WORDPRESS SAFETY CHECKLIST

Courtesy of Coder Scoop, programmers of safe web and mobile apps! https://coderscoop.com

NEVER DO THIS

- ☐ Avoid installing plugins and themes that are no longer being maintained by the author(s).
- ☐ Never use an obvious admin username, such as one generated from the website's domain. Hacker scripts will automatically check for the most likely combinations.
- ☐ Avoid installing new plugins and themes from amateur programmers as opposed to companies making a living from it, as they're the most likely to not be maintained in the future as well as having a higher chance of having security holes. Be aware that Wordpress DOES NOT check 3rd party plugins and themes for security, contrary to popular belief.
- ☐ Never use the same password in more than one of your web sites. Hackers know that people do that and will try your stolen credentials on your other sites.
- ☐ Avoid using the "kid next door" to tinker with your Wordpress site. They may very well create vulnerabilities unless they truly know what cyber security means!
- ☐ Never allow unmoderated comments, not even after an initial approved. comment. Comments are most frequently from spam bots and often bear links to malware infected sites.

ALWAYS DO THIS

- ☐ Always install the Wordfence or Sucuri plugin, or even both, and configure all available options.
- ☐ Always have your site run ONLY under https NOT http (redirect http to https). SSL certs can be obtained cheaply on sites like Namecheap.com, or even free (but those expire after only 90 days!)
- ☐ If your site has been hacked, take it offline rather than letting it potentially infect visitors with malware or being hijacked for botnet attacks.
- ☐ If you absolutely MUST use a dubious plugin or theme, check it for vulnerabilities in any of the many large vulnerability databases before activating.
- ☐ Remove plugins and themes you don't need, as even inactivated they could pose a risk.