Stolen domain checklist

What to do when your domain name is stolen. Work down the list in order and tick each step as you finish it. The full guide, with the reasons behind every step, is at confirmedstolen.com/domain-name-theft/.

In the first hour

- [ ] **Confirm it is theft, not an expiration or a DNS outage**
  Run an RDAP lookup and check the registrar of record, the registrant, the nameservers and the status codes. A new registrar or registrant you did not authorize points to theft. Use ICANN Lookup (lookup.icann.org/).

- [ ] **Secure the email account tied to your registrar account**
  Change the password from a clean device, revoke unknown sessions and app passwords, remove forwarding rules you did not create and turn on multi-factor authentication (MFA).

- [ ] **Check your mobile number for signs of a SIM swap**
  Sudden loss of service or unexpected port-out messages suggest your number was moved. Contact your carrier and see the SIM swap guide (confirmedstolen.com/sim-swap/).

- [ ] **Try to log in to the registrar account and change its credentials**
  If you still have access, reset the password, remove unknown users and API keys, and replace SMS codes with an authenticator app or security key.

- [ ] **Contact the registrar's abuse or security desk**
  Use contact details from the registrar's official website, not from any email you received. State that the domain was transferred or changed without authorization and ask for a ticket number.

Within 24 hours

- [ ] **Ask the registrar to lock the domain and freeze further changes**
  Request that no transfer, registrant change or nameserver change be processed while the case is reviewed.

- [ ] **Capture WHOIS and RDAP records and screenshots with timestamps**
  Save current lookups and any historical WHOIS records you can obtain, plus screenshots of the registrar dashboard, the live website and the DNS records.

- [ ] **Preserve every notification email and log**
  Keep transfer approval requests, registrant change notices, login alerts and password reset messages in their original form, including full headers.

- [ ] **Gather proof that you are the rightful registrant**
  Collect invoices, renewal receipts, payment records, account history, trademark filings and records showing your business used the domain.

- [ ] **Ask your original registrar whether it will open a transfer dispute**
  If the domain moved to another registrar, your original (losing) registrar is the party that can file a dispute under the Transfer Dispute Resolution Policy (TDRP).

This week

- [ ] **File a complaint with ICANN Contractual Compliance if a registrar is unresponsive**
  ICANN reviews whether an accredited registrar followed its obligations. Start at icann.org (www.icann.org/) and find the Contractual Compliance complaint forms.
- [ ] **File a report with the FBI Internet Crime Complaint Center**
  Describe the unauthorized transfer, the losses and the timeline at ic3.gov (www.ic3.gov/), and keep the confirmation.
- [ ] **Report the theft to local police and request a report number**
  A police report number supports registrar, insurance and court processes. See USA.gov (www.usa.gov/report-crime) for reporting options.
- [ ] **Tell customers, partners and email contacts what happened**
  Warn them not to trust email or payment requests from the domain until control is restored.
- [ ] **Consult a lawyer about court options**
  Ask about civil claims, including in rem actions (cases brought against the domain itself) in courts where the registry is located.

Prevent it happening again

- [ ] **Turn on MFA everywhere the domain can be changed**
  Protect the registrar account, the linked email account and the DNS hosting account with an authenticator app or hardware security key.
- [ ] **Ask your registrar about registry lock for high-value domains**
  Registry lock requires manual, out-of-band verification before changes are made at the registry level.
- [ ] **Enable DNSSEC and remove stale nameserver delegations**
  Sign your DNS so tampering can be detected, and delete delegations to DNS providers that no longer host your zone.
- [ ] **Keep registrant contact details current and set auto-renew**
  Accurate contact data ensures transfer and renewal notices reach you, and auto-renew prevents an accidental lapse.
- [ ] **Report the stolen domain to Confirmed Stolen for verification**
  Submit details through the report page (confirmedstolen.com/report/) so the domain can be reviewed for the confirmed list (confirmedstolen.com/domain-names/).

Your case record

Domain name

Registrar ticket number

Registrar contact and date

ICANN complaint reference

IC3 complaint number

Police report number

Notes

Version November 6, 2026. General information, not legal advice. Agencies change their procedures, so confirm each step with the organization named. Confirmed Stolen is an independent reference; it is not law enforcement and does not recover property. Free to print and share with attribution.