How was my website or email hacked or compromised?

2024/05/03 03:56:42

FAQ Article Print

Category:	Abuse Issues	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	16:55:01 - 2015/01/26

Keywords

hacked compromised

Symptom (public)

Problem (public)

My website or email was hacked, how?

Solution (public)

Websites

Causes:
1. The most common cause of website compromisations is out of date content management systems. Many web developers do not update the content management software they have used to create websites immediately when new versions are released, nor do they update plugins they use to develop websites when new versions of them are released.

Do not immediately blame the web developer. If you bought your site development from a company, you should be paying a monthly fee for this to be taken care of. If you're not paying a monthly fee, then this is your first problem.

If your developers do not offer this service, please contact us.

Operating a website means that the owner must take the responsibility to ensure that the software running on their site stays 100% up to date, as does every other component including plugins and themes (yes, themes can introduce security vulnerabilities). Almost every website in this day and age uses a content management system, and just like your PC it must be kept 100% up to date, especially as its on the Internet and open for the world to access.

2. The second most common cause of website compromisations is when weak and default usernames and passwords are used in the CMS for the "admin" login.

3. The third most common cause is badly, incorrect, insecure CMS software setups and no security plugins. Proper setup of the CMS software to lockout hacking attempts is key and can mitigate future possible attacks, there is a wide range of plugins available for this.

Suggestions:
1. Ensure that the CMS software stays up to date. If the CMS software has an automated update feature or you have used our software installers to install it, setup automated updates. If the plugins have automatic updates, set that up. If the themes you use have automatic updates, set that up. Subscribe to the announcement mailing lists to ensure you stay up to date.

This is a service your web developer should offer. We suggest you use it. If they do not offer this service please contact us.

Within hours of a vulnerability being discovered we see probes against client sites, while a very large number is blocked by our security team who works around the clock monitoring this sort of thing and creating signatures, its certainly not a guarantee that anyone will be safe running out of date software and software with security vulnerabilities.

2. Install a security plugin, for WordPress we recommend the "Wordpress All In 1 Firewall".

3. Ensure that your CMS admin username is not the default and the password is strong and secure.

4. Regular backups. Should your site be compromised we require removal from our platforms. See our [1]Why must my site be deleted? FAQ. If you have a backup, your web designer could install it locally, update it, secure it and re-upload it. If not, your site would need to be recreated.

If you do not have anyone who can assist you with the above, please contact us.

Email

Causes:
1. Compromised user PC, keylogger, screen grabber, trojan, virus ... etc (including pirated Operating System software). The most common cause of compromised accounts is a compromised PC. If the machine the email account is setup on has been compromised or running illegal software, it is very likely that a hacker has acquired the username and password and has downloaded all the mail in the account. The most common place to find deeply embedded keyloggers, screen grabbers, trojans and viruses is illegal software downloaded off the internet.

2. The second most common causes of email account compromisation is 3rd party systems being hacked and the username/email address and password on that system being acquired by hackers. The first thing a hacker would do is try mail.<domain name> and use the password and email address they just acquired.

Suggestions
1. Run up to date PC software and anti-virus. Ensure that daily updates are done and ensure you receive alerts when updates fail so they can be done manually.

2. Ensure that strong passwords are used and do not use them in multiple places.

3. Do not run pirated software. This compromises the integrity of your system and opens you up for attack.

FAQs
- [2]My site was hacked, why must it be deleted?

- [3]Abuse Department 3 step process FAQ

[1] https://servicedesk.iitsp.com/faq/6
[2] https://servicedesk.iitsp.com/faq/2
[3] https://servicedesk.iitsp.com/faq/7