BK Modules

Hacked PrestaShop Store Cleanup terms

VERSION
1.0

IN FORCE SINCE
11/12/2026

WHO IT IS FOR
Whoever orders the cleanup of a hacked PrestaShop store on bkmodules.com

This is the contract for the Hacked PrestaShop Store Cleanup: what we do in your shop and on its server, how quickly, what we need from you, what the guarantee covers and when we refund your money. It is a contract between businesses, only for businesses and professionals who sign up for their trade or profession (section 1). Read it before you sign up: when you pay, you tick a box saying you accept it. We send you a PDF copy with the order confirmation, and you can always find it in that order, in your account.

What you have signed up for

What you sign up for is ticked in your personalised copy (the one you open when you pay and the one kept in your order), and at the end it has the "Economic summary" with its price.

- ☐ Cleanup of one hacked PrestaShop shop and its server, in under 24 hours and with a 30-day guarantee (sections 5, 7 and 8).

The price is fixed and does not change with the hours the work takes us. It is not in this text because it depends on the currency and the terms of your account: it is the price you see when you pay, before you confirm the order, and it appears in the "Economic summary" at the end of your copy of this contract and in your order, with the currency, taxes and discounts, if any. It is paid in full in advance, and we start once payment is confirmed. If your country requires you to declare a tax on this purchase, that declaration is your responsibility.

1. Who the parties to this contract are

On one side, BK Modules LLC, trading under the name BK Modules: a limited liability company formed in the State of New Mexico (United States), with its address at 102 Gold Ave SW, Albuquerque, NM 87102, United States, and US Employer Identification Number (EIN) 35-2838640. Email: bkmodules@bkmodules.com. Phone: +1 (813) 214-0078. In this contract, "we" or "us".

On the other, the business or professional that signs up with their bkmodules.com account. In this contract, "you". If you sign up on behalf of a business or one of your clients, you confirm that you are authorised to do so and that the business or client is bound by this contract.

Only for businesses and professionals

This contract is only for businesses and professionals who sign up for the cleanup for their trade, business or profession. By signing up, you declare that this is your case. Consumer protection legislation does not apply, and there is no right of withdrawal.

2. What this contract governs

The Hacked PrestaShop Store Cleanup is a service you pay for once: we clean an attacked PrestaShop shop and its server, close the hole the attackers got in through and give you a 30-day guarantee. It does not renew and is not charged again. For anything this contract does not cover, the bkmodules.com general terms and conditions of sale apply, and if the two say different things about the cleanup, this contract prevails.

3. Words we use

- **Shop**: the PrestaShop installation you state when you sign up, with its domain. The cleanup covers a single Shop.
- **Server**: the machine the Shop is installed on, whether it is a server, a VPS or a hosting account. The cleanup covers a single Server.
- **Access Credentials**: the usernames, passwords, keys and connection details you give us to work on the Shop and on the Server.
- **Malicious code**: anything someone has put in the Shop or on the Server without your permission to steal data or payments, send your visitors elsewhere, send spam or get back in. It can be a file, code slipped into a legitimate file, data in the database, a user, a key or a scheduled task.
- **Entry point**: the weakness the attacker got in through. For example, a module with a known security flaw, a stolen password or a file left behind on the Server.
- **Report**: the document we send you at the end, with what we found, what we did and what we recommend.
- **Handover**: the moment we send you the Report and tell you the work is done.
- **Reinfection**: Malicious code turning up again in the Shop or on the Server after the Handover.

4. What we need to work: your Access Credentials

To start, we need two Access Credentials: SSH access to the Server as the root user, which means full control of the Server, and the PrestaShop back office with a SuperAdmin profile. Without root we do not touch anything: the clock does not start, and if you cannot get it within 7 days of payment, the refund in section 9 applies.

You give them to us in your bkmodules.com account, in the form we link to with the payment confirmation. If you are on shared hosting, ask your provider whether they will give you root before you sign up.

What an attacker leaves behind is usually outside the shop folder, in scheduled tasks, in other system users or in files that limited access cannot see or touch. With limited access we would not know whether the Server is clean, so we only start with root. If root stops working while we are on the job, we stop until it is back.

Module updates

We also need the updates for the modules that need updating, because a module with a security flaw is still an open door. We tell you which ones as soon as we find them. Modules from other developers are downloaded from your account on their website or on PrestaShop Addons, because the licence is yours: you give us the files or access to that account. If downloading the new version means buying or renewing a licence or support, that payment is yours.

If a job needs your hosting panel (for example, Plesk or cPanel), your Google Search Console account or another service, we ask you for it and you give it to us through the same form.

How we keep your Access Credentials

- Encrypted, in a password manager. Never in emails, tickets or documents.
- They are used only by the people working on your Shop, who are bound by confidentiality, and only for this contract.
- We do not give them to anyone, unless a law or a court requires us to. In that case, if we are allowed to, we let you know.
- We keep them until the guarantee ends, so that we can get back in if there is a Reinfection. If you ask us to delete them sooner, we do, and to use the guarantee afterwards you will have to give them to us again.
- When the contract ends, we delete them. If we installed an SSH key of our own on the Server, we remove it, as long as we still have access. Even so, we recommend that you change the passwords you gave us.
- If we suspect that someone may have learned your Access Credentials without permission, we let you know without delay so you can change them.

5. What we do

1. Before touching anything, we copy the Shop's files and database exactly as they are. The copy lets us undo a change if needed, and it is a record of what was there.
2. We look for Malicious code in the files of the Shop and the Server, in the database, in the users, in the scheduled tasks and in the Server logs, and we work out what the Entry point was.
3. We remove the Malicious code from the files and the database, along with any users, keys and tasks the attacker left behind. If a PrestaShop or module file has been altered, we replace it with the original from the same version.
4. We close the Entry point so they cannot get in that way again: depending on the case, we update or fix the flawed module, remove the forgotten file or change the stolen password. With the files you give us (section 4), we also update the Shop's other modules that have a known security flaw.
5. We do some basic hardening. We change the passwords and keys of the PrestaShop administrators, the database and the Server, and give you the new ones. We remove any administrators and users you do not recognise, the install folder and any files that should not be there, set the file permissions correctly and stop code from running in the folders where images and documents are uploaded.
6. We bring the Server up to date with every change within our reach: package updates, security patches, configuration and, if needed, the PHP version, which we take up to the highest one your PrestaShop and its modules support. The only thing we do not do is move the Server to

another version of the operating system (section 6).
7. If Google or the browser is warning your visitors that the Shop is dangerous, or your domain is on a spam list and your emails are not arriving, once we finish we ask whoever issued the warning to review the Shop. We ask Google through Search Console, with your access. Removing the warning is their decision, and it usually takes anywhere from a few hours to a few days.
8. We send you the Report with what we found, how they got in, what we did and what we recommend. The recommendations needed for the guarantee are marked, each with its deadline.

Anything the attack or our cleanup breaks in the Shop, we fix as part of this work. If cleaning means closing the Shop to the public for a while, or a change may affect sales, we explain it to you beforehand and wait for your approval.

We keep the copy from the first point until the guarantee ends, and then we delete it. If you want to report the attack to the police, ask us for it before then and we will give it to you.

6. What the cleanup does not include

- Updating PrestaShop, whether to another version or to a patch of the same version, even when your version does not support any PHP version that still receives security patches. If the Entry point can only be closed by updating it, we tell you so in the Report and quote for it separately.
- Moving the Server to another version of the operating system. If that is needed, the Shop may have to move to another server or hosting, which we quote for and agree with you separately.
- Maintenance after the Handover. Monitoring the Shop, updating it and fixing whatever fails from then on is another contract, PrestaShop Maintenance.
- Recovering data the attack has deleted or damaged, such as orders, customers, products or images. If you have a clean backup, we tell you what can be brought back from it, as separate work.
- Fixing faults that do not come from the attack, developing new features or changing the design.
- Buying licences or renewals for modules from other developers.
- Recovering the visits or Google rankings you have lost because of the attack. As for warnings from Google, browsers and spam lists, what is included is requesting the review (section 5).
- Other websites, shops or accounts on the same Server, and email accounts. If we see that they are infected too, we tell you.
- A forensic examination or a report that can be used as evidence in court, reporting the attack to the police, and notifying your customers, your bank, your payment gateway or the data protection authority.

Anything not included, we assess and quote for separately, and you decide.

7. How long it takes

We hand the Shop back to you clean in under 24 hours, counted straight through, day and night, every day of the week, weekends and public holidays included.

- The 24 hours start when we have both Access Credentials in section 4 and they work: root SSH

and the SuperAdmin back office. We do not start work before then. If one is missing or does not work, we tell you as soon as we notice.
- The clock stops while we wait for something only you can give us, from when we ask you until we have it: a module update, another access, root if it stops working, or your approval of a change that affects sales.
- The time period ends with the Handover.

8. 30-day guarantee

If there is a Reinfection within 30 days of the Handover, we clean the Shop and the Server again at no cost, provided all the work in section 5 could be done. For that, all of the following must hold:

- All the modules we asked you to update were updated.
- You applied, within their deadlines, the recommendations the Report marks as needed for the guarantee.
- If the Entry point could only be closed by updating PrestaShop or the operating system, that update has been done.
- Nobody has undone what we did or reopened the Entry point.

When there is no guarantee

The guarantee does not cover a Reinfection in these cases:

- A module we asked you to update is still not updated, or you did not give us its files.
- You did not apply the recommendations marked as needed for the guarantee.
- Someone (you, your team, another provider or your hosting company) changes what we did, installs new modules or themes or makes changes on the Server, and that reopens the Entry point or opens a new one.
- The attacker gets in with a valid password stolen outside the Shop and the Server: from your computer, your email, your hosting panel or a member of your team.
- The attack comes from other websites or accounts on the same Server that are not part of the cleanup, or from your hosting provider's infrastructure.
- The attack exploits a security flaw that was not publicly known on the day of the Handover.
- You tell us after the 30 days.

How to claim it

Email us at bkmodules@bkmodules.com within the 30 days and tell us what you are seeing. We check whether it is a Reinfection and whether the guarantee covers it, and we let you know. If it does, we clean it in under 24 hours from when we have working Access Credentials, root included, under the rules in section 7, and the guarantee runs for another 30 days from that new Handover. If it does not, we explain why and give you a quote for the cleanup.

9. When we refund your money

If we cannot do the work for a reason on our side, we refund everything you paid.

If it cannot be done for a reason that does not depend on us, we refund what you paid minus €99 for operating costs, which cover the time we set aside for your Shop, reviewing what you give us, and handling the payment and the refund. If you paid in another currency, we deduct the

equivalent amount in that currency shown in the “Economic summary”. This applies only in these cases:

- Within 7 days of payment you have not given us the Access Credentials in section 4 with root, even though we have asked you for them and reminded you. Since we do not start without root, once those 7 days are up we refund the amount minus that deduction.
- The Access Credentials you give us do not work, or root stops working while we are on the job, and you do not fix it within 7 days of our notice.
- Your hosting provider prevents the work, because it does not give root access, suspends the account or blocks the intervention, and this is not resolved within 7 days.
- You cancel the job before we start, that is, before we first log in to the Shop or the Server with your Access Credentials.
- What needs cleaning is not what you signed up for, because it is not a PrestaShop shop or there are several shops or servers, and you do not accept the quote for whatever goes beyond one Shop and one Server.

If the work is left half done for one of these reasons, we also send you what we have found up to that point.

Once the Handover has taken place, there is no refund. Outside the cases in this section, what you have paid is not refunded.

We refund the amount within 14 days of the case arising, by the same means you paid with.

10. Your obligations

- To give us the Access Credentials in section 4, with root, and the module updates, and to keep the Access Credentials up to date until the guarantee ends.
- To pay for any licences or renewals of modules from other developers that are needed.
- To answer our questions as soon as you can. While we wait for your reply, the clock stops.
- Not to change anything in the Shop or on the Server while we are working, or let others do so. If another person or company is also working on them, let us know.
- To apply the recommendations in the Report, especially those marked as needed for the guarantee.
- To have the right to use what is in the Shop: the theme, the modules and their licences, and the content.
- To use the service for lawful purposes, without asking us for anything that is against the law or the rights of others.

11. Confidentiality and personal data

Everything we see of your business while working on the Shop and the Server (data, sales, configuration, code, documents) is confidential. We use it only for this contract and do not disclose it to anyone, including after the contract ends. This does not apply to anything that is already public or that a law or a court requires us to disclose.

How we process your data is set out in the privacy policy.

When working on the Shop we process personal data of your customers. For that data, you are the

controller and we are your processor, with the commitments in the section “Your customers' data when we work on your shop” of the general terms and conditions, which form part of this contract: to process it only for this work and in accordance with your instructions, with confidentiality and appropriate security measures; to tell you without delay of any breach; not to engage other processors without informing you first; to help you respond to your customers' requests to exercise their rights; and to delete whatever we hold at the end. As we are in the United States, access to that data takes place with the safeguards the European Union recognises for these cases, described in the privacy policy.

If the attack has exposed your customers' data

In the Report we tell you which of your customers' data was within the attacker's reach and, if it can be established, whether it was taken. Deciding whether to notify the data protection authority, your customers or your payment gateway, and doing so, is up to you as controller. In the European Union, the authority must be notified within 72 hours of becoming aware of the breach, so if you think this applies to you, start preparing the notification without waiting for the Report.

12. Liability

We work on your Shop with the diligence and expertise of a professional, and we undertake to do the work in section 5 properly, within the time in section 7, and to honour the guarantee in section 8. Nobody can promise that a shop will never be attacked again, and if there is a Reinfection, what we owe you is that guarantee.

We are not liable for:

- indirect loss, such as loss of profit, loss of sales, customers or data, and interruption of your business;
- the consequences of the attack, such as data or payments that were taken, fines, claims from your customers and warnings from Google and antivirus software;
- anything caused by your hosting provider, by third-party modules, themes and services, by changes made by others to the Shop or the Server, or by missing Access Credentials or backups;
- anything we do following your instructions.

Our total liability under this contract does not exceed what you paid us under it. Nothing in this section limits our liability for wilful misconduct or gross negligence, or any liability that cannot be limited by law.

Nor are we liable for delays caused by events beyond our reasonable control, such as widespread internet or power grid outages, or outages of payment gateways or of the third-party services we depend on.

13. When the contract ends

- When the guarantee ends, 30 days after the Handover or after the last cleanup under guarantee, or when we refund your money (section 9).
- We may stop the work if you ask us for something unlawful or use the Access Credentials or the service to harm others, after notifying you, unless the seriousness of the matter requires us to

act immediately.
- At the end, we delete your Access Credentials as set out in section 4, the copy of the state we found the Shop in and the working copies. The Report is yours to keep.

14. Electronic communications

You agree that this contract, the Report and all other communications about the cleanup will reach you electronically: by email to your account address and in your bkmodules.com account. To receive them, all you need is a web browser, an email program and the ability to open a PDF. You can ask us for a free paper copy of any of them. Keep your email address up to date, because notices we send to it count as delivered.

15. Changes to this contract

We may update this contract. Each version has its own number and its date of entry into force, and applies to cleanups ordered from that date. Your cleanup, including its guarantee, is always governed by the version you accepted when you paid.

16. Governing law and jurisdiction

This contract is governed by the laws of the State of New Mexico and by the applicable federal laws of the United States.

Any dispute is settled by the state or federal courts located in Bernalillo County (Albuquerque, New Mexico).

17. Contact

BK Modules LLC · 102 Gold Ave SW, Albuquerque, NM 87102, United States · bkmodules@bkmodules.com · +1 (813) 214-0078