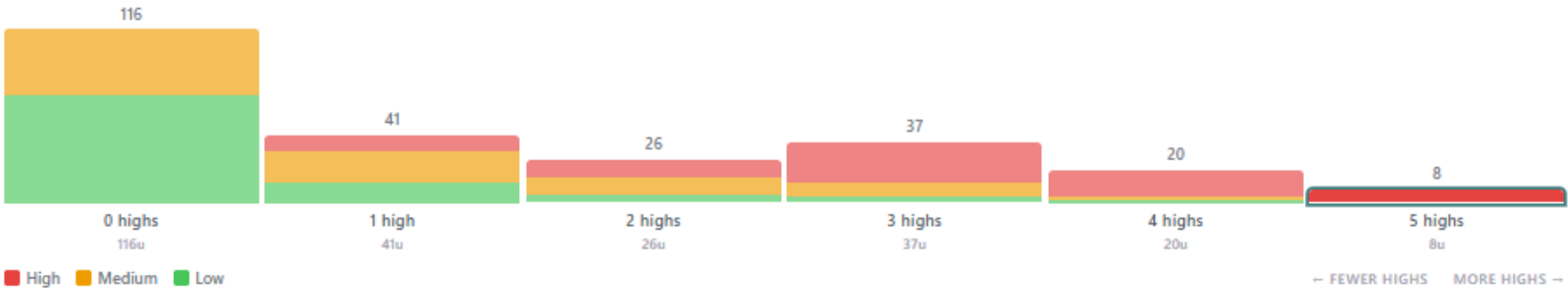
Take care with inbound attachments form decorator

Visited webmail site low frequency form decorator

Heatmap

Classification Count Distribution

1 group selected Clear



Search users...

8 of 248 users

☒	RANK ↓	USER	ENVELOPE	CHECKTHESE...	CHECKTHESE...	CLICKED LIN...	TAKE CARE ...	VISITED WEB...	HIGH IN	ACTIVE
☒	1	da9d82373f88d613...	HH	HIGH 88	HIGH 208	HIGH 10	HIGH 115	HIGH 16	5 / 5	5 / 5
☒	2	e7...						HIGH 14	5 / 5	5 / 5

28 users selected

Assign Group

+

-

Add tag...

Clear

Guide, educate, prevent, CHANGE



Understand human behaviour

- Traditional training relies on the idea that:
 - knowledge, skills and understanding of the risk
 - all impact intention,
 - which leads to behaviour
- But...
 - Context interferes
 - Sub-conscious decisions / cognitive bias / heuristics
 - Habit-based decisions bypass executive function

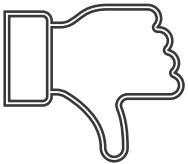


How we really decide under pressure



Bounded Rationality

Nudge theory recognizes that individuals make decisions using limited time, information, and mental resources.



Heuristics and Cognitive biases

Heuristics are “rules of thumb” that help us make quick decisions without exhaustive analysis. They are efficient but can lead to systematic errors in judgment – Cognitive biases

Availability bias

Salience bias

Optimism bias

Affect heuristic

Authority bias

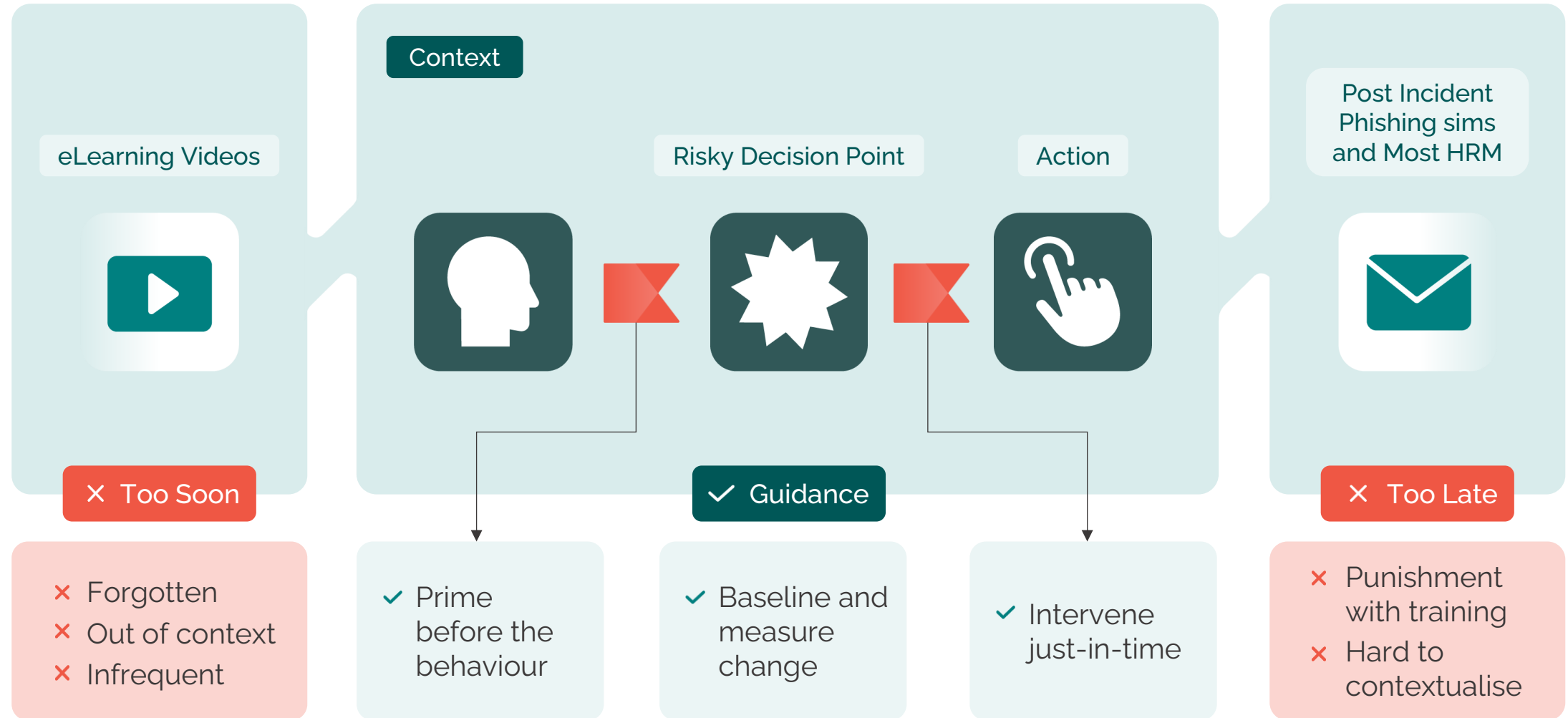
Confirmation bias

Familiarity bias

Conformity bias

Priming bias

Pre-emptive behaviour change



AI Use Case : Global Business Leader



Some of the key AI behaviours that are tracked

- **Tracking & nudging on visits to download page(s) of unapproved AI agents**
- **Tracking use of M365 copilot in browser and via desktop app & use of non-M365 Copilot**
- **Nudging users on the nonM365 version** to redirect them to the M365 version/encourage sign in with corporate credentials if using Copilot for work purposes
- **Tracking on visits to & uploads to unapproved AI sites** like ChatGPT, and nudging on uploads to these sites to point users to approved solutions instead.

- **Growing concern:**
Employees are building agents in copilot browser/desktop app: *What these agents are being granted access to?*
- **New nudge request :**
nudging when users are building agents in copilot browser/desktop app to reinforce principle of least privilege

AI “Stories”

Focus on key learning points

Provide actionable security advice, with click-through for more information

Desktop ‘overlay’ format

Low friction but conspicuous.

Engaging paged content including Q&A

Engagement tracking

Measurement of dwell time and click-through statistics

Ease, timeliness, salience, availability



AI poisoning

AI tools have rapidly integrated into daily life, but they are a whole new frontier for secure development and implementation.

Read on to learn more about poisoned AI tool attacks and how you can secure against these.



Click to continue

Read time <60 seconds



Check your AI

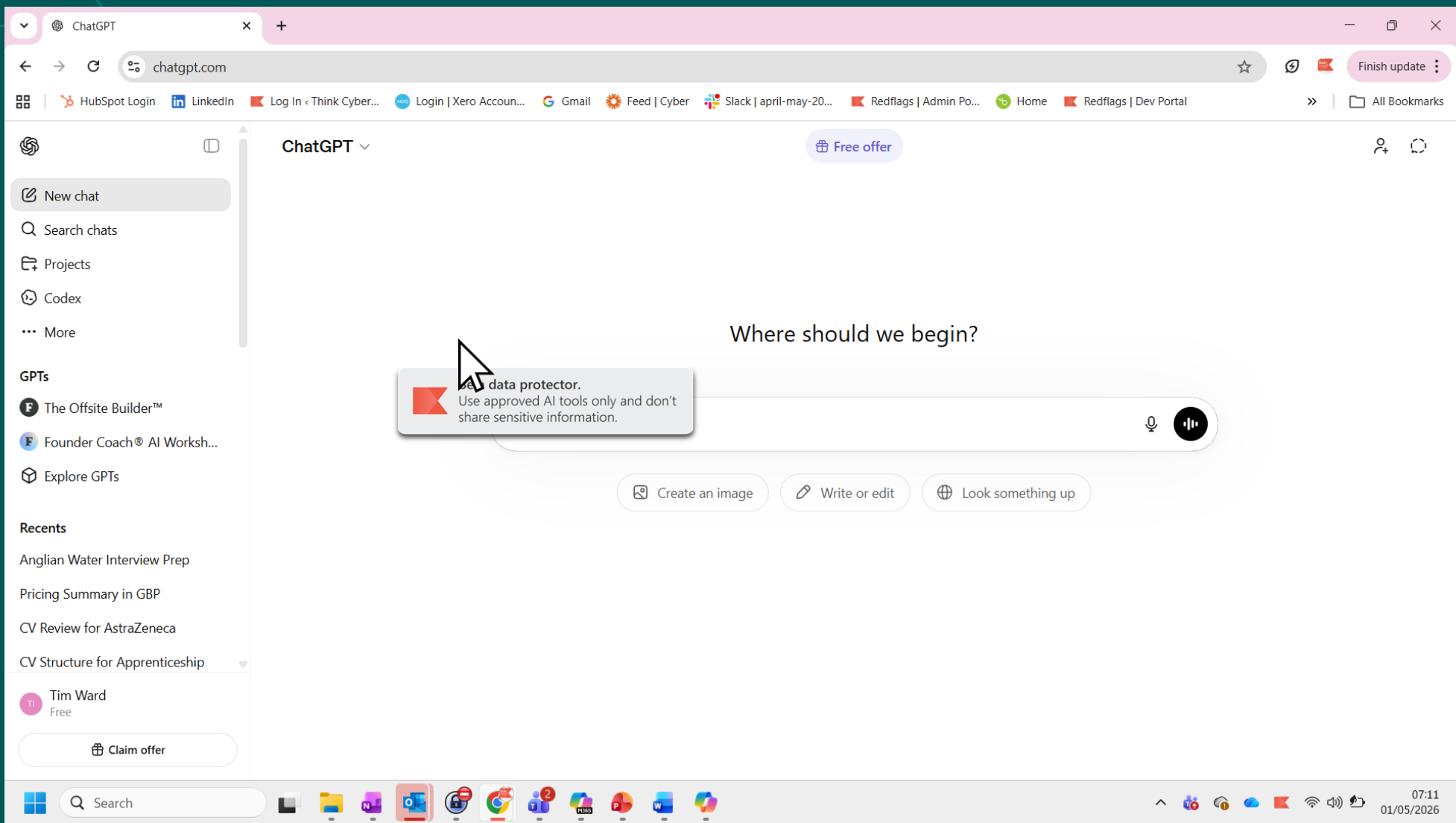
AI tools are a useful starting point for many tasks, but it's important to be aware of their limitations and to carefully check output generated by AI.

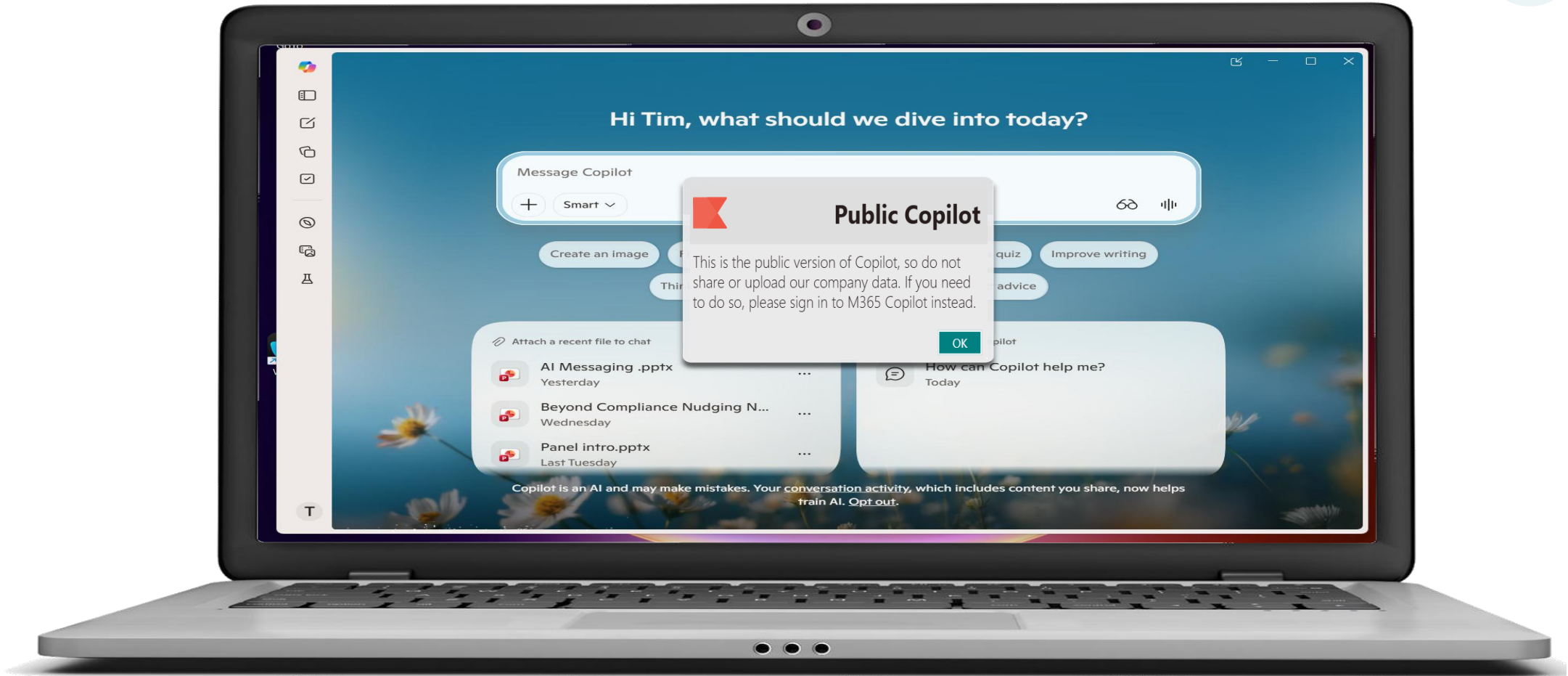


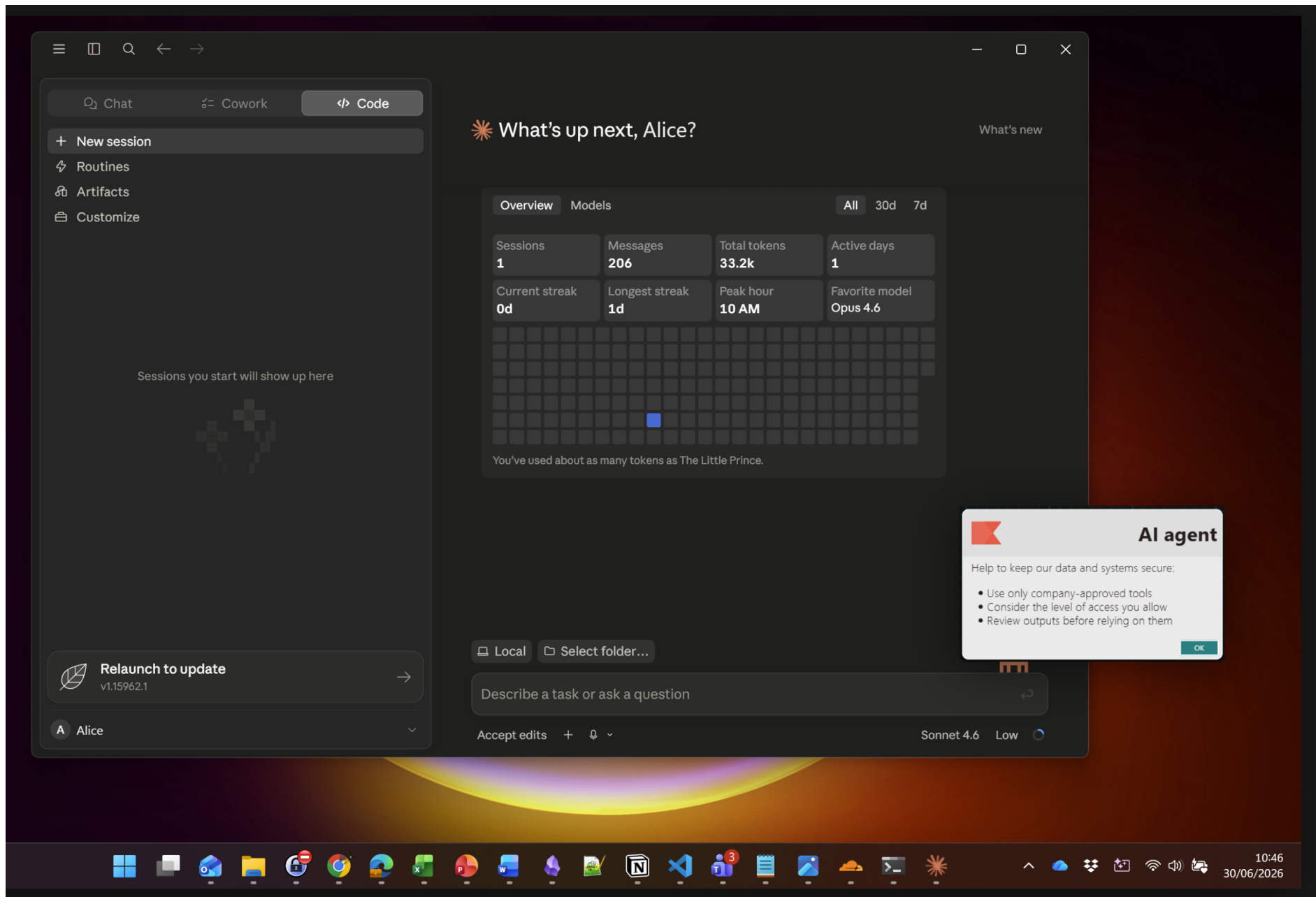
Click to continue

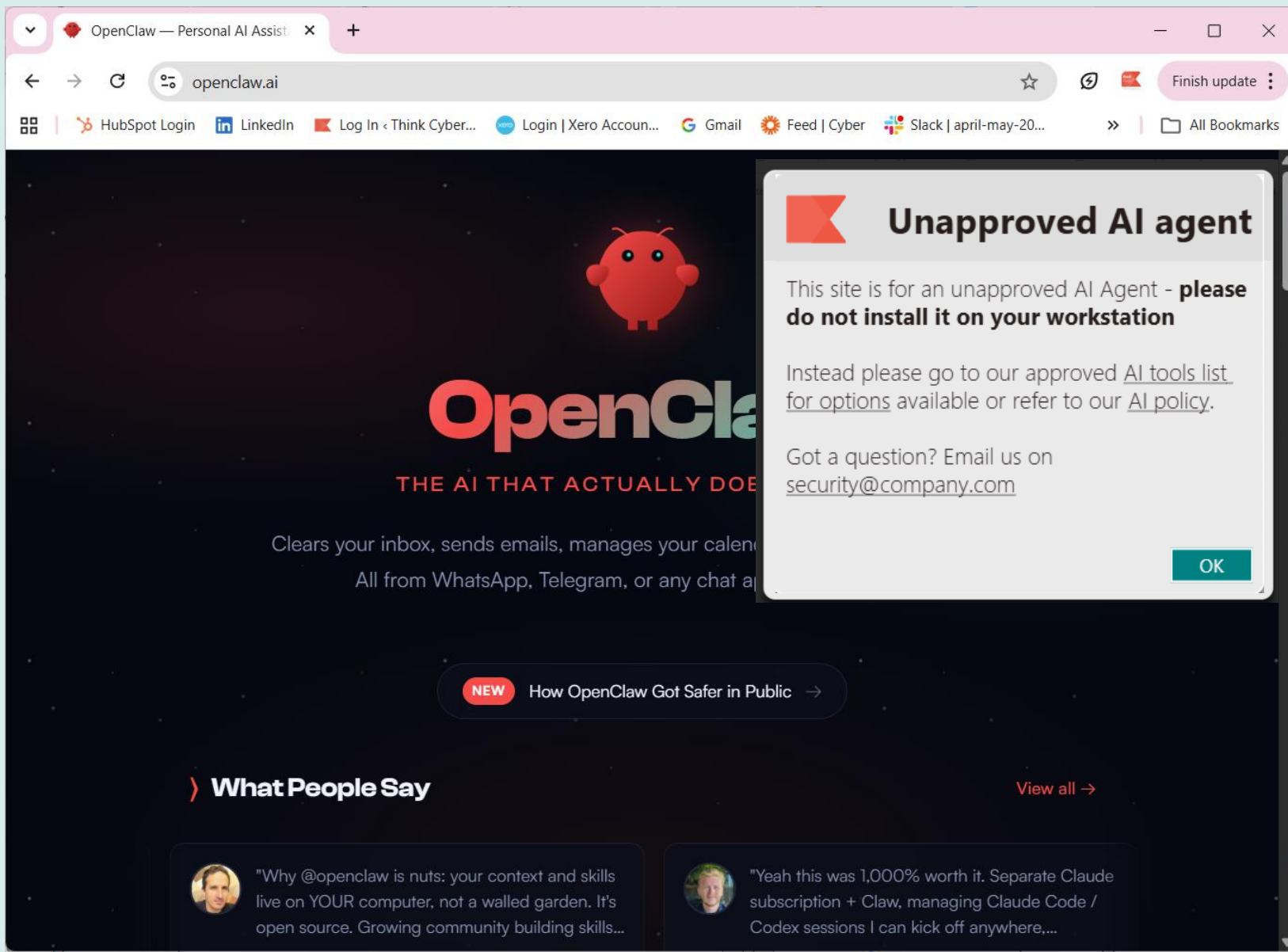
Read time <60 seconds











Lead with outcome-led compliance



Changing regulation

- Outcomes > activities → evidence of risk reduction matters, not training completion
- Behavioural cyber risk → human actions are treated as both risk drivers and risk controls
- Continuous improvement → maturity assessed over time, not point-in-time
- Integration of governance, policy and operations → policies must be understood and applied by people in real situations

No longer assessed on “delivering” training.

Organisations must now prove:

- People **recognise real threats**
- People **behave securely in context**
- **Incidents are reported** correctly and quickly

Human behaviour measurably reduces risk

Compliance report

View which users have completed training that contributes to each compliance framework. This report reflects training coverage, not certification status.

Export CSV

ISO 27001

SOC 2

Cyber

229

90% of 254 users

COMPLIANT USER

Search users...

USER

9c5b3e49869975620e8ad

791eed613637f8e150aae2e

44989a02931aa255a9e0f4

e98d45754fc6ea9cf3f676f

b56aee5c33eb480886b58

User Report



User timeline

4782ce2474...

80%

Engagement

11m

Total dwell

18

Events

COMPLIANCE COVERAGE

CE+

ISO 27001

GDPR

All

Content

Events

Quiz

Nudge

Search timeline...

CAMPAIGN

All campaigns

DATE RANGE

All dates



First seen — Client registered

Browser extension installed and registered with the portal

10 December 2025



19 DECEMBER 2025

2 items

Phishing Awareness — Slide 3

Q1 Phishing Awareness · 13:50

Content

2m 13s

DWELL

64%

ENGAGEMENT

ORGANISATION

Super Bank ▾

Dashboard

Campaign
ManagerUser
ManagementNudge
LibraryCampaign
Library

Studio

Reports ▾

Content
ReportBehaviour
Report

Risk Report

Intelligence
Pack

Updates

Show Impact

[← Back to Behaviour Reports](#)

Intervention Timeline

View behaviour trends over time with campaign content overlaid. Click a content marker to see the population shift before and after deployment.

CAMPAIGN

Phishing Awareness 2025 ▾

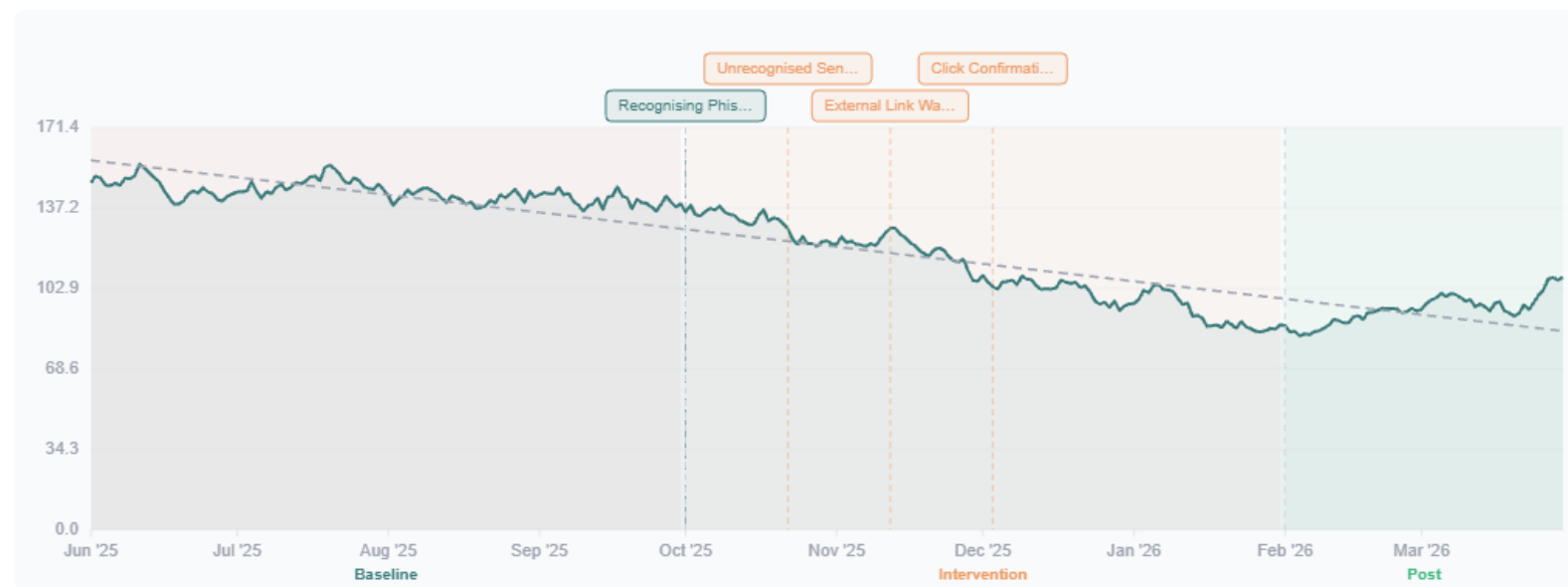
TRACKERS

Suspicious Link Hovers 210u
-35%Phishing Link Clicks 169u
-32%Credential Entry on
Untrusted Sites 98u
-29%

CONTENT ITEMS

 Recognising Phishing Emails
1 Oct 2025 Unrecognised Sender Badge
22 Oct 2025 External Link Warning
12 Nov 2025 Click Confirmation Dialog
3 Dec 2025

Suspicious Link Hovers PHISHING_RECON



● Baseline avg 144.1 events/day ● Intervention avg 111.07 events/day ● Post avg 93.97 events/day ↗ Overall change -35% 👤 Users responded 47%



Delivered in context

Nudge the user when they encounter a link in an email from an external sender

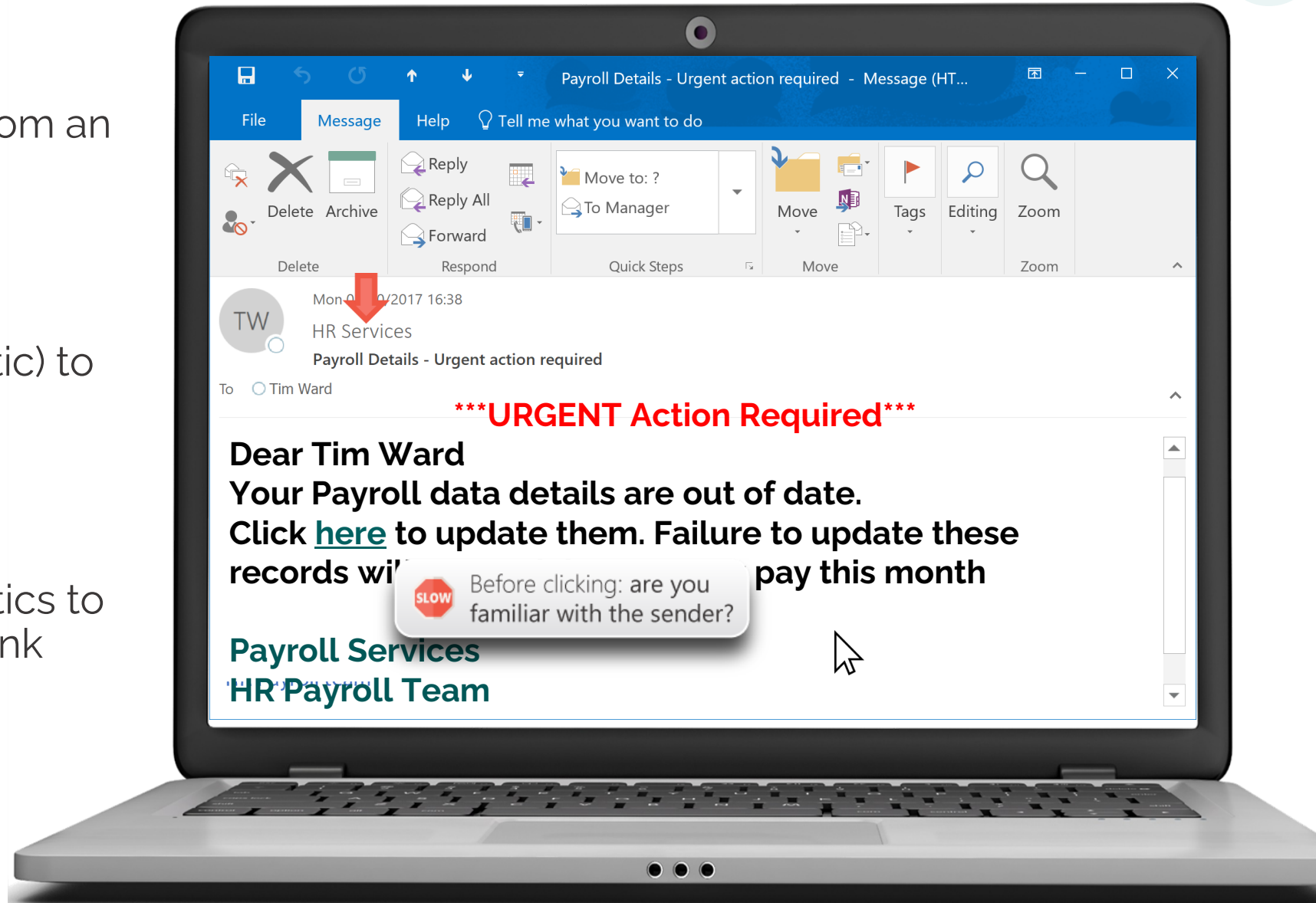
Promotes desired behaviour

Move from System 1 (automatic) to System 2 (deliberate) thinking

Engagement tracking

Measurement of nudge statistics to track trends: link hovered vs link clicked

“Disruptor” or “Spark”



In context nudges

Delivered in context

Nudge the user when they enter credentials AFTER clicking

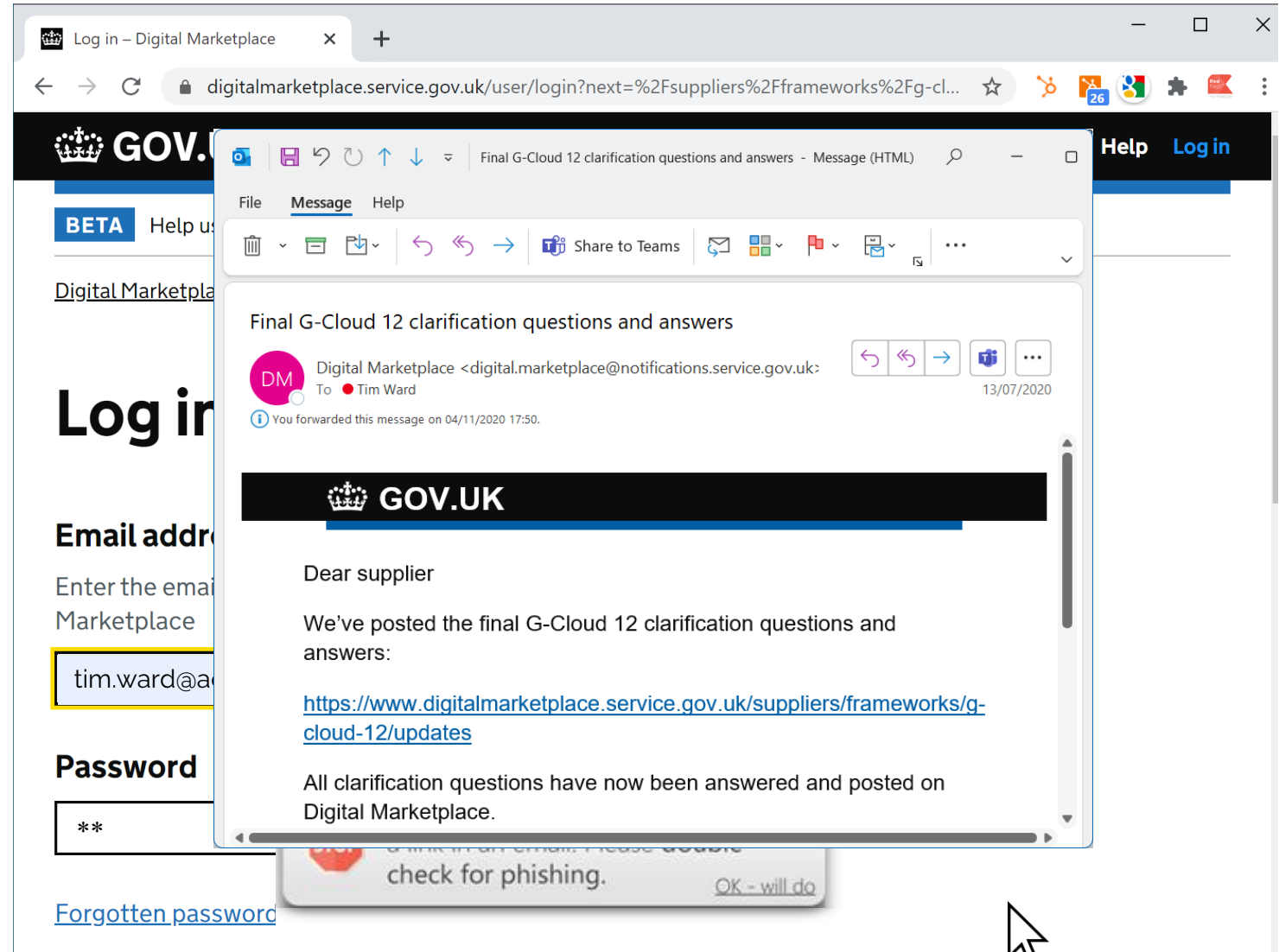
Promotes desired behaviour

Move from System 1 (automatic) to System 2 (deliberate) thinking

Engagement tracking

Measurement of nudge statistics to track trends

Timely, relevant



Final thoughts

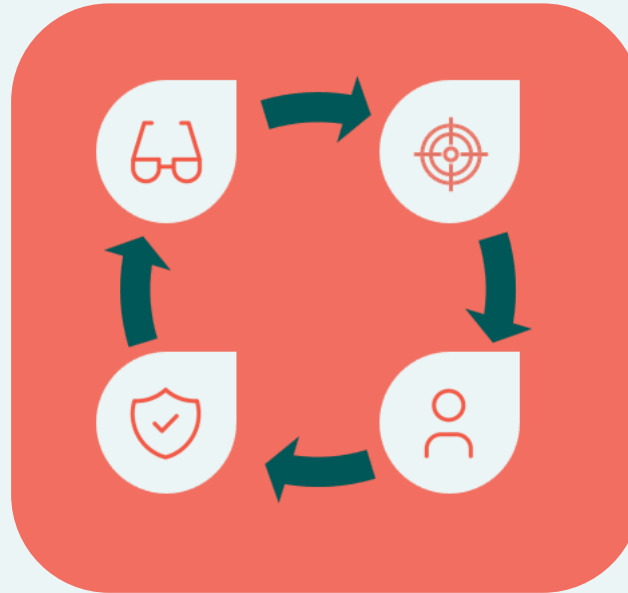
CISOs rising concerns

"Every CISO I talk to has discovered some form of shadow AI..."

"It's not the AI part of shadow AI that concerns them. It's the data that's being provided to an AI by the employee."

Andrew Walls, Gartner VP Analyst, quoted in CSO Online

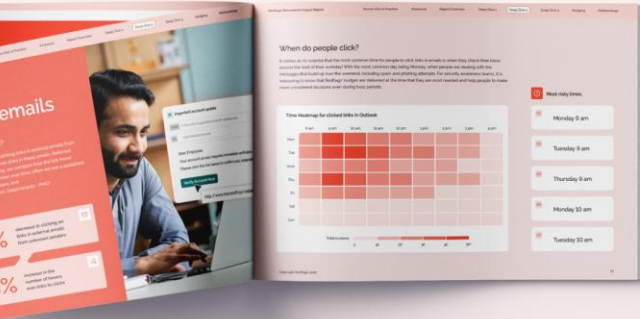
AI: The Enabler for both Defenders and Attackers



Mixed Blessing

- An Enabler for business and security teams' efficiency
- A significant enabler for attackers with wider attack surfaces being exploited
- Security teams often have **no visibility and no way to enforce governance**
- This **remains a behavioural challenge** to
 - get telemetry on tool usage
 - distinguish sanctioned and unsanctioned
 - target risk
 - intervene in context to change behaviours
 - Delivering outcome-led compliance

What Went Into The Redflags Behavioural Impact Report



493,938
minutes spent engaging
with security content

Redflags Behavioural Impact Report 2026

[Download Report Now](#)



29,324,301
real-time nudges
delivered



28,544
employees
reached





Cyber in the Boardroom: Is your SLT ready for a crisis?

Ade Clewlow MBE
Senior Advisor, NCC Group



- **Cyber in the Boardroom:**

- Is your SLT ready for a crisis?

- **Ade Clewlow MBE**

- Senior Advisor

- 9th July 2026

- Making a more secure digital future

- Classification: Public

Who would be a CISO?







CYBER RESILIENCE MATURITY

MANAGED

**You know there are
unmitigated risks.
You control what you can.**

*Your senior leaders believe they're
doing enough.*

**You know the risks.
You control the risks.**

*Your risk appetite is clearly
articulated by your SLT/Board, which
has adopted an operational
resilience mindset.*

UNCERTAINTY

**You don't know all the risks.
You don't control any of them**

*Leadership, governance and
accountability for cyber resilience is
absent at the executive level.*

CERTAINTY

**You know the risks.
You don't have controls in
place to mitigate them.**

*Your senior leaders have not
embraced cyber resilience as an
operational/business resilience
issue.*

UNMANAGED







- QUESTIONS

• Thank you.

• Classification: Public



Case study and discussion: What can CISOs learn from fraud victims that can protect their people before, during and after a breach?

Liz Murray

Chief of Staff, The SASIG

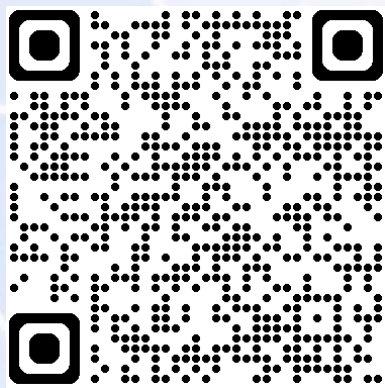
In conversation with

Matt Niblett

Senior Policy Advisor, Which?

Networking lunch

We'll be back at 2pm



PLEASE SCAN HERE to...

- Share **FEEDBACK** on today's event
- Suggest **TOPICS** for us to explore
- **CHAIR** one of our webinars
- **SPEAK** at a future session
- **HOST** one of our events





Phishing Isn't an Email Problem - It's an Enterprise Risk Problem

James Hickey
Principal Sales Engineer, Cofense



Phishing Isn't an Email Problem — It's an Enterprise Risk Problem

Why resilience, not prevention, is becoming the
defining security capability

Agenda

- The Modern Attack Surface is Human
- Where Legacy Thinking Fails
- Why Security is a Board-Level Risk
- What Good Looks Like...
- Questions You Should be Asking
- 5 Key Takeaways
- Q&A

Speaker



James Hickey
Cofense Principal Sales Engineer

The Modern Attack Surface is **Human**

Communication channels are multiplying
& threats have evolved for success!

Enterprise Communication

- Email
- Teams
- Slack
- Zoom
- SMS
- WhatsApp
- Voice
- CRM
- HR Systems
- Vendors

Evolution of Threats

- Email
- Smishing
- Vishing
- Teams/Slack
- QR Codes
- Deepfake-assisted social engineering
- Multi-channel attacks

Attackers focus on weakness for entry:

- ✓ Trusted relationships
- ✓ Interconnected communications
- ✓ Processes

It's no Longer a **Fair Fight**

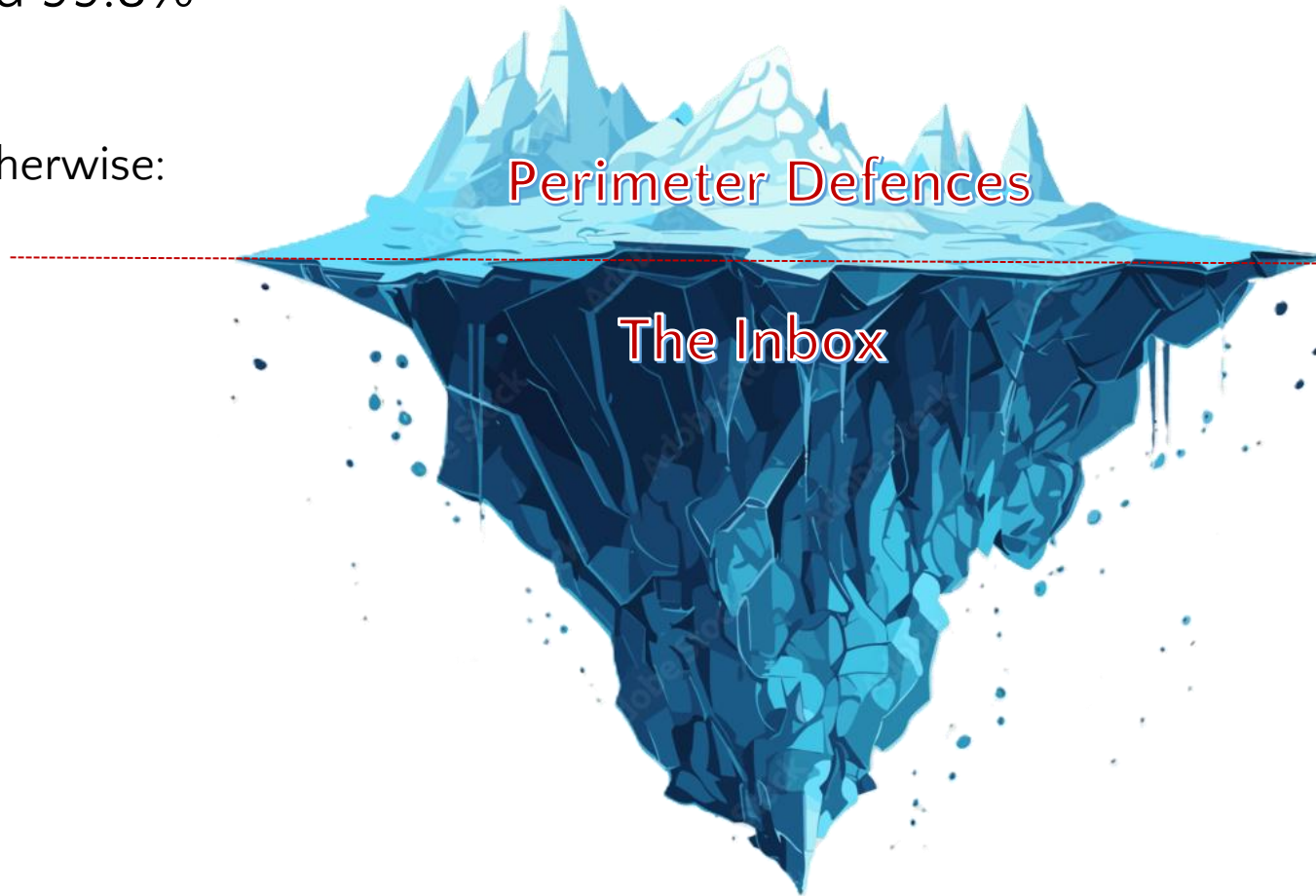
AI has:

- Increased speed
- Increased scale
- Increased believability
- Lowered attacker skill requirements

The Dangerous Illusion of Security

"We Blocked 99.8%"

Reality says otherwise:



Visible & Stopped:

- Known Threats
- Blocked emails
- Gateway metrics

Hidden:

- Unknown Threats
- Missed attacks
- Business process abuse
- Credential compromise
- Lateral movement
- Fraud attempts

Where Legacy Thinking Fails

Traditional Model

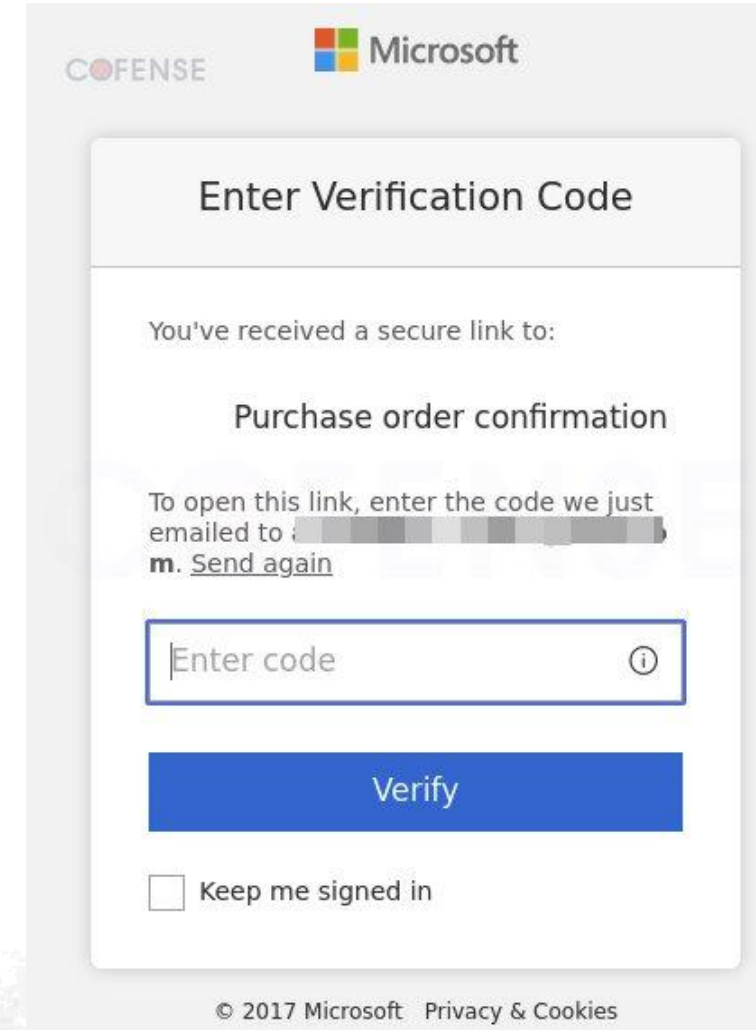
Prevent → Detect → Respond

Modern Threat Reality

Exploit → Pivot → Escalate → Disrupt

Critical question:

“How quickly can the organisation identify, escalate, contain, and recover at speed?”



The screenshot shows a web interface for entering a verification code. At the top, there are logos for 'COFENSE' and 'Microsoft'. The main heading is 'Enter Verification Code'. Below this, it says 'You've received a secure link to:' followed by 'Purchase order confirmation'. Then, it says 'To open this link, enter the code we just emailed to:' followed by a redacted email address and a link 'm. Send again'. There is a text input field labeled 'Enter code' with an information icon. Below the input field is a blue 'Verify' button. At the bottom, there is a checkbox labeled 'Keep me signed in'. The footer contains the text '© 2017 Microsoft Privacy & Cookies'.

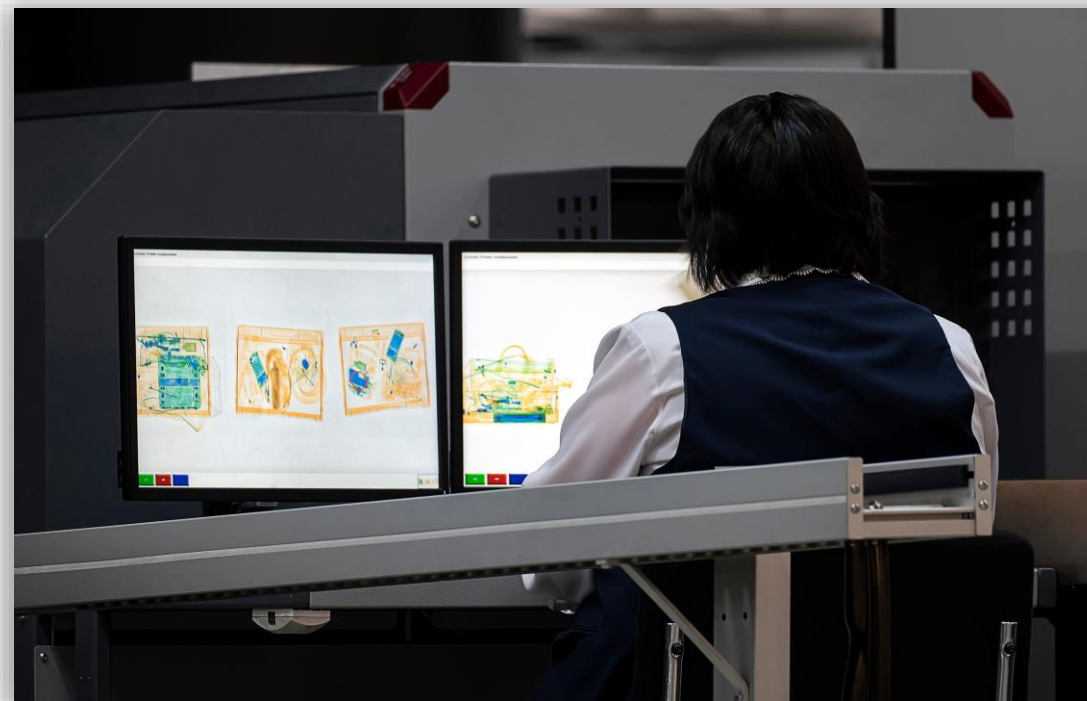
Why This Is Now a **Board-Level Risk**

Risks Created:

- Financial loss
- Operational disruption
- Regulatory exposure
- Customer impact
- Brand damage
- Supply chain risk

Speed is everything...

AI Alone is not enough



AI-Only Strategies Create Their Own Problems

Lack of human context
+
Lack of Visibility/
Transparency
+
Diminished Data Protection
=
AI Black Box

What Regulators Are Actually Asking For

KEY FACTORS:

NIS2:

- ✓ Governance
- ✓ Risk management
- ✓ Incident readiness
- ✓ Supply chain resilience

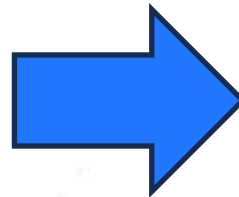
ISO 27001:

- ✓ Organisational controls
- ✓ Human factors
- ✓ Continuous improvement

The Shift from Security Metrics to Resilience Metrics

Traditional Metrics

- ✗ Emails blocked
- ✗ Spam volume
- ✗ Gateway efficacy
- ✗ Click rates



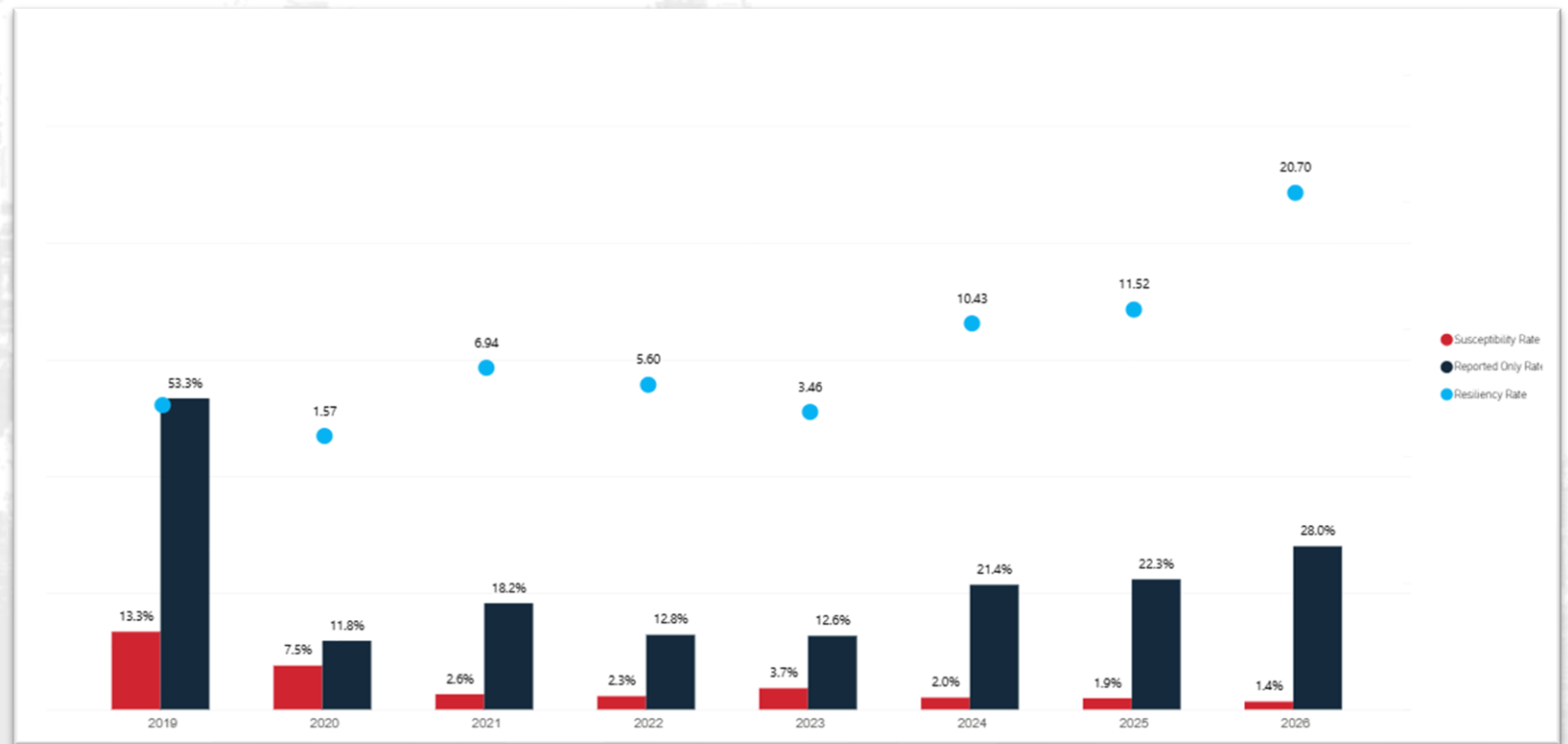
Resilience Metrics

- ✓ Detection speed
- ✓ Reporting rates
- ✓ Escalation confidence
- ✓ Process integrity
- ✓ Investigation speed
- ✓ Containment time

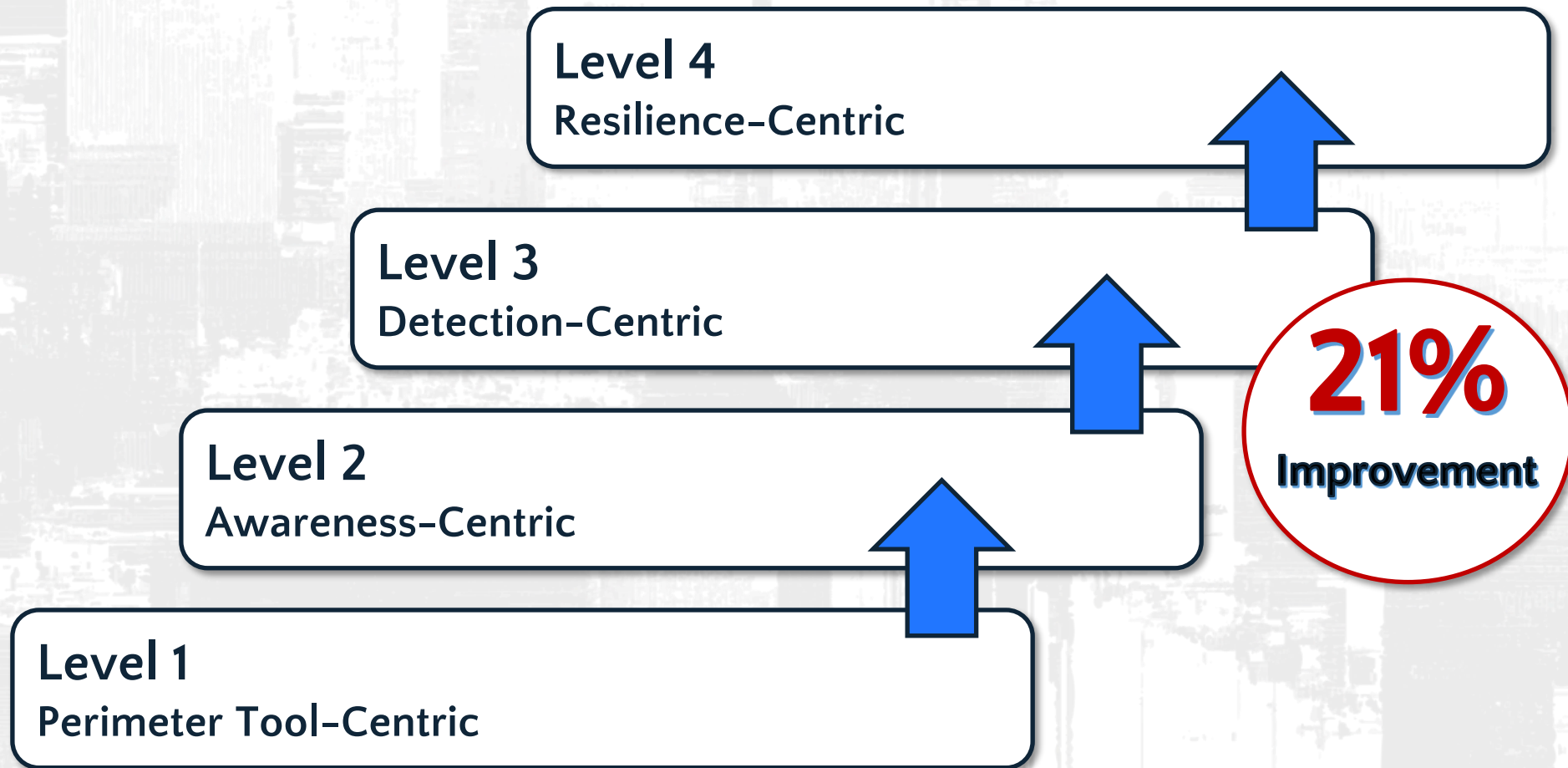
What Good Looks Like...

Four Pillars:

1. Governance
2. Culture
3. Visibility/ Collaboration
4. Response Readiness



The New Maturity Model

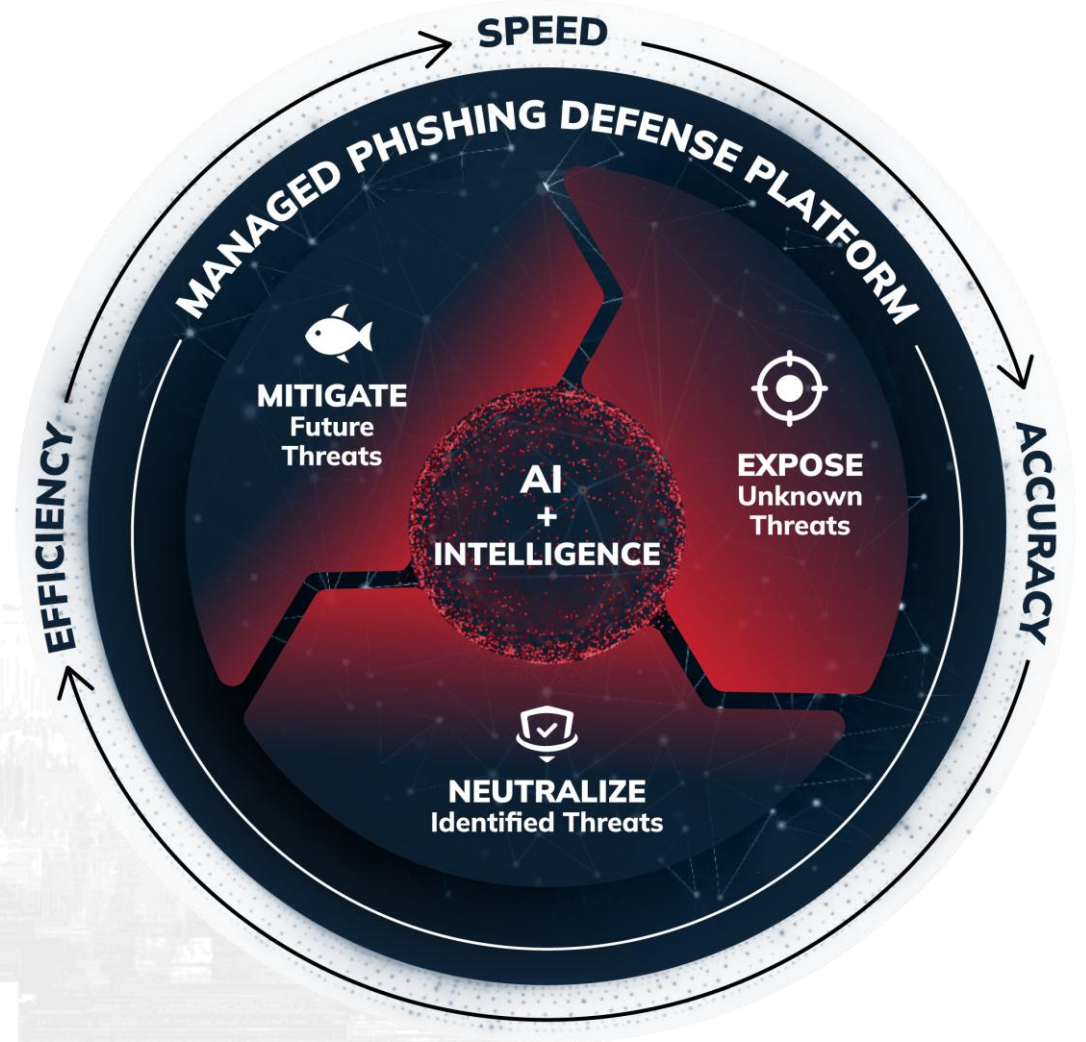


Building Unified Enterprise Phishing Resilience

People + Process + Technology + Governance

=

Resilience



Executive Questions Every Organisation Should Ask

1. How quickly would we detect a successful phishing attack?
2. Would employees know exactly what to do?
3. Are escalation paths trusted, seamless and integrated across functions?
4. Could we contain compromise rapidly?
5. Can we measure readiness today?

Five Biggest Takeaways for Leaders

1. Human–AI partnership will define cyber resilience in 2026.
2. The Automation Paradox is here and it's shrinking the window between attack and compromise.
3. Tooling alone cannot create resilience; validation will add the continuous improvement in phishing detection.
4. Governance, culture, and process are becoming decisive differentiators.
5. The winning organisations will measure readiness—not just prevention.



**5 Key
Takeaways**



THANK YOU

Find more information on our website:

Cofense.com/blog

Cofense.com/webinars

Find me on LinkedIn

<https://www.linkedin.com/in/jamesthomashickey>



Prompt behaviour: Why AI governance fails without behavioural security

Oz Alashe
CEO & Founder, Cybsafe



Interactive session: Leading change through collaboration

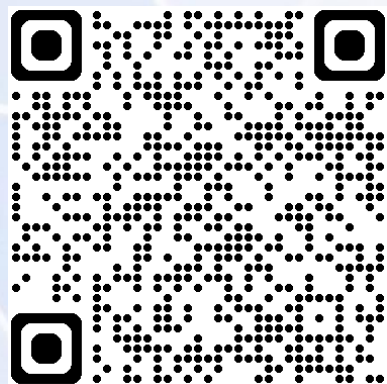
Simon Turner

Head of Infosec & Technical Risk, Which?

Kerrie Grier

Cybersecurity Strategy Delivery Manager, Which?

End of Meeting



PLEASE SCAN HERE to...

- **Share FEEDBACK** on today's event
- **Suggest TOPICS** for us to explore
- **CHAIR** one of our webinars
- **SPEAK** at a future session
- **HOST** one of our events

