Design 'N' Buy

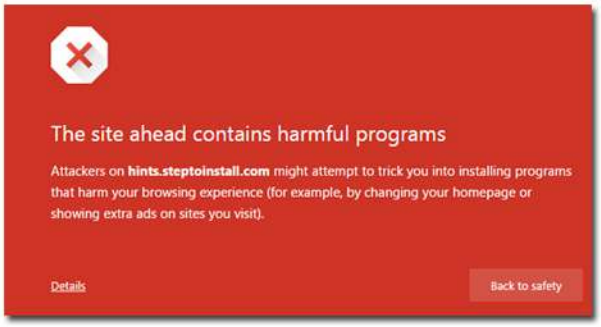
1. IDENTIFY THE HACK

There are two main reasons to hack Magento website.

- ✓ Outdated Magento version
- ✓ Magento security patches missing

1.1 Symptoms of a hacked Magento website

Whenever a Magento store is compromised, one of the primary concerns is to determine the hack. Here are some of ways that can help you to determine that you are Magento store hacked.



- ✓ Blacklist warnings by search engines
- ✓ Strange credit card activities
- ✓ Abnormal behaviour of checkout page
- ✓ Redirection on hacked page/adult site
- ✓ Database hacking
- ✓ Disturbance in orders and sales
- ✓ Spam keywords and details in product listings and other pages
- ✓ Your hosting provider suspends your store for malicious activities
- ✓ Your domain gets blacklisting warnings
- ✓ Change in files and folders
- ✓ Modifications in the Magento core integrations
- ✓ Unknown sessions and admin users in Magento backend

1.2 Scan your site:

There are free online tools you can use to scan your Magento installation remotely. (e.g.: SiteCheck, MageReport, Foregenix, Github Magento Malware Scanner, MageScan, VirusTotal, etc.) These can help you identify credit card swipes, malicious payloads, intermediary domains, and other security issues.

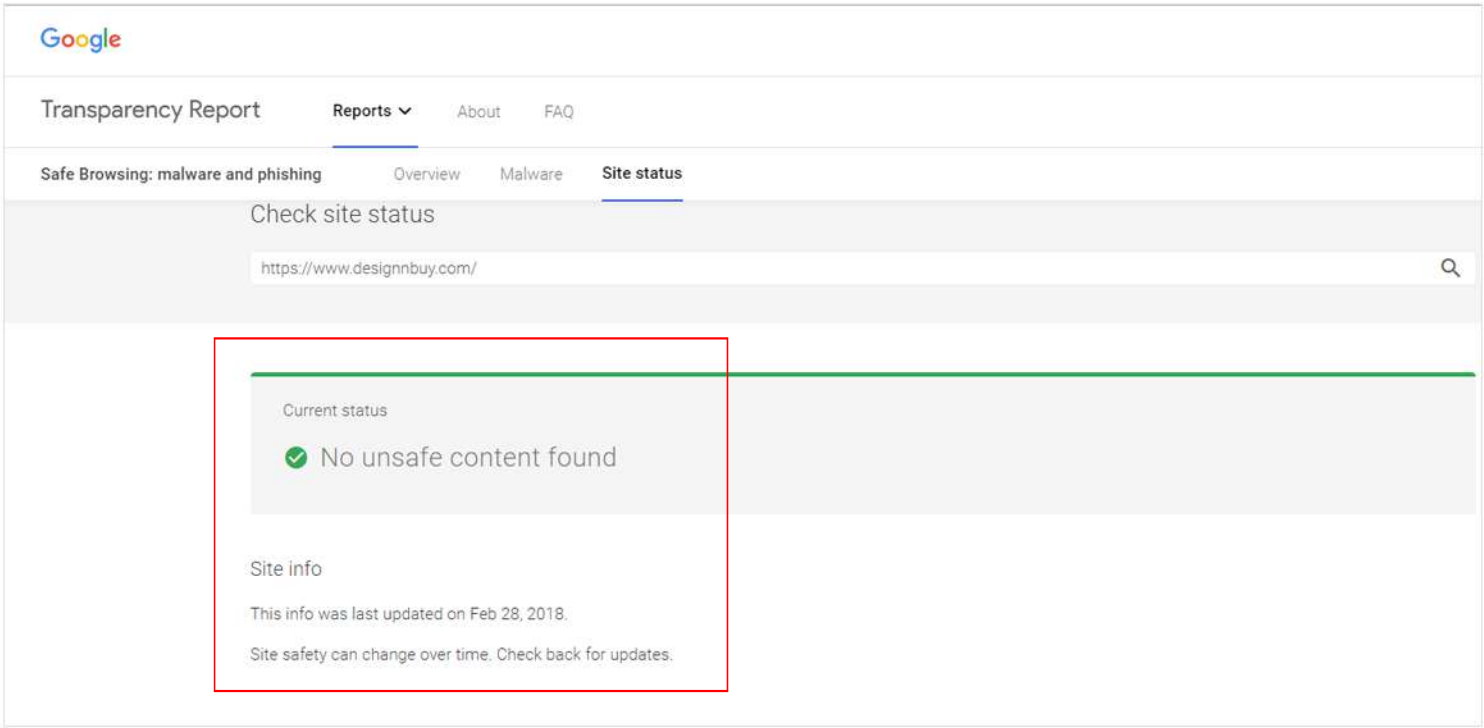
To scan Magento for malware and security issues, visit the 'Sitecheck' website
Enter your **Magento website URL > Click scan website**

If the site is infected, a warning message will display. We recommend scanning all websites on the same server because cross-site contamination is one of the leading causes of re-infection. We also encourage every website owner to isolate their hosting, SFTP/FTP, and SSH accounts.

Note:
A remote security scanner browses your site, but does not have access to the server. Some issues cannot be detected in a browser (i.e., backdoors, phishing, and server-based scripts). The most comprehensive approach to scanning includes both remote and server-side scanners. Learn more about how remote scanners work.

1.3 Check Google Transparency Report

- ✓ Enter your site URL and click the icon to search
- ✓ On this page you can check:
  - ✓ Site Safety Details: information about malicious redirects, spam and downloads
  - ✓ Testing Details: most recent Google scan date with malware detected



You should also check if any customers have reported fraudulent purchases shortly after ordering something from your site.

1.4 Check Core File Integrity

Any file that's been modified recently on your server might be a part of the hack. In this case, your Magento files and folders should be checked thoroughly against malware injections. Compare your Magento core files with a fresh copy of Magento core files by using the diff command in SSH Terminal. If you are not familiar with the command line, you can manually check your files using any file management client.

You can also download and use 'DiffMerge' to compare files. Remember, when comparing your store with new Magento files, make sure to use the same version of Magento including extensions and any applied patches. We'd also advise to remove and reinstall all the themes, extensions, and custom modules, etc., after a hack to ensure that they are functioning free of malware.

Note:
We recommend using SFTP/SSH/FTPS rather than unencrypted FTP to access your server for improved security.

To check core file integrity with SSH commands:

```
$ mkdir magento-2.1.3
$ cd magento-2.1.3
$ wget https://github.com/magento/magento2/archive/2.1.3.tar.gz
$ tar -zxvf 2.1.3.tar.gz
$ diff -r 2.1.3 ./public_html
```

The final diff command will compare the clean Magento files with your installation. The output will also report additional modules you have added, and these can be compared with known good files in a similar manner. Remember to remove the known good files from your server after testing.

To manually check recently modified files, log into your Magento web server

- If using SSH, you can list all files modified in the **last 15 days** using this command:

  `$ find ./ -type f -mtime -15`

- If using SFTP, review last modified date column for all files on the server.

Note any files that have been recently modified. Unfamiliar modifications in the last 7-30 days may be suspicious and require further investigation

Note:
Some malware infections hide by changing the file modification date. You can also try using other online scanners and Magento extensions to look for indicators of compromise, malicious payloads, and security issues.

1.5 Audit User Logs

Hackers often create malicious user accounts on compromised Magento sites. Verify all of your Magento user accounts, especially administrators and delete unwanted users from the admin panel.

To check for malicious users, **System > Permissions > Users**

Review the list, especially ones with an abnormal or recent ID number and delete any unfamiliar users that may have been created by hackers

2. FIX THE HACK OR RECOVER

2.1 Clean Hacked Database Tables

To remove a malware infection from Magento database tables:

- ✓ Log into your database admin panel
- ✓ Make a backup of the database before making changes
- ✓ Search for suspicious content (i.e., spammy keywords, links)
- ✓ Open the table that contains suspicious content
- ✓ Manually remove any suspicious content
- ✓ Test to verify the site is still operational after changes
- ✓ Remove any database access tools you may have uploaded

You can manually search your Magento database for common, malicious PHP functions such as eval, base64_decode, gzinflate, preg_replace, str_replace, etc. Additionally, the most common location for Magento malware is the core_config_data table. Within this table, they specifically target the site's footer and header area (i.e. Design/head/includes and design/footer/absolute_footer).

Note:
These functions are also used by Magento extensions for legitimate reasons, so be sure to back up, test, or seek assistance so you do not accidentally break your ecommerce site.

2.2 Clean hacked website files

To manually remove a malware infection from your Magento files:

- ✓ Log into your server via SFTP or SSH.
- ✓ Create a backup of the site files before making changes.
- ✓ Search your files for reference to malicious domains or payloads noted.
- ✓ Identify recently changed files and confirm whether they are legitimate.
- ✓ Review files flagged by the diff command during the core file integrity check.
- ✓ Restore or compare suspicious files with clean backups or official sources.
- ✓ Remove any suspicious or unfamiliar code from your custom files.
- ✓ Test to verify the site is still operational after changes.

CAUTION

Be careful not to overwrite the database configuration file local.xml in Magento 1.x, or app/etc/env.php in magento 2.x because this will break your site!

2.3 Remove hidden backdoors

To remove backdoors by comparing Magento files confirm your Magento version in the bottom right hand corner of your dashboard. Download the same version of known good core files from the official Magento community and log into your server via SFTP or SSH. Do not forget to create a backup of the site files before making changes.

- ✓ In your FTP client, compare your site with the known good download. Investigate any new files on your server that do not match or are not the same size as the known good files and remove any suspicious content or replace the file with a known good copy
- ✓ Log into the Magento admin panel **System > Tools > Cache Management > Flush Magento Cache** (and flush cache storage on Magento 1.x)
- ✓ Test any changes

The majority of malicious code we see uses some form of encoding to prevent detection. Aside from premium components that use encoding to protect their authentication mechanism, it's very rare to see encoding in the official Magento repository. It is critical that all backdoors are closed to successfully clean a Magento hack, otherwise your site will be re-infected quickly.

Note:

Always remember to compare files using the same Magento version and applied patches.

2.4 Reset user passwords

You should reset all user passwords with unique, strong passwords to avoid reinfection. If your magento version is unpatched, you may want to patch your site first. Attackers can steal your magento user credentials from the backend if your patches are not up to date.

To remove user passwords in Magento, log into your Magento administrator area

- ✓ System > Permissions > Users or All users > Click on any user in the list
- ✓ Enter a new password for the user in the new password and password confirmation fields
- ✓ Enter your password in the 'your password' field (if using magento 2.x) and click save user

You should reduce the number of user accounts with an administrator role for Magento. This extends to your FTP accounts and website systems. Only give users the access they need for as long as they need it.

Note:
All accounts should use strong passwords. A good password is built around three components – complexity, length, and uniqueness. Some say it's too difficult to remember multiple passwords. This is true. That's why password managers were created!

2.5 Fix Malware Warnings

If you were blacklisted by Google, McAfee, Yandex (or any other web spam authorities), you can request a review after the hack has been fixed. Google is now limiting repeat offenders who knowingly host/spread malware on their site to one review request every 30 days. Be sure your site is clean before requesting a review!

To remove malware warnings on your site call your hosting company and ask them to remove the suspension. You may need to provide details about how you removed the malware. Fill in a review request form for each blacklisting authority (i.e. Google search console, McAfee SiteAdvisor, Yandex webmaster). The review process can take several days.

Note:
You should have only one antivirus actively protecting your system to avoid conflicts. If your Magento admin user's computers are not clean, your site can get re-infected easily.

3 PROTECT THE SITE

3.1 Create a custom admin path

An unaltered path makes it easy for hackers to navigate through admin page and use Brute Force Attacks to open up gateways to guess your user name and password. It is recommended that you constantly change the admin path. But remember when you change it; don't alter the Admin Base URL settings in the admin segment of the system configuration.

- ✓ Go for a long and complicated Admin Username and Password
- ✓ Keep your Magento admin password entirely unique
- ✓ Don't save the password on your PCs and laptops
- ✓ Update your passwords before and after working with outside developers

3.2 Use Two-Factor Authentication

Two-factor authentication extensions guarantees that only trusted devices can access your Magento back-end.

This provides an extra coating of security which demands you to know your unique username, password and security code which is randomly generated. Just after 30 seconds of the entire process on a smart phone app you will be able to purchase from the Magento Connect Marketplace.

3.3 Limit Admin access to only approved IP addresses

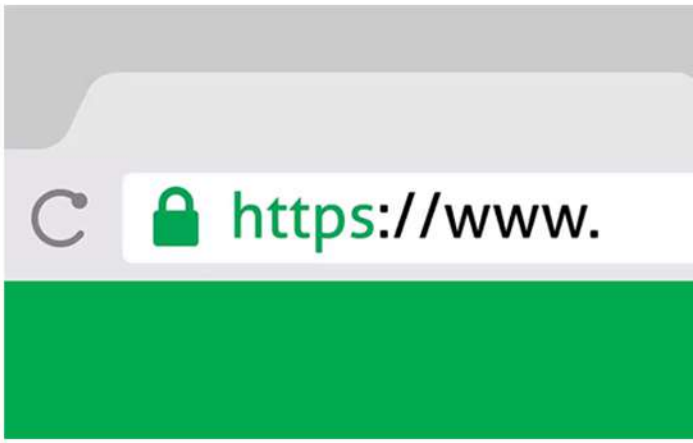
In case the points discussed above were not enough for you (because of PCI compliance requirements), then you can certainly restrict admin access to only the IP addresses you have white listed. This can be done through Apache directive Location Match:

However, in the above example always remember to change "admin" to your fresh and unique admin login page.

```
<code>
<LocationMatch "admin">
Order Deny,Allow
Deny from All
Allow from 10.10.10.0/24
</LocationMatch>
</code>
```

3.4 Require HTTPS/SSL For All Your Login Pages

Every time you use your username and password without an encryption connection, you take the risk of getting seized by a hacker. Banish this possibility by using HTTPS/SSL in Magento.



System > Configuration > Web > Secure (Here you can alter the base URL of your store) > Select 'Yes' for both 'Use Secure URLs in Admin' and 'Use Secure URLs in Front-end' > Save Config

3.5 Use a secure FTP

One of the simplest ways to hack a Magento store is to intercept an FTP password. To block this happening use secure FTP passwords and FTP-SSL (Explicit AUTH TLS) or SFTP (SSH File Transfer Protocol).

Now if you want a higher level of security, I will recommend you to use SFTP and a Public Key Authentication. Also, limit unsecured FTP access to prevent unpleasing scripts from creating havoc. Other security measures that you can take to boost the security of your website are:

- ✓ Change your file permissions
- ✓ Secure your Local.xml file
- ✓ Lock your Magento connect manager
- ✓ Disable any dangerous PHP functions
- ✓ Disable directory indexing
- ✓ Use only trusted Magento extensions

Always remember to go with the latest version of Magento. As they often come out to shield recently discovered security risks in the software. Keep your anti-virus software which is up to date. A secure website is a hassle free website which diminishes a major headache and improve the conversion rate by increasing the trust factor.

Summing it all up

This e-book sheds light on the many ways through which you can recover your hacked Magento store and some great tips to keep your store secure. The best practices include keeping your Magento and its extension versions up to date, using smart and unique usernames and passwords, custom admin login path, and SSL certificate, etc.

Most of these recommendations above can be implemented within few minutes. But if you want to keep your Magento store more secure from hackers, you will need a robust Magento hosting provider that offers you almost everything mentioned above including extra layers of security like server configuration and management, server monitoring, automated server security patches, advanced firewall protection, and a lot of other things.

Contact Us

Sales: inquiry@designnbuy.com **Support:** support@designnbuy.com

INDIA
601, Parshwanath Esquare, Corporate Road,
Nr. Prahalad Nagar Garden, Satellite, Ahmedabad – 380015, Gujarat
+91-79-66630254

USA
667, East Royal Lane, Apt 1068,
Irving, TX 75039
+1-347-647-9799

GERMANY
Alexanderplatz 4th Floor, Gontardstraße 11,
Berlin - 10178, Germany
+49-322-1421-9620