



ANCHOR CYBER SECURITY LLC

Phishing Simulation Field Reference

How to design, run, and act on a phishing simulation program — the metrics that matter, industry benchmarks, and the ethical guardrails that keep it a training exercise, not a trap.

\$ phish-sim --why

Why Simulate Phishing at All

Awareness training tells your team what to watch for. A simulation is the only way to find out whether it worked — and phishing remains the most common single way attackers get in.

16%

of all breaches start with phishing — the most common single initial-access vector (Verizon 2025 DBIR)

21 sec

median time for a user to click a phishing link after receiving it (Verizon 2025 DBIR)

28 min

median time for a user to report one instead (Verizon 2025 DBIR)

That gap — seconds to click, minutes to report — is exactly what a simulation program is built to close.

\$ phish-sim --metrics

Metrics That Actually Matter

These three numbers measure different failure points. Collapsing them into one "click rate" headline hides where the actual risk is.

Click Rate

Opened the link. Lowest-severity signal on its own — browsing to a page isn't compromise, but it's the funnel's top of the top.

Credential Submission Rate

Entered real credentials on a simulated login page. The highest-impact failure mode — this is the number that maps to actual account-takeover risk.

Report Rate

Flagged it instead of acting on it. The behavior you're actually trying to build — a workforce that reports is a detection layer, not just a weak point.

\$ phish-sim --benchmarks

Benchmarks — two sources, two different things

Verizon's 2.7% average click rate and KnowBe4's 33.1% baseline "Phish-Prone Percentage" are not the same measurement — different samples, different methodology, different definition of a "fail." Don't average them together or treat one as validating the other. Use each on its own terms.

INDUSTRY	BASELINE PHISH-PRONE %
Hospitality & Education (highest-risk sectors)	~50%+
Healthcare & Pharmaceuticals	41.9%
Insurance	39.2%
Retail & Wholesale	36.5%
Global average, all industries	33.1%
Finance & Banking	29.8%
Technology	28.5%
Same population, after 12 months of ongoing training	4.1%

Per Verizon's separate 2.7% figure: training moves the *report rate* far more than the *click rate* — trained users report at 21% versus 5% for untrained users, but the click-rate improvement is smaller. A simulation program without a training and reporting workflow attached mostly just produces a scary number — it doesn't reduce risk on its own.

\$ phish-sim --program-design

Designing a Program, Not Just a Test

A single campaign tells you one data point. A program — run on a cadence, across pretext types relevant to your actual risk — tells you a trend.

- **Start with a baseline, generic-pretext campaign**
Establishes an honest starting point before anything is tailored — click, submission, and report rate, with no advantage given either way.
- **Move to pretexts relevant to your actual environment**
Invoice fraud, vendor impersonation, or internal IT requests test what your organization would realistically face — not a generic template everyone's seen before.
- **Test credential submission specifically, not just clicks**
A safe, simulated login page isolates the highest-impact failure mode from simple curiosity-clicking.
- **Don't ignore non-email vectors**
QR-code-based lures ("quishing") skip most email security filters entirely, since the payload is an image, not a scannable link — test it separately if your organization uses printed materials or posted codes.
- **Re-test on a fixed cadence, not once and done**
A single snapshot tells you where you stand. A repeated cadence tells you whether training is actually changing behavior.

```
$ phish-sim --ethics
```

Ethical & Legal Guardrails

A phishing simulation is a test of a process, not a trap for individuals. The SANS Institute's own guidance on this is explicit: deceiving employees without care for what you're asking them to react to is its own kind of harm.

Written authorization, always

Documented leadership sign-off on scope, targets, and pretext before anything launches — never informal or verbal-only.

Results reported in aggregate

Leadership sees organization- and department-level trends, not a public list used to single anyone out.

Fixed scope, fixed duration

A defined campaign with a start and an end — not standing surveillance of employee inboxes.

Avoid emotionally manipulative pretexts

Layoffs, medical results, personal finances, or salary/bonus promises cause real distress disconnected from the security lesson. Keep pretexts professional and calendar-relevant.

Never spoof a personal account

Simulations target the organization's systems and workflows — not an employee's personal email or social accounts.

Pair every attempt with a learning moment

A click or submission should immediately show what the red flags were — not just log a failure silently.

```
$ phish-sim --from-results
```

Turning Results Into Actual Risk Reduction

The results themselves don't reduce risk. What you do with them does.

- ❑ **Debrief leadership in plain language, not a raw data dump**
What happened, what it means, and what's being done about it — not a spreadsheet that gets filed away unread.
- ❑ **Target follow-up training at repeat clickers specifically**
A targeted micro-training for the people who actually need it outperforms a mandatory all-hands refresher nobody retains.
- ❑ **Invest in the reporting workflow, not just the test**
A one-click "Report Phishing" button is the single highest-leverage tool here — it's the behavior simulations are ultimately trying to build.
- ❑ **Track the trend across campaigns, not the score on one**
A high click rate on a well-crafted targeted pretext isn't the same failure as a high click rate on a generic template — read results in context, not as a single pass/fail number.

Sources: Verizon 2025 Data Breach Investigations Report, KnowBe4 2025 Phishing By Industry Benchmarking Report, SANS Institute "Ethical Phishing" guidance. Anchor Cyber Security LLC.

```
exit 0
```

