The Egenz Guide

HOW TO PROTECT YOUR WEBSITE BEING HACKED

WEBSITE SECURITY

Is your website secure?

It is important to know how to protect your website being hacked.

Besides spending time on your marketing, you should spend time in understanding how to protect and make sure your website is secure.
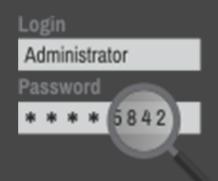
STAY UPDATED

Whether you are using open source (Wordpress, Joomla.. etc) or you build the website from scratch, always make sure it is up to date.

Make sure your theme is up to date.

If you are using 3rd party plugin or extension, make sure all the plugins stay up to date as well.

STRONG USERNAME & PASSWORD

Never use username like 'admin' and password '123456'.

It is very easy for hackers to hack into your cms (content management system).

A strong password should include a combination of alphanumeric characters, upper case, lower case, symbols and should be at least 10 characters long.

egenz.com

UPDATE YOUR PASSWORD REGULAR

It is important to update your password regularly to avoid being hacked easily.

Whenever you update your password, always make sure you update a strong password.

LIMIT WRONG LOGIN ATTEMPTS

Hackers will keep trying to login with different username and password until it is success, which we normally call brute force.

You can temporary lock the IP or the account when this happen, it will slow down the process.

There are lots of plugin or extensions able to prevent brute force, make sure you download and install it into your website.

HYPER TEXT TRANSFER PROTOCOL SECURE (HTTPS)

HTTPS://

With HTTPS, any data transfer from web server to a browser will be encrypted; hence, it is secure and protected.

HTTPS will also improve your website SEO.

Google tends to rank website with HTTPS higher than normal HTTP.

egenz.com

HIDE ADMIN DIRECTORIES

Most of the website was done with cms (content management system), make sure your admin directories not easily guess by outsiders.

Never make your admin directories indexed by search engine (Google, Yahoo, Bing).

egenz.com

SCAN REGULARLY

We may not aware when the hackers hack into your website.

You should scan your website regularly to avoid being infected by any malware or suspicious code.

If your website is infected, make sure you fix the issue instead of uploading the backup files; your website most probably will get hacked again.

BACKUP FREQUENTLY

Always have a backup file just in case your website may be hacked one day.

Back up all your files, your database, at least once a week.

For Ecommerce store, you should backup daily.

egenz

CONTACT US

You are important to us and we value your feedback.
If you have any enquiries about our services, please let us
know so that we can assist you.

Level 27, Penthouse Centrepoint North,
Mid Valley City,
59200 Kuala Lumpur.

+603 2280 6288

www.Egenz.com

info@egenz.com