Phishing abuse report checklist

Send the same evidence to every party, at the same time. Templates for each are in the Phishing Takedown Playbook and at sentrike.ai/downloads/phishing-abuse-report-templates.txt.

PHISHING URL _____ CASE NUMBER _____ DATE (UTC) _____

WHO GETS THE REPORT

	SEND TO	ASK THEM TO	FIND THE CONTACT	TICKET / DATE
☐	**Registrar**	Suspend the domain	RDAP: "Registrar Abuse Contact Email" (lookup.icann.org)	
☐	**Hosting provider**	Remove the page, close the account	IP owner in its regional registry (ARIN, RIPE, APNIC…)	
☐	**CDN or proxy**	Forward to host and owner	The CDN's abuse form, phishing category	
☐	**Platform**	Remove the site	Vercel, Netlify, Shopify…: abuse form	
☐	**Google Safe Browsing**	Warn Chrome, Safari, Firefox users	safebrowsing.google.com/safebrowsing/report_phish	
☐	**Microsoft SmartScreen**	Warn Edge users	Microsoft's report unsafe site form	

BEFORE YOU SEND

- ☐ **Full URL** of the page that collects data, not just the domain
- ☐ **Screenshot** with date and time (UTC)
- ☐ **What it collects** (form fields) and **what it imitates**
- ☐ Domain details: registered date, nameservers, IP and network owner
- ☐ Page is **live now** (re-checked); note if it only shows on mobile or in one country
- ☐ Address of **our real page**, for comparison
- ☐ **How victims reach it** (lure sample, with email headers)
- ☐ Who we are: **brand owner** or **authorized representative**

IF NOBODY ANSWERS

01 Follow up once in the same thread after **one business day**, with a fresh screenshot.

02 Report to the **registry** that runs the extension (e.g. Verisign for .com).

03 Complain to **ICANN Contractual Compliance** (generic domains).

04 Report to shared feeds such as the **APWG**.

05 Involve your **national CERT** for persistent or cross-border cases.

CLOSE THE CASE

Only when the site is **offline everywhere**: every URL, from several countries and devices. Keep the evidence, and watch for the same kit on new domains.