KrebsonSecurity

In-depth security news and investigation

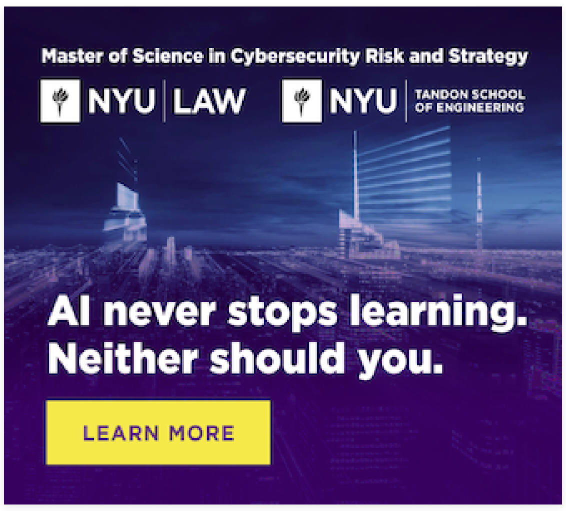
HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Bad .Men at .Work. Please Don’t .Click

June 11, 2018 79 Comments

Web site names ending in new top-level domains (TLDs) like **.men**, **.work** and **.click** are some of the riskiest and spammy-est on the Internet, according to experts who track such concentrations of badness online. Not that there still aren’t a whole mess of nasty **.com**, **.net** and **.biz** domains out there, but relative to their size (i.e. overall number of domains) these newer TLDs are far dicier to visit than most online destinations.

There are many sources for measuring domain reputation online, but one of the newest is The 10 Most Abused Top Level Domains list, run by **Spamhaus.org**. Currently at the #1 spot on the list (the worst) is .men: Spamhaus says of the 65,570 domains it has seen registered in the .men TLD, more than half (55 percent) were “bad.”



Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Recent Posts

Booking.com Phishers May Leave You With Reservations

Change Healthcare Breach Hits 100M Americans

The Global Surveillance Free-for-All in Mobile Ad Data

Brazil Arrests ‘USDoD,’ Hacker in FBI Infragard Breach

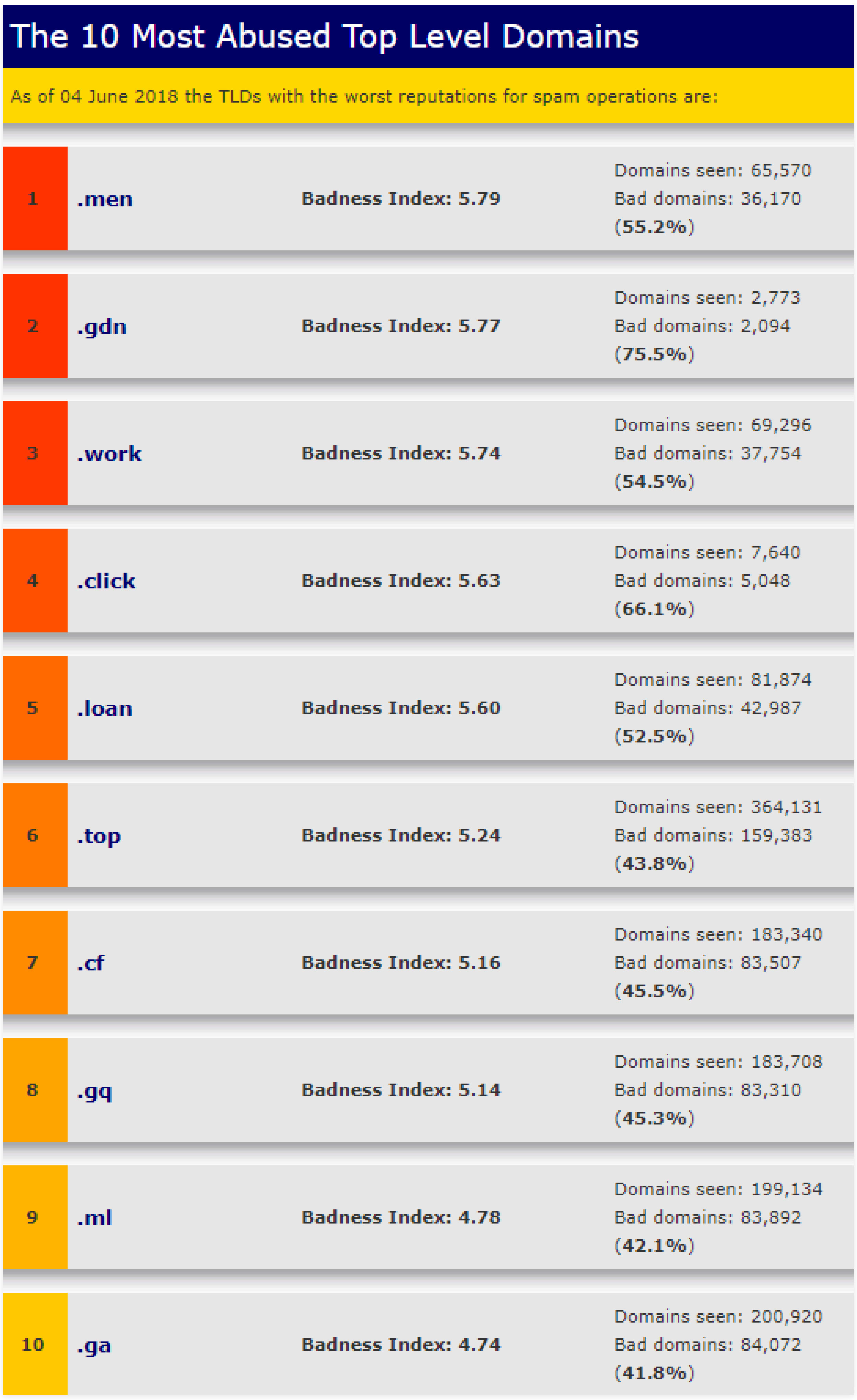
Sudanese Brothers Arrested in ‘AnonSudan’ Takedown

Story Categories

A Little Sunshine

All About Skimmers

Ashley Madison breach



The 10 Most Abused Top Level Domains

As of 04 June 2018 the TLDs with the worst reputations for spam operations are:

1	.men	Badness Index: 5.79	Domains seen: 65,570 Bad domains: 36,170 (55.2%)
2	.gdn	Badness Index: 5.77	Domains seen: 2,773 Bad domains: 2,094 (75.5%)
3	.work	Badness Index: 5.74	Domains seen: 69,296 Bad domains: 37,754 (54.5%)
4	.click	Badness Index: 5.63	Domains seen: 7,640 Bad domains: 5,048 (66.1%)
5	.loan	Badness Index: 5.60	Domains seen: 81,874 Bad domains: 42,987 (52.5%)
6	.top	Badness Index: 5.24	Domains seen: 364,131 Bad domains: 159,383 (43.8%)
7	.cf	Badness Index: 5.16	Domains seen: 183,340 Bad domains: 83,507 (45.5%)
8	.gq	Badness Index: 5.14	Domains seen: 183,708 Bad domains: 83,310 (45.3%)
9	.ml	Badness Index: 4.78	Domains seen: 199,134 Bad domains: 83,892 (42.1%)
10	.ga	Badness Index: 4.74	Domains seen: 200,920 Bad domains: 84,072 (41.8%)

According to Spamhaus, a TLD may be "bad" because it is tied to spam or malware dissemination (or both). More specifically, the "badness" of a given TLD may be assigned in two ways:

"The ratio of bad to good domains may be higher than average, indicating that the registry could do a better job of enforcing policies and shunning abusers. Or, some TLDs with a high fraction of bad domains may be quite small, and their total number of bad domains could be relatively limited with respect to other, bigger TLDs. Their total "badness" to the Internet is limited by their small total size."

More than 1,500 TLDs exist today, but hundreds of them were introduced in just the past few years. The nonprofit organization that runs the domain name space — the **Internet Corporation for Assigned Names and Numbers** (ICANN) — enabled the new TLDs in response to requests from advertisers and domain speculators — even though security experts warned that an onslaught of new, far cheaper TLDs would be a boon mainly to spammers and scammers.

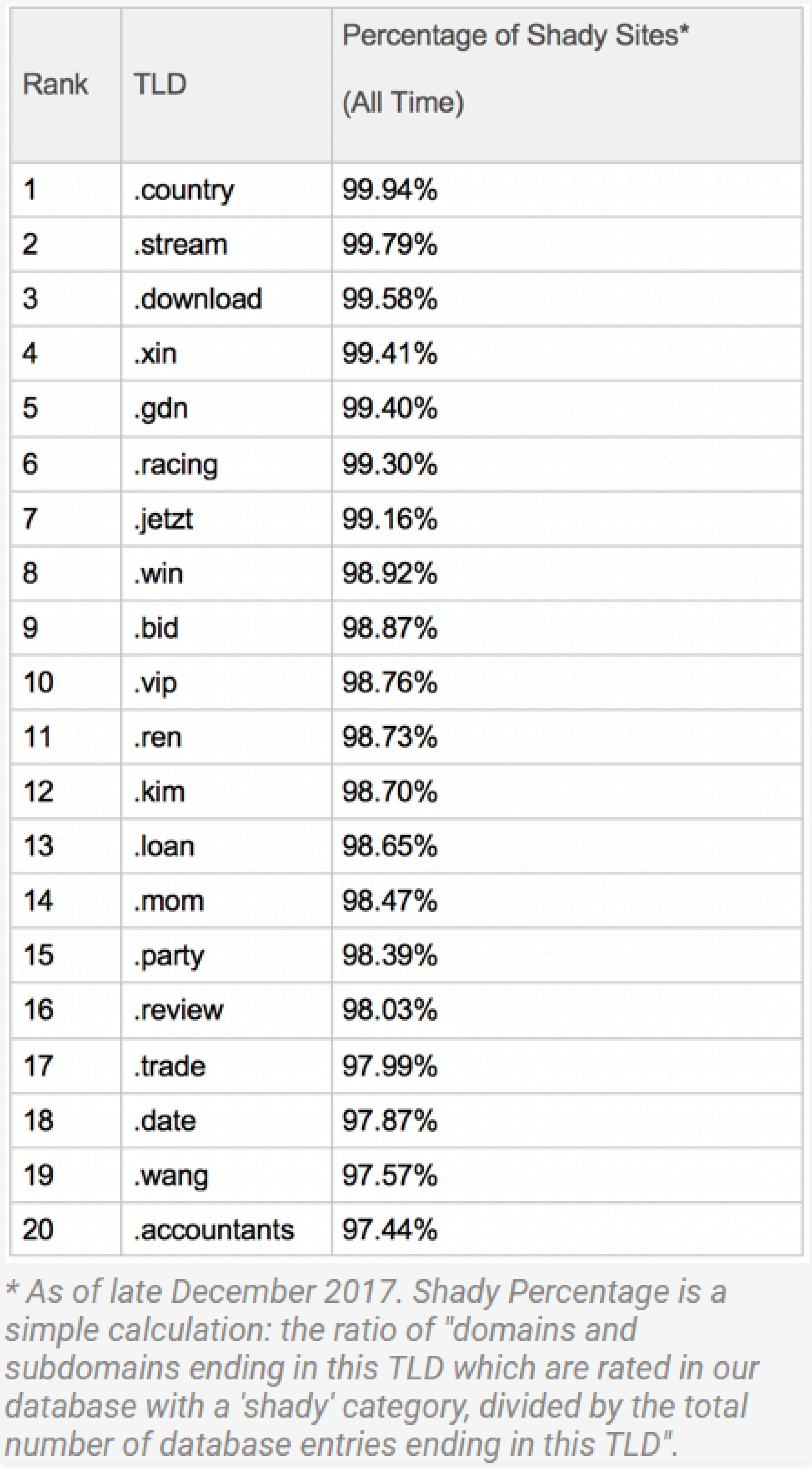
And what a boon it has been. The newer TLDs are popular among spammers and scammers alike because domains in many of these TLDs can be had for pennies apiece. But not all of the TLDs on Spamhaus' list are prized for being cheaper than generic TLDs (like .com, .net, etc.). The cheapest domains at half of Spamhaus' top ten "baddest" TLDs go for prices between $6 and $14.50 per domain.

Still, domains in the remaining five Top Bad TLDs can be had for between 48 cents and a dollar each.

Breadcrumbs
Data Breaches
DDoS-for-Hire
Employment Fraud
How to Break Into Security
Internet of Things (IoT)
Latest Warnings
Ne'er-Do-Well News
Other
Pharma Wars
Ransomware
Russia's War on Ukraine
Security Tools
SIM Swapping
Spam Nation
Target: Small Businesses
Tax Refund Fraud
The Coming Storm
Time to Patch
Web Fraud 2.0

Why So Many Top Hackers Hail from Russia

Security firm **Symantec** in March 2018 published its own Top 20 list of Shady TLDs:



Rank	TLD	Percentage of Shady Sites* (All Time)
1	.country	99.94%
2	.stream	99.79%
3	.download	99.58%
4	.xin	99.41%
5	.gdn	99.40%
6	.racing	99.30%
7	.jetzt	99.16%
8	.win	98.92%
9	.bid	98.87%
10	.vip	98.76%
11	.ren	98.73%
12	.kim	98.70%
13	.loan	98.65%
14	.mom	98.47%
15	.party	98.39%
16	.review	98.03%
17	.trade	97.99%
18	.date	97.87%
19	.wang	97.57%
20	.accountants	97.44%

** As of late December 2017. Shady Percentage is a simple calculation: the ratio of "domains and subdomains ending in this TLD which are rated in our database with a 'shady' category, divided by the total number of database entries ending in this TLD".*

Symantec's "Top 20 Shady TLDs," published in March 2018.

Spamhaus says TLD registries that allow registrars to sell high volumes of domains to professional spammers and malware operators in essence aid and abet the plague of abuse on the Internet.

"Some registrars and resellers knowingly sell high volumes of domains to these actors for profit, and many registries do not do enough to stop or limit this endless supply of domains," Spamhaus' World's Most Abused TLDs page explains.

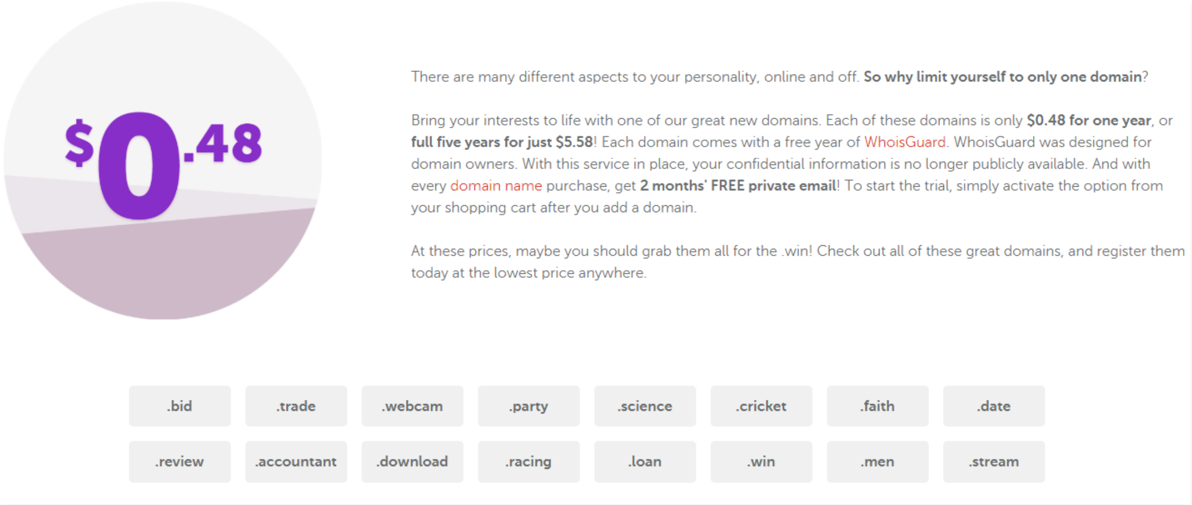
Namecheap, a Phoenix, Ariz. based domain name registrar that in Oct. 2017 was the fourth-largest registrar, currently offers by a wide margin the lowest registration prices for three out of 10 of Spamhaus' baddest TLDs, selling most for less than 50 cents each.

Namecheap also is by far the cheapest registrar for 11 of Symantec's Top 20 Shady New TLDs: Namecheap is easily the least expensive registrar to secure a domain in 11 of the Top 20, including .date, .trade, .review, .party, .loan, .kim, .bid, .win, .racing, .download and .stream.

I should preface the following analysis by saying the prices that domain registrars charge for various TLD name registrations vary frequently, as do the rankings in these Top Bad TLD lists. But I was curious if there was any useful data about new TLD abuse at tld-list.com — a comparison shopping page for domain registrars.

What I found is that although domains in almost all of the above-mentioned TLDs are sold by dozens of registrars, most of these registrars have priced themselves out of the market for the TLDs that are currently so-favored by spammers and scammers.

Not so with Namecheap. True to its name, when it is the cheapest Namecheap consistently offers the lowest price by approximately 98 percent off the average price that other registrars selling the same TLD charge per domain. The company appears to have specifically targeted these TLDs with price promotions that far undercut competitors.



There are many different aspects to your personality, online and off. **So why limit yourself to only one domain**?

Bring your interests to life with one of our great new domains. Each of these domains is only **$0.48 for one year**, or **full five years for just $5.58**! Each domain comes with a free year of WhoisGuard. WhoisGuard was designed for domain owners. With this service in place, your confidential information is no longer publicly available. And with every domain name purchase, get **2 months' FREE private email**! To start the trial, simply activate the option from your shopping cart after you add a domain.

At these prices, maybe you should grab them all for the .win! Check out all of these great domains, and register them today at the lowest price anywhere.

Namecheap is by far the lowest-priced registrar for more than half of the 20 Top Bad TLDs tracked by Symantec earlier this year.

Here's a look at the per-domain prices charged by the registrars for the TLDs named in Spamhaus's top 10:

The lowest, highest, and average prices charged by registrars for the domains in Spamhaus' Top 10 "Bad" TLDs. Click to enlarge.

This a price comparison for Symantec's Top 20 list:

The lowest, highest, and average prices charged by registrars for the domains in Symantec's Top 20 "Shady" TLDs. Click to enlarge.

I asked Namecheap's CEO why the company's name comes up so frequently in these lists, and if there was any strategy behind cornering the market for so many of the "bad" and "shady" TLDs.

"Our business model, as our name implies is to offer choice and value to everyone in the same way companies like Amazon or Walmart do," **Namecheap CEO Richard Kirkendall** told KrebsOnSecurity. "Saying that because we offer low prices to all customers we somehow condone nefarious activity is an irresponsible assumption on your part. Our commitment to our millions of customers across the world is to continue to bring them the best value and choice whenever and wherever we can."

Kirkendall said expecting retail registrars that compete on pricing to stop doing that is not realistic and would be the last place he would go to for change.

"On the other hand, if you do manage to secure higher pricing you will also in effect tax everyone for the bad actions of a few," Kirkendall said. "Is this really the way to solve the problem? While a few dollars may not matter to you, there are plenty of less fortunate people out there where it does matter. They say the internet is the great equalizer, by making things cost more simply for the sake of creating barriers truly and indiscriminately creates barriers for everyone, not just for those you target."

Incidentally, should you ever wish to block all domains from any given TLD, there are a number of tools available to do that. One of the easiest to use is **Cisco**'s OpenDNS, which includes up to 30 filters for managing traffic, content and Web sites on your computer and home network — including the ability to block entire TLDs if that's something you want to do.

I'm often asked if blocking sites from loading when they're served from specific TLDs or countries (like .ru) would be an effective way to block malware and phishing attacks. It's important to note here that it's not practical to assume you can block all traffic from given countries (that somehow blacklisting .ru is going to block all traffic from Russia). It also seems likely that the .com TLD space and US-based ISPs are bigger sources of the problem overall.

But that's not to say blocking entire TLDs a horrible idea for individual users and home network owners. I'd wager there are whole a host of TLDs (including all of the above "bad" and "shady" TLDs) that most users could block across the board without forgoing anything they might otherwise want to have seen or visited. I mean seriously: When was the last time you intentionally visited a site registered in the TLD for Gabon (.ga)?

And while many people might never click on a .party or .men domain in a malicious or spammy email, these domains are often loaded only after the user clicks on a malicious or booby-trapped link that may not look so phishy — such as a .com or .org link.

Update: 11:46 a.m. ET: An earlier version of this story incorrectly stated the name of the company that owns OpenDNS.

This entry was posted on Monday 11th of June 2018 10:42 AM

A LITTLE SUNSHINE

.ACCOUNTANT .BID .CLICK .COUNTRY .DATE .DOWNLOAD .GDN .JETZT .KIM .LOAN .MEN .MOM .PARTY .RACING .REN .REVIEW .STREAM .TRADE .VIP .WANG .WIN .WORK .XIN ICANN INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS NAMECHEAP NEW TLD SPAM NEW TLDS OPENDNS RICHARD KIRKENDALL SPAMHAUS SYMANTEC TOP 20 SHADY TOP-LEVEL DOMAINS

← Adobe Patches Zero-Day Flash Flaw

Microsoft Patch Tuesday, June 2018 Edition →

79 thoughts on "Bad .Men at .Work. Please Don't .Click"

Jason Nester
June 11, 2018

You incorrectly list OpenDNS as being a Google product. Cisco owns OpenDNS.

Google does have their own DNS solution, but it is not security focused.

- BrianKrebs Post author

-

June 11, 2018

Doh! You're right. I knew that, and I don't know why I put Google there. Fixed and noted, thanks!

Russ

-

June 11, 2018

You beat me to that comment.

Gnecht

June 11, 2018

Repeated experience: computer repair client gets a tech support scam from malvertising, which forwarded to a random-number domain from Namecheap. Web hosting is… elsewhere. Namecheap says the scam site is not their problem, and refuses to take down the domain.

Ben

-

June 11, 2018

Because it's not their problem. They register the owner of a domain name and allow for DNS records to be forwarded. User education is the solution to these problems, not making a registrar police every domain they sell.

NickDanger

-

June 16, 2018

Eh, what? By that standard, bit.ly & other URL-shorteners have no responsibility to remove redirect URLs used in spam when reported. If anything, I would argue that Namecheap has a *greater* responsibility than mere URL shorteners, because they are actually providing hosting with their redirects – as opposed to just sending a response header that redirects to another server. I've never been a Namecheap customer, but it looks like they offer something that other providers (Tucows) call a "masked-redirect": essentially just a full page frame/iframe that displays the content of another site.

By definition, that requires actual hosting (even if it's extremely limited & the customer has no access to upload/modify files directly) to host/generate the HTML document with the frame code. Regardless of where the actual content lives, the URL advertised in the spam EMail is hosted on Namecheap's servers – meaning that they are providing web hosting in support of spamming. And while that's somewhat less clear-cut than if the content of the offending sites were actually hosted on their servers, there's also the simple fact that, if an EMail containing a link to a masked-redirect on Namecheap is reported through Spamcop, it's the Namecheap-hosted URL that Spamcop will consider the "spamvertised" site, not the site that's loaded inside the iframe. So Namecheap has an incentive to deal with those abusers – or at least they would in theory, if they had any concern for the reputation of their network.

Incidentally, I've had almost the exact same experience as the original poster: I've reported masked redirects hosted on Namecheap to them, and they've consistently refused to do anything about them – arguing that it's not their responsibility because the actual content of the spam sites is hosted elsewhere. Of course, that's not the *whole* story: it usually takes the better part of a month to get even that much of a response out of them, and then only after publicly chasing them about it on Twitter (THEN tickets that have gone ignored for 2-3 week get a response within 1-2 hours, as if by magic). And to top it off, their support/abuse handling staff seem to be utterly clueless about basic aspects of their own field (and even basic reading comprehension), such as the differeces between EMail, websites, and domain names: almost every time I report a spam website to Namecheap, they first protest that it's not their responsibility because the EMail didn't come from their servers (even after I've clearly spelled out that it's a website I'm reporting, not an EMail). And/or they say that they can't suspend the domain name – when that's clearly not the issue I reported, nor would that even be necessary to address the issue in the first place.

When it comes to dealing with abuse complaints, it's clear that Namecheap's only real concern is keeping paying customers around – it doesn't mater if they're spammers, just so long as the pay their bills. And they will use hide behind any excuse they can to continue knowingly providing service to spammers. That's what makes their CEO's response so laughable: his company is fully aware using their network/services, they consistently fail to address it, and he's whining because someone criticized them for that? If he doesn't like the publicity, then maybe he should stop knowingly providing a haven for spammers – rather than acting like a precious little princess when someone points that out.

Joe

-

June 11, 2018

This is a known Namecheap procedure. Essentially, they have an URL forwarding server that is obviously abused by spammers.
And Namecheap refuses to do anything about it.
People have written about it years back, e.g.: - https://tacit.livejournal.com/608386.html

NaN

-

June 11, 2018

I have previously experienced the exact same issue with the namecheap's 'redirect' service. They seem to knowingly not care what kind of malicious activity the redirect service is used for (it is not just limited to spam). A blast from the past for @BrianKrebs probably – for awhile darkode.cc used the same namecheap redirect service to redirect to a version of the site post-takedown (probably wasn't real but still).

- Richard K.

-

June 13, 2018

False and false. We use - https://www.spamexperts.com on all mail forwarded through our redirection servers.

I'll await the next wild accusation here.

Jamie

-

June 14, 2018

False.

Read above, these people are talking about URL forwarding, not email forwarding.

Perhaps actually understand what you are doing before labeling things as "wild accusations."

NickDanger

-

June 16, 2018

Seriously…? You're (supposedly) the CEO of a domain registrar/hosting provider, and you can't even understand the difference between EMail and web forwarding? SERIOUSLY? I've heard of "the crap rising to the top," but that's *truly* pathetic. But if nothing else, the inability of your support/abuse department to distinguish between EMail, websites, and domain names makes a WHOLE lot more sense now.

(And that's the generous interpretation – giving the benefit of the doubt by assuming that you're not being deliberately obtuse, *a la* the Upton Sinclair line that "It is difficult to get a man to understand something, when his salary depends upon his not understanding it" – with "salary" replaced with "income from spammer customers" in this case).

Joe

-

June 11, 2018

Oh, and I've also been hit by spam with links to domains registered with Namecheap, using their URL forwarder.
At that time I used to have my domains registered with Namecheap. After realizing that they aren't willing to do anything about their URL forwarder, it

became clear to me that they are spam supporters, and I moved my domain registration elsewhere.

Scott Hartlaub

June 11, 2018

Just out of curiosity, what are your thoughts on the .Bank effort?

Phil

June 11, 2018

I think OpenDNS is no longer a Google thing, it has a header bar on the top of the homepage pointing to Cisco.com

Phil

-

June 11, 2018

Would've been 1st if it hadn't been for a phonecall I just finished!

The Sunshine State

June 11, 2018

Don't get me going when it comes to Namecheap and spamvertised websites !

techvet

June 11, 2018

OpenDNS has a free version and I have recommended it to my family and friends who are looking for something inexpensive to block inappropriate sites on their home network. Cisco bought it three years ago but as far as I can tell, has not substantially altered the offering (good). Cloudflare has a new DNS service (1.1.1.1) but I don't know if it addresses the security angle like OpenDNS does.

One thing this brings to mind is that not all ISPs allow you to modify the DNS settings. I am thinking of a national provider we left some years ago who provided the wireless router but wouldn't let you change the DNS server settings. That is one of the reasons we no longer use them at our house.

Robert

-

June 11, 2018

The free version of OpenDNS sucks for filtering. Heres links to two independent tests that overall, get the same results where they overlap:

1) - http://www.spotswood-computer.net/articles/DNS_Protection_Apr2018.pdf

2) - https://medium.com/alphasoc/theres-a-hole-in-your-umbrella-960ab0cc7e6e

techvet

-

June 12, 2018

Thank you for posting. I will investigate the free options, if any. Last night, I actually discovered that the settings for the DNS servers on our ASUS router had been altered (DNS hijacking), with the primary setting pointing to a known phishing server. The firmware was not behind that much but I changed the settings and updated the firmware. Googling the issue showed that a few other ASUS users had made the same complaint earlier this year.

Lucas

June 11, 2018

Thanks, blocked 29 .tlds at the web filter because of this article.

Richard K.

June 11, 2018

Namecheap responsibly and thoroughly investigates every allegation of reported abuse. We have never processed a single case where it was determined that we acted irresponsibly, and our record shows that. Last year we responded to over 92,000 third party reported abuse incidents, with more than 200,000 correspondences from investigating each report. Additionally, we self identified and investigated over 13,000 potential abuse cases that we identified based on our own security monitoring. While this may not satisfy everyone it satisfies our obligations according to ICANN.

We have a large dedicated team, that works 24/7 investigating any complaints we receive, and wherever there is evidence of abuse, we take action. Registrar accreditation requires us to respond and investigate abuse cases in all forms. We have been accredited by ICANN for nearly 10 years with no issues or warnings regarding abuse inaction from our side. Our record speaks for itself.

With 10M domains under management, we are now the second largest retail registrar in the world and this is reflected in the numbers you see here. You need to take that into consideration when viewing these numbers.

- Richard K.

-

June 11, 2018

By the way Brian, I appreciate that you used my statement as intended and without much twisting. That’s refreshing in this day and age. Much appreciated.

Jamie

-

June 12, 2018

By the way, a quick search for “Namecheap spam” reveals many many posts of people pointing the finger at you over spam, whois inaccuracies etc.

My favourites are the ones where you personally, the CEO of Namecheap, respond with aggressive threats of libel and litigation on Internet forums. Your company has an absolutely dire reputation. Enjoy being CEO.

- Richard K.

-

June 13, 2018

Love being CEO of this company with millions of satisfied customers and quickly growing. Thank you.

NickDanger

-

June 16, 2018

> Love being CEO of this company with millions of satisfied customers and quickly growing. Thank you.

Why hello, Argumentum Ad Populum! And in only your fourth post in this thread, don’t think I’ve ever seen someone go from chest-thumping bluster to desperation so quickly…

- Richard K.

-

June 13, 2018

We have millions of very satisfied customers and quickly scaling. I love being the CEO of this company. Thank you.

- Richard K.

-

June 13, 2018

This reply was meant to be posted elsewhere not as a reply to this specific thread.

Dave

-

June 15, 2018

I’ve gotta say, in my dealings with NameCheap they haven’t been sleazy, unlike my previous registrars Network Solutions and GoDaddy. Their prices are better, their web control panel is far more useable, their tech support seems competent, and in the past the company has supported ‘net freedom. Maybe they do sell to spammers. The gas station near my house has sold gasoline to known criminals, too, whatcha gonna do? I dunno, I’ve never seen any problem, maybe my spam blocking works better than most, though I don’t do anything special apart from training Thunderbird to recognize the stuff that does get through.

NickDanger

-

June 16, 2018

> By the way Brian, I appreciate that you used my statement as intended and without much twisting. That’s refreshing in this day and age. Much appreciated.

The phrase “without **much** twisting” implies that you think there was SOME twisting. Care to actually back that up by posting your original statement so that we can see what ostensible “twisting” was done? Or should we conclude that that was just passive-aggression posturing?

Also… you MIGHT not want to thank him, since the part(s) of your statement that Brian posted make you look like an angry, defensive man-child.

- BrianKrebs Post author

-

June 16, 2018

You’re welcome. I don’t believe there was any twisting involved. Pretty sure it was what you said verbatim.

Reader

-

June 12, 2018

It is the poor student who does no more than the bare minimum that is required.

Imagine your child brought home a school report card with barely passing grades. Would you announce it to the press or encourage your child to try for more?

You and your company should do more than merely pass bureaucratic inspection. You should proactively and manually screen every domain applicant.

You should want to be more effective than the rest of your shady competitors in that sector of commerce.

You should want to spend time selectively approving legitimate domains, rather than chasing down complaints about spam domains (some paid for with stolen funds!)

Unless you sleep better knowing that you did the bare minimum.

- Richard K.

-

June 13, 2018

So you’r rather have us shut down domains simply because we receive an abuse complaint?

I’d love to see your reaction when someone submitted an abuse complaint to your registrar and had your website shut down because of a knee-jerk reaction to an abuse complaint.

Frankly, I find your expectations of this much more dangerous to the stability of the internet than receiving a few spam emails while a complaint is properly and thoroughly investigated.

I apologize of you may have been a bit inconvenienced by having to click delete on a spam email while legitimate customers are protected by due process of complaints. How very unselfish of you…

Joe

-

June 13, 2018

Are you saying that Namecheap is unable to parse email headers and content and can not distinguish between legitimate email and spam?
Your statement basically says that you are a-ok with spam. QED.

- Richard K.

-

June 14, 2018

We use SpamExperts for our redirection servers and are pro-active monitoring our network as you can see from the statistics I posted above.

You do realize that domain names can use outside dns and ip's don't you?

My statement was exactly what I meant it to be. Some people especially in this segment of the internet population, would rather de-stabilize the internet than receive a single piece of spam. I detest spam as much of the next person but some of the demands of the anti-spam nazis are ridiculous when it comes to their expectations.

Our number one priority is to safeguard the stability of our legitimate customers and their domain names and websites. That requires due process. If even one of them is disrupted because of false demands, it is unacceptable.

- Dave Horsfall

-

June 14, 2018

You refer to "anti-spam nazis"; by Godwin's Law (look it up), this means that you have just lost the argument.

I wonder how many of your "millions of satisfied customers" are actually satisfied spammers/scammers? Not that you'd care, of course, as it's become all too common these days for providers to simply wash their hands of problems for which they are responsible, claiming that it's your customer at fault, whilst knowingly assisting them.

Believe me, if I can find an easy way to block all TLDs hosted by spam-support services such as yourself then I would.

Go ahead and sue me; I'm waiting…

Richard K.

-

June 14, 2018

Where's your complaints against the telecoms and the mailman that is supposedly, in your twisted view, spamming your phone lines and your mailbox? Show me the proof you are in a hissyfit against those messengers.

Until then, if it walks like a duck…

NickDanger

-

June 16, 2018

> Where's your complaints against the telecoms and the mailman that is supposedly, in your twisted view, spamming your phone lines and your mailbox? Show me the proof you are in a hissyfit against those messengers.

Oh sweet merciful crap, you're going to trot that one out too? That bit of spam apologetics was already considered old-hat in NANAE years ago – but at least you're making this easy, because I can just quote the standard refutation: the difference between EMail spam and postal junk mail is that postal junk mailers pay a non-trivial cost for sending out their advertisements, while the recipients pay most of the cost for EMail spam (in terms of bandwidth, storage space, time spent dealing with it, etc).

And that was from 20 years ago – before spam was being widely used to distribute things like ransomware, banking trojans, and all other manner of malware. Again, that you would try to use that argument – and HERE – is truly astounding.

- Richard K.

-

June 14, 2018

And by all means, block every tld you think might deliver you a piece of spam and be done with it. I even encourage you to do so.

Honestly, we have no skin in this game. As a domain name registrar, we are here to provide a service and sell domain names that are available to our customers. Whether they are .com or anything else. Let the customer decide. It’s all about choice and market demand in the end and like I said before, my preference would have been to not even have these new tld’s as what we had before in the namespace was more than perfectly adequate.

Quite frankly, people like you would rather not adjust just so you have something to complain about. Try finding a hobby.

NickDanger

-

June 16, 2018

> We use SpamExperts for our redirection servers and are pro-active monitoring our network as you can see from the statistics I posted above.

…which does absolutely nothing to address the huge number of spam-support sites that you provide hosting for via frame “redirects” – functionality that seems to have very little legitimate purpose to begin with, and appears to be primarily used as a way for spammers to hide the actual URLs of the sites they’re spamming for.

> You do realize that domain names can use outside dns and ip’s don’t you?

Did you have a point, or was that just more passive-aggressive posturing…? You do realize that most hosting providers have policies against the use of their services for hosting spam support websites/URLs, regardless of where the spam EMails themselves were sent from… right? And you are aware that spammers often send spam from different hosts than the ones they use for the websites they’re advertising, which is precisely why* most providers have the aforementioned policy… right? Right?

*Well, that and the policy of some RBL maintainers to list hosts that, as Spamhaus puts it, "knowingly provide a for-profit spam-support service"

> I detest spam as much of the next person but some of the demands of the anti-spam nazis are ridiculous when it comes to their expectations.

What, you mean like the expectation that you actually remove spammers & spam-support URLs from your network? Or the expectation that you do so in a timely fashion – instead of days/weeks after it would have any useful effect? You poor, poor little thing – it must be such a terrible burden, having people constantly expecting you to manage your network like a responsible service provider. My heart truly weeps for you.

> Our number one priority is to safeguard the stability of our legitimate customers and their domain names and websites. That requires due process. If even one of them is disrupted because of false demands, it is unacceptable.

WTF are you talking about? Investigating a spam complaint isn't a court proceeding, determining the validity of a spam/spam-support website complaint shouldn't take more than 5-10 minutes for anyone who has the slightest clue what they're doing.

And nice Godwin invocation, by the way – stay classy!

Reader

-

June 14, 2018

Richard,

You didn't indicate to whom you're replying.

In the event you're responding to me, I'll answer.

The right thing to do is manually approve domain registrations and investigate complaints. Reject complaints and registration applications that cannot be verified with a phone call.

When someone buys several domains, ask why.

When the same credit card is used twice, check if the same applicant used it. Make a phone call to the apllicant and see who answers.

You can still offer cheap domains by being more proactive, because you'll be spending less time being reactive.

- Richard K.

-

June 14, 2018

First of all, we do investigate each and every complaint as I stated in my original reply.

We also proactively monitor our own network and take action against abuse.

Asking us to effectively verify the 10's of thousands of domains registered with us daily and then monitor their content and actions would be logistically impossible and for the latter unethical.

It's like asking the phone company to monitor their customers and their phone calls on top of it.

The reality of the situation is that a registrar needs to remain neutral until abuse takes place. We aren't the internet gestapo and the laws in place by both ICANN and the US government support this.

- Dave Horsfall

-

June 14, 2018

You write: "We aren't the internet gestapo…"; you really can't help yourself, can you?

Here's a hint which every CEO ought to know: "When you're in a hole, stop digging!"

Reader

-

June 15, 2018

Richard,

The phone company sucks because laws and regulations require them to connect all calls, even abusive, harrassing spammers. They can't charge spammers more to use to make bulk calls, either. Thanks government!

The Postal service isn't allowed to refuse delivery of junk mail, with only a few exceptions, e.g. obscene materials and fraud. Thanks government!

Domain registrars don't have to monitor content. Yet! But keep mentioning additional laws and some idiot politician will be happy to saddle you with that burden!

Cloudflare took a hit by being associated with a journalist, neonazis, spammers, and terrorists. While they dropped the journalist and the neonazis, there are plenty of companies that still won't do business with Cloudflare.

You made it so easy and cheap for criminals to use your service, it's no wonder you're associated with junk. Spammers, especially, rely on the lack of verification, automation, and cheap domains to further their crimes. There's a reason criminals flock to you and other businesses don't consider you legitimate.

Claiming you get too many registrations to verify is a lousy excuse. Charge a few dollars more to hire the necessary employees. With better verification, you'd waste less money on complaints, too.

My use of "you" and "your" refers to your industry, mostly, but not exclusively.

- Richard K.

-

June 14, 2018

BTW, I expect all of you to be picketing the US postal service and the offices of AT&T next.

After all the price the charge for phone calls and stamps these days is pretty cheap.

If you all would like effect real change, change the system and the laws, that's the first place I would start.

You also have the great option as I've seen here of blocking all the new tlds you disagree with.

Frankly, I think we were just fine with .com .net .org and the country code tlds to begin with.

Reader

-

June 17, 2018

Richard wrote: "I think we were just fine with .com .net .org and the country code tlds to begin with."

If you included .edu, .mil, and .gov, then removed the preposition at the end of the sentence, I could agree 100% with you.

NickDanger

-

June 16, 2018

> I'd love to see your reaction when someone submitted an abuse complaint to your registrar and had your website shut down because of a knee-jerk reaction to an abuse complaint.

Oh don't worry, I don't think you have to worry about ANYONE here accusing you of "knee-jerk" reactions to abuse complaints… It is interesting, though, that you seem to be either trying to suggest that the abuse complaints you receive are not valid, and/or that the person you're replying to would engage in/allow activity that would generate abuse complaints to their registrar.

> Frankly, I find your expectations of this much more dangerous to the stability of the internet than receiving a few spam emails while a complaint is properly and thoroughly investigated.

A "few" spam EMails? You have a knack for understatement – it's more like dozens/hundreds. As for "while a complaint is properly and thoroughly investigated" – now THAT is pure comedy gold. The people staffing your support/abuse department can barely UNDERSTAND the details of most abuse complaints (if they even bother to respond at all), the idea of them actually investigating a complaint successfully is laughable.

> I apologize of you may have been a bit inconvenienced by having to click delete on a spam email while legitimate customers are protected by due process of complaints. How very unselfish of you…

Wow. Just… WOW. Seeing the old "what's the problem, you can just delete them" chestnut brings me back – did this comment thread suddenly fall through a timewarp back to NANAE circa 1998? What's next, are you going to start accusing people of being secret agents of the Lumber Cartel (TINC), trying to stamp out spam to protect their revenues from paper junk mail? Or that trying to shut down spammers violates their "frea speach"?

To see that sort of old-hat spam apologetics, not only here of ALL places – but from the CEO of a domain registrar/hosting provider? It just boggles the mind. I have an incredibly difficult time believing that you're genuinely unaware of the myriad of reasons why spam is a real, genuine problem – hell, there's entire series of articles on this very site going over that exact topic.

Jamie

-

June 12, 2018

ICANN are really well know for taking decisive action.

Your business profits from fraudsters and malicious actors. However you try to sell this as "helping the poor", you won't fool anybody here.

NickDanger

-

June 16, 2018

> We have never processed a single case where it was determined that we acted irresponsibly, and our record shows that.

So, in other words, you're bragging about getting all As… on a report card that you wrote for yourself? Not exactly a convincing argument, even if you WERE a credible source.

> While this may not satisfy everyone it satisfies our obligations according to ICANN

So you do the absolute bare minimum that you're contractually obligated to, and that's supposed to be praise-worthy?

> We have a large dedicated team, that works 24/7 investigating any complaints we receive, and wherever there is evidence of abuse, we take action.

Not in my experience – in almost every instance where I've reported spam to Namecheap, your staff attempted to weasel out of responsibility with the excuse that the content of the spam website was hosted elsewhere (even though the actual spamvertised URL relies on your servers). The only exception? One instance where your staff *initially* claimed that the issue had been resolved – but then after I checked & pointed out that the offending URL was still hosted on NC servers, they fell back on the same "hide behind weaselly excuses" tactic as before.

> We have been accredited by ICANN for nearly 10 years with no issues or warnings regarding abuse inaction from our side. Our record speaks for itself.

Oh? Does this mean that you FINALLY started registering domains directly, rather than just reselling for ENom?

> With 10M domains under management, we are now the second largest retail registrar in the world and this is reflected in the numbers you see here. You need to take that into consideration when viewing these numbers.

Ah yes, OVH is fond of using a nearly-identical excuse (though in their case, it's "we're the third-largest hosting provider"). And did you have an actual point, or is that hand-waving bluster?

If anything, taking that into consideration paints you in an even worse light: if ANYONE should have the necessary resources to properly deal with spammers on their network, it's the "second largest retail registrar." If you chose to adopt a bargain-basement business model that doesn't actually give you the resources to manage your network responsibly, then that's your problem.

oldtaku

June 11, 2018

I find it amusing and appropriate that .men is mostly scumbags. And even more so for .country.

Bob

-

June 14, 2018

Jeez! Misandry much?

Let's have a .women for all the evil women in the world so we're back to that equality we hear so much about.

On topic I just wish that it was possible to just cut all bad actors off the Internet. No politics, no corporate greed, no agendas, just a totally unbiased global authority that can just so that as soon as they have enough evidence. Make an AI to control it!

ShadowVet

June 11, 2018

Maybe someone needs to come up with a means of blocking all sites from specific Registrars…. That might promote a more robust monitoring effort at the registration level.

NickDanger

-

June 17, 2018

THERE's an idea. There's already a SpamAssassin addon that allows filtering by country, something that the same – but by registrar – would be very handy. Especially if it could also apply to the domains of links in the messages too.

SkunkWerks

June 11, 2018

Still waiting for the needle to drift more towards Security and away from Convenience.

In particular where it might interfere with "making boatloads of cash", I gather I'm going to be waiting till the heat death of the universe.

Gary

June 11, 2018

I 550 bounce many of those tlds in postfix. Nothing but spam comes from them.

I have used those cheap tlds from namecheap to set up a server, then switch to the real domain name later. That is the only use I have for those tlds.

Matthew Steinhoff

June 11, 2018

Block 'em all.

When the first batch of gTLDs were released more than a decade ago, I made the reckless and impulsive decision to add them to our mail server's deny list. I figured, sooner or later, someone would come to me complaining of delivery problems and I'd allow them, one by one, as needed.

Ten years later, no complaints. Nothing removed from the original block list. Maybe we've been missing some critically important email. But I doubt it. Checking the logs, I see thousands of rejected messages based on domain (bestbootjune.bid, displays.competemap.stream, l8bookanything.stream, etc.).

Just checked our config: 497 gTLDs set to deny. Looks like there are more than 1,200 currently issued. Now I'm faced with a problem: do I add the new ones to our block list or just white list TLDs that existed pre-2005 and lock the internet in time?

Older and wiser me says I should do more research, convene our technical panel and do a simulation given the last couple million messages we have received. Practical me – riding high on my earlier success – says just white list OG TLDs and call it a day.

Cheers,
Matt

JCitzen

-

June 11, 2018

I say kudos to you Matthew! 😜

Gunter Königsmann

June 11, 2018

The last bad domain I followed a link to was amazon.net. It actually contained a very plausibly-looking login form. But before inputting any passwords I always double-check if I am at the right place.

Joseph Newell

June 11, 2018

ICANN's mission statement: "Preserve and enhance the operational stability, reliability, SECURITY, and global interoperability of the Internet."

https://archive.icann.org/en/committees/evol-reform/working-paper-mission-06may02.htm

and yet they pollute the namespace because they're captured by scummy registrars like Namecheap.

Dave Horsfall
June 11, 2018

ICANN is utterly out of control, as they slowly work their way through the dictionary; I wonder if the principle of "follow the money" applies?

In the meantime, I'll continue to accept email only from the "Big N" (where "N" is a small integer), and I filter even those… Just up the road from me is a .clinic, FFS, and I've seen a .plumber… They're fine for wanky marketoids who want a "cute" name for their site, but I see no reason whatsoever to accept email from them.

Reader
-
June 12, 2018

Don't be elitist. It's an ugly look.

- Dave Horsfall (who's not afraid to use his real name)
-
June 14, 2018

Well, Mr/Ms Reader (you must've had cruel parents to give you a name like that), would you care to elaborate upon your "elitist" accusation? Or are you simply incapable of forming a reasoned argument?

There's a saying in the anti-spam community (or the "anti-spam nazis" like the esteemed Richard said — funny how some people here don't appreciate our efforts); "my server, my rules"; yes, I run my own mail/web server (it's about 10 ft away from me) so I guess that makes me elitist… If I can find a simple way to block every domain that spam-support services like Namecheap issue then I would.

Mike
June 11, 2018

OpenDNS limits blocks to 25 domains

Onx
June 12, 2018

Namecheap is good project!
Btw you can pay with bitcoins coz nowdays everybody have bitcoins and everybody all my friends and co workers dealing with bitcoins. Also its good nanecheap have good prices for domains. Just good service keep up!
Also every serious business minded person likes this kibd of business what namechrap provides.
Also you can open ananoumosly domain name its good coz many people who do business related with cryptocurrency like to be anonoumous.

I forgot my username again
June 12, 2018

.ml/.ga/.cf/.gq can be registered for free at freenom.com

Ebvalaim
-
June 12, 2018

I was surprised to see that those domain were listed as costing ~$14 minimum and wanted to point this out – but you were quicker 😉

Reader
June 12, 2018

you can add wildcard dns blocking on windows from a python script:
https://github.com/dzzie/dnsblock

Bob
June 12, 2018

In addition to OpenDNS, there a number of free DNS providers that offer some level of protection and/or performance improvements over the ISPs (Quad9 comes to mind, DNS 9.9.9.9)

A somewhat comprehensive list is here: https://www.lifewire.com/free-and-public-dns-servers-2626062

Rico Finelli

June 12, 2018

Love those titles you come up with, Brian.

The gTLD.club

June 13, 2018

Thank you for this great article but my understanding of it is that I should move away from ".COM : "It also seems likely that the .com TLD space and US-based ISPs are bigger sources of the problem overall".

Correct?

🙄

Bill

-

June 13, 2018

A larger raw *amount* of spam email comes from .com, yes.

However, a much larger *percentage* of email from the new TLDs (basically 100%) is spam. There is no detectable legitimate email usage of the new TLDs. This is why so many are successfully blocking them all and not suffering any ill consequences (even though they still do get a large amount of spam from .com, obviously).

Actually, I've gone to changing my email every year… yes… every… single… year… to reduce spam. I get no spam at all this way. I just take a couple hours to change my email address everywhere during January each year (using my password manager as a list). And for close friends I explain what the changing pattern is to them, they get it.

NickDanger

-

June 17, 2018

> A larger raw *amount* of spam email comes from .com, yes.

I'd also point out that that is almost certainly skewed by the amount of spam that comes from the big freemail services using .com domains (gmail.com, hotmail.com/outlook.com, yahoo.com, etc).

OT: speaking of GMail, anyone know why there's so much more spam from them all of a sudden? Starting about 2 months ago, I've started getting 20-30 spam per day from Indian SEO/web dev companies, split about 60/40 between free gmail.com accounts & spammers who are apparently paying for & spamming from paid GSuite accounts (the messages came from non-Google domains, with MX records pointing at Google servers, and headers indicating the messages came from there too).

Gene

June 13, 2018

I operate a spam-filtering service, and we block ALL of those garbage domains- about 500 of them.

Our clients do not want email from TLDs like ".party", ".wang", ".men", ".love", etc etc etc. We've never seen real email from any of them and likely never will.

ICAANs expansion of TLDs has been nothing but a headache for the internet.

SkunkWerks

-

June 19, 2018

Well, don't get me wrong here, but if you can- by way of elimination- excise all of those new TLDs from any legit mail system and suffer little to no loss save a whole lot of crap you're not receiving…

That sounds less like “headache” and more like “a handy way for spam-merchants to self-identify”.

And in that sense you ~could~ look at the cut-rate offerings by domain merchants with admittedly few standards as a way of assuring that self-selection.

hammertime

June 13, 2018

So is it .accountants, or .accountant, or both? I believe it should be the singular form. And don’t get me started on link shorteners. Block ’em all. btw I use dnsfilter fwiw. It lets me put all these gtlds and cctlds in one huge long blacklist.

Andrew

June 14, 2018

Does resetting your computer to IBM’s DNS server I believe it’s called Cloudfare at 1.1.1.1, protect you from some bad sites/hacks…?

Antonio

June 15, 2018

Well… I just updated my DNS blacklist…

NickDanger

June 17, 2018

Another one to block: .OVH

Yup, that’s right – notoriously spam-friendly French provider OVH went out and got their own goddamn And they’re selling .ovh domains for £0.99 apiece (discounted from £2.99) – unsurprisingly, I’ve seen dozens of spam EMails from .ovh domains already, as well as advertising spam-support sites using .ovh.

I’ve joked in the past that OVH is a “full-service” spam support provider (send spam from their servers, advertising a site that they host, AND using a domain registered with them? Sure, they don’t care) – but to setup their very own spammer-haven TLD as well? I almost have to grudgingly admire that…

SkunkWerks

June 18, 2018

So, I guess the only burning question I still have is: if those three TLDs are dangerous, then what’s the value in ‘.safety’ or ‘.dance’?

IA Eng

June 28, 2018

just block the top tlds in Spamhaus and Symantec. Then while your at it, go the this place and download the list, slap it in as well. The world will be a better place around you.

https://cinsarmy.com/active-threat-intelligence/

Comments are closed.