All I Want for Christmas Is My Keyword Data Back via @tonynwright

[unable to retrieve full-text content]https://feedpress.me/link/13962/14163036/390327

How to Benefit from “SEO Power” of Links to Old Press Release Pages? via @martinibuster

[unable to retrieve full-text content]https://feedpress.me/link/13962/14162770/390774

Stuck in Procurement Purgatory? How to Win Big Clients for Your SEO Agency

via @seomonitor

[unable to retrieve full-text content]https://feedpress.me/link/13962/14162231/390249

Google on How it Handles Sites With Too Many Ads via @MattGSouthern

[unable to retrieve full-text content]https://feedpress.me/link/13962/14161789/390751

SEO and cybersecurity: Incorporating cybersecurity into your SEO strategy

30-second summary:

- Website security directly impacts the SEO performance of the website, as the non-compliance with the security requirements can cause low rankings or Google penalties.

- Blacklisting, malicious bots interfering with the crawling process, and spam attacks are among the main consequences of low website security.
- The “site not available” warning, the presence of strange JavaScript code, not working login credentials and frequent error messages can be the warning signs of a cyberattack on your website.
- Making security checks a part of your SEO strategy would help you create a website that is resistant to cybersecurity attacks.

Every site needs to be secure and there are no “too small” or “too unnecessary” sites for malicious attacks. Online businesses are fully centered on high search rankings for online reputation and profits. For this purpose, they often implement the most effective SEO tactics, from link building to great content marketing, to land up on the front page of Google search. Nevertheless, apart from delivering the best content to the users, Google is also aimed at making the internet a safe environment, hence placing importance on websites’ cybersecurity practices.

In fact, hacks may not only be destructive for your reputation but also for your site’s organic search performance. Hence, cybersecurity and SEO go hand in hand towards building a firm’s online reputation. If the website doesn’t mean the latest security compliance it can be blacklisted by Google, suffer from spam attacks or activities of malicious bots.

So we want to share effective advice on how to recognize the security vulnerabilities in time, how to integrate the security checks into your development strategy, why you should regularly scan your website, and how to protect your local networks.

Four main steps to improve website security

Security or the absence of security may seriously affect your SEO. We all know that the HTTP certificate is no longer a reliable way to secure the site and the HTTPS has, for the most part, become the poster boy of the security standard. In 2014, Google started to prioritize the sites with HTTPS in the search results.

Focusing on SEO and security will help your business to step on the steer of success. The struggle to improve the website's ranking and keeping it cybersecurity is common for many companies so here what we suggest:

#1: Learn to recognize the earliest warning signs

Cyber attacks can cause malicious bots activity. Bots will always represent a part of your traffic but not all bots are harmless to the site's security. Cybercriminals, however, launch bots to crawl sites in the search for vulnerable parts, data theft, or content crapping. Malicious bots use the same bandwidth as the "good" bots and normal visitors do. If your server is a subject of repetitive tasks by malicious bots, it may lead to the server to stop serving pages.

Cybercriminals always rely on the website's weak sides to hack it. Thus, it's essential to stay ahead and pay attention to the following warning signs of cyberattacks that are supposed to make your inner radar shout. Cybercriminals can cause malicious bots activity.

Google Alerts and notifications

In case you received a Google alert notification or see a "Site not available" warning in search results, we have bad

news. This is a sign that your website has been hacked. To confirm this fact, go to the Google Search Console, the Security Issues section, and look for the hacked URLs that Google has detected.

Presence of strange JavaScript code

The presence of a weird Java code in the source code of your website is a reliable alert sign. Javascript codes are often used by hackers to steal precious personal data like credit card details or passwords from your site. If you see any trace of strange-looking code, get rid of it immediately.

Your login credentials don’t work

Not hard to guess that something goes wrong when you enter the valid login info and get the “wrong password” notification. Your login credentials have been altered by cybercriminals.

You get frequent random popups or error messages

More than half of malicious attacks on websites are performed by “black” SEO’s who are aimed at improving their own site’s ranking. They target the sites with prominent search rankings and insert links or use Javascript to redirect users to their own malicious websites. SEO spamming allows scammers to use high-ranking websites in order to promote low-quality content to low masses and, consequently, push their rankings. SEO spam has several negative impacts:

1. The site will get blacklisted by the search engine.
2. The site’s spam ranking may reduce the site’s ranking
3. The business reputation will get dramatically spoiled as visitors will see lots of spamming content.

Very often hackers use cross-site scripting or insert their own code into the source code of your website to bypass its security system. So if you get any kind of these notifications, don’t ignore them. It’s time to run a serious scan in order to discover the malicious software.

#2: Make security check a part of your developing strategy

If you ever become the subject of a cyber attack, financial losses are not the only concerning consequence. The compromised website may face a range of penalties by Google and distort the search results. When potential customers will look for your website, they will most probably first meet a warning page that will dissuade them from visiting your site. Consequently, it is essential to make cybersecurity a part of your SEO strategy.

Trusting Google alerts is a good piece of advice there’s more than that to be done. Learn to predict the possible threats and control the cybersecurity level. In addition to involving your team of IT-specialists, hire one more cybersecurity professional. Only a qualified specialist will help you discover the site’s vulnerabilities and elaborate on the cyber protection strategy for your eCommerce business.

#3: Use effective scanning tools

One more way to get rid of malicious intervention is by using a file malware scanner. The system looks at the website code to check web pages for malware or strange PHP or HTML files on your server. The examples of scanners that can prevent your site from being penalized, blacklisted, and maintain your search engine rankings are Sucuri SiteCheck or Web Inspector.

In addition, open-source web analytics tools like AWStats can scan your log files for suspicious activity. This tool offers data on every bot that crawled your site, bandwidth consumed, last crawled date, and total hits, allowing you to detect malicious activity.

For example, a bot’s throughput does not exceed a few megabytes per month. If you face thousands of page hits from a single IP address within a short time period the available

bandwidth will be limited.

Finally, use tools like Ahrefs and Majestic to check your backlink profile. They will not only improve your site’s SEO but also track down unnecessary backlinks from SEO spammers.

#4: Protect your security and privacy with VPN

No matter where you are in a remote area, at home, or office, local network security should be tightened under any circumstances. A large network is highly susceptible to human error, and the risks cannot be underestimated compared to a small network. All users need to ensure that they’re compliant with all standard security measures. Despite the time and place of their work, they must ensure that the traffic is controlled with the Web Application Firewall and the connections are encrypted with a stable VPN.

There are three main ways in which a VPN significantly increases the security of your website. First, it encrypts all the sensitive data, so hackers can’t access it. Second, VPN intercepts any malicious software or phishing attempts stopping them from infiltrating your system. And third, VPNs are a must-have for companies having remote employees who might be accessing companies’ systems using public hotspots as doing that without a VPN can lead to security vulnerabilities.

Today’s market does not experience any shortage of quality VPN suppliers. So do your research and choose the VPN that would meet all of your business needs.

Conclusion

Internet security matters and it matters a lot. The security breach in your website’s operation may cause dramatic damage to the eCommerce web site’s reputation and income.

Cybersecurity needs to become a part of your SEO strategy for all eCommerce companies that want to take the leading position on the market of online sales. Now when you know that safety is crucial within the web, it’s time for the SEO and IT team to unite the forces and make up a reliable strategy that will raise the website’s ranking and maintain the security of your site.

Connie Benton is a chief content writer, guest contributor, and enthusiastic blogger who helps B2B companies reach their audiences more effectively. You can find her on Twitter at @ConnieB34412379.

More about:

https://www.searchenginewatch.com/2020/12/14/seo-and-cybersecurity-incorporating-cybersecurity-into-your-seo-strategy/

YouTube SEO for Beginners: 10 Best Practices to Get You Started via @brentcsutoras

[unable to retrieve full-text content]https://feedpress.me/link/13962/14160691/388392

Google: Sometimes Copied Content is More Relevant via @martinibuster

[unable to retrieve full-text content]https://feedpress.me/link/13962/14160321/390595

Automated Title Tag Optimization Using Deep Learning via @hamletbatista

[unable to retrieve full-text content]https://feedpress.me/link/13962/14155567/390207

Google on Penalizing Misinformation via @martinibuster

[unable to retrieve full-text content]https://feedpress.me/link/13962/14155223/390473

B2B paid search forecast: What to expect in 2021

30-second summary:

- Google surprised marketers with a few changes in 2020 – an updated search query report, new ad extensions, and new audience targeting, to name a few – which forced advertisers to adjust their SEM strategies and tactics in order to maintain or increase their ROI.
- B2B advertisers are testing and investing in different campaign types besides the traditional search and display campaigns, and are seeing good performance with Discovery Campaigns.
- In the wake of the changes Google made to the search query report in September, Dynamic Search Ads can complement existing search campaigns and improve CTR, CPC, and ROAS.
- Expect to see higher adoption of auction-time bidding, dynamic extensions, and dynamic search ads.

2020 was a tough year for many industries, but for the B2B industry, demand remained strong. Paid search budgets increased in many cases, as B2B companies invested more in digital marketing. The end of Q1 hurt performance, but things started to normalize in Q2, and we observed the usual seasonality the rest of the year.

In addition to the pandemic, Google also surprised us with a

few changes – an updated search query report, new ad extensions, and new audience targeting, to name a few. All such changes forced advertisers to adjust their SEM strategies and tactics in order to maintain or increase their ROI.

After an eventful 2020, here are 6 PPC trends B2B advertisers should watch in 2021:

1. SEM campaigns diversify

Given the high competition in the B2B space, advertisers need to differentiate themselves in order to get their target audience's attention and drive demand. B2B advertisers are testing and investing in different campaign types besides the traditional search and display campaigns. B2B advertisers are seeing a good performance with Discovery Campaigns – with CTR higher than display, and CPL more efficient than search – so we expect them to increase their investment in this campaign type in 2021.

Quick tip

When launching Discovery Campaigns, be patient. Let them run for a couple of weeks without making changes as the bidding algorithm is learning during that period and you will see fluctuations in all metrics. After that, you can prioritize the audiences that are performing well. Performance improves consistently after 4-5 weeks of launch.

2. Dynamic Search Ads (DSA) gain in popularity

DSA campaigns will become even more popular with B2B advertisers after the changes Google made to the search query report in September 2020. Now that the report includes only terms that a significant number of users searched for, and with advertisers losing visibility into low-volume keywords

that drive traffic and can generate leads, DSA campaigns offer an efficient way to find new keywords. Their search query reports can help reveal gaps in keyword coverage. DSA can complement your existing search campaigns and improve CTR, CPC, and ROAS.

Quick tip

For lead generation accounts that have strict lead and CPL goals, create separate campaigns for DSA so you have more control over the budget. Start by targeting your SEM landing pages so you can have some control over potential queries and headlines.

3. PPC managers embrace automation

More B2B advertisers are using automation tools and machine learning in order to improve performance, increase efficiency, and save time. Some of our favorite automated features – automated bidding strategies, responsive search ads, and the optimize ad rotation in Google Ads – will continue to gain popularity in 2021. We should also expect to see higher adoption of auction-time bidding, dynamic extensions, and dynamic search ads as B2B advertisers seek to optimize and scale their paid search campaigns.

Quick tip

When evaluating automated bidding strategies for lead generation accounts, don’t worry about higher CPCs as you will likely be paying more for higher quality clicks. If you are seeing a high volume of leads at a low CPL, you are going in the right direction. And always set your target CPA based on the last 30 days’ average, even if it is higher than your goal. Otherwise, you will see a decrease in lead volume.

4. YouTube ad investment increases

Online video ads have become more important for B2B marketers during COVID-19 times. B2B buyers are using online video ads more often to inform purchase decisions: 64% of B2B buyers have increased their use of online video and 51% have increased their use of search, according to eMarketer. We expect B2B advertisers to increase their YouTube investment in 2021 and to launch video campaigns both to generate brand awareness and to generate leads. In addition, B2B advertisers will invest more in creating video content – and YouTubes' new betas will make that content easier to create.

Quick tip

For a full-funnel video strategy, prioritize videos that are 6-, 15- and 30-seconds long as short videos engage users the most. Also, avoid salesy videos and try to create videos that show the personality of your brand so you can connect with your audience.

5. Mobile investment drops

Lower mobility driven by COVID-19 has decreased the number of mobile buyers while increasing time in front of computers, leading to strong desktop growth. During the pandemic, paid search desktop traffic is up 60%, while mobile traffic has dropped 7% compared to the pre-COVID period. Moreover, the conversion rate for desktop has increased by 4% while the conversion rate for mobile decreased by almost 19%.

Quick tip

Leverage automated bidding strategies to save time and prioritize the devices that are performing best. And don't forget to look at the assisted conversions report when evaluating mobile performance if you are still using last-

click attribution.

6. Paid search messaging becomes increasingly customer-centric

B2B buyers are looking for new solutions as they accelerate purchases, and are expecting more from their solution providers according to the 2020 B2B Buyer Behavior Study. So, we'll see more ads from B2B companies highlighting features, functionality, customer support services, product training, and implementation support in order to attract and engage B2B buyers. For successful SEM campaigns, promoting relevant content that speaks to industry needs will be a must.

Quick tip

If you have lead generation campaigns and prefer to drive traffic to a landing page with a form, use site links and callouts to highlight the additional services or training you have available for your customers.

With new campaign types and messaging to test, and more automation features and tools at hand, 2021 promises to be fun for B2B advertisers.

Lucia Rodas-Estrada is Senior Search Director at Merkle | DWA.

More about:

https://www.searchenginewatch.com/2020/12/10/b2b-paid-search-forecast-what-to-expect-in-2021/