IN-DEPTH GUIDE SECURITY AND COMPLIANCE

Hacked site: the guide to take over

Actions to take immediately if your website has been hacked or infected, in order, with what really helps and what doesn't help.

G

GXN
Senior expertise · Digital governance

Quebec First
Quebec business context

July 31, 2026
Updated

SECURITY AND COMPLIANCE

Hacked site: the guide to take over

TL;DR

The answer in one minute

If your site has been hacked, stay calm, it's more common than you think and it is almost always correct. The first steps are to immediately change all passwords related to the site, to make a copy of the current condition before touching anything else, to identify the visible extent of the problem, and to proceed with the cleaning and closing of the entrance door that allowed the incident. After cleaning, the step that almost everyone forgets is to harden security to prevent it from happening again.

01 · BACKGROUND GUIDE

First, breathe

A pirated site is scary, but in the vast majority of cases, it's not catastrophic and it's settled. Automated attacks that affect most small and medium-sized sites are usually not directed personally against you. They target known large-scale vulnerabilities at thousands of sites at the same time. You're probably not a specific target, you're a door that someone found.

02 · BACKGROUND GUIDE

Immediate actions, in order

Change all site-related passwords. Hosting, site administration, associated email, everything that could have been compromised at the same time.

- Make a copy of the current state before cleaning anything. Even infected, it can help to understand what happened.

- Look what's visible. The site displays strange content, redirects it to another site, a browser displays a security warning. This observation helps to determine the extent of the problem.

- Check if your host has suspended the site on its own initiative, which sometimes happens automatically in case of malicious content detection.

- Stay calm and don’t delete anything in a rush. Hasty deletions can destroy valuable evidence to understand exactly how the breach entered.

DECISION CARD

The four angles to keep together

01

First, breathe

02

Immediate actions, in order

03

What is done next, the actual cleaning

04

The step everyone skips

GUIDE READING GRID

Angle	Dimension to examine	Use in the decision
01	First, breathe	Setting the Context
02	Immediate actions, in order	Identify dependencies
03	What is done next, the actual cleaning	Compare options
04	The step everyone skips	Preparing for the next step

03 · BACKGROUND GUIDE

What is done next, the actual cleaning

Identify the entrance door. Almost always, it's not updated software, a weak password, or a forgotten account with still active access.

- Remove malicious content injected into the files or database from the site.
- Close the identified entrance door. There's no point cleaning if the rift remains open for the next attack.
- Restore from a healthy backup if manual cleaning is too complex or incomplete.
- Request review from Google or other services if security warnings have been publicly posted.

INTERACTIVE TOOL

Set your decision

Select the dimensions that describe your situation. The result is to organize the next conversation, not to replace an analysis.

WHAT CONCERNS YOU NOW

- 01 **First, breathe**
- 02 **Immediate actions, in order**
- 03 **What is done next, the actual cleaning**
- 04 **The step everyone skips**

Urgent decision 5

Current control level 5

RECOMMENDED ANALYSIS

Several dimensions must be treated together

Avoid an isolated decision. Map out the dependencies and agree on an intervention order.

45 / 100

The step everyone skips

Once the site is cleaned and released online, the natural reflex is to turn the page and move on. This is exactly the time to tighten security, not relax vigilance. Update all software, review all accounts with access, set up continuous monitoring, and check that backups actually work, not just in theory.

Jumping this step is cleaning once and waiting for the next attack, which will probably come by the same path.

05 · BACKGROUND GUIDE

What we can do, and what we don't do

We perform technical clean-up, identify entry points, harden security, and restore after incidents. We don't conduct formal legal investigations or certified intrusion analysis for insurance purposes. If your situation requires this level of investigation, we'll be upfront about it and direct you to appropriate resources.

06 · BACKGROUND GUIDE

What I see on the ground

Almost every hacked site I cleaned in 20 years shared the same profile. Updates delayed for months, sometimes years. Accounts of former employees or suppliers never deactivated. No verified backup, or a backup that existed in theory but had never been tested.

The attack itself was almost never sophisticated. It was accumulated negligence that opened the door, not a computer crime genius.

When this guide is not enough

If personal data from customers have potentially been exposed, the situation goes beyond mere technical cleaning and involves notification obligations that fall under your legal counsel. If you suspect a targeted criminal intent against your company, rather than a generic automated attack, consultation with the appropriate authorities becomes relevant in addition to technical work.

QUESTIONS AND ANSWERS

Frequently asked questions

01 **Do I have to pay a ransom if asked?**

Generally no, there is no guarantee that paying will solve anything, and it encourages the continuation of these practices. Restoring from a healthy backup is almost always preferable.

02 **How long does a complete cleaning take.**

03 **I'll lose my position on Google after a hack.**

04 **How do I know if my site is still infected after cleaning.**

EDITORIAL METHOD

In-depth guide prepared by GXN based on real business situations. Recommendations remain independent of brands and suppliers.

OFFICIAL SOURCES

References to be checked according to your situation

These references support the external rules and frameworks cited in this guide. They are not a substitute for legal or professional advice tailored to your organization.

Canadian Center for Cyber Security

Basic Cybersecurity Controls for Small and Medium Organizations ↗

G

ABOUT THE PUBLISHER

GXN

Senior expertise directly accessible, supported by specialists when the project requires it.

Discover GXN ↗

NEXT STEP

If this is currently underway, the digital SOS section of our site is designed for this particular emergency.

Otherwise, free assessment gives you an honest reading of your current security situation.

No call required. No sales sequence.