CISO Roundtable
The practical, emotional and legal challenges faced by CISOs

Tuesday 25 November 2025

Chair

Martin Smith MBE
Chairman and Founder, The SASIG

House rules

sasig

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!

Give us your feedback
Let us know what you thought of today’s event as well as any ideas you have for the future using our short survey – there will be a QR code available today and we’ll email you a link.

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

Discovering today's threat landscape: The 2025 Elastic Global Threat Report
11am, Wednesday 26 November

Women in cybersecurity: Powering innovation and inclusion
11am, Friday 28 November

Discovering today's threat landscape: The 2025 Elastic Global Threat Report
11am, Monday 1 December

Just one detection needed: Turning the tables on SharePoint attackers
11am, Wednesday 3 December

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

Upcoming in-person events

Financial Services SASIG: The challenges remain
Thursday 4 December – City of London

SASIG Christmas Networking Lunch
Tuesday 9 December – Mayfair, London

Data Management - Security, resilience and application in the face of growing threats
Tuesday 13 January – London

Threat intel and incident management
Thursday 29 January– London

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

Our Supporters and Contributors

sasig

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

Qualys. Redflags® WAVESTONE

CROWDSTRIKE ncc group exabeam™

Vanta CYBSAFE censys SOPHOS

KUDELSKI SECURITY Patrowl PHISHME COFENSE

KELA Bridewell elastic jamf

CISO Roundtable
The practical, emotional and legal challenges faced by CISOs

Tuesday 25 November 2025

Chair

Martin Smith MBE
Chairman and Founder, The SASIG

Keynote panel session: What keeps CISOs awake at night?

Facilitator

Martin Smith MBE Chairman and Founder, The SASIG

Panellists

Susanne Bitter Head of Regional Strategic Alliances, Cyber Security Forum Initiative
Liz Banbury CISO, Thames Water
Paul Haywood Global CISO, WTW
Ali Dyer Group CISO, Associated British Foods (ABF)

A CISO's guide to people-centric security

Tim Ward

CEO and Co-Founder, Redflags

CISO's Guide to People-Centric Security

Fan heaters vs Thermometers

Agenda

01

CISO Worry list

02

Why people centric security?

03

Traditional approaches

04

Human Risk Management in practice

05

Understanding human behaviour

06

Proving impact and building resilience

CISO worry list

- Reduce operational / business risk
- Meet regulatory and compliance obligations
- Build organisational resilience
- Protect against emerging threats
- Measure impact and ROI
- Maintain exec / Board confidence

Why people-centric?

Organisations that ignore human risk:

Risk reputational damage, regulatory fines, and operational disruption – even if their tech stack is world-class.

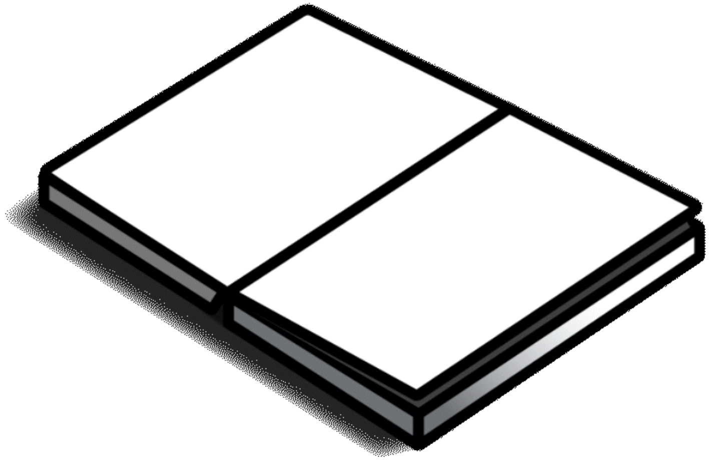
- Tech controls tangible, measurable easier to justify in budgets
- People / behaviour is the root cause in 70-90% breaches
  - Technical controls can be bypassed by a single click or decision.
  - Attackers increasingly exploit psychology (urgency, trust) rather than technical flaws.
  - Diminishing returns from tech controls
- A security-aware workforce enables safe adoption of new tech (cloud, AI) without creating unmanaged risk.

“But we are doing this aren’t we?”

Where have we been going wrong?

First understand 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
- Phishing sims fly in the face of behavioural research
  - Multiple longitudinal studies highlight ineffectiveness
  - Teaching at point of failure ineffective

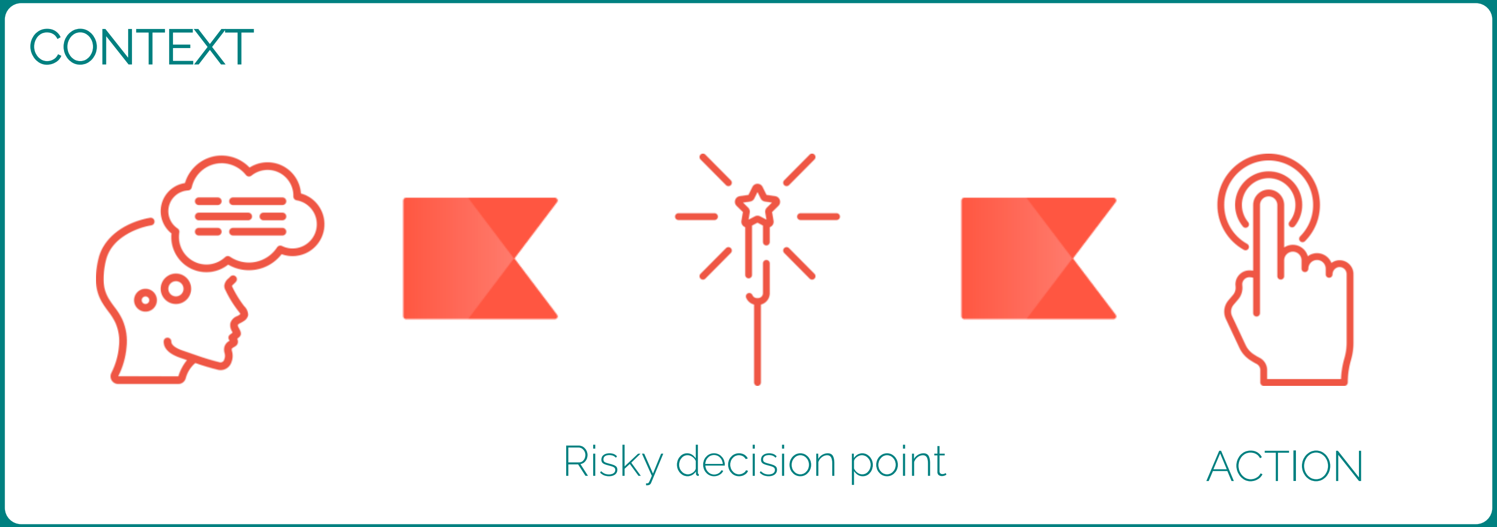


How should we help people?

eLearning
Videos

TOO SOON

Quickly forgotten
Out of context



CONTEXT

Risky decision point

ACTION

Post incident
simulations

TOO LATE

Punishment with training
Hard to contextualise

People centric objectives

- Embed a people centric security culture
- Use tools to measure and intervene
- Continuous awareness and reinforcement
- Measure change, not just completion
- Balance tech and people centric aspects of security

Is *"Human Risk Management"* the answer?

What is Human Risk Management?

The thermometer

- Aggregate data from systems you already have
- Create comprehensive dashboards / risk scores
- Generate reports for executives
- *Then leave you to figure out what to do about it*

SECURITY AWARENESS MANAGERS
HRM SOLUTIONS
HERE'S YOUR RISKS BUT IN A PIE CHART FORMAT
imgflip.com
Gudim.

What is Human Risk Management?

The thermometer

- Aggregate data from systems you already have
- Create comprehensive dashboards /risk scores
- Generate reports for executives
- *Then leave you to figure out what to do about it*

- Great for vendors:
  - 6-12 month integration projects = professional services revenue
  - More systems integrated = harder to rip out
  - Complexity justifies enterprise pricing
  - "We have all your data" = vendor lock-in

"Here's Sarah's risk score" (now you figure out what to do)

The fan heater

- Focus on: What intervention works for THIS person RIGHT NOW?
- Deliver interventions automatically
- Prove behaviour actually changed

- Great for organisations large and small
  - Fast time-to-value
  - Minimal friction deployment
  - Measurable behaviour change outcomes
  - Proving actual ROI

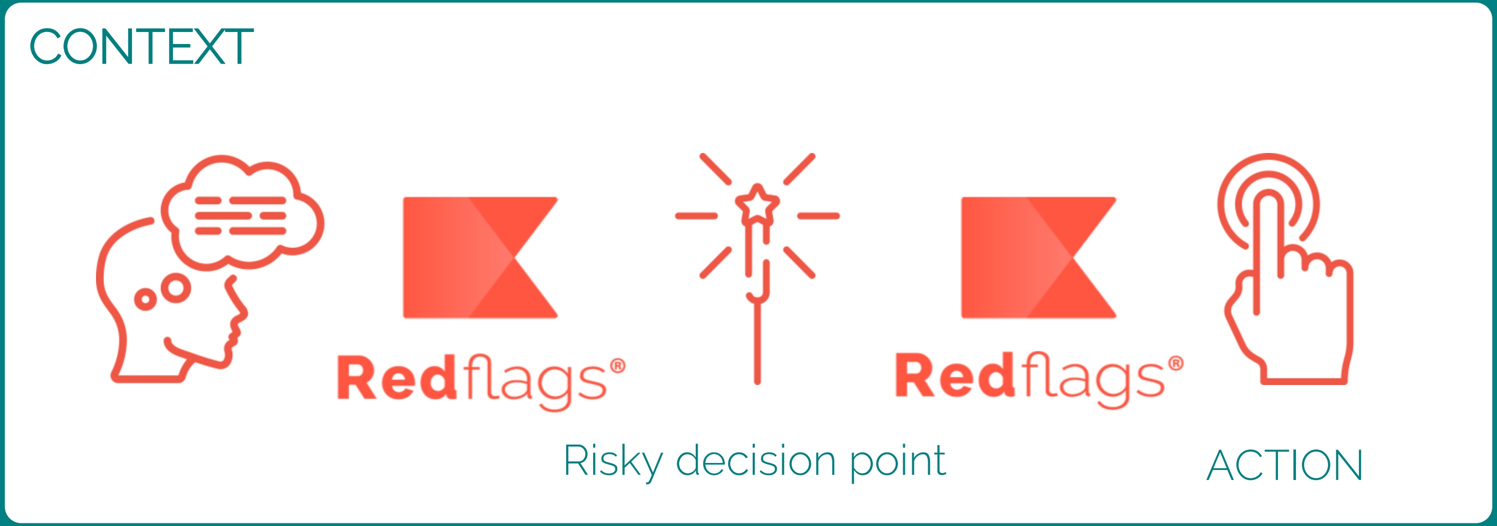
"Here's what's targeting Sarah, here's what will work for her, here is the intervention and here's proof it worked"

Measure and intervene - in context

eLearning
Videos

TOO SOON

Quickly forgotten
Out of context



CONTEXT

Risky decision point

ACTION

Prime before
the behaviour

Intervene
just-in-time

Baseline and
measure change

Post incident
simulations

TOO LATE

Punishment with training
Hard to contextualise

Why Nudging Works

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

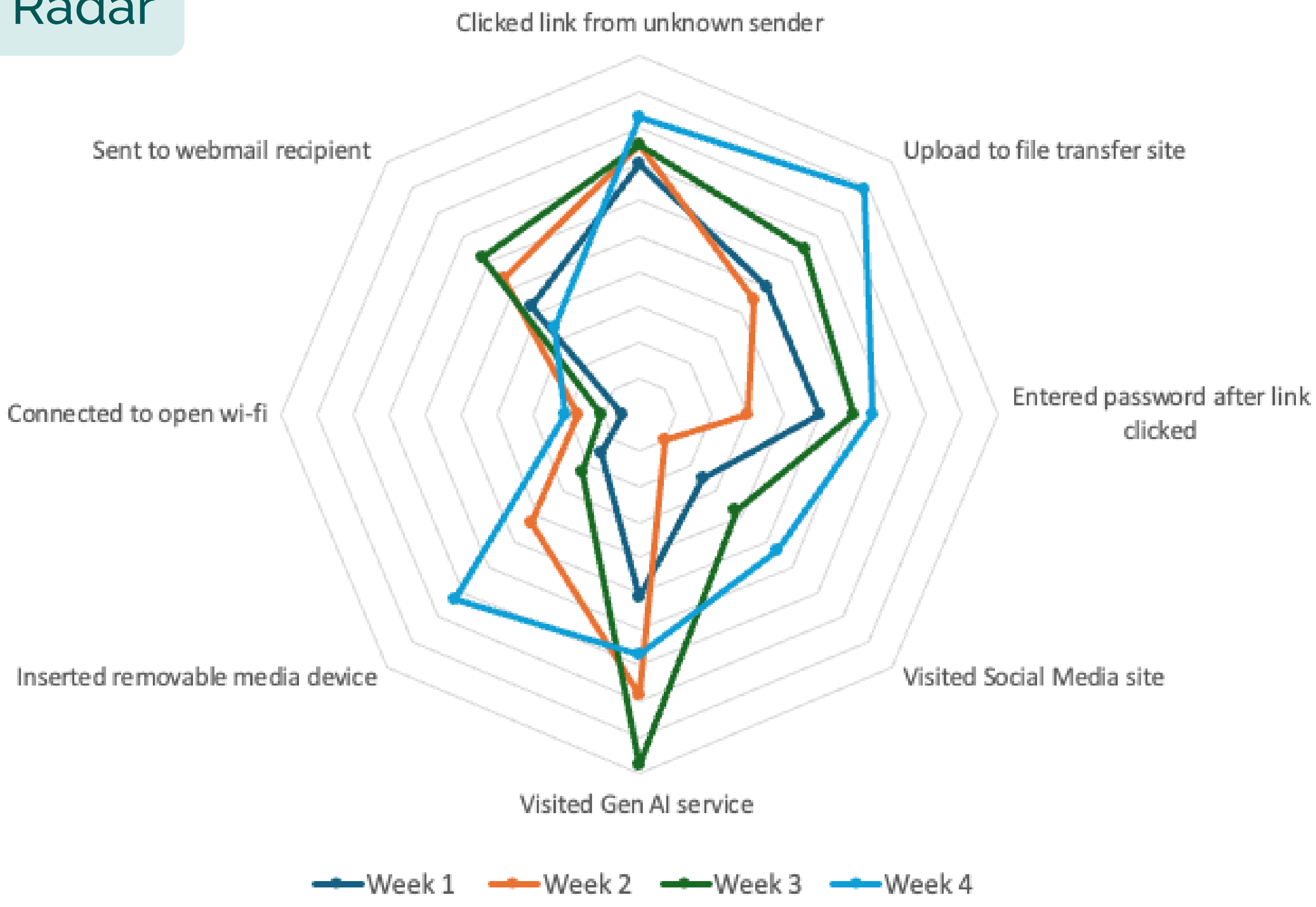
Familiarity bias

Conformity bias

Priming bias

Understand risk… and do something about it

Risk Radar



> *"This helps me to target security awareness programmes to the real risks, and elevates my reporting."*

Redflags®

Real operational Risk Reduction

Real impact

44.0% Phishing sims clicks down

72.3% Unknown sender clicks down

68.0% Security reporting increase

59.4% Browser upload down

63.4% Screens left unlocked down

57.8% Credential sharing down

20.9 million interventions

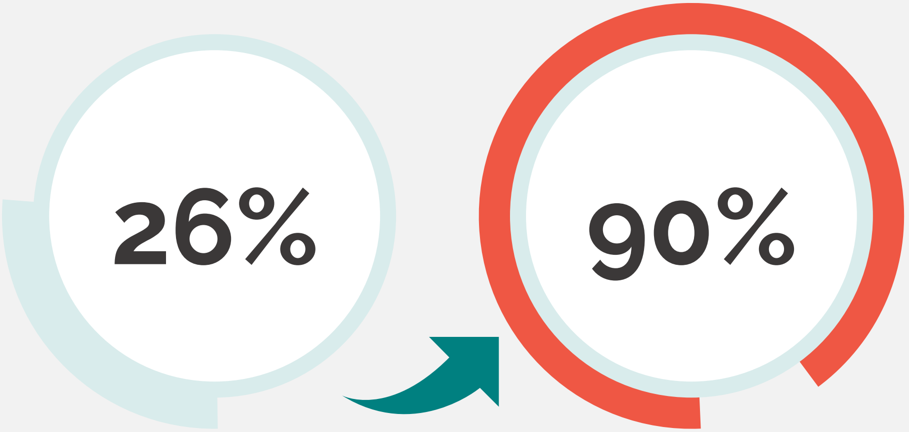
Even if only 0.1% could have been an incident = 1745 incidents avoided

Redflags®

Happy staff

- 92% of staff see training snippets as useful
- 96% see content as relevant
- 89% are learning more.

Compliance goals met



Total Engagement across 4 years

Total monthly engagement

Focus on key learning points

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

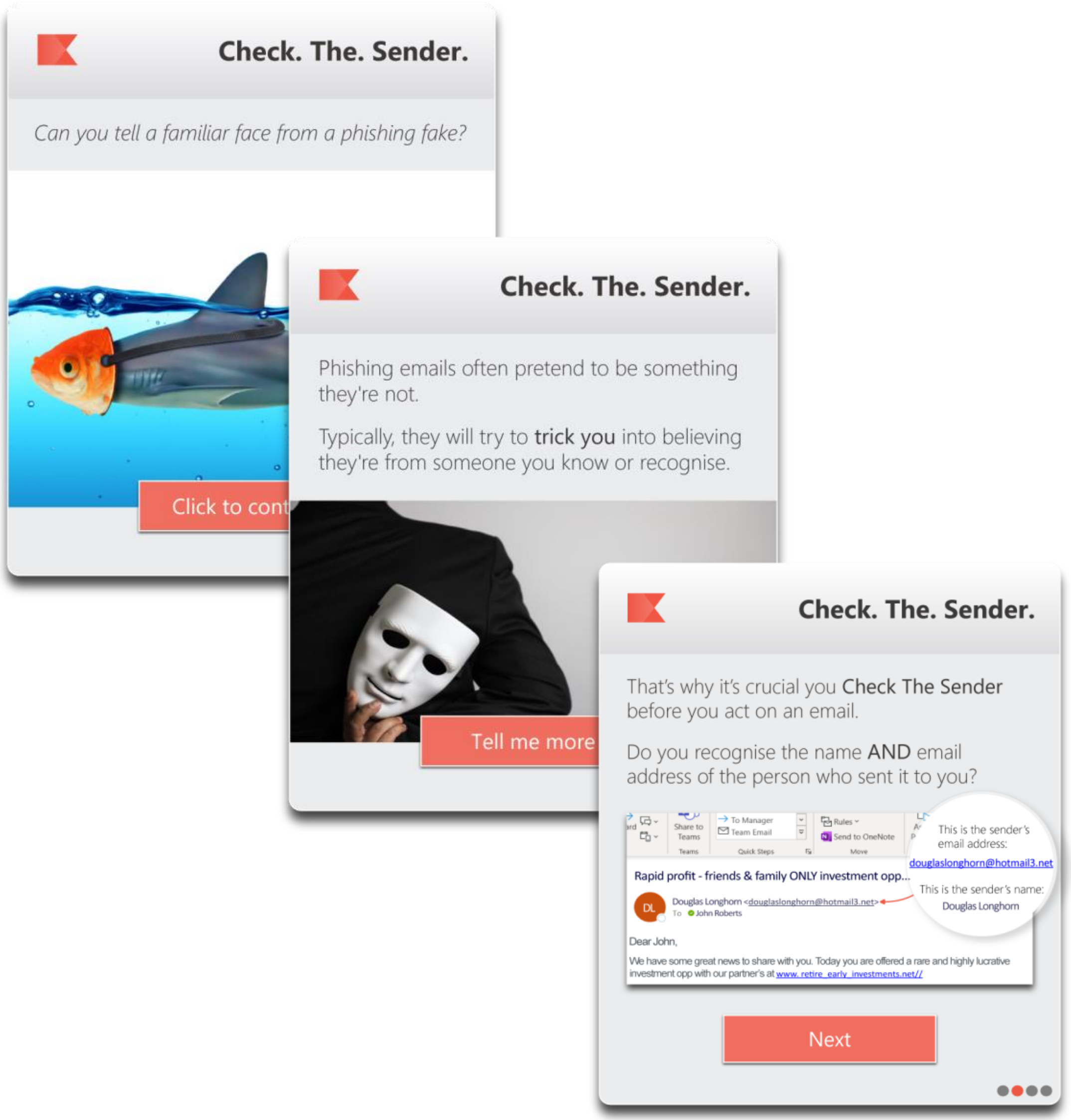
Desktop ‘overlay’ format

Low friction but conspicuous.
Engaging paged content including Q&A

Engagement tracking

Measurement of dwell time and click-through statistics

Ease, timeliness, salience, availability



Check. The. Sender.

Can you tell a familiar face from a phishing fake?

Check. The. Sender.

Phishing emails often pretend to be something they're not.

Typically, they will try to **trick you** into believing they're from someone you know or recognise.

Check. The. Sender.

That's why it's crucial you Check The Sender before you act on an email.

Do you recognise the name **AND** email address of the person who sent it to you?

Rapid profit - friends & family ONLY investment opp...

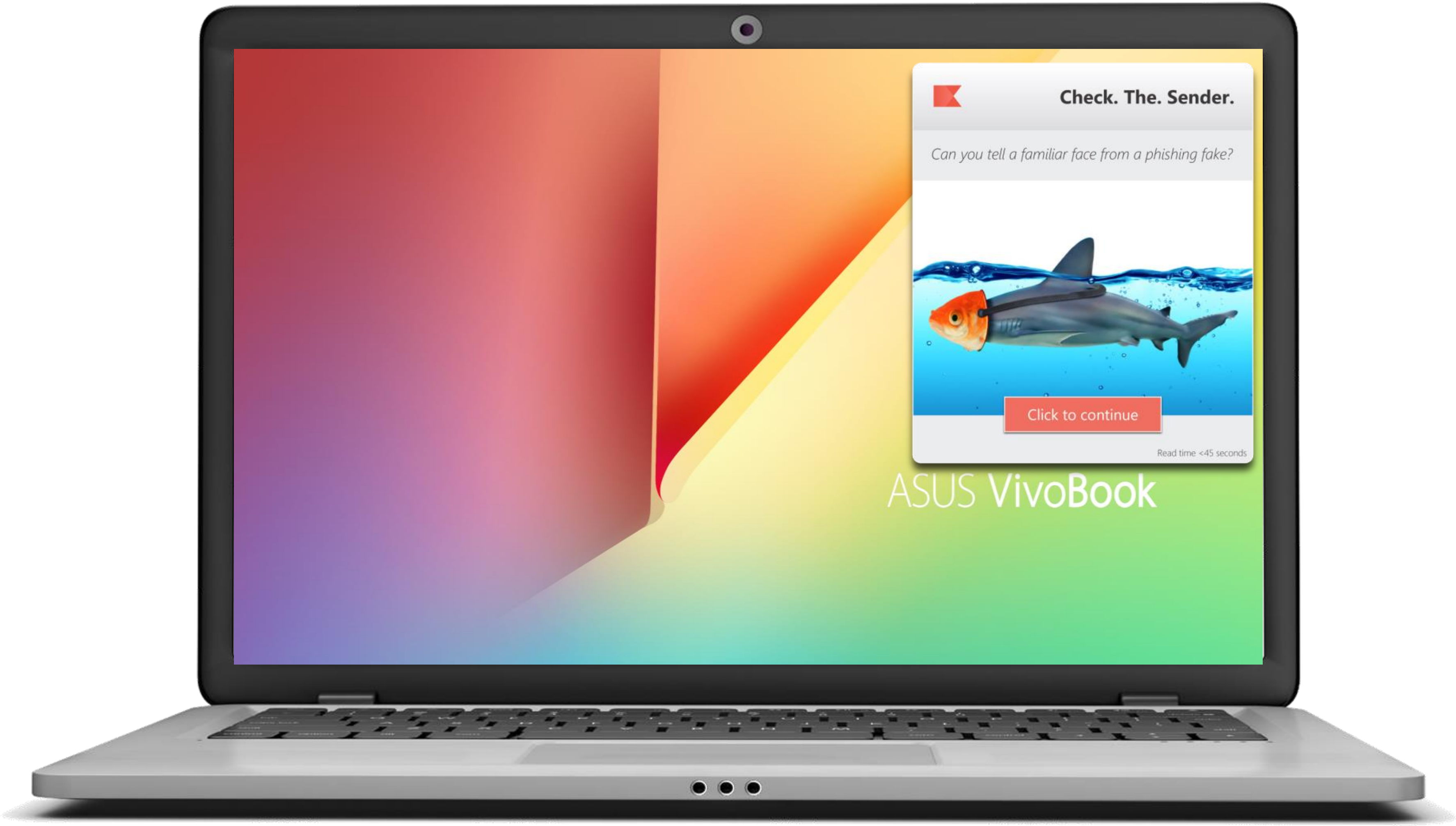
Douglas Longhorn <douglaslonghorn@hotmail3.net>
To John Roberts

This is the sender's email address:
douglaslonghorn@hotmail3.net

This is the sender's name:
Douglas Longhorn

Dear John,

We have some great news to share with you. Today you are offered a rare and highly lucrative investment opp with our partner's at www. retire_early_investments.net//



Check. The. Sender.

Can you tell a familiar face from a phishing fake?

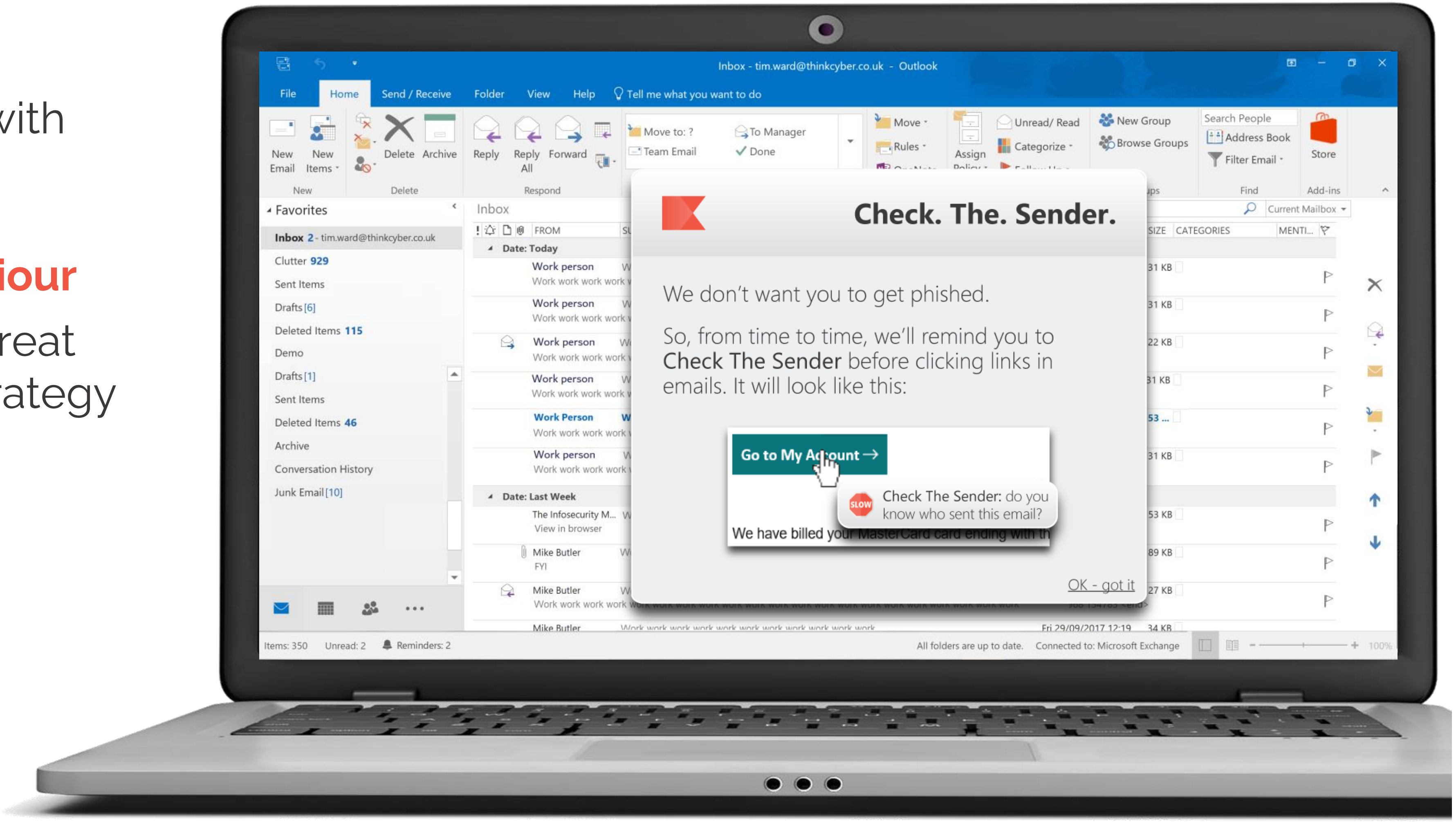
Delivered in context

Reminder when interact with email

Promotes desired behaviour

Reminds people of the threat
Offers a simple coping strategy

Timely, salient, priming



Check. The. Sender.

We don't want you to get phished.

So, from time to time, we'll remind you to **Check The Sender** before clicking links in emails. It will look like this:

Check The Sender: do you know who sent this email?

We have billed your MasterCard card ending with th

OK - got it

Delivered in context

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

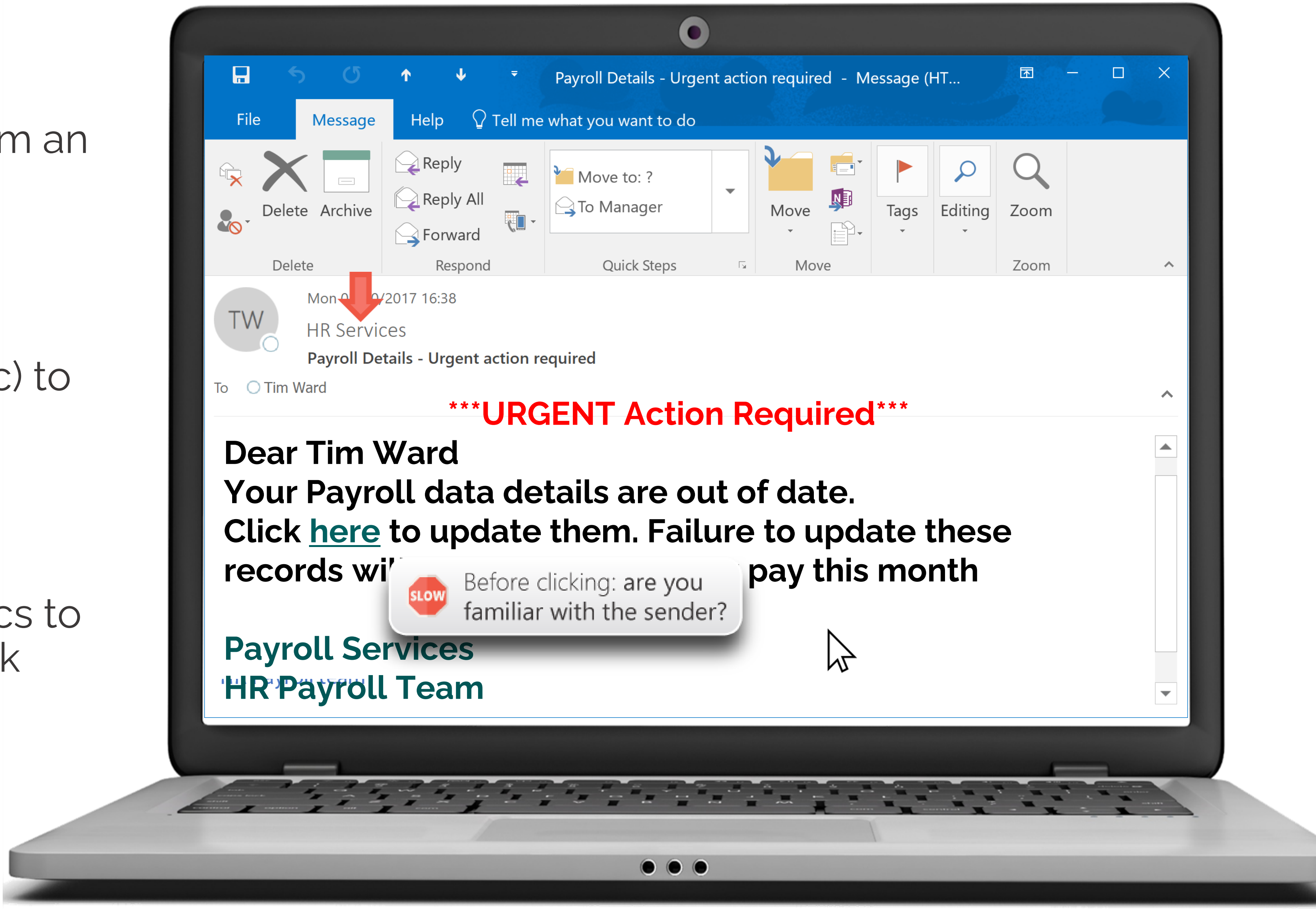
Promotes desired behaviour

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”



Mon 0 0/2017 16:38

HR Services

Payroll Details - Urgent action required

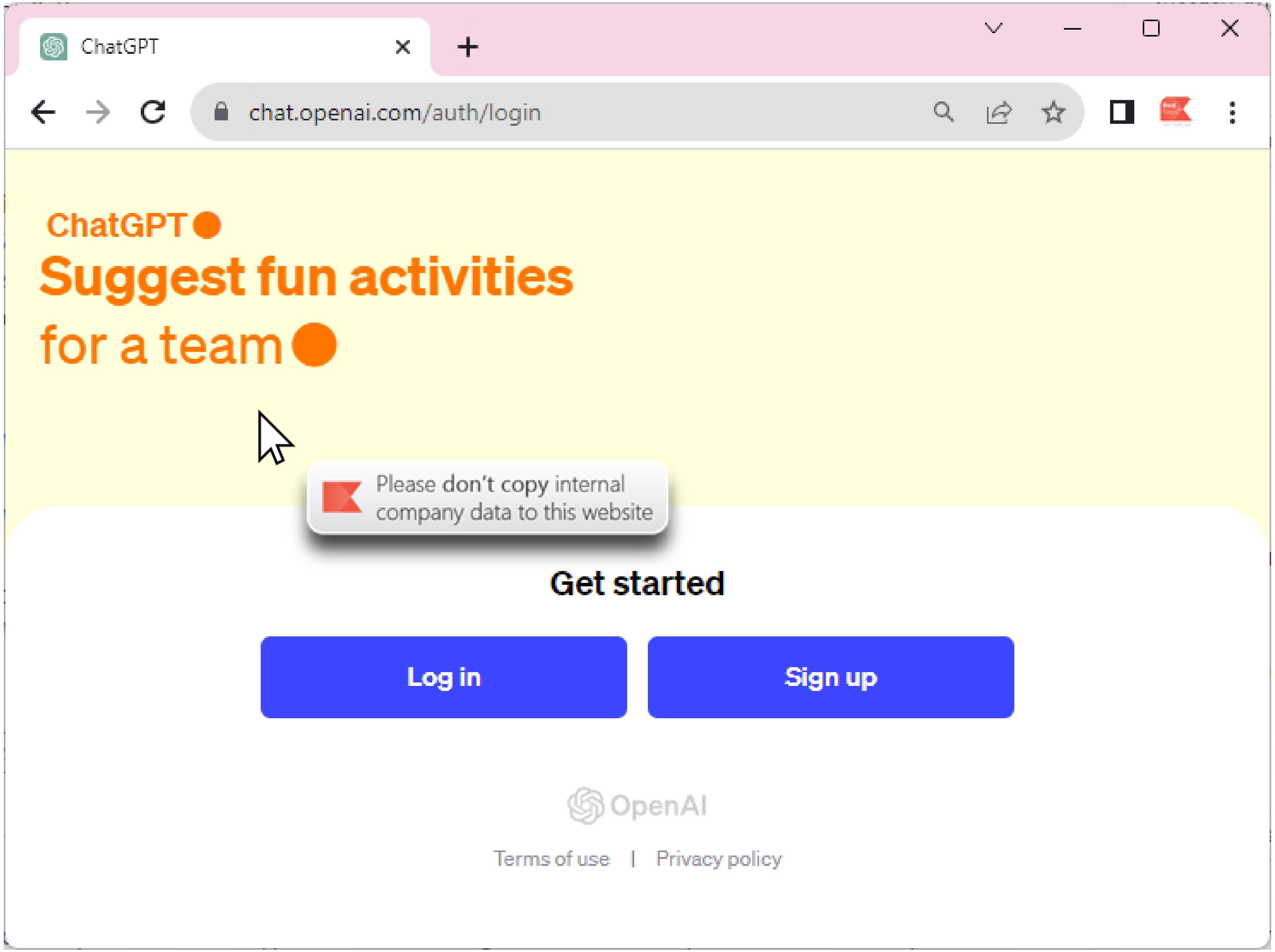
To Tim Ward

URGENT Action Required

Dear Tim Ward
Your Payroll data details are out of date.
Click here to update them. Failure to update these records wi pay this month

Before clicking: are you familiar with the sender?

Payroll Services
HR Payroll Team

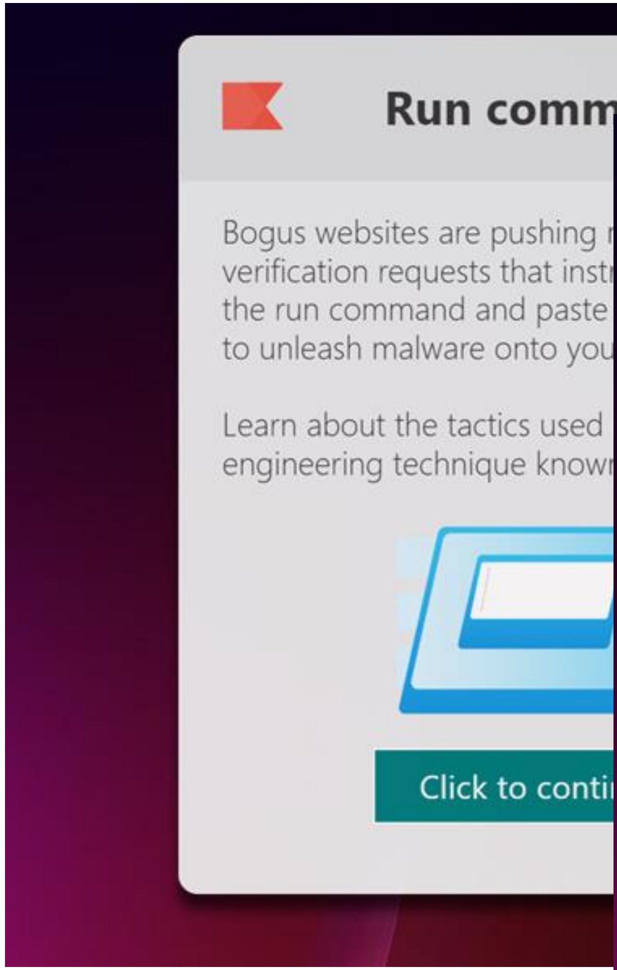


ChatGPT ●

Suggest fun activities for a team ●

Please don't copy internal company data to this website

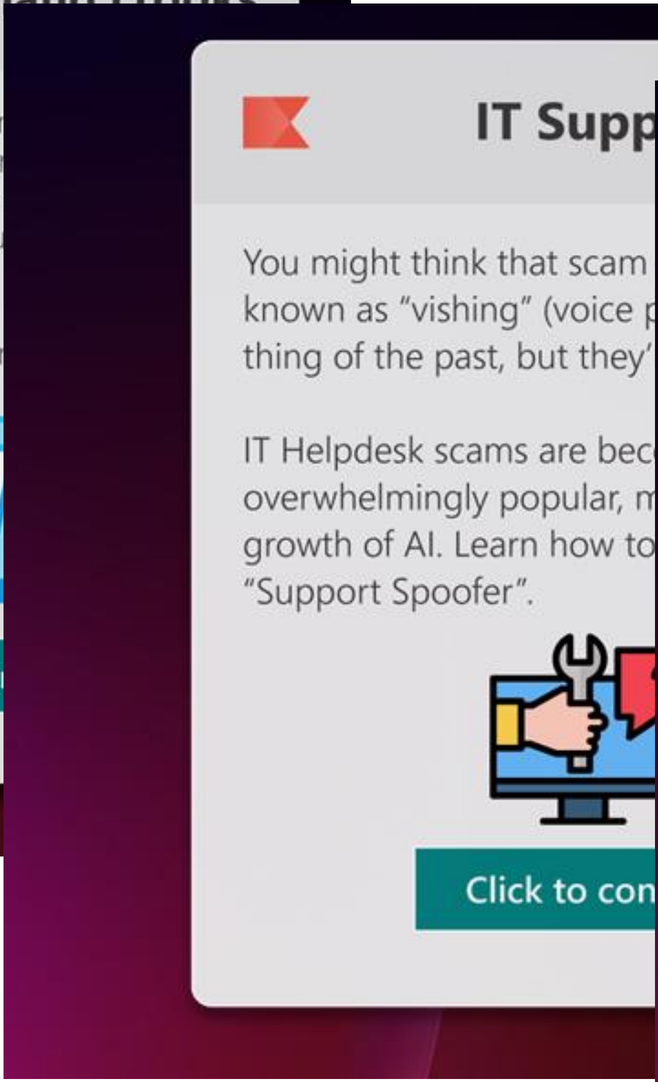
Get started



Run command crooks

Bogus websites are pushing r
verification requests that instr
the run command and paste
to unleash malware onto you

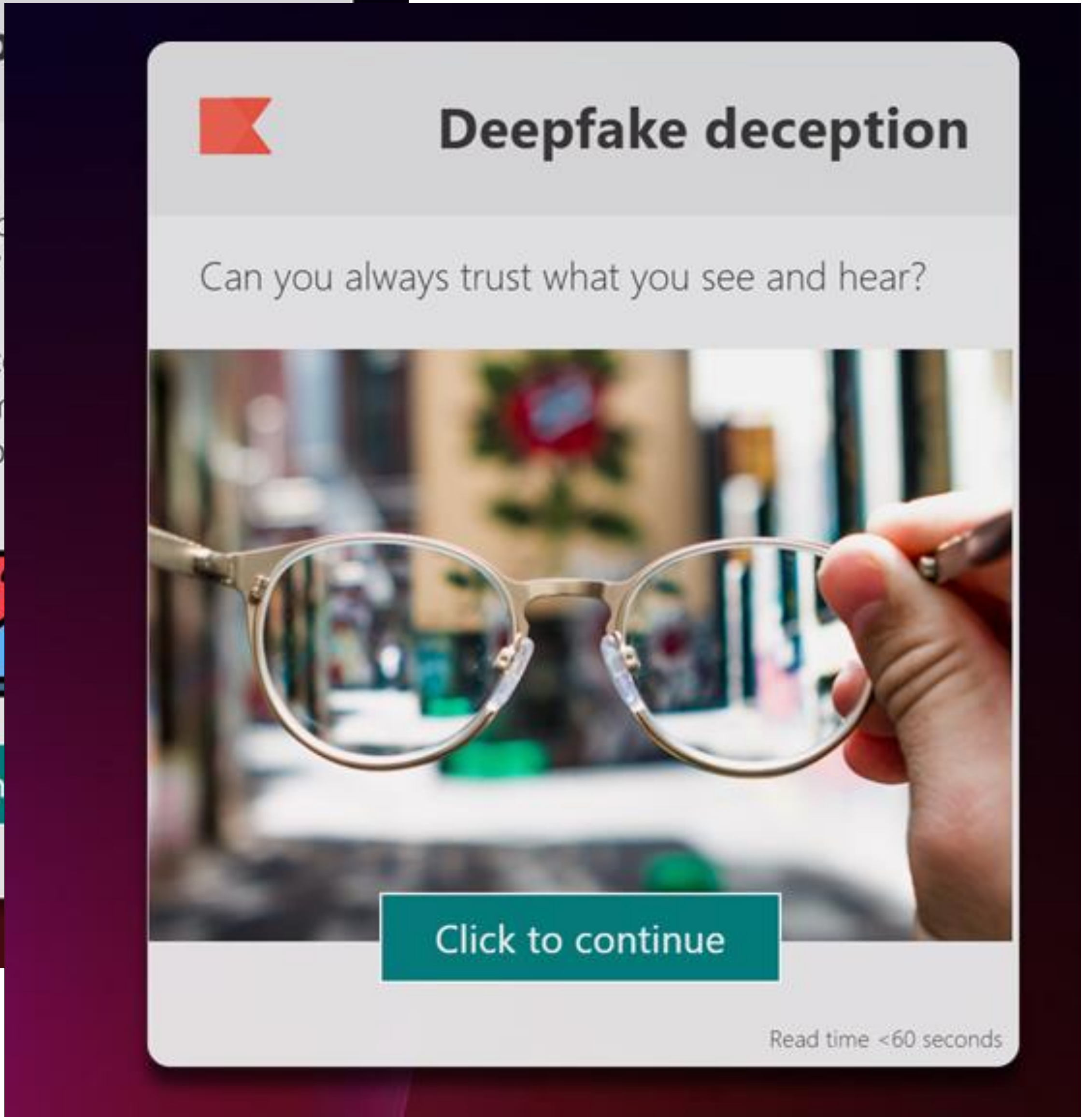
Learn about the tactics used
engineering technique know



IT Supp

You might think that scam
known as "vishing" (voice p
thing of the past, but they'

IT Helpdesk scams are bec
overwhelmingly popular, m
growth of AI. Learn how to
"Support Spoofer".



Deepfake deception

Can you always trust what you see and hear?

Read time <60 seconds

CISO worry list - revisited

Reduce operational / business risk

Proactive interventions at points of risk.
Measurable changes in staff risky behaviours.

Meet regulatory and compliance obligations

High measures of engagement, ongoing education, evidence of impact and evolution.

Embed practices in daily workflows with low friction

Build organisational resilience

Empowering nudges embed secure behaviours

Keep security front of mind

Intelligent interventions, when and where it matters

Protect against emerging threats

Proactive real time nudges allow rapid comms as well as nudging on new threats

Measure impact and ROI

Clear metrics with visible cause and effect

Baseline, impact, trends and outliers.

Maintain exec / Board confidence

Translate risk into actionable insights – and act on them!

Visible interventions, convincing data

People centric security is possible

Through a behaviour led approach

- Focusing on
  - Speed to measurable behaviour change
  - Effectiveness of interventions
  - Minimal deployment friction
  - Provable reduction in high-risk behaviours
- How?
  - Moving on from elearning, phishing sims and compliance "performance"
  - Tying intervention to real behaviours - immediately
  - Applicable to organisations of any size
- A security copilot, for your staff, and your security team

"I just got the ChatGPT Nudge.

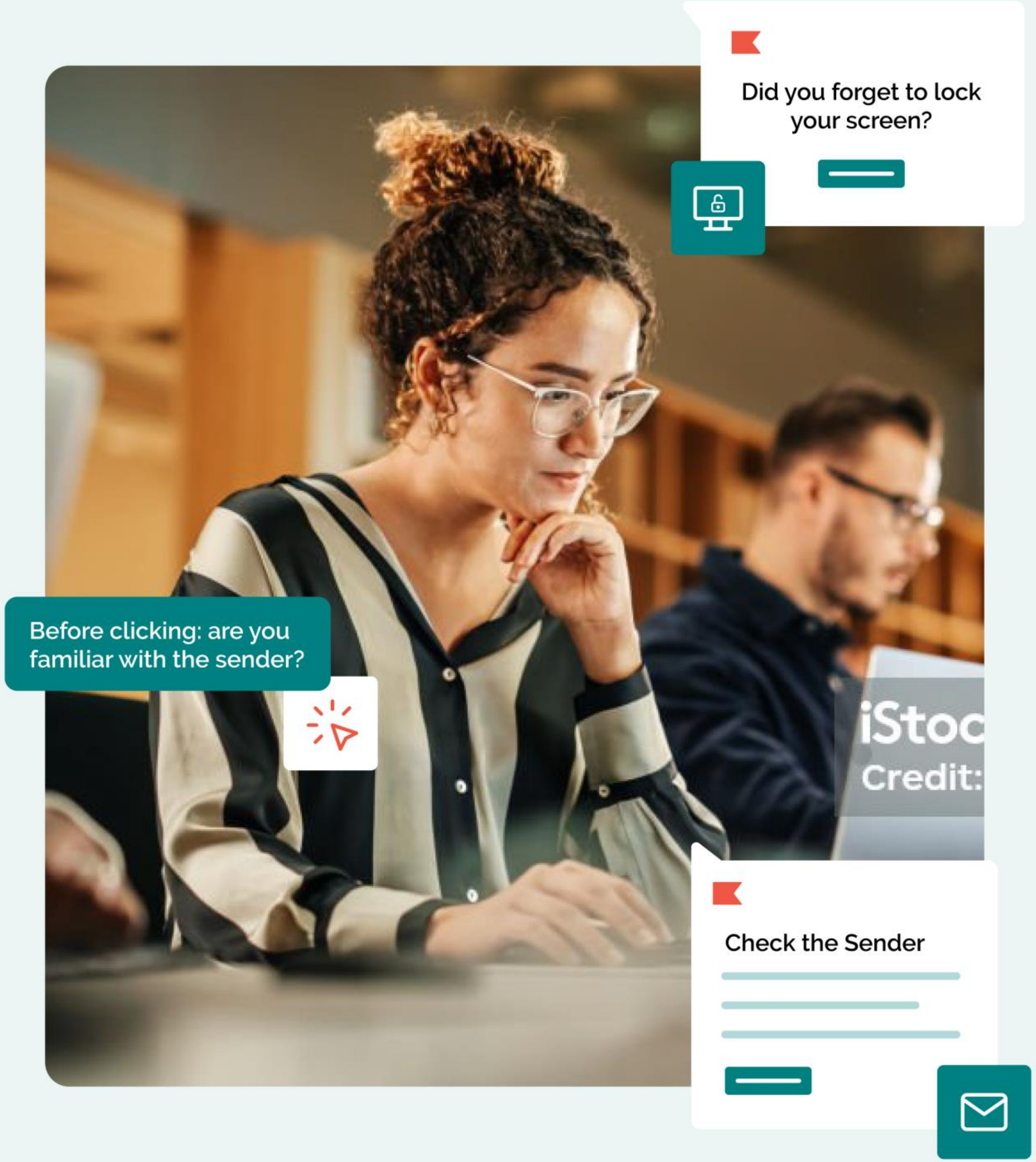
It feels like I have an angel on my shoulder"

Redflags®

Redflags®

Thank you!

To find out more visit reflags.io


Did you forget to lock your screen?
Before clicking: are you familiar with the sender?
iStoc
Credit:
Check the Sender

Tea, coffee & networking break

We’ll be back at 12.15pm

Please scan here to give us your feedback on today’s event

Understand Europe's Evolving Cybersecurity Threat Landscape

Burak Agca

Sr. Regional Sales Engineer, CrowdStrike

The behavioural and cognitive overlap between modern cyber attackers and recreational gamers

John Madelin

President, Ethical Hacking Incubator, The Hacking Games

sasig

Networking lunch

We’ll be back at 2pm

Please scan here to give us your feedback on today’s event

From Disgruntled to Defected:
Strategies in Dealing With Modern Insider Threats

Findlay Whitelaw
Cybersecurity Strategist and Researcher, Exabeam

Panel session: Managing the threat landscape in a world of political turmoil

Facilitator

Martin Smith MBE Chairman and Founder, The SASIG

Panellists

Karoliina Ainge Associate Director, Independent Diplomat
Melanie Garson Associate Professor in International Security, University College London (UCL)
Ivan Milenkovic VP Cyber Technology Risk, Qualys

End of meeting

Get home safely

Please scan here to give us your feedback on today's event