

Overcoming 4 black hat SEO techniques that spammers and scammers use to harm your search rankings

This might come as an utter shock, but not everyone on the web plays by the rules.

The dark side of SEO can be particularly crippling to a business if they aren't aware of how to fight back.

All those algorithms Google and other search engines use to identify sites that demonstrate genuine value to its audience – and to reward accordingly with higher search rankings – also include mechanisms to suppress sites that do a poor job at offering relevant, useful information.

Unfortunately, competitors, scammers, and other disgruntled parties that want to digitally damage a business' reputation have a number of negative SEO techniques at their disposal.

Here are four negative (or black hat) SEO tactics to keep a keen eye out for, and how you can protect your site – and your business – from being a victim.

1) Link farms and spammy backlinks have framed your site as the bad guy

In this particularly infuriating technique, bad actors will use link farms to direct high volumes of spam-quality links to your site. The attacker's goal here is making it look like *your* site is trying to cheat the algorithms with a horrendously executed link-building campaign. Yes, it's a digital frame job.

The malicious party will likely repeat content associated with the backlinks across a range of sites that themselves have negative reputations. By doing so, the search algorithms are certain to flag your site as engaging in bad SEO practices, and you will be penalized accordingly.

Checking for potential spammy backlinks

Your solution: Link monitoring and reporting

Up-to-date and accurate knowledge of where your website's traffic is coming from is critical to stopping this. Recognizing a negative SEO backlink campaign in its earliest stages will help mitigate its detrimental effects.

Allowing it to proceed unchallenged for even a few weeks can result in significant damage to your site's reputation that will be much more difficult to repair.

Active link monitoring is also a good habit to get into to proactively combat link farms and nefarious backlinks. When bad links point to your site, submit a list of the domains through Google Search Console and disavow these backlinks. Do this regularly to ensure that any spam links from unscrupulous domains do not influence your search rankings.

2) Someone is duplicating your original content and spreading it with link farms

High-quality content takes a good deal of effort to create, so perhaps it's no surprise that other sites might be tempted to copy it from yours and present it as their own.

This is, of course, copyright infringement, and it is bad enough when done just for the benefit of the stolen content itself.

However, black hat SEO types like to take it a step further by scraping content *before* search engines crawl it. They then duplicate the content across link farms so that confused search engines actually penalize *your* site for posting spammed blog posts, whitepapers, or whatever great content you created.

Your solution: Report copyright infringement immediately

Again, vigilance is the answer. When you find that your content is being used elsewhere, an appropriate first step is to contact the site and let them know.

Ideally at this point, a known content contributor is responsible and the website's management was wholly unaware (and will gladly take down what is not rightfully theirs).

If that option is exhausted and you still have an issue, however, the search engines need to be made aware. Use Google's Online Copyright Infringement form to establish yourself as the rightful owner of the content in question; doing so will protect your site from SEO penalties related to that content.

Share this article

Related articles

3) Your site is hacked and content has been altered

Hacking and malware attacks are growing concerns for just about any website today, but the subtle application of these methods to harm your SEO may come as a surprise to many.

This technique is especially dangerous because it may go completely unnoticed: attackers that gain access to your site may target older or less viewed pages, or they might make changes that aren't apparent on the surface.

A malicious actor with access to your site – perhaps the lifeblood of your business – is a scary prospect. They might fill your site with duplicated, low-quality, or unwholesome content that is sure to be flagged by search engines. Links on your webpages might also be redirected to problematic external sites.

Making matters worse, your content can be altered in several kinds of ways, including at the HTML level where only a careful look at the code can reveal what has actually been done.

Your solution: Site audits and monitoring

A watchful eye on webpage performance across your site can usually expose any anomalies caused by hacked content. For example, traffic spikes on pages with normally consistent traffic, new backlinks to old pages, abnormal backlinks, or ranking increases for abnormal keywords can be telltale signs of subtle content changes that need to be investigated.

Websites should also be sure to take care in controlling access to content. It is not unheard of in these situations that the culprit is actually a former employee or contributor, intent on causing mayhem by using legitimate credentials that should have been revoked when the business (and the site) parted ways with them.

4) Fake reviews are bringing down your company's reputation

It remains relatively easy to fill review sites such as Yelp, Google, and a host of others with false and/or negative sentiments in an effort to discredit a business. These efforts can absolutely reduce your local SEO, which will almost assuredly hamper web traffic and sales.

Fake reviews can be recognized by a few typical attributes. A sudden spike in negative reviews, with no corresponding event to explain them, should immediately be suspect. Negative reviews all posted in the same window of a few hours or days are worth investigating as well.

Fake reviews tend to be short and not very descriptive, since there's no actual experience for them to describe. The reviewers' profiles offer clues as well: if a reviewer lacks a history of posting reviews, it may well be an account created specifically for this negative SEO attack.

Your solution: Report fake reviews

Any business can expect some degree of negative feedback, and most might even view it as useful criticism when appropriate. However, fake reviewers don't require feedback or courtesy.

Review sites – including Google and Yelp, two of the most important to many businesses and their SEO – usually offer the review subject a mechanism for flagging fake reviews. Protect your site by being diligent in doing so.

The solutions above contain a clear running theme: the price of freedom from negative SEO is constant vigilance. By monitoring key metrics of your site and your digital presence (and taking swift action when necessary), you can keep your site and its standing with search engines safe no matter what black hat SEO types try.

Kim Kosaka is the Director of Marketing at alexa.com, whose tools provide insight into digital behavior that marketers use to better understand and win over their audience.

Want to stay on top of the latest search trends?

Get top insights and news from our search experts.

Related reading

Ri
ch
re
su
lt
s
ar

e
th
e
se
ar
ch
re
su
lt
s
wh
ic
h
ha
ve
a
li
tt
le
ex
tr
a
pa
na
ch
e,
in
wh
ic
h
Go
og
le
di
sp
la
ys

more information about the results rather than just the traditional little, UR L an

d
me
ta
de
sc
ri
pt
io
n.
In
th
is
gu
id
e,
we
'll
ll
lo
ok
at
wh
at
's
ne
w
wi
th
ri
ch
re
su
lt
s
in
20
18

,
as
we
ll
as
ho
w
to
gi
ve
yo
ur
se
lf
th
e
be
st
ch
an
ce
of
ge
tt
in
g
th
em
.

Sl
ow
-
lo
ad
in
g

we
b
pa
ge
s
ca
n
sl
ow
ly
be
co
me
th
e
le
ad
in
g
ca
us
e
of
hi
gh
bo
un
ce
ra
te
s,
lo
w
us
er
en
ga

ge
me
nt
,
lo
st
tr
af
fi
c
op
po
rt
un
it
ie
s,
an
d
ab
an
do
ne
d
sa
le
s
jo
ur
ne
ys
.
If
yo
u
ha
ve

a
Wo
rd
Pr
es
s
si
te
,
th
er
e
ar
e
a
nu
mb
er
of
ea
sy
an
d
ef
fe
ct
iv
e
me
th
od
s
yo
u
ca
n
us

e
th
at
wi
ll
si
gn
if
ic
an
tl
y
in
cr
ea
se
yo
ur
si
te
's
lo
ad
in
g
sp
ee
d.

Wh
er
e
is
th
e
bi
gg

es
t
op
po
rt
un
it
y
in
ma
rk
et
in
g
at
th
e
mo
me
nt
?
Wi
th
3.
5
bi
ll
io
n
se
ar
ch
es
pe
r
da
y

be
in
g
ca
rr
ie
d
ou
t
by
Go
og
le
,
no
t
to
me
nt
io
n
on
ve
rt
ic
al
-
sp
ec
if
ic
we
bs
it
es
li
ke

Amazon,
YouTube
and
Pinterest,
there
is
a
huge
sea
of
data
available
on
customer

in
te
nt
wh
ic
h
ma
rk
et
er
s
sh
ou
ld
be
ta
ki
ng
ad
va
nt
ag
e
of
.

Cl
ic
k-
th
ro
ug
h
ra
te
(C
TR

)
has
historically
been
an
important
factor
in
gauging
the
quality
of
results
in

in
fo
rm
at
io
n
re
tr
ie
va
l
ta
sk
s
—
an
d
se
ar
ch
is
no
ex
ce
pt
io
n.
Bu
t
to
tr
ul
y
un
de
rs
ta

nd
ho
w
Go
og
le
in
te
rp
re
ts
“s
uc
ce
ss
”
in
se
ar
ch
re
su
lt
s,
we
ne
ed
to
un
de
rs
ta
nd
so
me
th
in

g
ca
ll
ed
se
ar
ch
sa
ti
sf
ac
ti
on
.

<https://searchenginewatch.com/2018/02/21/overcoming-4-black-hat-seo-techniques-that-spammers-and-scammers-use-to-harm-your-search-rankings/>