SECURITY & RECOVERY

Signs your site was hacked and what to do

Recognize warning signs, contain the issue, and work with your provider to recover.

FOR SMALL BUSINESS OWNERS

PLAN THE WORK

Recognize signs that deserve a closer look

Unexpected redirects, pages you never published, new administrator accounts, and browser or Search Console security warnings can point to compromise. Individual symptoms may have other causes. Record what happened, when, and which page was affected. A customer’s screenshot or the exact address can help your provider investigate.

Contain harm and preserve evidence

Contact your host or developer using a known contact method. Ask them to contain the affected site or isolate the suspicious part, preserve logs and a current snapshot, and identify the likely exposure period. Avoid deleting files or restoring over the current site before evidence is captured.

Check whether customer data is involved

Tell the incident lead if the site handles orders, accounts, payments, or sensitive inquiries. If customer information may have been exposed, involve qualified incident-response and legal support promptly to assess scope and notification obligations. Notify your payment provider if payment data may be involved.

PUT IT INTO PRACTICE

Recover from a verified clean state

Have your provider identify and fix the entry point, remove unauthorized access, and restore or rebuild from a verified clean copy. Coordinate password and key rotation from a trusted device, revoke active sessions when appropriate, and enable multi-factor authentication. A backup can contain the same problem if it was taken after the compromise began.

Verify before reopening

Test key pages and forms and check for unusual accounts or redirects. Monitor for recurrence. If Google reported a security issue, use Search Console to request review after correcting the reported issues. Keep a short incident timeline and record what changed to prevent a repeat.

WORKED EXAMPLE

Modesto retailer with an unexpected redirect

Two shoppers report being sent to a different site on mobile. The owner saves the affected URLs and times, calls the host, and asks for containment and log preservation. The provider confirms what changed before restoring service. If order information may have been exposed, the owner escalates it for qualified review.

PRINTABLE WORKSHEET

Your next steps

Assign each task and check it off when you verify it.

- [ ] **Record the symptoms**
  Save screenshots, affected URLs, and the time first noticed.
  OWNER / DUE _____

- [ ] **Contact your host or developer**
  Ask who will contain the issue and preserve evidence.
  OWNER / DUE _____

- [ ] **Assess exposure**
  Flag checkout, inquiry records, and account data to the incident lead.
  OWNER / DUE _____

- [ ] **Confirm cleanup and access changes**
  Verify the entry point was corrected and access secured.
  OWNER / DUE _____

- [ ] **Test and monitor**
  Check the customer journey and follow up on any security warnings.
  OWNER / DUE _____

FIRST ACTION _____

FTC · Data breach response for businesses

Google Search Console · Security Issues report