My Account Was Hacked

If your account has been hacked or compromised in some way - don't worry, we may be able to help. We offer a Managed Security Clean Up Service - for more information see our website or contact Technical Support by phone, chat, or ticket.

- How was my account hacked?
- How do I recover?
    - Helpful Links

How was my account hacked?

There are two common ways account are compromised:

1) The hacker successfully authenticated and accessed your account like a regular user. The attacker already knew your password (e.g., because your home computer has a virus or other program logging your keystrokes) or was able to guess your password (e.g., using a brute force or dictionary attack).

2) The attacker exploited a security vulnerability in a script or application installed on your account. This is most likely the case if you are running old or outdated software that has known security vulnerabilities (e.g., Joomla 1.0). This type of vulnerability can also occur in the database through a MySQL injection, as such your database integrity is also most likely compromised.

How do I recover?

To help mitigate future attacks, we recommend performing all of the following:

– Before doing anything else, run a complete computer scan for viruses and malware. Ensure that your system is running up-to-date anti-virus and anti-malware software.

– Login to your cPanel and change your main cPanel, e-mail, FTP users, and MySQL users passwords. Make sure the new passwords are secure; they should contain a mix of upper- and lowercase letters and numbers. For extra security, also add symbols or punctuation characters to your passwords. You can find out how to change your password here: How To Change Your cPanel/FTP/SSH Password

– Change the passwords for any administration-type areas of your web site (e.g., WordPress control panel, shopping cart administration).

– Visit cPanel and install any updates that are available to your installed applications. Periodically check Fantastico/Softaculous/Installatron for updates to software and install these updates as soon as they become available. Updated versions often contain important security patches.

– Check for the newest versions of scripts and applications that you've manually installed on your account. cPanel does not keep track of custom applications, so you need to periodically check the developers' website and make sure you install important security updates for all of your manually-installed scripts.

– Adjust the security settings for PHP in your php.ini file. The options for "allow_url_fopen", "allow_url_include", and "register_globals" should be set to "off" if at all possible.

– Search the Internet for further ways to secure your specific web applications. There are usually quite a few extra steps that can be taken specific to each application.

– Make frequent backups of your account files and your databases. Also keep an eye on the files within your account in general. Pay attention to files that aren't yours or recently modified files, for example. This will help ensure that your backups are usable and not infected with malicious code.

Lastly, if web browsers are giving warning message because Google is currently classifying your web site as dangerous, you'll want to create a free Google Webmaster Tools account at http://www.google.com/webmasters/. Once you have logged into your Google Webmaster Tools account and added your web site, you will be able to click on a link to request a review of your site. Google will visit your site again and verify that the malicious code has been removed, then remove the "This site may harm your computer" warnings.

Helpful Links

We have an article on protecting WordPress here.

Also, the following external links may be of use for Joomla and WordPress users:

WordPress: http://codex.wordpress.org/FAQ_My_site_was_hacked

Joomla: http://docs.joomla.org/Security_Checklist/You_have_been_hacked_or_defaced