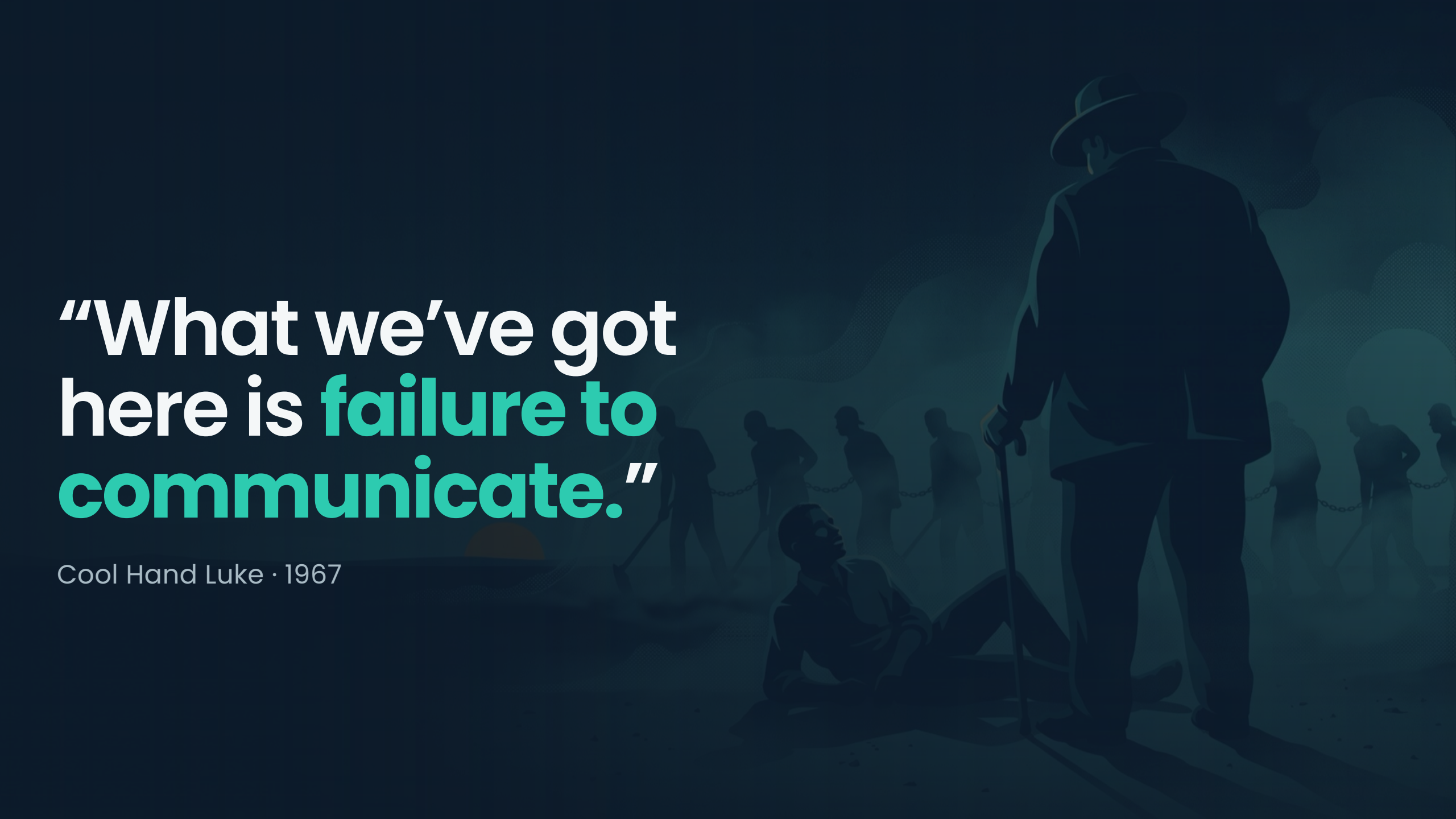

“What we’ve got here is failure to communicate.”
Cool Hand Luke · 1967

SAINTCON 2026 · CURIOUS AND SECURE

What social engineers know about you that your security team doesn't.

Sixteen years on the attacker's side. The most useful thing it taught me isn't how to attack people — it's how not to train them.

Lee Anderson Get curious. Stay secure.

THE DESIGN FLAW

The social engineer studied your users more carefully than your awareness program did.

Awareness training

Urgency. Authority. Fear. Deadlines, consequences, “from IT Security.”

Meant to switch skepticism **on**.

Social engineering

Urgency. Authority. Fear. Deadlines, consequences, “from IT Security.”

Engineered to switch skepticism **off**.

WHAT ATTACKERS ACTUALLY EXPLOIT

Social engineers don’t find vulnerabilities in systems. They engineer states in people.

A vulnerability is patched once. A state can be produced on demand, in anyone, with a sentence.

URGENCY · SCARCITY · DEADLINES

43%

of phishing emails lean on **scarcity** — a deadline, a limited window, act now.

5%

of legitimate email does.

Pan et al. 2026 · 340,912 emails · *Expert Systems with Applications*

Scarcity and a **sensitive request** — credentials, payment, personal data — were the two strongest independent predictors of phishing in the corpus.

WHEN THE ATTACKER IS A PERSON

A call, a lobby, a pretext — the dominant exploit is helpfulness.

Email runs on urgency and authority. In person, the attacker shows up as the answer to a problem you already have.

From the field, not the literature.



FOUR MECHANISMS

Urgency **Authority** **Emotion** **Helpfulness**

Every one of them is a state, not a skill gap.

Which is why a rule about URLs doesn't reach the person who is scared, deferring, or relieved.

THE ADMINISTRATION PROBLEM

802

reboots. The residents saw through it every time. He reset the people instead of fixing the design.

The Good Place · “Dance Dance Resolution”



THREE STUDIES · THREE DESIGNS · ONE ANSWER

The training didn't change the clicking.

15 mo

14,733 employees. People shown a training page after clicking became repeat clickers **more** often.

ETH Zurich · Lain, Kostiainen & Čapkun · IEEE S&P 2022

19,500

employees, 8 months. Recent annual training had **no significant effect**.

UC San Diego Health · Ho et al. · IEEE S&P 2025

9.8 → 10.5

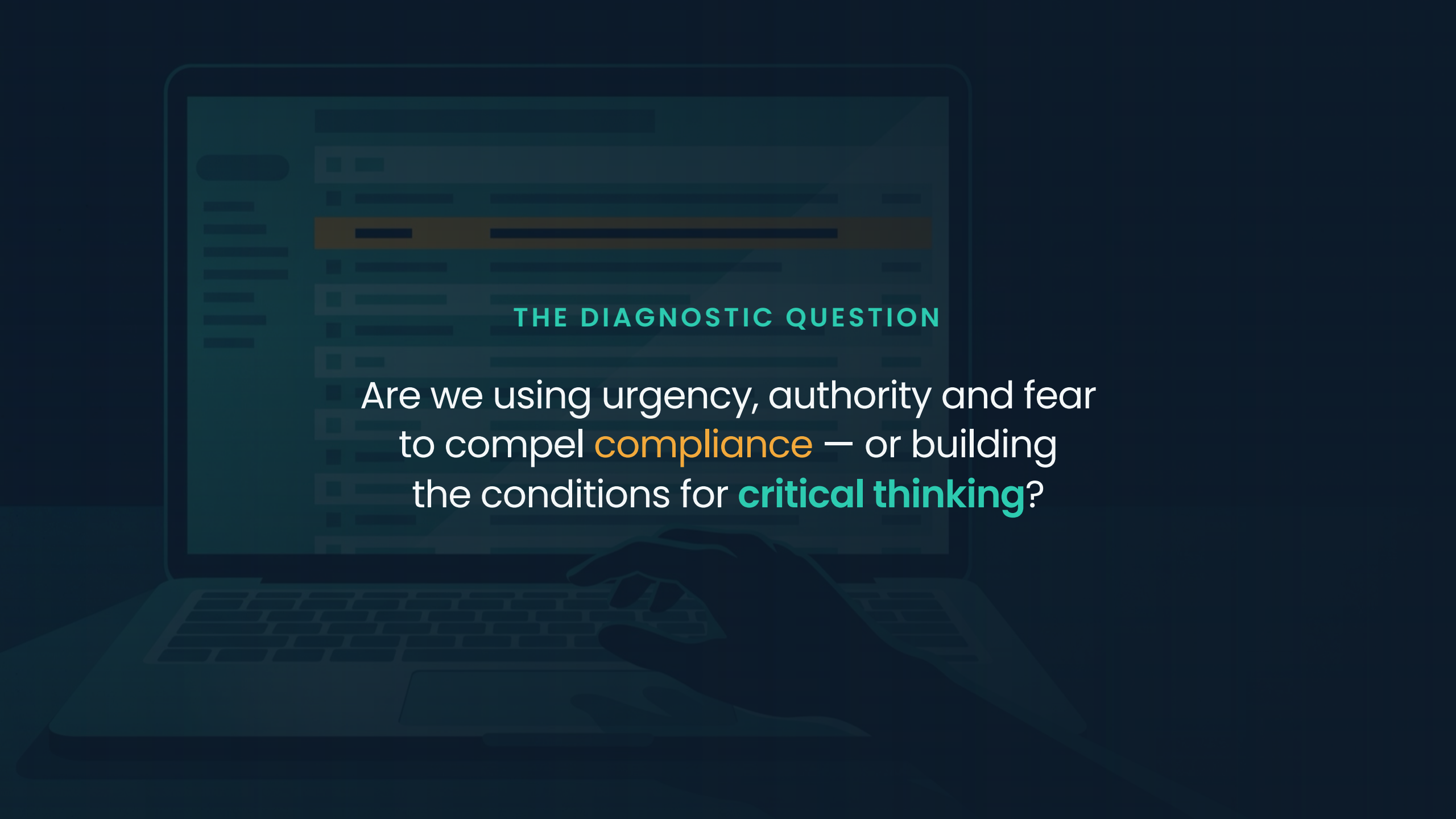
Randomized trial, **12,511** employees. Untrained clicked 9.8%; trained clicked 10.5%. **No significant difference.**

US fintech · arXiv 2506.19899 · 2025 preprint

In the same ETH Zurich study, one thing did work:

A warning banner cut clicks from 3,964 to about 1,400.

A banner did what fifteen months of training couldn't.


THE DIAGNOSTIC QUESTION
Are we using urgency, authority and fear to compel compliance — or building the conditions for critical thinking?

WHAT ACTUALLY INTERRUPTS THE PATTERN

Reactive

The itch to click and resolve an unknown. What attackers exploit. Fast, automatic, feels like *doing something*.

Reflective

The deliberate pause that asks **“does this make sense?”** Same faculty, opposite direction. Trainable.

Jensen et al. 2017 · *JMIS* · n=355: mindfulness training beat rule-based training on a simulated phish.

ETH Zurich’s banner was friction at the moment of decision. Reflective curiosity is that banner, carried with you.

IN PRACTICE

Two questions that interrupt the automatic response.

1 **Does this fit my life?**

2 **Who wants me to hurry?**

Plus permission to be slow — and a report channel that is **safe**, because psychological safety to report is the organizational half of reflective curiosity.

ATTACKER-LENS THINKING · TAKE THIS HOME

Three questions for any awareness campaign.

1. Which cognitive state is this training designed to produce?
2. Does that state feed urgency, authority, emotion and helpfulness — or build **reflective curiosity**?
3. What would a malicious social engineer think of this training?

ONE THING TO CHANGE WHEN YOU GET BACK

“What we’ve got here is failure to communicate.”

— the Captain said it first.

Run your next campaign through the three questions. Rewrite the one message that fails.



Curious & Secure

Get curious. Stay secure.

Lee Anderson

lee@curiousandsecure.com

Instagram & YouTube: @curiousandsecure

X: @curiousnsecure

Facebook: Curious and Secure

linkedin.com/in/leeanderson

BRING THIS TO YOUR TEAM

Hack Attack: Defense team sessions

curiousandsecure.com/for-corporations