FalconryAware

PART OF FALCONRYTRUST

FALCONRYAWARE · PROGRAMME OVERVIEW

People who spot it, report it and stop it.

FalconryAware: the complete security awareness and phishing simulation programme within FalconryTrust, run on Falconry360.

Trust at the speed of transformation

falconrytrust.com · contact@falconry360.com

WHY MOST PROGRAMMES STALL

Completion rates tell you people clicked through a module. Nothing more.

FalconryAware is built the other way round: a year-long programme, a behaviour measure that moves, and results that land in the same record as every other risk.

The four reasons

- **Annual and generic.** One course for everyone, forgotten by the second month.
- **Measured on attendance.** Completion tells the Board nothing about exposure.
- **Disconnected from risk.** Results sit in a training tool, not the risk register.
- **Built on blame.** Naming people who click teaches them to hide mistakes.

PROGRAMME

Twelve months, eight role paths, Arabic and English

MEASURED BY

Report rate, click rate, human-risk score and culture

RUN AS

Client-led, co-managed or fully managed

CONNECTED TO

Risk register, control evidence and Board report

ONE ILLUSTRATIVE PROGRAMME YEAR

23% → 61%

Phishing report rate

18% → 7%

Click rate

58 → 72

Human-risk score

THE PROGRAMME IN ACTION

A year that is planned, delivered and measured.

THE TWELVE-MONTH CALENDAR

JAN
Phishing basics
Baseline simulation and culture pulse

FEB
Passwords and MFA
MFA-fatigue scenario for admins

MAR
Social engineering
Voice-phishing drill for customer teams

APR
Handling data
Data-handling module and attestation

MAY
Working remotely
QR-code lure

JUN
Using AI safely
AI acceptable-use attestation

JUL
Travel and devices
Lost-device and public Wi-Fi guidance

AUG
Invoice fraud
Payment-diversion scenario for finance

SEP
Insider risk
Manager briefing pack

OCT
Awareness month
Organisation-wide campaign and leadership message

NOV
Privacy at work
Privacy refresher and HR-themed simulation

DEC
Seasonal scams
Delivery and gift-card lures, year-end Board report

EIGHT ROLE PATHS

All staff
The monthly theme, three to seven minutes at a time, and how to report a suspicious message in one click.

Executives and Board
Targeted attacks on leaders, deepfake voice and video, decision fraud and what the Board should ask about human risk.

Finance and payments
Invoice and payment-diversion fraud, supplier bank-detail changes and call-back controls that hold under pressure.

HR and people
Fake candidates, payroll diversion, handling personal data and running the programme fairly.

IT and privileged administrators
Help-desk impersonation, MFA fatigue, privileged credential handling and admin-console lures.

Developers
Secrets in code, poisoned packages, repository access and safe use of AI coding assistants.

Customer-facing teams
Voice phishing, SIM-swap and account-takeover pretexts, and verifying a caller without breaking service.

OT and field staff
Removable media, vendor remote access, tailgating and the safety consequences of a single click on site.

Seven steps, one campaign, every result on the record.

1 Plan

A scenario is chosen from the current threat picture and set to the right difficulty for each audience. HR, legal and communications approvals are recorded before anything is sent.

2 Send

Delivery is staggered across working hours so word does not spread, and set up with your mail team so simulations arrive like real mail.

3 The moment

The person sees the message in their inbox. Everything that follows is measured from here.

4 Teachable moment

Anyone who clicks sees a 60-second page showing the red flags they missed. It explains; it does not blame.

5 Report

One click on the report button. Reporters are thanked straight away, and real suspicious messages go to your security team.

6 Measure

Opened, clicked, credentials entered, reported and time to report, by department, role and location.

7 Follow up

Coaching for repeat clickers, a targeted scenario for the riskiest group, confirmed password resets and a brief for every manager.

SIMULATED PHISHING · FOR TRAINING

From HR Team <hr-updates@yourcompany-policies.com> 1

To You

Subject **ACTION REQUIRED: updated leave policy, confirm by 5pm today** 2

Dear colleague,

Following the annual review, the leave and remote-working policy has been updated. All staff must read and acknowledge the new policy by 5pm today. Requests not confirmed may affect your leave balance. 3

Review and acknowledge policy 4

`hr-portal-verify.co/acknowledge`

Sign in with your company email and password to continue. 5

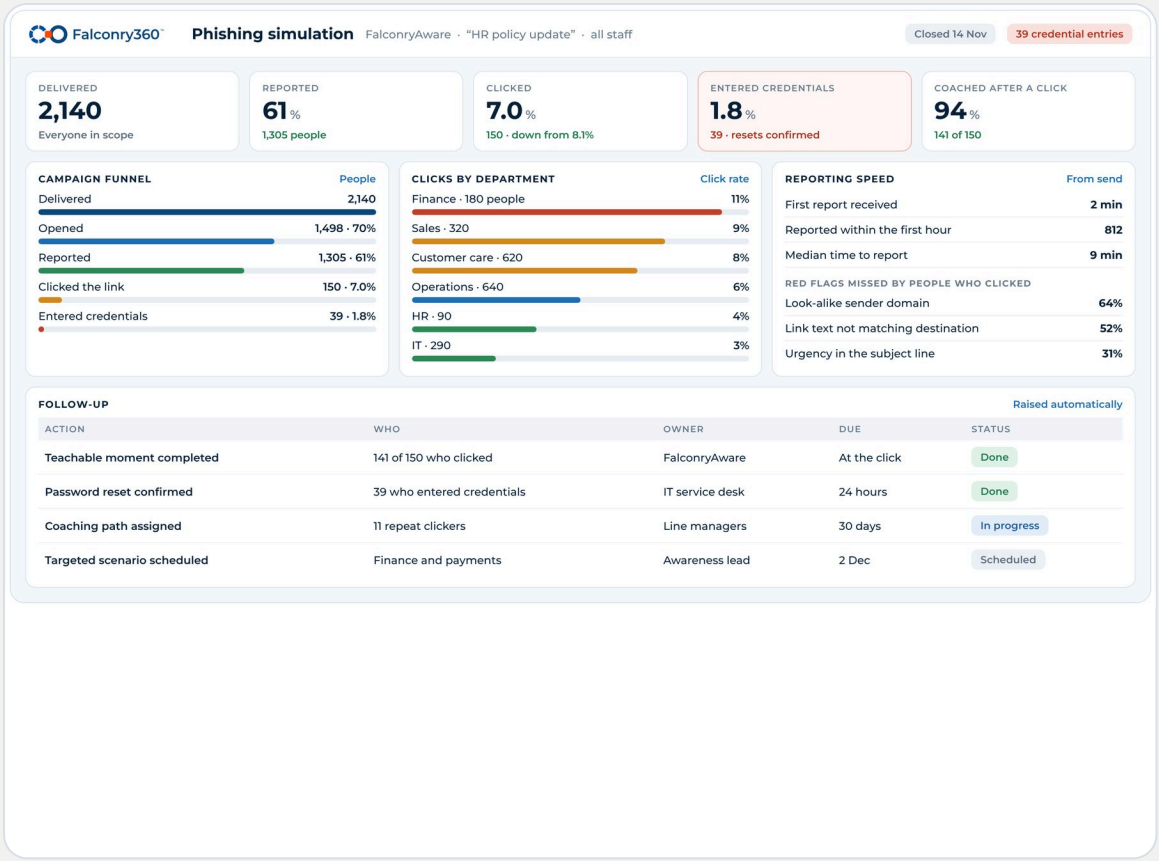
Regards,
Human Resources

THE FIVE RED FLAGS

- **1. Look-alike sender domain** The address reads as HR, but the domain is not yours. It is the flag missed most often.
- **2. Urgency in the subject line** A deadline of today is there to stop you thinking.
- **3. A consequence if you do not act** Threatening your leave balance is pressure, not policy.
- **4. The link goes somewhere else** Hover before you click: the button text and the real destination do not match.
- **5. It asks for your password** Your HR team will never ask you to sign in from an email link.

WHAT GETS MEASURED

One campaign, and the score the Board follows.



HUMAN-RISK SCORE	WEIGHT	MEASURES
Simulation behaviour	35	Clicks and credential entries across recent campaigns, weighted to the most recent.
Reporting behaviour	25	Whether the person reports, and how quickly. A fast report is worth more than a rare click.
Access and privilege	15	Privileged accounts and access to sensitive data raise the stakes of a mistake.
Training currency	15	Role path complete and current for the person's job.
Policy attestation	10	Acceptable use, data handling and AI use acknowledged in the current year.

Starting weights, agreed with you in month one and documented so internal audit can test the method. Higher is better.

FAIR TO YOUR PEOPLE, AND RUN YOUR WAY

Built to be trusted, because it only works if people report mistakes.

Fair to your people

- **No naming and shaming.** No public leaderboards; coaching first.
- **Approved scenarios.** HR, legal and communications approve each campaign.
- **Told, not tricked.** Staff know a programme runs, not when.
- **Privacy by design.** Run to the data protection laws your people are covered by.

CLIENT-LED

Your team runs it

On Falconry360 with the FalconryAware content library and reporting.

CO-MANAGED

We run the campaigns

Your team owns communications, approvals and follow-up.

FULLY MANAGED

We run the programme

End to end, with monthly and quarterly reporting.

Obligations it helps evidence

ISO/IEC 27001:2022 A.6.3 · NCA ECC-2:2024 subdomain 1-10 · SAMA Cyber Security Framework · UAE IA Regulation · UK GDPR accountability · PCI DSS v4.0 12.6 · NYDFS Part 500.14 · HIPAA §164.308(a)(5). Indicative; applicability confirmed during scoping.