My Account Has Been Hacked What Do I Do

This article is for cPanel Accounts. Determine where your account is with this guide.

Hosting accounts can be hacked for a variety of reasons. A hack can be for the personal achievement of the hacker, to host phishing content which will steal passwords or personal data, to spread viruses or malware, or to send spam e-mail through an account. After being hacked, you will need to restore your website to a backup. Below you will find the steps for restoring a website from a backup.

1. **Restoring Backups on Site Manager**
   Please contact Support.
2. **Restoring Backups on cPanel for a cloud resller account**
   On cPanel, you can restore backups through cPanel >> R1Soft.
3. **All other accounts must be restored manually via FTP/PHPMyAdmin**

The following section will show you how to improve security on your hosting account.

Backups

Backups are one of the best ways to recover from a hacked account. WestHost creates backups every 6 hours. Backups should be available for at least the past 3-5 days. If your account has been recently hacked, you may be able to restore your site files with a backup from your cPanel >> R1Soft tool.

Backups are not guaranteed, so we recommend that you keep a local copy of the latest clean files for your website -- you should also download and maintain copies of your database files as well.

If your account was hacked before the available backups from WestHost, then the R1Soft or Site Manager backups will not retain clean versions of the content -- they will only have the cracked files.

You can create a manual cPanel backup through the cPanel >> Backups tool, which you can use later to restore through the same tool. If you need a copy of your database from backup, please do so from PHPMyAdmin. If you need a database backup restored, that is done manually and you will need to submit a support request through https://cp.westhost.com/ >> Support.

Remember that whether you are able to restore your site from a backup or not, you will want to continue reading and following the steps in this article below. If your account was hacked there IS an issue or vulnerability IN YOUR ACCOUNT that you will need to fix.

> we HIGHLY recommend your maintaining incremental backups of your account, stored off-server. You can create backups in cPanel >> Backups.

Cleaning and Prevention

Below are steps that you can take to restore your account security and prevent future possible compromise. You will want to read this section very carefully and follow its directions.

The most common method that we see used to compromise a hosting accout is vulnerabilities in user scripts, especially populare scripts such as WordPress, Joomla, or any major PHP shopping cart or content management system.

Updating

First, ensure that all script you have installed are running the latest version. Popular scripts are especially notorious for being hacked. Since so many sites use them, they are constantly being searched for vulnerabilities by hackers.

Older versions of scripts will sometimes have security vulnerabilities that have been patched by a new release.

> that any addons, plugins, modules, or themes for a script should ALSO be kept updated. Be sure that everything is the latest version and is secure from possible compromise. ALWAYS do your research before installing a 3rd-party addon, script, theme, or module.

If anyone else has had issues with a specific addon, you can usually find information about it posted online. Use your favorite search engine to look for "XYZ WordPress module vulnerability" and if you find any results -- especially concerning the latest version -- DO NOT INSTALL IT to your account.

You can update your scripts easily if you originally installed them using the Softaculous tool in cPanel. Softaculous will be able to update any script that is installed, but NOT your custom modules, themes, addons, or plugins.

Many later version of popular scripts will have easy update installers in their admin/backend areas. You usually just need to log in and follow the prompts to successfully update your account's script.

If you cannot access the Admin or Backend for your script, or the update is not working, you can visit the website for your script to find more detailed support documentation for things like hacked installs and manual updates. I have included some links at the end of this document specific to hacked popular script installs that you may find useful.

Scanning

The **Second** most common method for a hack is the use of malicious files on the computers that have account access. Many types of virus /malware/adware will look for hosting accounts and password to send to attackers.

The second step in account cleaning and security is to scan ALL computers that you use to log in to your account via cPanel, FTP, e-mail, Site Manager, etc. for malware and viruses.

After a full virus scan, WestHost highly recommends funning the free version of Malwarebytes Anti-Malware [you can download Malwarebytes from http://www.malwarebytes.org/]. This is a great application for cleaning malicious malware and adware.

File Checks

Third, be sure to check EVERY FILE that you are hosting! If the attacker has left a vulnerable file on your account, they can likely use it to gain access to your account again in the future.

Look for files that do not belong, or that you did not upload. Download and view the source code for all your files to check for suspicious or hacked script injections. Some hacks will insert malicious code at the very top or bottom or your legitimate files. This is why checking your files -- every single one -- is critical!

Permissions

Fourth, be sure that all the files on your account have the correct permissions, and are not giving too much permission. Having too much permission on a file might pose security vulnerabilities.

You can set permissions using FTP or through cPanel >> File Manager. 777 or "full permissions" should NEVER be used for files and/or directories, even when specified by installation instructions. 755 provides plenty of permissions in the place of 777.

Directories should be set to 755 by default. PHP, HTML, and the majority of all web files should have 644 permissions [or the lowest that works for your website], and ANY files that contain MySQL database or other login credentials [configuration files, usually] should be set to 400 permissions so they are ONLY readable by the account owner and the server itself.

Passwords

Fifth, and MOST IMPORTANT of any step, change ALL of your account passwords to HIGHLY SECURE PASSWORDS in order to cut off further attacker access. This includes your main account [cPanel or Site Manager] password, all e-mail account passwords, and custom FTP user account passwords. Without changing these, the attacker may not have full account access, but can still get into enough portions of your site to check for remaining vulnerabilities or to gather personal information until they ARE able to gain full access.

A large number of exploits are due to the use of weak passwords and are easily preventable. Passwords should NEVER be based on common "dictionary" words as these are easily guessed or cracked by such means as a brute force attack [guessing until they get it right]. The cPanel system has an excellent password generator, or you can use online generators to create a highly secure password like: https://secure.pctools.com/guides/password

Be extremely careful with whom you trust your password to! Be sure that anyone who has access to your account also knows to always use secure scripts, and has a malware and virus free computer.

> you should change your account passwords **AFTER** securing your computer, account files, and scripts because if a vulnerability remains in one of these places the exploit can continue to get your new password with each change.

Additional Resources

WestHost clients who use cPanel can get immediate help to resolve your hacked account. Submit a ticket to our support team and request your account is reviewed so that we can clean your account fast. If you are not using cPanel, submit a ticket to our support team to review your account for a migration to cPanel.

Google's Cleaning Your Site Guide: http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=163634

Removing Malware From Your Site: http://knoll.google.com/k/riona-macnamara/removing-malware-from-your-site/2vl8me364idq/1#

StopBadware's Information for Website Owners: http://www.stopbadware.org/home/webmasters

SPECIFIC RESOURCES FOR HACKED WORDPRESS SITES
WordPress Hacked FAQ: http://codex.wordpress.org/FAQ_My_site_was_hacked

Reset Admin Password: http://codex.wordpress.org/Resetting_Your_Password

Hardening WordPress (to avoid future hacks): http://codex.wordpress.org/Hardening_WordPress

SPECIFIC RESOURCES FOR HACKED JOOMLA SITES

Joomla! Security Hacked Site Guide: http://docs.joomla.org/Security_Checklist_7

Your Joomla! Is Hacked. Now What? http://www.instantphp.com/news/37-tips-and-tricks/133-your-joomla-is-hacked-now-what.html

Joomla! Security http://docs.joomla.org/Security

SPECIFIC RESOURCES FOR HACKED DRUPAL SITES

Drupal Security Team: My Drupal was Hacked, Now What? http://drupal.org/node/213320

Securing Drupal: http://drupal.org/security/secure-configuration