Cybersecurity in SEO: How website security affects SEO performance

Website security – or lack thereof – can directly impact your SEO performance.

Search specialists can grow complacent. Marketers often get locked into a perception of what SEO is and begin to overlook what SEO *should* be.

The industry has long questioned the permanent impact a website hack can have on organic performance.

And many are beginning to question the role preventative security measures might play in Google's evaluation of a given domain.

Thanks to the introduction of the GDPR and its accompanying regulations, questions of cybersecurity and data privacy have returned to the fray.

The debate rages on. What is the true cost of an attack? To what extent will site security affect my ranking?

The truth is, a lot of businesses have yet to grasp the importance of securing their digital assets. Until now, establishing on-site vulnerabilities has been considered a different skillset than SEO. But it shouldn't be.

Being a leader – both in thought and search performance – is about being proactive and covering the bases your competition has not.

Website security is often neglected when discussing long-term digital marketing plans. But in reality, it could be the signal that sets you apart.

When was the last time cybersecurity was discussed during your SEO site audit or strategy meeting?

How does website security affect SEO?

HTTPS was named as a ranking factor and outwardly pushed in updates to the Chrome browser. Since then, HTTPS has, for the most part, become the 'poster child' of cybersecurity in SEO.

But as most of us know, security doesn't stop at HTTPS. And HTTPS certainly does not mean you have a secure website.

Regardless of HTTPS certification, research shows that most websites will experience an average of 58 attacks per day. What's more, as much as 61 percent of all internet traffic is automated – which means these attacks do not discriminate based on the size or popularity of the website in question.

No site is too small or too insignificant to attack. Unfortunately, these numbers are only rising. And attacks are becoming increasingly difficult to detect.

1. Blacklisting

If – or when – you're targeted for an attack, direct financial loss is not the only cause for concern. A compromised website can distort SERPs and be subject to a range of manual penalties from Google.

That being said, search engines are blacklisting only a fraction of the total number of websites infected with malware.

GoDaddy's recent report found that in 90 percent of cases, infected websites were not flagged at all.

This means the operator could be continually targeted without their knowledge – eventually increasing the severity of sanctions imposed.

Even without being blacklisted, a website's rankings can still suffer from an attack. The addition of malware or spam to a website can only have a negative outcome.

It's clear that those continuing to rely on outward-facing symptoms or warnings from Google might be overlooking malware that is affecting their visitors.

This creates a paradox. Being flagged or blacklisted for malware essentially terminates your website and obliterates your rankings, at least until the site is cleaned and the penalties are rescinded.

Not getting flagged when your site contains malware leads to greater susceptibility to hackers and stricter penalties.

Prevention is the only solution.

This is especially alarming considering that 9 percent, or as many as 1.7 million websites, have a major vulnerability that could allow for the deployment of malware.

If you're invested in your long-term search visibility, operating in a highly competitive market, or heavily reliant on organic traffic, then vigilance in preventing a compromise is crucial.

2. Crawling errors

Bots will inevitably represent a significant portion of your website and application traffic.

But not all bots are benign. At least 19% of bots crawl websites for more nefarious purposes like content scraping, vulnerability identification, or data theft.

Even if their attempts are unsuccessful, constant attacks from automated software can prevent Googlebot from adequately crawling your site.

Malicious bots use the same bandwidth and server resources as a legitimate bot or normal visitor would.

However, if your server is subject to repetitive, automated tasks from multiple bots over a long period of time, it can begin to throttle your web traffic. In response, your server could potentially stop serving pages altogether.

If you notice strange 404 or 503 errors in Search Console for pages that aren’t missing at all, it’s possible Google tried crawling them but your server reported them as missing.

This kind of error can happen if your server is overextended

Though their activity is usually manageable, sometimes even legitimate bots can consume resources at an unsustainable rate. If you add lots of new content, aggressive crawling in an attempt to index it may strain your server.

Similarly, it’s possible that legitimate bots may encounter a fault in your website, triggering a resource intensive operation or an infinite loop.

To combat this, most sites use server-side caching to serve pre-built versions of their site rather than repeatedly

generating the same page on every request, which is far more resource intensive. This has the added benefit of reducing load times for your real visitors, which Google will approve of.

Most major search engines also provide a way to control the rate at which their bots crawl your site, so as not to overwhelm your servers' capabilities.

This does not control how often a bot will crawl your site, but the level of resources consumed when they do.

To optimize effectively, you must recognize the threat against you or your client's specific business model.

Appreciate the need to build systems that can differentiate between bad bot traffic, good bot traffic, and human activity. Done poorly, you could reduce the effectiveness of your SEO, or even block valuable visitors from your services completely.

In the second section, we'll cover more on identifying malicious bot traffic and how to best mitigate the problem.

3. SEO spam

Over 73% of hacked sites in GoDaddy's study were attacked strictly for SEO spam purposes.

This could be an act of deliberate sabotage, or an indiscriminate attempt to scrape, deface, or capitalize upon an authoritative website.

Generally, malicious actors load sites with spam to discourage legitimate visits, turn them into link farms, and bait unsuspecting visitors with malware or phishing links.

In many cases, hackers take advantage of existing vulnerabilities and get administrative access using an SQL injection.

This type of targeted attack can be devastating. Your site will be overrun with spam and potentially blacklisted. Your customers will be manipulated. The reputation damages can be irreparable.

Other than blacklisting, there is no direct SEO penalty for website defacements. However, the way your website appears in the SERP changes. The final damages depend on the alterations made.

But it’s likely your website won’t be relevant for the queries it used to be, at least for a while.

Say an attacker gets access and implants a rogue process on your server that operates outside of the hosting directory.

They could potentially have unfettered backdoor access to the server and all of the content hosted therein, even after a file clean-up.

Using this, they could run and store thousands of files – including pirated content – on your server.

If this became popular, your server resources would be used mainly for delivering this content. This will massively reduce your site speed, not only losing the attention of your visitors, but potentially demoting your rankings.

Other SEO spam techniques include the use of scraper bots to steal and duplicate content, email addresses, and personal information. Whether you’re aware of this activity or not, your website could eventually be hit by penalties for duplicate content.

How to mitigate SEO risks by improving website security

Though the prospect of these attacks can be alarming, there

are steps that website owners and agencies can take to protect themselves and their clients. Here, proactivity and training are key in protecting sites from successful attacks and safeguarding organic performance in the long-run.

1. Malicious bots

Unfortunately, most malicious bots do not follow standard protocols when it comes to web crawlers. This obviously makes them harder to deter. Ultimately, the solution is dependent on the type of bot you're dealing with.

If you're concerned about content scrapers, you can manually look at your backlinks or trackbacks to see what sites are using your links. If you find that your content has been posted without your permission on a spam site, file a DMCA-complaint with Google.

In general, your best defense is to identify the source of your malicious traffic and block access from these sources.

The traditional way of doing this is to routinely analyze your log files through a tool like AWStats. This produces a report listing every bot that has crawled your website, the bandwidth consumed, total number of hits, and more.

Normal bot bandwidth usage should not surpass a few megabytes per month.

If this doesn't give you the data you need, you can always go through your site or server log files. Using this, specifically the 'Source IP address' and 'User Agent' data, you can easily distinguish bots from normal users.

Malicious bots might be more difficult to identify as they often mimic legitimate crawlers by using the same or similar User Agent.

If you're suspicious, you can do a reverse DNS lookup on the

source IP address to get the hostname of the bot in question.

The IP addresses of major search engine bots should resolve to recognizable host names like ‘*.googlebot.com’ or ‘*.search.msn.com’ for Bing.

Additionally, malicious bots tend to ignore the robots exclusion standard. If you have bots visiting pages that are supposed to be excluded, this indicates the bot might be malicious.

Share this article

Related articles

2. WordPress plugins and extensions

A huge number of compromised sites involve outdated software on the most commonly used platform and tools – WordPress and its CMS.

WordPress security is a mixed bag. The bad news is, hackers look specifically for sites using outdated plugins in order to exploit known vulnerabilities. What’s more, they’re constantly looking for new vulnerabilities to exploit.

This can lead to a multitude of problems. If you are hacked and your site directories have not been closed from listing their content, the index pages of theme and plugin related directories can get into Google’s index. Even if these pages are set to 404 and the remaining site is cleaned up, they can make your site an easy target for further bulk platform or plugin-based hacking.

It’s been known for hackers to exploit this method to take control of a site’s SMTP services and send spam emails. This can lead to your domain getting blacklisted with email spam

databases.

If your website's core function has any legitimate need for bulk emails – whether it's newsletters, outreach, or event participants – this can be disastrous.

How to prevent this

Closing these pages from indexing via robots.txt would still leave a telling footprint. Many sites are left removing them from Google's index manually via the URL removal request form. Along with removal from email spam databases, this can take multiple attempts and long correspondences, leaving lasting damages.

On the bright side, there are plenty of security plugins which, if kept updated, can help you in your efforts to monitor and protect your site.

Popular examples include All in One and Sucuri Security. These can monitor and scan for potential hacking events and have firewall features that block suspicious visitors on a permanent basis.

Review, research, and update each plugin and script that you use. It's better to invest the time in keeping your plugins updated than make yourself an easy target.

3. System monitoring and identifying hacks

Many practitioners don't try to actively determine whether a site has been hacked when accepting prospective clients. Aside from Google's notifications and the client being transparent about their history, it can be difficult to determine.

This process should play a key role in your appraisal of existing and future business. Your findings here – both in terms of historic and current security – should factor into

the strategy you choose to apply.

With 16 months of Search Console data, it can be possible to identify past attacks like spam injection by tracking historical impression data.

That being said, not all attacks take this form. And certain verticals naturally experience extreme traffic variations due to seasonality. Ask your client directly and be thorough in your research.

How to prevent this

To stand your best chance of identifying current hacks early, you'll need dedicated tools to help diagnose things like crypto-mining software, phishing, and malware.

There are paid services like WebsitePulse or SiteLock that provide a single platform solution for monitoring your site, servers, and applications. Thus, if a plugin goes rogue, adds links to existing pages, or creates new pages altogether, the monitoring software will alert you within minutes.

You can also use a source code analysis tool to detect if a site has been compromised.

These inspect your PHP and other source code for signatures and patterns that match known malware code. Advanced versions of this software compare your code against 'correct' versions of the same files rather than scanning for external signatures. This helps catch new malware for which a detection signature may not exist.

Most good monitoring services include the ability to do so from multiple locations. Hacked sites often don't serve malware to every user.

Instead, they include code that only displays it to certain users based on location, time of day, traffic source, and

other criteria. By using a remote scanner that monitors multiple locations, you avoid the risk of missing an infection.

4. Local network security

It’s equally as important to manage your local security as it is that of the website you’re working on. Incorporating an array of layered security software is no use if access control is vulnerable elsewhere.

Tightening your network security is paramount, whether you’re working independently, remotely, or in a large office. The larger your network, the higher the risk of human error, while the risks of public networks cannot be understated.

Ensure you’re adhering to standard security procedures like limiting the number of login attempts possible in a specific time-frame, automatically ending expired sessions, and eliminating form auto-fills.

Wherever you’re working, encrypt your connection with a reliable VPN.

It’s also wise to filter your traffic with a Web Application Firewall (WAF). This will filter, monitor, and block traffic to and from an application to protect against attempts at compromise or data exfiltration.

In the same way as VPN software, this can come in the form of an appliance, software, or as-a-service, and contains policies customized to specific applications. These custom policies will need to be maintained and updated as you modify your applications.

Conclusion

Web security affects everyone. If the correct preventative measures aren’t taken and the worst should happen, it will

have clear, lasting consequences for the site from a search perspective and beyond.

When working intimately with a website, client, or strategy, you need to be able to contribute to the security discussion or initiate it if it hasn’t begun.

If you’re invested in a site’s SEO success, part of your responsibility is to ensure a proactive and preventative strategy is in place, and that this strategy is kept current.

The problem isn’t going away any time soon. In the future, the best SEO talent – agency, independent, or in-house – will have a working understanding of cybersecurity.

As an industry, it’s vital we help educate clients about the potential risks – not only to their SEO, but to their business as a whole.

William Chalk is a cybersecurity researcher and digital privacy specialist. He covers these issues for leading tech publications to help support our digital freedoms.

Want to stay on top of the latest search trends?

Get top insights and news from our search experts.

Related reading

marketers, generating traffic and leads is the toughest challenge. Here are our

top three tips for lead generation for ecommerce businesses.

You're on a ques

t
to
im
pr
ov
e
th
e
te
ch
ni
ca
l
st
at
e
of
yo
ur
si
te
.
He
re
ar
e
ei
gh
t
of
th
e
be
st
fr
ee
te

chnical SEO tools that can help you do that.

Eight link building techniques to

add to your repertoire this year. Link building a crucial part of the SEO ecosyste

m, here’s how to get started.

How did the 2018 SERP changes impact organic list

ings? More importantly, how should you react? The year of updates in review, and

tips to respond to each.

Want to stay on top of the latest search trends?

Get top insights and news from our search experts.

Cybersecurity in SEO: How website security affects SEO performance