

Contabo Guide: Phishing

Many abuse complaints are caused by unintended actions at the end of the customer. Your server might got hacked; through e.g. email, FTP, SSH user, or through a security vulnerability in your system such as a web application (or its addons/plugins).

What can I do to resolve the issue?

- Delete the harmful content shown in forwarded complaint.
- Update/patch your system and all its components.
- Change your passwords and make sure to use only strong passwords.
- Check if there are any suspicious processes or network connections to other servers.
- Check your PHP parameters and secure them if not yet done.
- Scan your server for installed rootkits.

The steps shown above mean a proper starting point to get rid of the issue, but attackers could have installed a backdoor in order to compromise your system again. Therefore, if you are unsure that you have fully resolved the issue, we recommend to reinstall your server and upload a clean backup of your files. To start a server reinstallation, please go to [Customer Control Panel](#) and hover your mouse pointer over the "Manage" button and click on the "Reinstall" button. During the reinstallation process you have to set a root/administrator password. Please use a new and strong server password.

Is Contabo responsible to secure my rented service?

At Contabo we provide unmanaged services which means that we are responsible for the provision of hardware, but maintaining and configuring servers on operating system level and above remains the responsibility of the customer.

What can I do to enhance the security of my system?

1. Maintain regular backups.
2. Keep your whole system up-to-date all the time, meaning install updates and patches of the software packages and web applications used regularly.
3. Install and run an antivirus software such as ClamAV or ClamWin to keep your server clean from malware.
4. Set up a firewall to close all ports that you do not need and to change default ports like 22 for SSH or 3389 for RDP to others.
5. Block brute force attacks by installing a suitable software such as cPHulk or Fail2ban.
6. Avoid using scripts that only work with insecure settings.
7. Never click any suspicious attachments or links in emails or visit shady websites.