همه چیز دربارهٔ لیست سیاه گوگل

وارد شدن به لیست سیاه گوگل کابوسی برای تمامی صاحبان وب‌سایت است چرا که سبب کاهش شدید ترافیک ورودی و درآمد حاصل از آن می‌شود. عوامل مختلفی سبب قرارگیری وب‌سایت‌ها در این لیست می‌شود که گوگل با هشدارهایی از ورود افراد به این سایت‌ها جلوگیری و از آنان در برابر آسیب‌ها محافظت می‌کند.

در این مقاله به بررسی کامل عوامل قرارگیری در بلک لیست گوگل پرداخته و همچنین مراحل خارج شدن از آن را گام‌به‌گام آموزش خواهم داد.

اگر صاحب یک وب‌سایت هستید احتمالاً نام **لیست سیاه گوگل (google blacklist)** به گوشتان خورده است. متأسفانه روزانه هزاران سایت در این لیست قرار گرفته و بخش عمده‌ای از بازدیدکنندگان خود را از دست می‌دهند. به همین دلیل تصمیم گرفتم در این مقاله عوامل گوناگونی که سبب قرارگیری سایت یا برخی از صفحات، در بلک لیست گوگل می‌شود را به طور کامل بررسی و راه‌حل‌هایی را برای رفع این مشکل ارائه دهم.

خواندن این مقاله برای هر کسی که وب‌سایت دارد بسیار ضروری است چرا که با عوامل ایجاد کننده این مشکل آشنا شده و با خودداری از انجام آن‌ها مانع از قرار گرفتن وب‌سایت خود در لیست سیاه گوگل می‌شود؛ همچنین اگر وب‌سایتتان در بلک لیست گوگل قرار دارد، آموزش خارج شدن از بلک لیست را به صورت گام‌به‌گام توضیح خواهم داد.

بنابراین پیشنهاد من به شما این است که این مقاله جامع و کامل را از دست ندهید و تا پایان همراه من باشید.

منظور از لیست سیاه گوگل چیست؟

روزانه میلیون‌ها نفر در رابطه با مسائل مختلفی در گوگل جست‌وجو می‌کنند که پاسخ‌شان در وب‌سایت‌ها قرار دارد. گوگل برای ارائه خدمات ایمن و جلوگیری از بروز هرگونه مشکل امنیتی، برخی از وب‌سایت‌ها را در لیست سیاه گوگل یا بلک لیست گوگل قرار می‌دهد.

وب‌سایت‌هایی که در این لیست قرار دارند عمدتاً دارای مشکلات امنیتی، نصب بدافزارها و غیره هستند که سبب آسیب رساندن به بازدیدکنندگان می‌شوند. در حالت کلی می‌توان گفت که گوگل این وب‌سایت‌ها را خطرناک شناسایی کرده و مانع از ورود بازدیدکنندگان به آن‌ها می‌شود. نتیجه این کار کاهش شدید ترافیک ورودی برای سایت است. البته توجه داشته باشید که برخی اوقات صاحبان وب‌سایت از سر بدشانسی (مانند نصب پلاگین آلوده، هک شدن سایت و غیره) سر از این لیست در می‌آورند.

شایان ذکر است که علاوه بر گوگل، آنتی‌ویروس‌های متعلق به شرکت‌های MCAfee ، AVG Avast و غیره نیز این وب‌سایت‌ها را در بلک لیست خود قرار می‌دهند و مانع از ورود بازدیدکنندگان به آن‌ها می‌شوند. گوگل روزانه حدود ۱۰ هزار وب‌سایت مشکوک را قرنطینه کرده و آن‌ها در لیست سیاه خود قرار می‌دهد. قرار گرفتن در این لیست برای وب‌سایت‌ها، اتفاقی بسیار تلخ و ناراحت‌کننده است چرا که سبب کاهش شدید تعداد بازدیدکنندگان و میزان فروش می‌شود. زمانی که وب‌سایتی در این لیست قرار گیرد در حالت کلی ممکن است دو اتفاق رخ بدهد:

- تا زمانی که صاحب وب‌سایت تمامی صفحاتی که در بلک لیست گوگل هستند را خارج نکند، سایر صفحات سالم نیز در نتایج جست‌وجو نشان داده نمی‌شود و همین امر سبب کاهش شدید بازدیدکنندگان می‌شود.

- زمانی که می‌خواهید به صفحاتی که در لیست سیاه گوگل هستند مراجعه کنید، مرورگرهای وب پیامی هشدار دهنده نمایش داده و مانع از ورودتان می‌شوند.

۶ روش برای تشخیص قرار گرفتن وب سایتتان در لیست سیاه گوگل

اگر میزان بازدیدکنندگان وب‌سایتتان به تازگی بسیار کاهش یافته و نمی‌دانید علت آن چیست، ممکن است در بلک لیست گوگل قرار گرفته باشید. همانطور که گفتم این یک احتمال است و شاید دلایل دیگری سبب این امر شده باشد. به همین دلیل در ادامه شش روش برای تشخیص قرارگیری در این لیست را معرفی خواهم کرد تا اگر در این لیست قرار دارید از این موضوع آگاه و نسبت به رفع این مشکل سریعاً اقدام کنید:

۱. ارور به هنگام سرچ کردن

شاید برای شما هم پیش آمده که در رابطه با موضوعی در گوگل جست‌وجو کرده و زمانی که به یکی از وب‌سایت‌ها مراجعه می‌کنید با پیام «This site may harm your computer» مواجه شده‌اید. در این حالت سایتی که به آن مراجعه کرده‌اید، در لیست سیاه گوگل یا همان بلک لیست گوگل قرار دارد. بنابراین می‌توان گفت که اگر زمانی بر روی سایت خودتان در بین نتایج کلیک کرده و با این پیغام مواجه شوید به این معنا است که در بلک لیست قرار گرفته‌اید. البته شایان ذکر است که علاوه بر هشدار گفته شده، هشدارهای دیگری نیز وجود دارد که متداول‌ترین آن‌ها عبارتند از:

- The site ahead contains malware/harmful programs
- ! Reported Attack Page
- Danger Malware Ahead
- This website has been reported as unsafe

همچنین توجه داشته باشید که اگر گوگل متوجه شود شما در قبال از بین بردن و رفع مشکلات ناشی از عوامل مخربی که در سایتتان وجود دارد، کاری انجام نمی‌دهید برای جلوگیری از ورود افراد به وب‌سایتتان هشداری همانند تصویر زیر نیز نمایش می‌دهد. این تصویر به معنای این است که سایتتان هک شده است.

۲. تغییرات در ظاهر یا پایگاه داده سایت

یکی دیگر از راه‌ها برای تشخیص اینکه آیا وب‌سایتتان در لیست سیاه گوگل قرار دارد یا خیر، توجه به تغییرات است. در صورتی که تغییرات مشکوکی در فایل‌های پایگاه داده یا ظاهر سایتتان ایجاد شده ممکن است فایل‌های مخربی در آن‌ها وجود داشته و سبب قرارگیری وب‌سایتتان در بلک لیست شده باشد.

۳. ارور آنتی ویروس

زمانی که شما از وب‌سایتی بازدید می‌کنید، آنتی‌ویروس‌تان با نمایش هشداری شما را از این کار منع می‌کند. در این حالت یعنی وب‌سایتی که به آن مراجعه کرده‌اید، دارای عوامل مخربی است که می‌تواند سبب آسیب رسیدن به کامپیوتر شما شود. خلاصه کلام، این وب‌سایت در لیست سیاه گوگل قرار دارد! اگر هنگام مراجعه به وب‌سایت خود با این ارور مواجه می‌شوید، یعنی در بلک لیست هستید.

۴ .مسدود شدن هاست

اگر سرور هاست بدون هیچ هشداری حساب کاربری شما را به حالت تعلیق درآورده و آن را غیرفعال کرده، این مورد یکی دیگر از احتمالات قرار داشتن سایتتان در بلک لیست گوگل است. به طور کلی عوامل مختلفی برای مسدود شدن حسابتان در سرور هاست وجود دارد که یکی از آن‌ها هک شدن سایتتان است. زمانی که سایتی هک می‌شود، امکان دستکاری آن توسط هکرها و قرار دادن بدافزارهای آلوده بر روی سایت بسیار افزایش می‌یابد. بنابراین شما باید سایتتان را از این عوامل مخرب پاکسازی و سپس از لیست سیاه گوگل خارج کنید.

یکی از این راه‌ها استفاده از آپشن Virus Scanner در سی پنل هاست می‌باشد.

۵ .سرچ کنسول

اگر هنوز هم کاملاً مطمئن نیستید که وب‌سایتتان در بلک لیست گوگل قرار دارد یا خیر، آخرین راه برای شما مراجعه به سرچ کنسول گوگل است. شما باید به قسمت Manual Actions یا Security Issues مراجعه کرده و به دنبال لینک‌هایی بگردید که سبب تشخیص وب‌سایتتان به عنوان یک سایت هک شده از طرف گوگل باشد.

اگر شما قادر به دیدن محتوای هک شده در لینک‌های سرچ کنسول نیستید، ممکن است محتوای هک شده از روشی به نام کلاکینگ (Cloaking) استفاده کنند. کلاکینگ روشی در سئو است که به زبان ساده یعنی محتوای ارائه شده به مخاطب با محتوای ارائه شده به موتور جست‌وجو متفاوت است. در نتیجه، این نوع بدافزار از شناسایی در امان می‌ماند. برای بررسی اینکه آیا در وب‌سایتتان از روش کلاکینگ استفاده می‌شود یا خیر باید از Hacked Sites Troubleshooter استفاده کنید و قابل ذکر است که این یک سرویس متعلق به گوگل است.

۶ .استفاده از Google Transparency Report service

برای اطمینان خاطر می‌توانید از سرویس دیگر گوگل با نام Google Transparency Report استفاده کنید. با استفاده از این سرویس می‌توانید صفحاتی که دارای محتوای مخرب هستند را به آسانی شناسایی کرده و تمرکزتان را برای حل مشکل بر روی آن‌ها قرار دهید. این سرویس برای وب‌سایت‌هایی که دارای صفحات زیادی هستند بسیار کاربردی است.

۶ عامل که سایت شما را در لیست سیاه گوگل قرار می دهد

به طور کلی تمام موتورهای جست‌وجو همانند گوگل، بینگ و غیره وب‌سایت‌ها را رصد کرده و در صورتی که شامل بدافزار، تروجان، اسپم سئو و غیره باشند، در لیست سیاه قرار می‌دهند که این کار بسیار به نفع بازدیدکنندگان است. اگر وب‌سایتتان در این لیست قرار دارد نگران نباشید، با انجام دادن یک سری کارها می‌توانید به آسانی از این لیست خارج و دوباره در رتبه‌بندی گوگل جای بگیرید.

اولین گام برای خارج شدن از این لیست، آشنایی با عوامل ایجادکننده آن است. در ادامه مهم‌ترین موارد را که می‌تواند سبب وارد شدن شما به بلک لیست شود را توضیح می‌دهم:

۱ .نرم افزارهای Malware

به زبان سادهMalware ها نوعی نرم‌افزار با کدهای زیان‌آور در وب‌سایت‌ها هستند که اگر بازدیدکنندگان، آن‌ها را دانلود کنند، سبب آسیب به کامپیوترهایشان شده (البته برخی اوقات این کار به صورت اتوماتیک انجام می‌شود) و مشکلات امنیتی برایشان ایجاد خواهد شد. به همین دلیل اگر وب‌سایت شما شامل این بدافزارها باشد یا به

بدافزارها لینک بدهد، گوگل آن را در لیست سیاه قرار می‌دهد و هشداری همانند تصویر زیر نشان خواهد داد. البته ممکن است شما از وجود این بدافزارها در وب‌سایتتان بی‌اطلاع باشید که جای نگرانی نیست، زیرا در ادامه این مقاله روش خارج شدن از بلک لیست گوگل را به صورت گام‌به‌گام توضیح خواهم داد تا وب‌سایتتان به حالت عادی بازگردد.

۲. استفاده از عناصر فریبنده

سایت فریبنده به سایتی گفته می‌شود که در آن از عناصری برای فریب دادن گوگل یا بازدیدکننده‌ها استفاده می‌شود. به عنوان مثال زمانی که از دکمه پخش در یکی از صفحات وب‌سایت استفاده شده اما به جای پخش کردن فایل صوتی، سبب بارگیری یا دانلود فایلی می‌شود به آن عنصر فریبنده گویند.

در مثالی دیگر می‌توان به مواردی اشاره کرد که شما به بازدیدکننده می‌گویید این لینک شما را به صفحه X هدایت خواهد کرد اما به صفحه Y هدایت می‌شود.

۳. استفاده از تکنیک های سئو کلاه سیاه

تکنیک‌هایی در سئو وجود دارد که هدفشان فریب دادن گوگل و به دست آوردن جایگاه در کمترین زمان است، به این روش‌ها سئو کلاه سیاه گفته می‌شود.

اگر می‌خواهید بیشتر در مورد این تکنیکها بدانید این مقاله را مطالعه کنید.

ممکن است سئوکار سایتتان از تکنیک‌های کلاه سیاه برای افزایش رتبه صفحات یا سئو وب‌سایتتان استفاده کرده و این کار او سبب قرارگیری وب‌سایتتان در بلک لیست گوگل شده است. از شایع‌ترین روش‌ها برای سئو کلاه سیاه می‌توان به موارد زیر اشاره کرد:

- بهینه سازی بیش از حد سایت، مانند تکرار بیش از حد کلمات کلیدی
- استفاده از کلاکینگ
- قرار دادن لینک و متن غیرقابل مشاهده و غیره

۴. کپی کردن مقالات و تصاویر

اگر شما از تصاویری که حق کپی رایت دارند یا برای تولید محتوا از مقالات وب‌سایت‌های دیگر استفاده کنید، در این صورت امکان قرار گرفتن شما در لیست سیاه گوگل وجود دارد. برای جلوگیری از بروز این مشکل باید پیش از افزودن تصویر، ویدئو، متن و غیره به وب‌سایتتان، از عدم تعلق داشتن آن به شخصی دیگر اطمینان حاصل کنید.

در صورتی که این مطالب مربوط به شخص دیگری باشند، وی با شکایت شما به گوگل می‌تواند سبب ورودتان به بلک لیست گوگل شود.

۵. هک شدن وب سایت

شاید شما هم در این لیست قرار گرفته‌اید و با خود می‌گویید که من همه چیز را مطابق اصول گوگل انجام می‌دادم، پس مشکل از کجاست؟

جواب آن ساده است، شاید شما هک شده‌اید!

بنابراین باید در گام اول نسبت به امن بودن وب‌سایتتان اطمینان حاصل کنید زیرا ممکن است شما اقدامات لازم را جهت تأمین امنیت سایتتان انجام نداده و سایتتان هک شده یا دامنه‌تان دزدیده شده باشد. در این حالت شخصی وبسایتتان را هک و نرم‌افزار مخرب را وارد سایتتان کرده و سرانجام سبب قرار گرفتن سایت شما در لیست سیاه گوگل شده است. هک شدن سایتتان دلایل گوناگونی می‌تواند داشته باشد که برخی از آن‌ها عبارتند از:

- استفاده از رمز عبور ساده
- استفاده از اتصالات ناامنFTP
- آسیب‌پذیری برنامه‌های وب
- عدم امنیت کافی سرور

۶ .فیشینگ

برخی اوقات ممکن است هکرها بر روی وب‌سایتتان لینک‌های فیشینگ قرار دهند و با استفاده از آن‌ها اطلاعات مختلف کاربران را جمع‌آوری و به سرور مخصوص خود بفرستند. یکی از متداول‌ترین کارهایی که با استفاده از این لینک‌ها انجام می‌شود، جمع‌آوری اطلاعات بانکی کاربران است.

اگر می‌خواهید بیشتر در مورد فیشینگ چیست بدانید این مقاله را مطالعه کنید.

۶ گام برای حذف بدافزارها

تا این قسمت از مقاله متوجه شدید که یک وب‌سایت زمانی در لیست سیاه گوگل قرار می‌گیرد که بدافزارهای مختلفی بر روی سایت نصب یا سایت هک شده باشد. بنابراین برای رفع این مشکلات دو راه دارید:

- **اگر دانش و مهارت کافی در این زمینه دارید، خودتان این کار را انجام دهید.**
- **در صورت نداشتن اطلاعات کافی، این کار را به یک فرد ماهر و کاربلد بسپارید.**

اگر تصمیم دارید که خودتان این مشکل را حل کنید و دوباره وب‌سایتتان را به حالت عادی بازگردانید، لازم است تا مراحل زیر را به صورت کامل دنبال کنید تا سایت خود را از لیست سیاه گوگل نجات دهید:

گام اول: تأیید کردن مالکیت دامنه

برخی اوقات گوگل تصور می‌کند وب‌سایت هک شده به همین دلیل باید مالکیت وب‌سایتتان را تأیید کنید. برای این کار کافی است طبق توضیحاتی که گوگل در صفحه Verify your site ownership ارائه کرده است، عمل کنید. البته توجه کنید که اگر نتوانید این کار را به درستی انجام دهید ممکن است دسترسی‌تان به گوگل آنالیتیکس و سرچ کنسول را از دست بدهید (اگر این مشکل برایتان وجود ندارد، می‌توانید از این مرحله عبور کنید).

گام دوم: سرچ کنسول

وب‌سایتتان را با استفاده از سرچ کنسول چک کنید تا از اینکه تمامی بدافزارها و عوامل مخرب حذف شده‌اند، اطمینان حاصل کنید. برای این‌کار از قسمتSecurity Issues ، می‌توانید تمامی مشکلات موجود در وب‌سایتتان را متوجه شوید تا بتوانید به بهترین شکل آن‌ها را حل و سایتتان را از لیست سیاه گوگل خارج کنید. همچنین از این پس باید از انجام دادن عواملی که سبب قرارگرفتن شما در این بلک لیست گوگل شده خودداری کنید و امنیت وب‌سایتتان را افزایش دهید.

گام سوم: بررسی فایل های مهم

هکرها به برخی از فایل‌های مهم توجه بیشتری داشته و اغلب از آن‌ها برای قرار دادن بدافزارهای خود استفاده می‌کنند، بنابراین شروع از این موارد برای پاکسازی عوامل مخرب موجود در سایت، می‌تواند گزینه خوبی باشد. این فایل‌های مهم عبارتند از:

- Index file در این فایل که اکثر مواقع به صورت index.php است، به سربرگ و پاورقی آن توجه کنید و در صورتی که کدهای غیرقابل شناسایی و متن غیرقابل فهم وجود دارد، آن‌ها را حذف کنید.
- htaccess file در این فایل اغلب هکرها مواردی را قرار می‌دهند که سبب هدایت بازدیدکنندگان به وب‌سایت‌های مخرب شده و همین امر سبب قرارگیری وب‌سایتتان در لیست سیاه می‌شود.
- Functions & wp-config در صورتی از وردپرس برای ساخت وب‌سایت خود استفاده می‌کنید، این فایل را به دقت بررسی کنید تا اطلاعات مشکوکی در آن وجود نداشته باشد چرا که حاوی اطلاعات بسیار مهم است.

گام چهارم: بررسی جداول پایگاه داده

یکی دیگر از مواردی که باید به دقت بررسی شوند جداول پایگاه داده‌ها است. هکرها اغلب از اسکریپت‌های مخرب در پایگاه داده برای گرفتن اطلاعات کاربران استفاده می‌کنند. در حالت کلی باید جداول از نظر اینکه دارای کد مخرب هستند یا خیر بررسی شوند و در صورت وجود موارد مشکوک، حذف شوند.

گام پنجم: پلاگین های معیوب

اگر وب‌سایتتان را با استفاده از وردپرس ساخته‌اید، ممکن است پلاگین‌های نصب شده حاوی بدافزار باشند. اگر مشکل از پلاگین باشد، در سرچ کنسول خود می‌توانید از قسمت Security متوجه این موضوع بشوید. بنابراین در صورتی که مشکل از پلاگین باشد سریعاً آن را حذف کنید و از نصب دوباره آن خودداری کنید تا مشکل‌ساز نشود.

گام ششم: نصب پلاگین امنیتی

یکی دیگر از راهکارهای خوب برای حذف بدافزارها، نصب پلاگین‌های امنیتی همانند Sucuri است. این نوع از پلاگین‌ها به صورت دوره‌ای محتوای وب‌سایتتان را از نظر وجود بدافزارها چک و در صورت وجود، آن‌ها را حذف خواهند کرد. توجه داشته باشید برای اینکه پلاگین نصبی‌تان دوباره سبب قرارگیری شما در لیست سیاه نشود، باید آن را از سایت رسمی وردپرس به آدرس WordPress.org دانلود و نصب کنید.

چگونه وب سایت خود را از لیست سیاه گوگل خارج کنیم؟

اگر تمامی اقدامات بالا را به درستی انجام داده‌اید، در این مرحله نوبت به آن رسیده که به گوگل اطلاع دهید تا وب‌سایتتان را از لیست سیاه حذف کند و دوباره آن را در نتایج نمایش دهد. برای این کار کافی است مراحل زیر را گام‌به‌گام جلو ببرید:

- وارد سرچ کنسول شده و بر روی قسمت Security Issues کلیک کنید.
- از اینکه تمامی مشکلات موجود حل شده‌اند، اطمینان حاصل کنید و در صورت حل آن‌ها بر روی گزینه «I have fixed these issues» کلیک کنید.

- بر روی گزینه‌ای با عنوان «Request A Review» کلیک کنید و توضیح دهید که چه کارهایی را برای رفع این مشکل انجام داده‌اید.
- حالا بر روی گزینه «Manual Actions» کلیک کنید.

زمانی که این کارها را انجام دادید، گوگل وب‌سایتتان را چک خواهد کرد تا از حذف شدن تمامی عوامل مخرب اطمینان حاصل کند. البته این روند ممکن است چند روز طول بکشد. در صورتی که مشکلی وجود نداشته باشد وب‌سایتتان از این لیست سیاه خارج، تمامی پیام‌های هشداردهنده حذف و وب‌سایتتان در نتایج جست‌وجو نمایش داده خواهد شد.

شایان ذکر است که وب‌سایتتان در صورت وجود مشکلاتی مانند بدافزارها و غیره دوباره می‌تواند در بلک لیست گوگل قرار گیرد به همین دلیل باید پیوسته وب‌سایتتان را از این نظر چک کنید و امنیت آن را قوی‌تر کنید.

بلک لیست گوگل کابوسی برای صاحبان وب سایت ها

وب‌سایت‌هایی که عوامل مخرب دارند در لیستی به نام لیست سیاه گوگل قرار می‌گیرند. نتیجه ورود سایت‌ها به این لیست، ممانعت از ورود بازدیدکنندگان به آن‌ها بوده به همین دلیل ترافیک ورودی سایت به شدت کاهش می‌یابد. از عوامل مهمی که سبب قرارگیری سایت در بلک لیست گوگل می‌شود می‌توان به نصب بدافزارها، هک شدن، فیشینگ، تکنیک‌های کلاه سیاه سئو و غیره اشاره کرد. برای خارج شدن از این لیست باید عوامل مخرب را حذف و سپس به گوگل از طریق سرچ کنسول، اصلاح شدن این موارد را اطلاع دهید تا وب‌سایتتان به حالت قبل برگردد و در نتایج نمایش داده شود.