THE CYBER ESCAPE ROOM CO.

CTRL+VISH

CLIENT EVENT · ONE DAY · FOUR PHONE BOXES

PHONE BOX *RESULTS*

104 vishing scenarios played on the day. 84% of attendees held firm all the way.



THE CYBER ESCAPE ROOM CO.

THE DAY IN *NUMBERS*

120

calls to the phone box line

104

full scam scenarios played

8 HRS

of talk time, about 4½ minutes a call

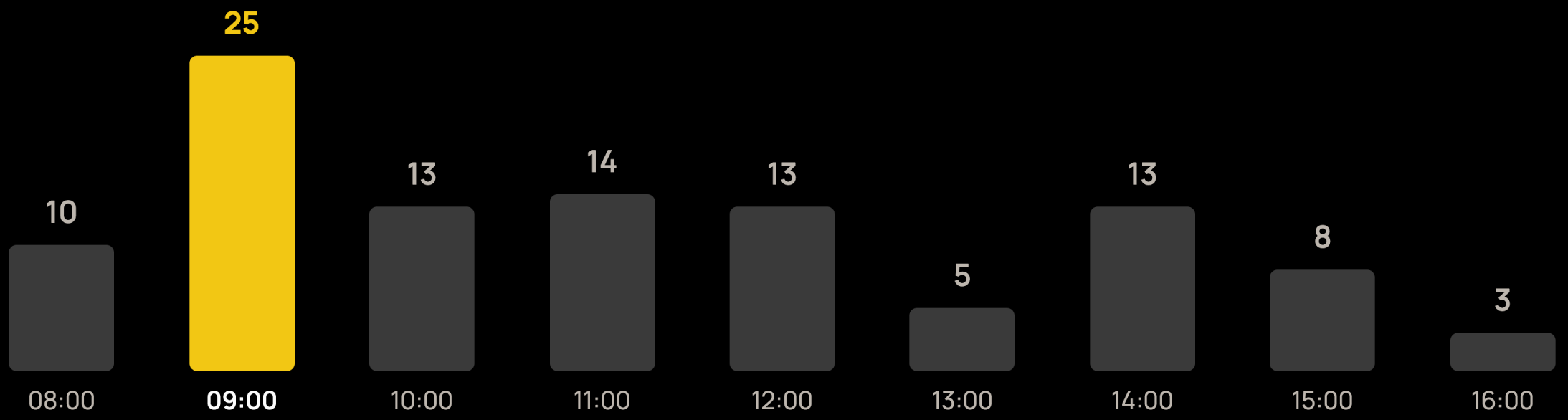
7:23

the longest call, in minutes and seconds

Scenarios ran from 08:33 to 16:30. The other 16 calls were hang-ups, walk-ups who weren't there for the demo, one misdial and one person called away to work.

THE CYBER ESCAPE ROOM CO.

THE 09:00 HOUR WAS THE RUSH: *25 CALLS*



Completed calls by the hour they started, 104 in total

THE CYBER ESCAPE ROOM CO.

THREE *SCAMS* TO CHOOSE FROM

IT SCAM

43%

"Laura from IT" needs your login for a network check or an urgent security update.

HR FRAUD

39%

"Olivia from HR" is updating records and wants your date of birth, NI number, employee ID or bank details.

CEO IMPERSONATION

18%

The boss needs an urgent £25,000 transfer, or system access for a consultant, today.

Attendees picked the scam and the goal. Three came back for a second scenario.

THE CYBER ESCAPE ROOM CO.

84% HELD FIRM ALL THE WAY



84%

HELD FIRM

Gave nothing away and challenged the caller.

11%

GAVE A LITTLE, THEN STOPPED

Usually name and date of birth to "HR", or a username to "IT", before refusing the NI number or password.

5%

HANDED OVER THE TARGET

Login details, bank details, a transfer agreed, revenue figures, personal data.

THE CYBER ESCAPE ROOM CO.

THE *RED FLAGS* THEY SPOTTED

- **Urgency and pressure** to act right now
- **IT asking for a password**, which real IT never needs
- **HR asking for details it should already hold**
- **No named manager or call-back number** to check against
- **A request outside normal channels**, like a payment by phone

THE CYBER ESCAPE ROOM CO.

MOMENTS FROM THE DAY

THE EXPERT

On the longest call, an attendee argued that updates in a company that size run through service accounts, so nobody needs a personal login.

PLAYING THE SCAMMER BACK

One attendee spotted the scam in their second scenario and fed the caller made-up details.

MONEY THROUGH HR

One attendee agreed to send money to "HR", then realised in the debrief that HR doesn't handle payments.

THE SETUP WAS THE SCAM

One attendee shared their extension and email, thinking it was still the setup. The friendly opening is already part of the attack.

WHAT IT TELLS *US*

STRONG ON THE BIG ASKS

Most people refused passwords and urgent payments outright.

WEAK ON SMALL DETAILS

Name, date of birth and usernames went to callers who sounded like internal teams, especially HR.

WHERE TO FOCUS NEXT

Training on HR-style data requests, and one habit: verify with someone you already know.