PULKIT AGRAWAL *Managing Director, UR Digital*
LinkedIn - https://www.linkedin.com/in/pulkit-agrawal-ur-digital/
Website - https://www.urdigital.com.au

SEO expert. Top 50 Small Business Leader 2022, Top 20 Australian Digital Marketer to work with in 2022. Board Member Bayside BEC. SEO Advisor ASBAS.

TIP 1. LOOK OUT FOR WARNING SIGNS

To hack a website, cybercriminals always rely on its weak points. Cybercriminals can activate malicious bots which may subject your server to repeat tasks, which could cause it to stop serving pages. Therefore, it is critical to stay alert and pay attention to the following cyberattack warning signs that are meant to make your inner radar shout. For example: Google notifications, suspicious JavaScript Codes, error messages, etc.

TIP 2. COLLABORATIVE SECURITY

In this digital world, no organisation can rely solely on internal security. So, they share data with third parties to prevent security gaps. As a result, any successful security plan must include all parties. Include specific security policies and practices in all agreements with third parties. Follow up with yearly risk evaluations of all the third parties you share data with. Review security guidelines and make any necessary updates.

TIP 3. MONITOR YOUR WEBSITE REGULARLY

There are many advantages to regularly monitoring your website and spotting any irregularities early enough to take appropriate action and prevent unpleasant consequences. However, an SEO spam attack will lead to link indexing, so the links will not be visible in third-party tools. It is always worthwhile to check them, though. There might be something odd there, like some rare misfit language.

TIP 4. VPN - YOUR BEST FRIEND

Larger networks are much more prone to risks, so they must adhere to all accepted security standards. They must make sure that the connections are encrypted with a reliable VPN and that the traffic is controlled with the Web Application Firewall regardless of where or when they are working. It intercepts any malicious software or phishing attempts and encrypts all sensitive data to prevent their entry into your system.

TIP 5. LONG PASSWORDS

Another easiest place where hackers can attack is passwords. Use passwords that are both longer and less complicated. Any password with 12 characters or more is impossible to crack because it would take too long for a computer, or hacker, to figure it out. Convert a simple phrase into a 20-character password with extreme security. Implementing two-factor authentication is a smart move for increased security.

TIP 6. SITEMAPS

Choose the Sitemap tab from the menu on the left of Google Search Console and access the address for your sitemap. Multiple sitemap indexes may be the first unusual thing you observe. You will notice hundreds of strange spammy pages that should not be there in the case of the SEO spam attack. So, you will need to carefully review your website.

TIP 7. SCANNING TOOLS

Another aspect of cybersecurity that you should be aware of is a few tools that will enable you to keep an eye out for online threats and defend against them before they can harm your website. Free web analytics tools provide information on each bot that crawled your website, the bandwidth used, the time since the last crawl, and the total number of hits, enabling you to identify malicious activity.

TIP 8. SECURE SOCKETS LAYER (SSL)

The SSL certificate works as a barrier to your privacy. No one who looks behind it can see what is going on. Therefore, your customer's credit card numbers will be safe if they enter payment information on your website. By creating a secure, encrypted connection between the website visitor's browser and the web server, an SSL certificate (or Secure Sockets Layer) aids in the protection of information entering your website.

TIP 9. STAY UPDATED WITH THE TRENDS

It is just as simple to lose track of trends for IT and cyber security professionals as it is to keep track of them. Numerous latest trends, protocols, and general advancements are being made in this area. Create Google alerts or register for RSS feeds. It is extremely busy, but if you focus on what you need and keep up with developments, it will help you stay secure.

TIP 10. KNOW YOUR NETWORK

Last but not the least, know your networks. Excellent cyber security can be carried out without being an IT expert. Every business owner should first take the time to understand how sensitive data is stored, transferred, and entered in their system. These interconnected components serve as a focal point for your cyber security strategy and offer insight into where one's vulnerabilities lie.