

What to do if you think your website is hacked

If you suspect there is some data on your website that you did not put there or authorize you must act immediately on this. A website hack can take many different forms. Detection early on is key to minimizing the damage done. How do I know my site been hacked.

- when your site is loading look at the bottom status bar in the browser, this will show where it is getting the data from, if there is a url with a .cn or .ru then the site has been hacked.
- the site takes longer than normal to load and when it does the page looks slightly different.
- your web browser warns there is a malicious code being downloaded and halts the opening of the site.
- data that was not entered by you appears on your site
- google search results say the site is hacked
- user actions on the website seem to take longer than normal
- your web referrer log is filled with .cn and .ru websites
- your virus control on your computer issues warnings and errors right after you visit an infected site
- auto updates on your PC have stopped happening without you stopping them
- auto updates of your virus control have stopped happening.
- a sudden spike in spam
- a sudden spike in bandwidth usage

If you notice these items or other behaviour that is not normal please notify your supplier immediately.

Willows do not repair hacked websites for free. Hack repairs are not covered by your hosting charges. Website hacks are acts of vandalism. Fixing hacks requires the setting up of a open isolated machine to allow the hacked files to be edited. This takes time to setup , edit files , clean the machine and then re-upload the site again.

Regular backups of your website are recommended.

We do not backup websites for clients.