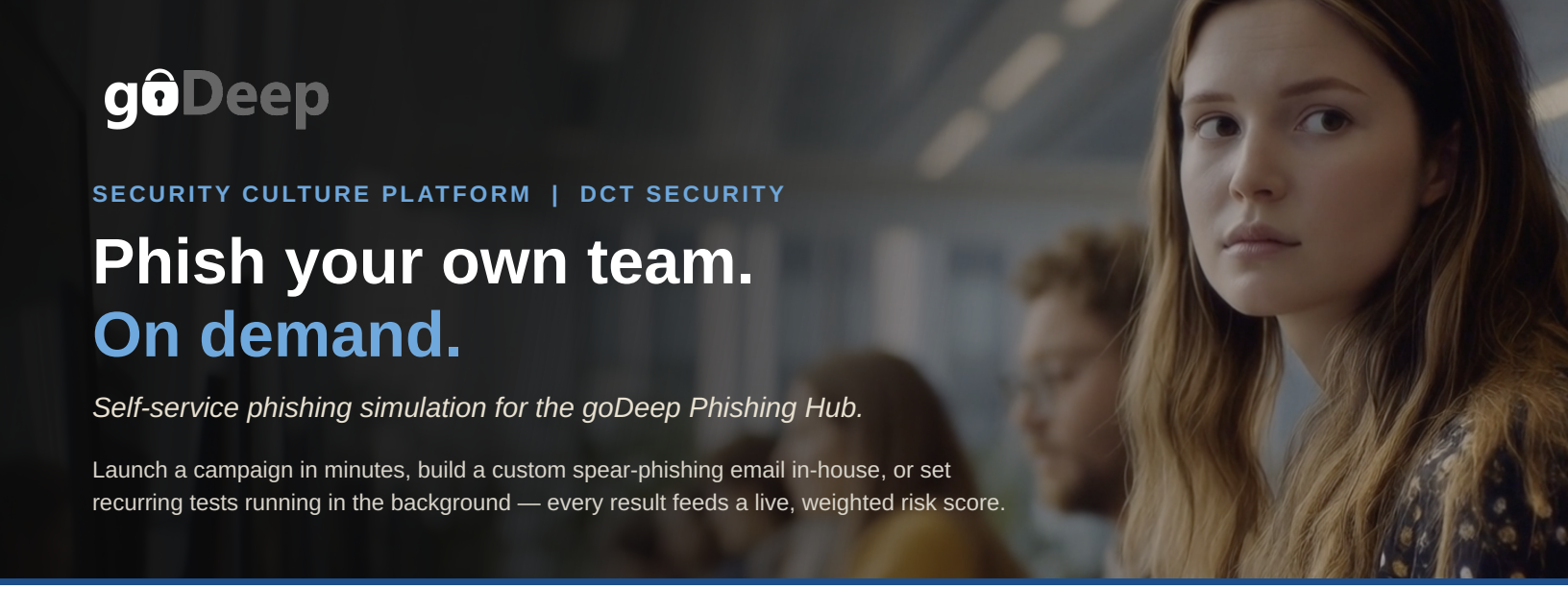


goDeep

SECURITY CULTURE PLATFORM | DCT SECURITY

Phish your own team. On demand.

Self-service phishing simulation for the goDeep Phishing Hub.

Launch a campaign in minutes, build a custom spear-phishing email in-house, or set recurring tests running in the background — every result feeds a live, weighted risk score.

01
Send
Pick a department or individual and fire off a realistic phishing email from the full template library.

02
Craft
Build fully personalised spear-phishing or QR-code emails for specific targets, using your own pretexts.

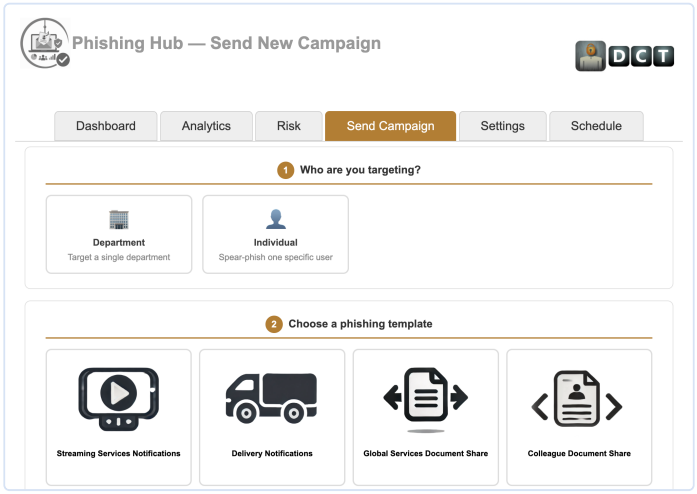
03
Schedule
Set one-off or recurring campaigns and let goDeep quietly test your team in the background.

01 Self-Service Phishing Simulation

A full template library
Choose from pre-built, realistic phishing emails covering the full range of attack types — delivery notifications, streaming service alerts, document shares, invoice fraud and more — sent from a controlled domain, targeted at a department or a single user in a couple of clicks.

Craft your own spear phishing
Go beyond the library and build fully personalised spear-phishing emails for specific individuals, using your own pretexts and detail. QR-code phishing scenarios are supported too.

Set-and-forget scheduling
Run a one-off campaign on a specific date, or set a recurring schedule — daily, weekly or monthly — so tests go out automatically with no ongoing admin effort.



The Phishing Hub — choose your target and template, then send or schedule.

Results you can act on — every campaign

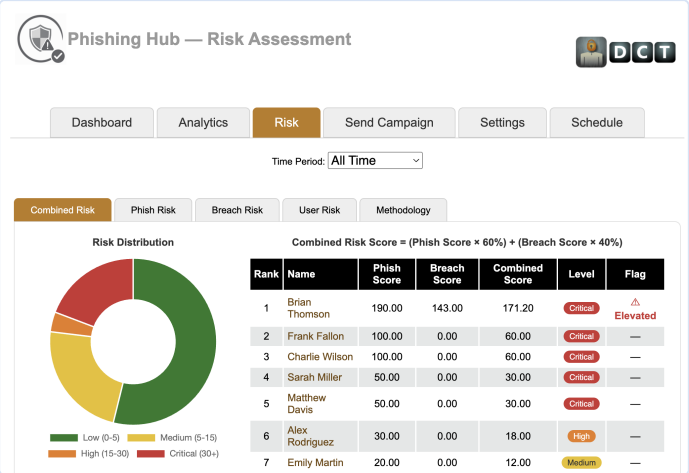
Deep analytics track click-rate trends, department comparisons, repeat clickers and who's improving vs. slipping.

goDeep

02 Risk Calculation

Every phishing response feeds a live, per-user Phish Risk Score — so risk isn't just a click count, it's a weighted, up-to-date measure of behaviour.

- **Scored by action** — clicking a link scores 5; submitting credentials on a fake login page scores 10.
- **Weighted by recency** — the most recent responses carry a 10x multiplier, tapering as they age, so the score reflects current behaviour, not ancient history.
- **Totalled per user** — scores across all responses are summed into a single Total Phish Risk Score, ranked and colour-coded from Low to Critical.

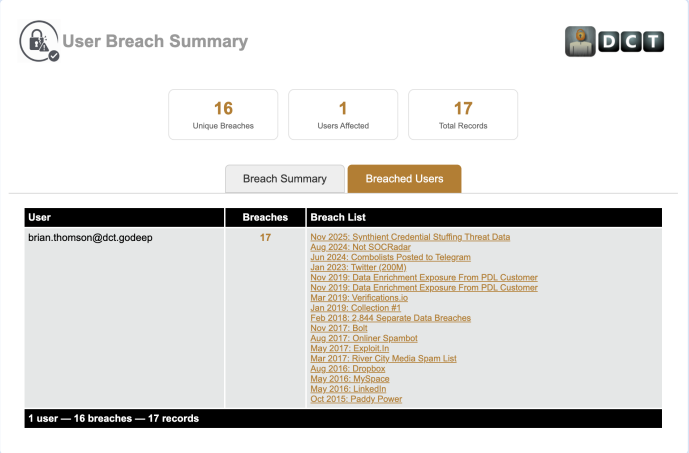


The Risk tab — combined score, distribution and a ranked, flagged user table.

03 The Have I Been Pwned Overlay

Phishing behaviour is only half the picture. goDeep layers in real-world breach intelligence — powered by the Have I Been Pwned (HIBP) database — to show which staff have already had credentials or personal data exposed in known public breaches.

- **Classified by severity** — a breach exposing usernames and passwords, for example, scores as critical.
- **Weighted by recency** — more recently reported breaches carry more weight, tapering as they age.
- **User-level detail** — drill into any breach to see exactly which users were included, and send a targeted breach notification directly from that view.



User Breach Summary — every publicised breach a user's address appears in.

Combined Risk Score = (Phish Score × 0.6) + (Breach Score × 0.4)

One weighted number per user, blending simulated behaviour with real-world exposure — so you always know exactly where to focus first.

ALSO IN THE PHISHING HUB

Controlled sending domain
Every simulation sends from a domain you can safely allow-list, so results are reliable.

QR-code phishing
Simulate QR-based attack scenarios alongside standard email campaigns.

Repeat-clicker tracking
Automatically surfaces users who click more than once within the last month.

Targeted notifications
Send breach or phishing follow-up emails to affected users directly from any results view.

Ready to run your first campaign?

Talk to DCT Security about switching on the Phishing Hub for your organisation. · www.dctsecurity.com

goDeep