SIMULATED PHISHING DRILL

# Authorisation to conduct a simulated phishing drill

This form authorises a controlled, simulated phishing exercise. Nothing in it permits access to, or change of, any live system of the Client.

| | |
|---|---|
| Client (legal entity) | _____ (registered name) |
| ABN / ACN · trading name | _____ _____ |
| Contact for this drill | Name _____ Role _____ |
| Email / phone | _____ _____ |
| Drill reference | _____ Supplier: **1st4scams** |

## 1 · AUTHORISATION

1. The Client authorises **1st4scams** to send **one or more simulated phishing emails** to the staff addresses listed in Schedule A, during the window and from the sender identities listed there, linking to the simulated landing pages listed there.
2. The Client authorises 1st4scams to record, per recipient: delivery; the time of any click; and whether the landing page form was submitted. **No credential value, card number, date of birth or tax file number typed by a recipient is stored** — only the fact of submission.
3. The Client authorises 1st4scams to issue the report (the **Score**): staff tested, clicked, submitted, fastest click, results by team, the tells, and debrief notes.

## 2 · AUTHORITY OF THE SIGNATORY

1. The person signing below warrants they are **authorised to give this authorisation** for the Client, and that any internal approval required (director, HR, IT, privacy officer) has been obtained.
2. Where the Client requires **IT allow-listing**, the Client will give its mail administrator the sender and tracking domains from Schedule A before the window opens.

## 3 · WHAT IS AND IS NOT AUTHORISED

1. **Simulation only.** The emails, domains and landing pages are controlled by 1st4scams. No payment is taken, no account is created or changed, no file is installed, and no software of the Client is exploited.
2. **Not a penetration test.** This is an awareness drill. It does not test, and must not be relied on as testing, the security of any network, application or control environment.
3. **Recipients.** Only the addresses in Schedule A, each a current worker of the Client with a consent basis recorded on the consent form.
4. **Excluded persons** are named in Schedule A and are never sent to. **Stop:** the Client may stop the drill by email; 1st4scams stops sending within one business day and reports on results to that point.
5. **Real incident.** If a recipient reports the email as a genuine attack, or a real campaign arrives during the window, the Client may ask for the sender domains, sending IP ranges and sample headers; 1st4scams supplies them within two business hours during the window.

**Signed for and on behalf of the Client**

Name and position

Signature · Date

**Signed for 1st4scams**

Name and position

Signature · Date

# Schedule A — Scope and rules of engagement

Completed by 1st4scams and confirmed by the Client before the first email is sent.

## DRILL DETAILS

| | |
|---|---|
| Drill reference | _____ |
| Window opens | _____ Window closes _____ (the drill stops at the close whether or not the link was clicked) |
| Staff tested | _____ recipients · list supplied by the Client as a CSV of email, name, team |
| Lure(s) | _____ e.g. au-asic-annual-review (difficulty 5) |
| Sender identity used | _____ display name _____ |
| Sender domain(s) | _____ |
| Tracking domain | **1st4scams.com** (links, redirects and the landing page may all resolve to this domain) |
| Debrief | _____ date, 20 minutes, delivered to the Client contact |

## IT ALLOW-LISTING VALUES

Give these to the Client's mail administrator before the window opens. A drill that lands in quarantine tests the spam filter, not the staff.

| | |
|---|---|
| Sending domain / DKIM | 1st4scams.com (and the lure sender domain in the row above, if separately verified) |
| Sending provider | Resend (ask 1st4scams for current sending IP ranges if your filter requires them) |
| Tracker + landing | 1st4scams.com (Cloudflare) |
| Header marker | X-Entity-Ref-ID: <drill reference> useful for mailbox rules and for proving the mail was ours |

## EXCLUSIONS AND SPECIAL HANDLING

| | |
|---|---|
| Excluded persons | _____ (names or roles — never sent to) |
| Staff on leave | Excluded automatically · confirm the list is current on the send date |
| Brands that must not be used | _____ e.g. the Client's own bank, or a client of the Client |
| Quiet period | _____ e.g. month-end, audit week, peak season |
| Results in performance management | ☐ Not used ☐ Used — staff notified in writing on _____ |

# Schedule B — Data collected and handling

What the drill records, where it is held, who sees it, and when it is deleted.

## SCHEDULE B — DATA COLLECTED AND HANDLING

| WHAT | DETAIL |
|---|---|
| Collected | Recipient email, name and team as supplied by the Client; per-recipient token; time of click; time and fact of form submission; a truncated, salted hash of the connecting IP; browser user-agent string. |
| Not collected | Any password, card number, CVV, date of birth, tax file number or BSB/account value typed by a recipient. Any file. Any screenshot of the recipient's screen. |
| Where it is held | Cloudflare (D1 database and KV store) and Resend (delivery events). Access is limited to 1st4scams and is key-protected. |
| How long | **90 days after the report is issued**, then the staff list and event rows are deleted. A de-identified aggregate (numbers only, no addresses) may be retained for reporting. |
| Who sees it | The Client contact named on page 1. 1st4scams does not sell, publish or share recipient-level data. Where the Client asks 1st4scams to send the report to an insurer or tender panel, the Client supplies the address or forwards it. |
| Access and correction | A recipient may ask what was recorded about them by emailing hello@1st4scams.com. 1st4scams answers within 10 business days and corrects errors. |

## WHY THIS BASIS HOLDS

1. **Privacy Act 1988 (Cth), Australian Privacy Principle 5** — an APP entity must take reasonable steps to notify individuals of the collection, purpose, disclosure and access. The notice above is drafted to satisfy APP 5 for the personal information collected in this drill.
2. **Spam Act 2003 (Cth)** — drill email is sent to the Client's own workers at their work addresses under the Client's authorisation, with the sender identified and a functional unsubscribe path. Consent is inferred from the existing employment relationship and the Client's authorisation.
3. **APP 11** — the data is held in Cloudflare's managed infrastructure, key-protected, and deleted on the 90-day schedule in Schedule B.
4. **Not an employee record.** The Score is a training result, not a performance record, unless the Client records otherwise in Schedule A.

RECIPIENT NOTICE

# Consent basis and notice to staff

Completed by the Client. One of the two routes below must be true, and recorded, before the first email is sent.

## ROUTE A — NOTICE GIVEN IN ADVANCE (RECOMMENDED)

The Client has told the listed workers, in a general way and without giving the drill away, that the business runs simulated phishing tests from time to time and that clicks may be recorded. The exact wording used, and the date it was given, is recorded here.

> Wording used (e.g. "As part of our cyber security program we run simulated phishing tests on staff email accounts. Results are used for training and are recorded against your name. Contact [role] with questions."):
>
> _____
>
> _____
>
> Date given _____ Method ☐ All-staff email ☐ Induction ☐ Intranet ☐ Employment contract / policy ☐ Other

## ROUTE B — NOTICE GIVEN AT THE CONCLUSION

Where notice was not given in advance, every recipient is told **immediately after the drill** that an email was a simulation, what was recorded, and how to ask for deletion. The landing "tells" page does this automatically, and the Client sends the debrief note within two business days.

> **Which route is right?** Route A is stronger and is what a privacy officer will ask for. Route B is lawful where the drill is a reasonable direction in the employment relationship and the notice follows promptly — but it is the weaker position, and it should not be used if results feed performance management.

## THE NOTICE STAFF RECEIVE

Whichever route is used, the following is the notice 1st4scams recommends, and the minimum the landing page delivers at the end of the drill:

> **What just happened.** The email you clicked was a simulated phishing email, sent by 1st4scams on behalf of _____ as part of our cyber security program.
>
> **What was recorded.** That the email was delivered, the time you clicked, and whether you submitted the form. **No password, card number or other value you typed was stored.**
>
> **Why.** So we can show people the one habit that stops these emails: never pay, sign in or change bank details from a link. Open the site you already know, or ring the number on the last invoice.
>
> **Questions or deletion.** Email hello@1st4scams.com or _____. Records are deleted 90 days after the report.

## CLIENT CONFIRMATION

_____

Name and position

_____

Signature · Date

**Route used:** ☐ A (notice in advance) ☐ B (notice at conclusion)

**Results in performance management:** ☐ No ☐ Yes

**Copy of notice attached:** ☐ Yes

PRE-SEND CHECKLIST

# Record of authorisation, consent and send

Completed by 1st4scams before sending, and kept with the drill ledger as the evidence trail for the report.

## CHECKS — ALL MUST BE TICKED BEFORE THE FIRST EMAIL IS SENT

- ☐ Form 1 signed by a person authorised by the Client, with the signatory's name and position recorded.
- ☐ Schedule A completed: window, recipient count, lure, sender identity and domains, exclusions, quiet period.
- ☐ Recipient list supplied by the Client, and every address is a current worker of the Client.
- ☐ No excluded person appears in the list. Staff on leave removed on the send date.
- ☐ Consent route recorded on Form 2, with the notice wording attached where Route A is used.
- ☐ IT allow-listing confirmed in writing by the Client, or the Client has accepted that filtering may affect results.
- ☐ Sending domain verified in the sending provider; test email delivered to the Client contact and to 1st4scams.
- ☐ Tracking link tested end to end: click recorded, landing page loads, submission recorded, tells page shows.
- ☐ Lure's sender domain and landing page do not impersonate the Client's own bank, auditor or a client of the Client, unless expressly authorised in Schedule A.
- ☐ Debrief date booked with the Client contact.

## SIGN-OFF

| ROLE | NAME | DATE | INITIALS |
|---|---|---|---|
| Authorising officer (Client) | | | |
| Drill operator (1st4scams) | | | |
| Send confirmed | | | |

## SEND RECORD

| | |
|---|---|
| Drill reference | _____ |
| Emails sent / failed | _____ sent · _____ failed (failure reason recorded in the ledger) |
| Sent at (AEST/AEDT) | _____ |
| Window closed | _____ |
| Report issued | _____ deletion due 90 days later: _____ |
| Deletion completed | _____ staff list and event rows removed from D1 and KV |

**Why this page matters.** It is the difference between a prank and a service. If a recipient complains, an insurer asks, or a tender panel wants evidence, this page plus the signed Form 1 and the drill ledger answer every question: who authorised it, who was told, what was recorded, where it is held, and when it was deleted.



1st4scams · hello@1st4scams.com · 1st4scams.com · ABN to be confirmed · Governing law: Tasmania, Australia. Forms may be signed electronically and exchanged as PDF; a signed copy is as valid as an original.