Phishing Awareness Program Checklist

A 12-month security awareness program for small and mid-sized teams, in four phases. Work top to bottom; each phase builds on the last. MSPs: run the same phases per client.

Phase 1: Foundation (before you announce anything)

- [ ] Get a leadership sponsor who will visibly back the program.
- [ ] Assign a program owner: [name]. One person accountable, even part-time.
- [ ] Pick your three metrics and how you will measure them:
  - Click rate: % of simulation recipients who click.
  - Report rate: % who report the simulation.
  - Time-to-report: minutes from delivery to first report.
- [ ] Run a baseline phishing simulation, unannounced, so your first numbers are honest.
- [ ] Record the baseline. You will measure everything against it.
- [ ] Adopt an employee phishing reporting policy (free template at resources.phishalert.ai) and pick the reporting method: report button or forward address.
- [ ] Choose your tooling. (PhishAlertPro combines simulations, one-click reporting, AI-assisted triage, coaching, and program records in one place, with per-client visibility for MSPs.)

Phase 2: Launch (month 1)

- [ ] Announce the program from leadership, leading with the no-blame commitment: prompt reporting is never punished, including after a click.
- [ ] Enable the report button in every inbox and show people where it is.
- [ ] Run a short kickoff training, 30 minutes maximum: what phishing looks like now, the red flags, exactly how to report.
- [ ] Put the red flags poster where people work: kitchen, meeting rooms, intranet home page.

- [ ] Send the first post-announcement simulation. Make it easy; the goal is practicing the reporting motion, not tricking people.
- [ ] Publicly celebrate reporters, never name clickers: “First report came in 4 minutes after delivery.”

Phase 3: Operate (every month)

- [ ] Run one simulation per month. Rotate themes (see calendar) and vary difficulty.
- [ ] Anyone who clicks gets 2-3 minutes of coaching the same week, tied to the exact lure they saw. (PhishAlertPro tracks clicks and can deliver this coaching in the platform, where configured.)
- [ ] Share one aggregate win with the whole team each month: reports made, fastest report, trend vs baseline.
- [ ] Onboard every new hire in their first week: reporting method, poster, policy acknowledgment.
- [ ] A few times a year, vary targeting by role: finance sees invoice fraud and bank-detail changes, HR sees resume attachments, executive assistants see gift card and wire requests.

Phase 4: Measure and improve (every quarter)

- [ ] Review the three metrics against baseline. North star: report rate above click rate, and rising.
- [ ] Adjust difficulty: click rate under [5%] means harder lures; flat report rate means retrain the reporting motion, not the spotting.
- [ ] Hold a blameless review of any real incidents this quarter; feed lessons into next month’s simulation theme.
- [ ] Send leadership a one-page summary: metrics, trend, incidents, next quarter’s focus.
- [ ] Keep the records: dates, participation, and metrics. Cyber insurers often ask for this at renewal; PhishAlertPro can help export program records where enabled.
- [ ] Refresh policy contacts and this checklist.

12-month theme calendar

Rotate so no two consecutive months feel the same. Shift months to match your fiscal and seasonal reality.

Month	Simulation theme
1	Password reset / account verification
2	Delivery and shipping notices
3	Invoice fraud / bank detail change
4	File-share and e-signature requests
5	Executive impersonation (gift cards, urgent wires)
6	MFA fatigue / login approval prompts
7	HR themes: benefits, policy updates, payroll
8	Vendor compromise: real-looking threads from known partners
9	QR code lures (posters, invoices, parking)
10	Seasonal: tax, open enrollment, or holiday shipping
11	Calendar invites and meeting links
12	Mixed-difficulty re-test of the year’s weakest theme

Metrics quick reference

Metric	Definition	Success
Click rate	% of recipients who clicked the simulation	Falling
Report rate	% of recipients who reported it	Rising
Time-to-report	Minutes from delivery to first report	Falling

A falling click rate with a flat report rate means people are ignoring phish, not defending against them. Reports protect the whole company; treat report rate as the number that matters most.

General guidance, not legal or compliance advice. Adapt frequencies and themes to your organization and any regulations that apply to you.

About PhishAlertPro. Get your baseline in 2 minutes with the free “How Phishable Is Your Team?” assessment at resources.phishalert.ai. PhishAlertPro helps run the simulation, reporting, triage, and coaching loop in one place: phishalert.ai