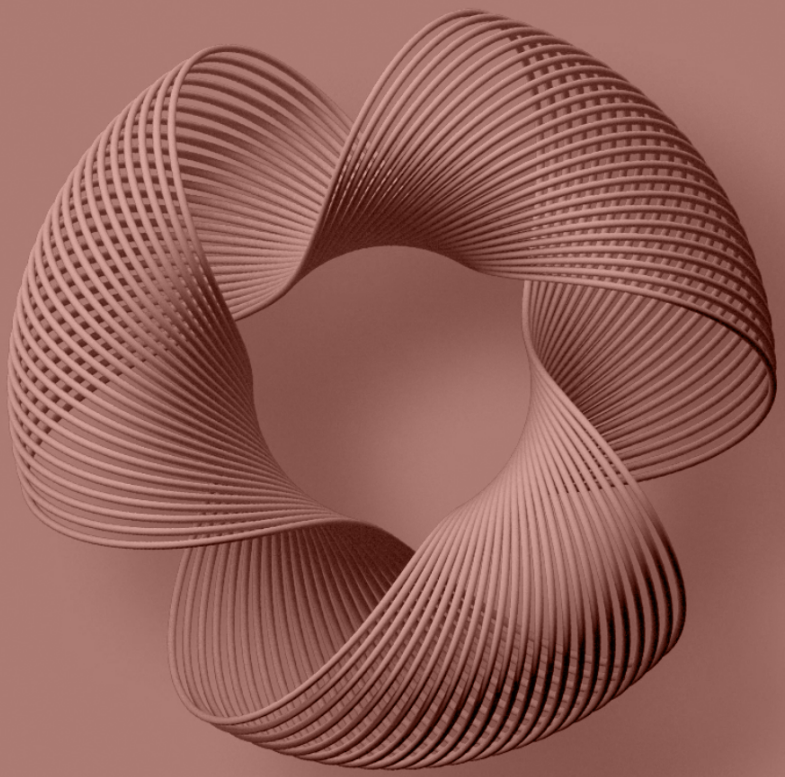
State of Phishing & Online Fraud

Q1 2020 Report

(COVID Edition)



BOLSTER

Executive Summary

Malicious hackers and scammers follow the fear. In Q1 2020, Bolster saw approximately 4 million suspicious pages and over 850,000 confirmed phishing and counterfeit pages. Approximately 30 percent of the confirmed phishing and counterfeit pages were COVID-19 related and attempted to take advantage of consumers' desire for information, supplies, and answers.

COVID-19 has contributed to record breaking cybercriminal activity. In March, at the peak of COVID-19 related developments, over 8,000 phishing and counterfeit pages were created. On 3/19, over 25,000 pages were created — a record high for all of Q1 2020.

Industries that endured mass strain due to the United States' work from home and economic shutdown mandates were highly targeted by cyber criminals — with SaaS, Telecom, and Finance as the most targeted industries for phishing and scam attacks. Remote work, counterfeit medical, and drug scams were criminal go-to's — with over 225,000 and 117,000 confirmed phishing scam sites, respectively. Stimulus checks, loans, and even fake COVID-19 cryptocurrency were used to lure unsuspecting victims into scam traps.

Overall, the online landscape was extremely impacted by COVID-19 in Q1 2020. The pandemic armed cyber criminals with fodder and bait to create some of the largest spikes in online scams, misinformation, and phishing we've ever seen. But we can turn the tide. By joining security forces, embracing employee security awareness training, and leveraging cutting-edge AI technologies, we can rise up to defend enterprises, SMBs, nonprofits, and the online community-at-large against this new wave of scams, phishing, and counterfeit products and services.

Key Findings

Exponential growth in phishing and website scams.

In Q1 2020, we detected 854,441 confirmed phishing and counterfeit pages and ~4M suspicious pages.

COVID creates a surge.

Of the total number of confirmed phishing and counterfeit pages, ~30% were related to COVID-19.

Daily phishing creation soars.

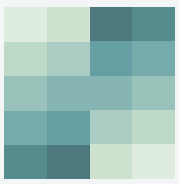
Over 3,142 phishing and counterfeit pages went live every day in January with that number increasing to 8,342 in March — due to the COVID-19 pandemic. Over 25,000 pages were created on 3/19 - a record for the quarter.

SaaS, Telecoms, and Finance suffer the most from phishing.

SaaS and Telecoms were the industries most impacted by phishing scams, followed by Finance, Retail, and Streaming.

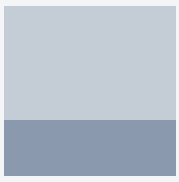
COVID medical scams play on a cure.

In the month of March alone, we found 102,676 websites related to medical scams, with 1,092 websites either selling Hydroxychloroquine or spreading misinformation about using it to cure COVID-19.



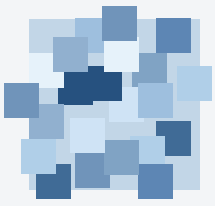
850K

SCAM PAGES



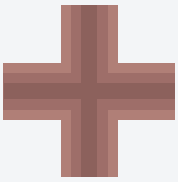
30%

RELATED TO COVID



25K

PAGES ON 3/19



100K

MEDICAL SCAMS

Key Findings

Stimulus checks and loans brought out the hackers.

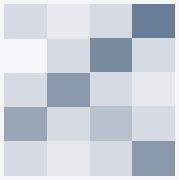
We found over 145,000 suspicious domain registrations with 'stimulus check' in them. The number of websites that claim to offer small business loans jumped 130 percent from February to March. Hackers spun up 60,707 banking websites to attempt to siphon off stimulus funds.

Hackers target remote workers and those quarantined.

Collaboration and communication phishing sites saw a 50% increase from January to March, as a large majority of the workforce began working from home. Streaming phishing sites saw an 85% increase from January to March, with over 209 websites being created per day — attempting to capitalize on those looking for entertainment during lockdowns.

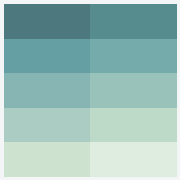
COVID gets its own malicious cryptocurrency.

We discovered multiple phishing websites peddling fake COVID cryptocurrencies and crypto wallets and aiming to siphon data for future phishing, targeted malware or credential stealing. One COVID-19 cryptocurrency bills itself as "The World's Fastest Spreading Crypto Currency" and attempts to get visitors to download suspicious files off GitHub. Another site prompts visitors to register to find out more information about a COVID coin that "gains value as more people die and get infected".



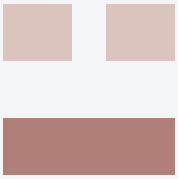
145K

FAKE STIMULUS WEBSITES



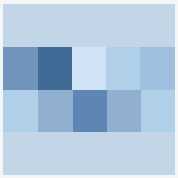
60K

FAKE BANKING WEBSITES



50%

INCREASE IN HACKING OF REMOTE WORK TOOLS

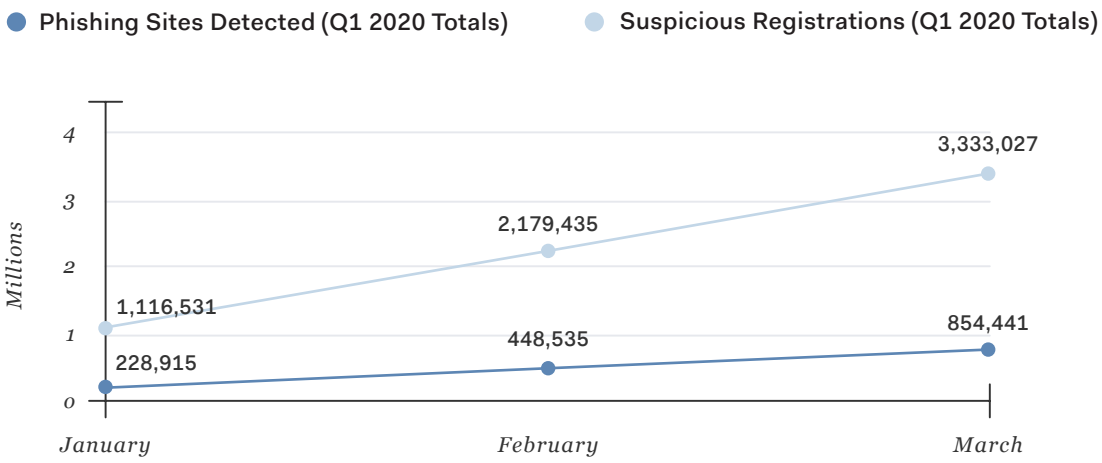


209

FAKE STREAMING SITES / DAY

Overview - Total Phishing

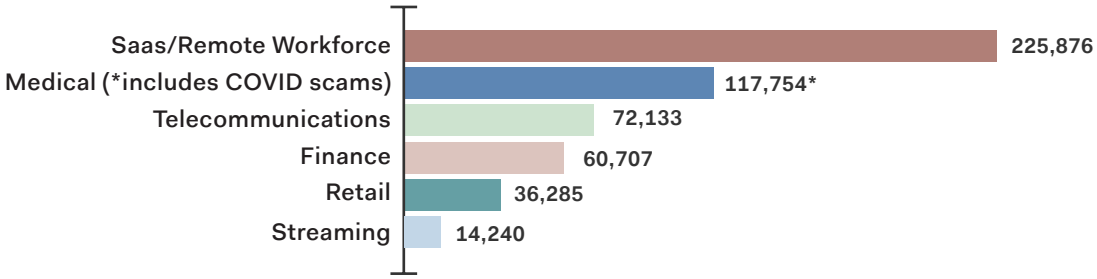
Phishing began to rise in February, but spiked in March. Over 8,300 phishing pages went live per day in the month of March.



Phishing by Industry

Many of the most targeted industries of 2019 continue to be top targets in Q1 2020. We saw detected phishing sites go up across all top-targeted industries.

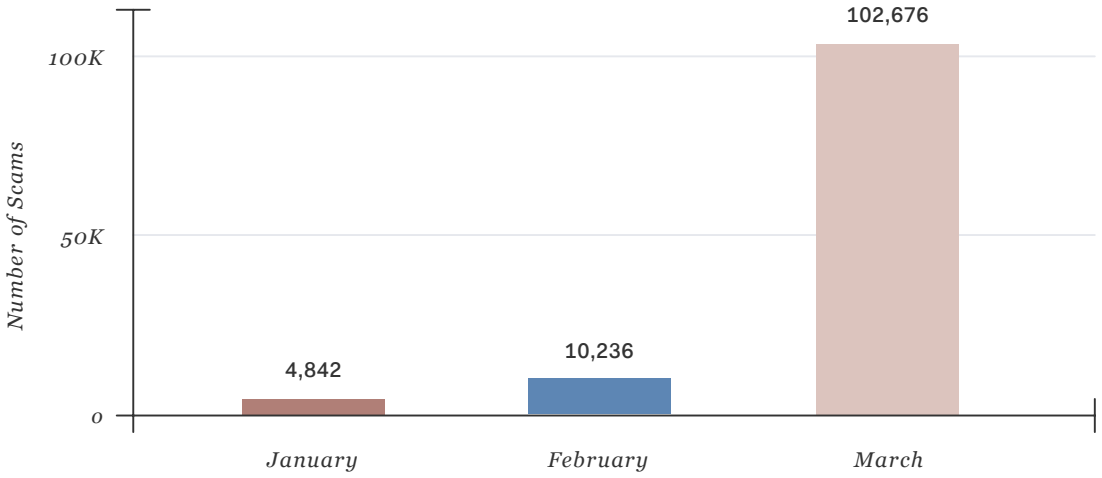
The COVID crisis and the shift in remote workforce employees have led to a spike in scams targeting the SaaS and Healthcare industries.



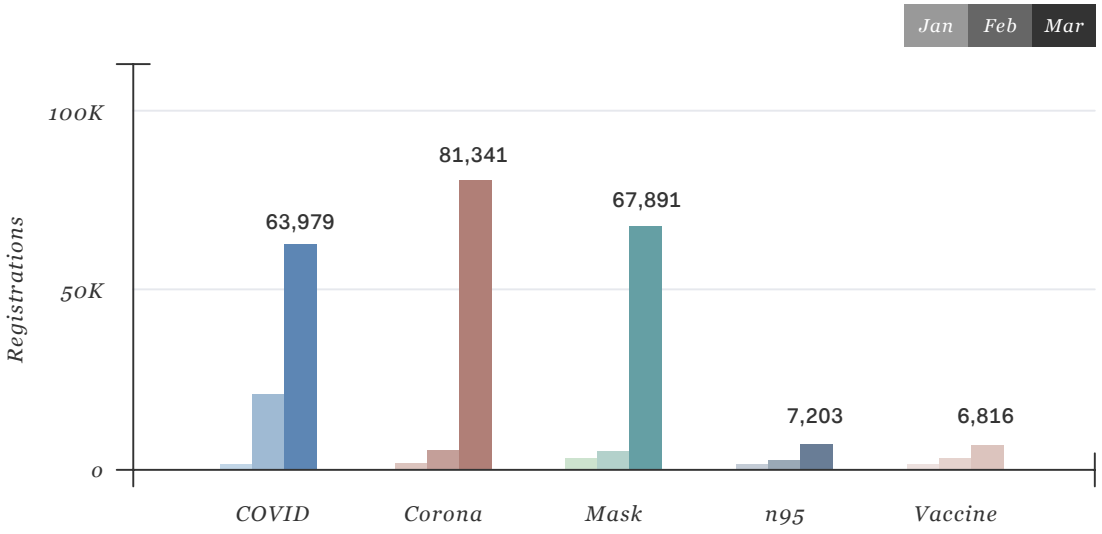
SAAS/REMOTE WORK: Microsoft, Outlook, WebEx, Skype, Zoom, Slack, etc
FINANCE/BANKING: Chase, PayPal, Itau, WellsFargo, CIBC, AMEX, etc
STREAMING: Netflix, Amazon, Hulu, etc
GAMING: Fortnite, CoD: Warzone, Animal Crossing, PUBG, Minecraft, etc

Source: https://checkphish.ai

COVID Scams Overview



COVID-19 phishing website domains used popular search terms and keywords to attract consumers looking for information, supplies, and treatments.



Suspicious registrations spiked in March for many covid-related keywords, such as, covid, corona, mask, n95, and vaccine. Though February saw a considerable 230%+ increase, March jumped even higher with a 1,624% increase.

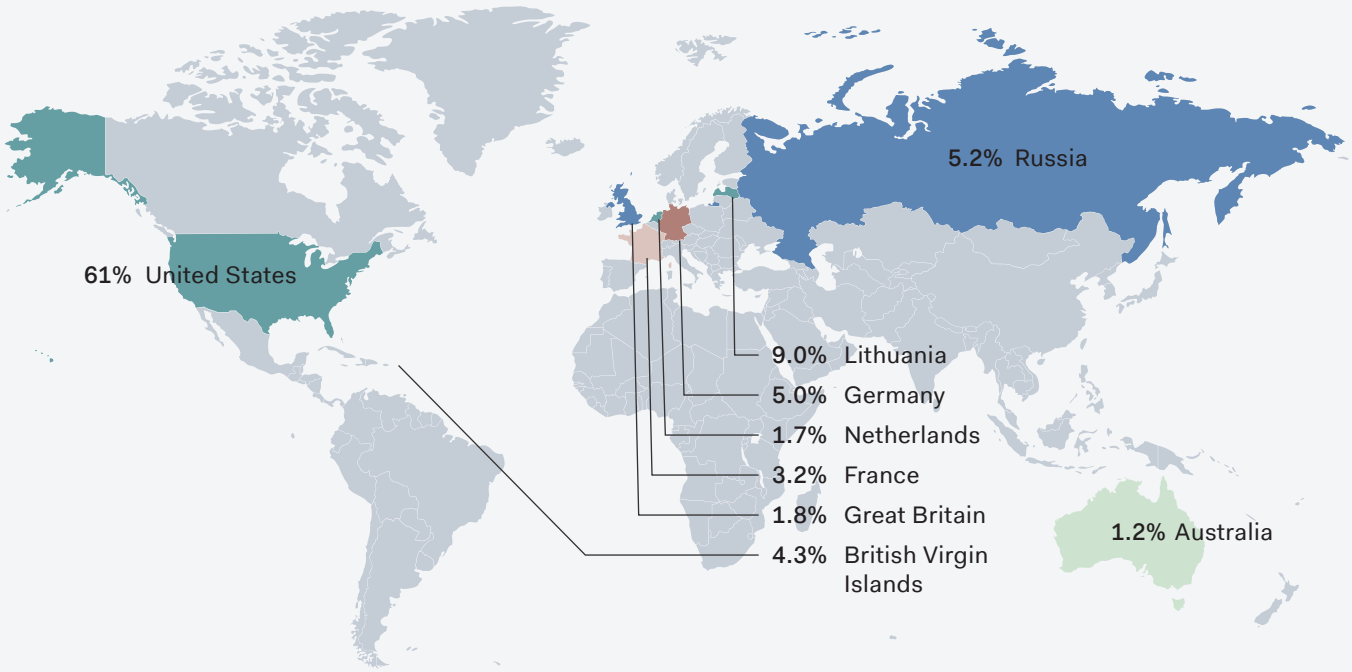
Source: https://checkphish.ai

Countries Hosting Phishing and Counterfeit Websites (Q1)

The United States continues to lead in hosting phishing and counterfeiting websites, but the relative percentage declined from 2019.

Lithuania, Russia, and Germany saw the biggest relative increases from 2019 to 2020.

Country	*%*
United States	61.0
Lithuania	9.0
Russia	5.2
Germany	5.0
British Virgin Islands	4.3
France	3.2
Netherlands	1.7
Great Britain	1.8
Australia	1.2



Source: https://checkphish.ai

Most Responsive Hosting Providers

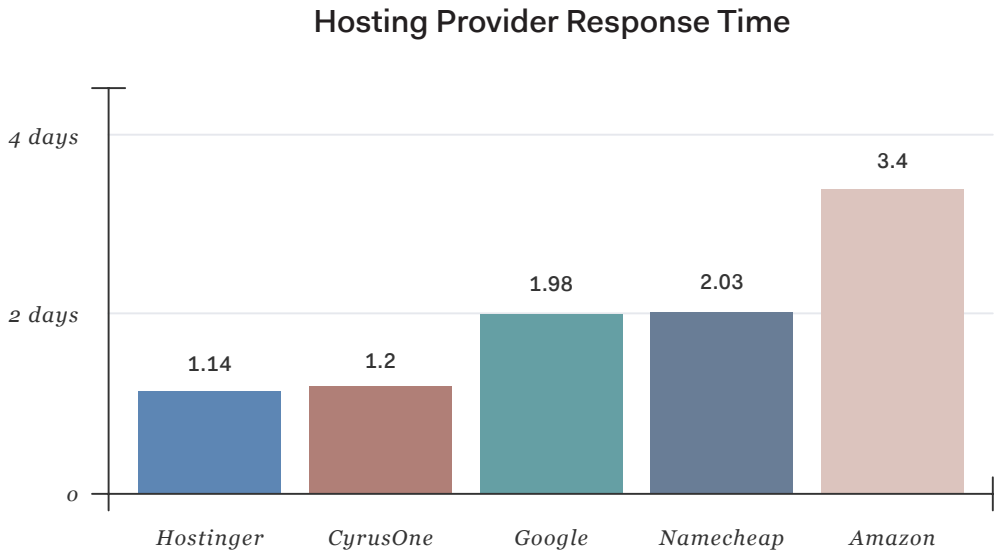
In Q1-2020 , we worked with several hosting providers worldwide to take down tens of thousands of phishing and counterfeit websites. Every top hosting provider decreased their average take down time in Q1-2020.

In this section, we talk about the most responsive hosting providers who took immediate action to bring such websites down.

Hostinger was the most responsive hosting provider in 2019, and continues to lead hosting providers in Q1-2020.

CyrusOne, Google, Namecheap, and Amazon follow closely behind with an average takedown time (in days) of 1.2, 1.98, 2.03 and 3.4 respectively.

Phishing and counterfeiting will be on the rise, and scammers will find new ways to spin up such websites on a large scale. We need hosting providers like these to help mitigate the impact and protect people online.



Source: https://checkphish.ai

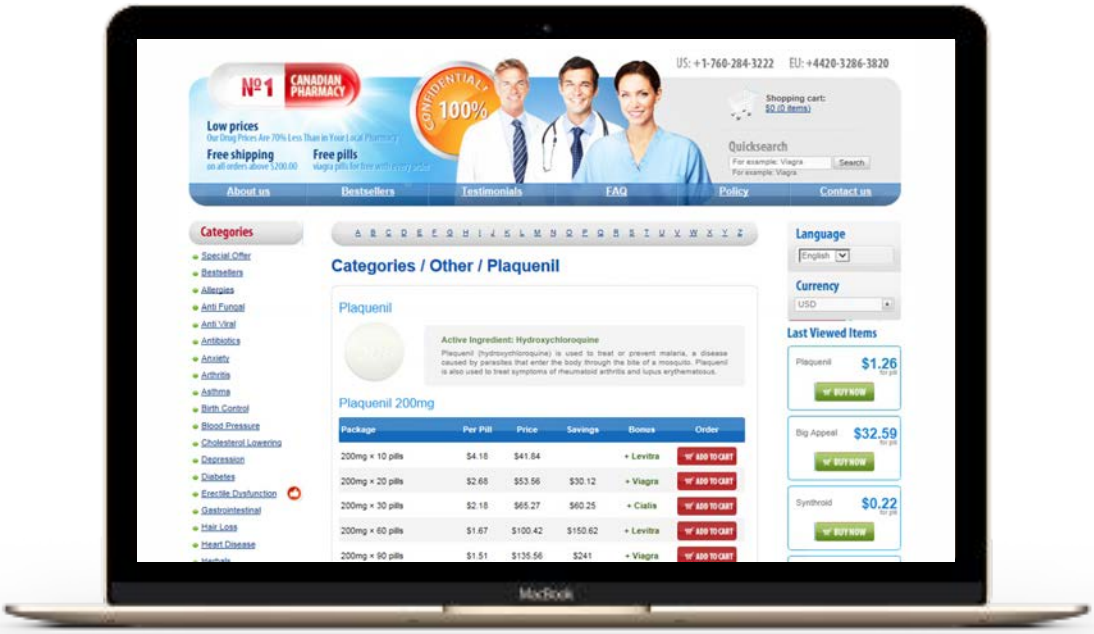
Popular Scams of Q1 2020

In this section, we talk about some of the most popular and interesting phishing / scam websites we detected in Q1 2020. Our researchers have pulled data on certain brands as examples of these scams, but we know countless others are impacted every day. Please note that these are not the only ones affected by the problem. Almost every brand with an online presence was impacted by counterfeiting in Q1 2020.

COVID-19 Scams - Medical

In the month of March alone, Bolster found 102,676 websites related to medical scams, with 1,092 websites either pretending to sell Hydroxychloroquine or spreading misinformation about using it to cure COVID-19. Feel free to take a deeper dive on our COVID-19 Scam Tracker page.

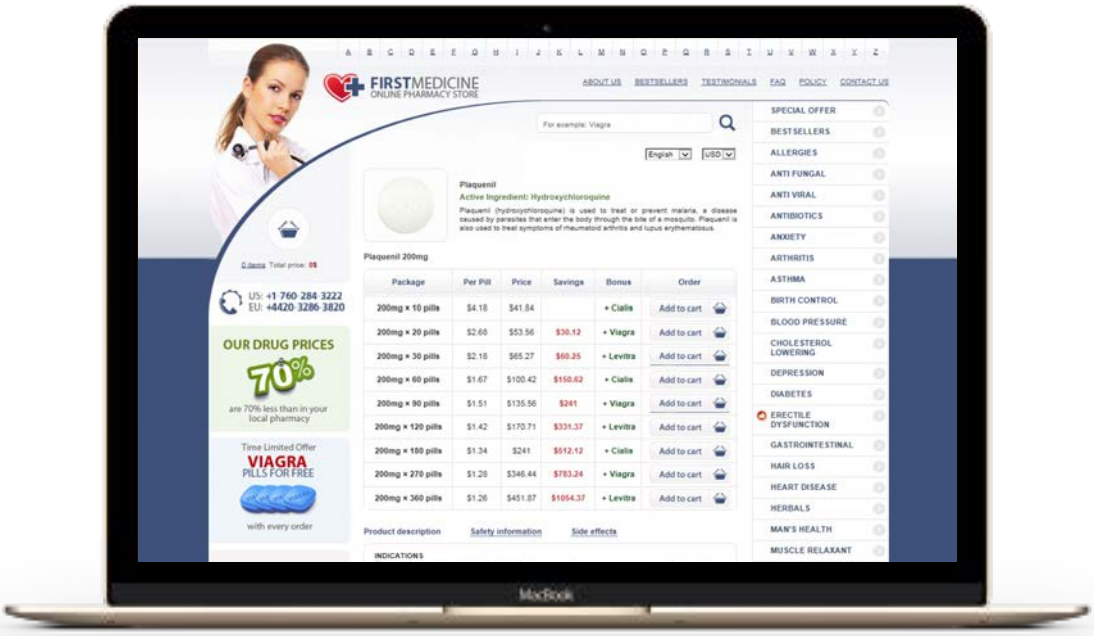
REFERRAL OR AFFILIATE SCAMS FOR FAKE PHARMACIES



hxxp://hydroxychloroquinelab[.]com/

One of the most popular Hydroxychloroquine scams is a low-quality counterfeit online pharmacy, purporting to sell hydroxychloroquine. This site has no intention of actually sending you any medication. It mimics the user interface of a generic online pharmacy with a simple screenshot, and then routes any click to a generic online pharmacy. The pharmacy can either sell you a real, and sometimes dangerous, medication, or simply phish your information for later use.

Source: https://checkphish.ai



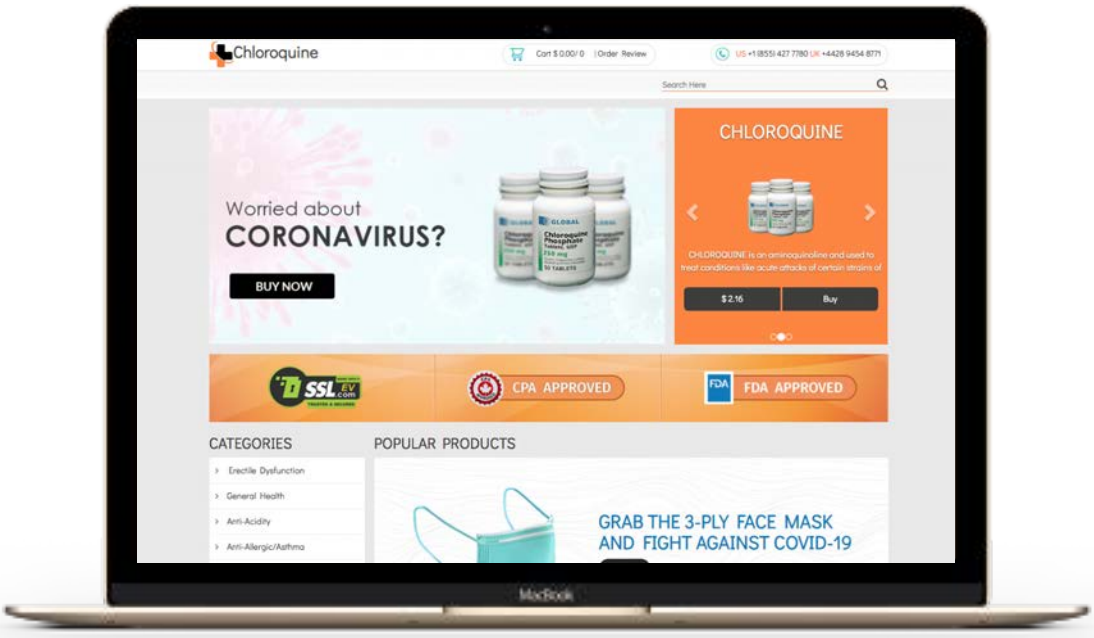
hxxp://hydroxychloroquine911[.]com/

hxxp://hydroxychloroquine sale[.]com

Source: https://checkphish.ai

High Quality Fake Pharmacies

Another popular HC scam is a high-quality counterfeit online pharmacy, purpose built for hydroxychloroquine sales and purporting to sell hydroxychloroquine. This site has no intention of actually sending you any medication. This type of scam looks like a generic online pharmacy. Once you try to pay, it takes you to another fake site. This fake pharmacy is not trying to send any medication, but instead it is trying to phish your information for later use.



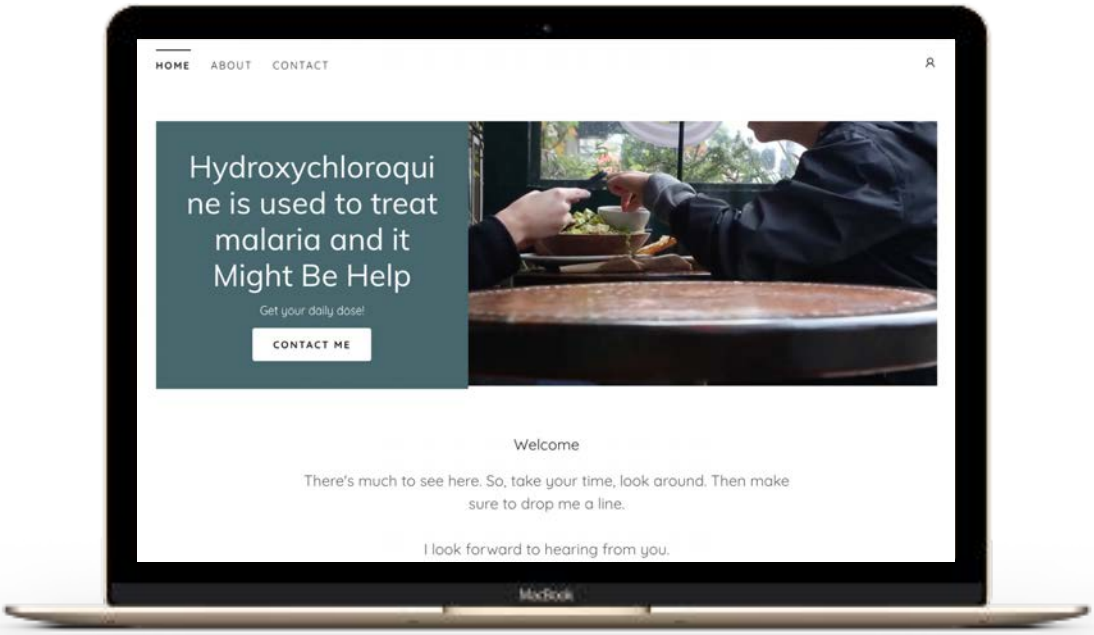
URLs:

hxxp://hydroxychloroquine 250[.]com
hxxp://hydroxychloroquine norx[.]com

Source: https://checkphish.ai

Hydroxychloroquine Misinformation Scams

Lastly, a popular kind of hydroxychloroquine scam revolves around spreading misinformation about the drug and its ability to treat COVID-10. These sites can either drive traffic to a fake online pharmacy, collect your sensitive information, or simply misinform.



hxxps://covid-19hydroxychloroquine[.]com

Source: https://checkphish.ai

Hydroxychloroquine Misinformation Scams, cont'd.

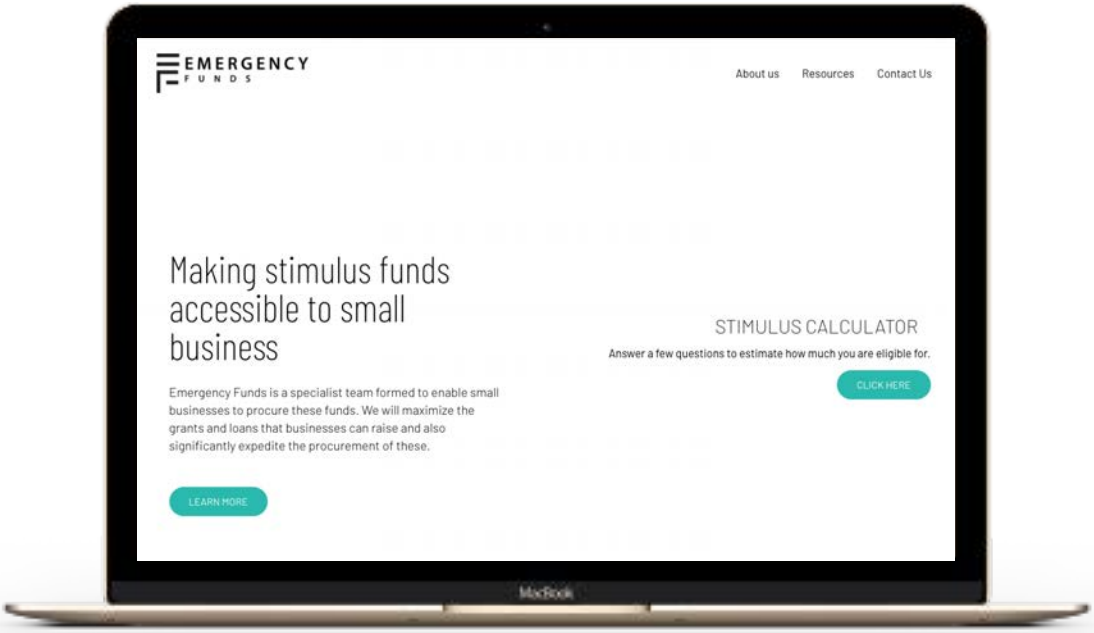
hxxp://hcqcovid19[.]com

Source: https://checkphish.ai

COVID Scams - Financial/ Stimulus

Stimulus checks and loans brought out the hackers. In Q1, we found over 145,000 suspicious domain registrations with ‘stimulus check’ in them. The number of websites that claim to offer small business loans jumped 130 percent from February to March. Hackers spun up 60,707 banking websites to attempt to siphon off stimulus funds.

STIMULUS CHECK SCAMS



hxxp://emergency funds[.]net

Source: https://checkphish.ai

COVID Scams - Financial/ Stimulus, cont'd.

hxxp://2020coronavirusstimuluscheck[.]com/

Source: https://checkphish.ai

Small Business Loan Scams

The number of websites that claim to offer small business loans jumped up 130% (from 273 in February to 628 in March).

hxxp://smallbusinessloanssf[.]com/

Source: https://checkphish.ai

COVID-19 Crypto Scams

This is a site that attempts to get people to download suspicious files by pretending to share a download for a special COVID-19 cryptocurrency wallet. The site may add additional phishing or scamming CTAs in the future.

EXAMPLE 1: POTENTIAL MALWARE

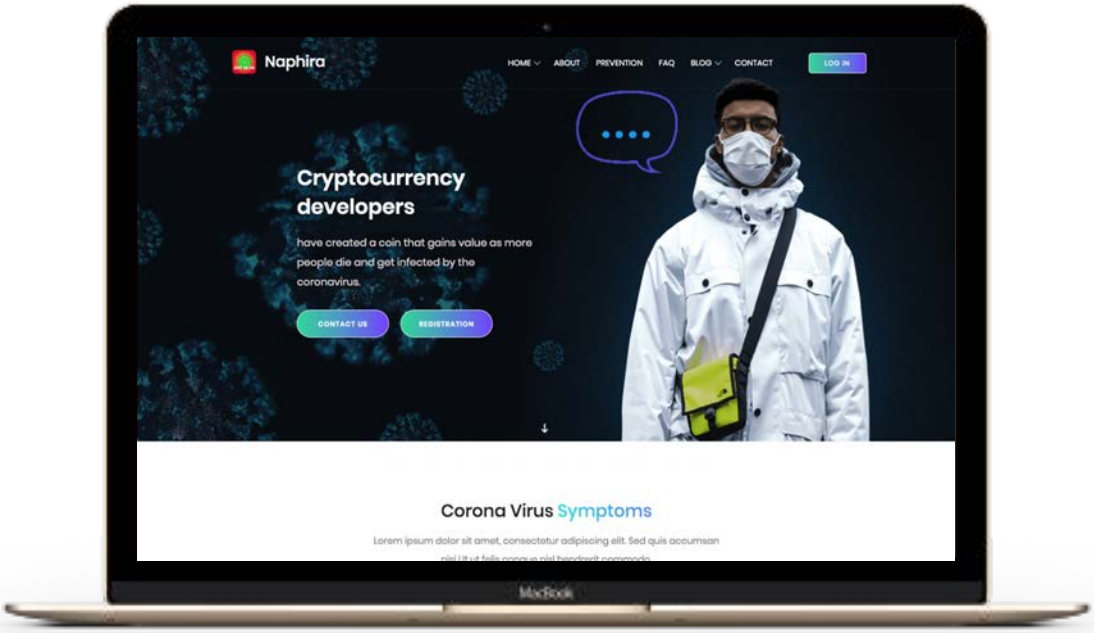
hxxp://covid19crypto[.]com/

Source: https://checkphish.ai

COVID-19 Crypto Scams, cont'd

This site attempts to get you to create an account for their fake cryptocurrency. The submitted account information might be used to guess the victim's credentials on other sites.

EXAMPLE 2: PHISHING



hxxp://covid19[.]finance/

Source: https://checkphish.ai

Conclusion

Thank you for reading the second installment of Bolster's quarterly State of Phishing and Online Fraud report. We anticipate phishing site creation to continue to increase, especially as we proceed further into a COVID-minded world. The phishing lures and tactics will change, but the underlying credential theft will not. We will continue to fight the world's phishing problem and provide meaningful research and data back to the broader community.

Though COVID-19 phishing attacks spiked in Q1, we were impressed by the broader cybersecurity community's mobilization. Cybersecurity organizations and professionals joined together to fight phishing and online fraud in their own unique and inventive ways. Additionally, top hosting providers improved their takedown times from prior quarters, making a real difference in the lives of online citizens. Together, we can raze phishing and online fraud.

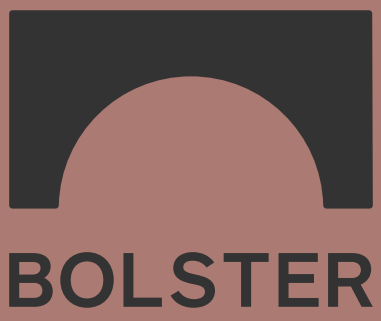
To stay updated on future quarterly reports and phishing/fraud trends, please submit the subscription form on bolster.ai/reports

Download our free COVID-19 threat intelligence feed or find more examples of COVID-19 phishing here: checkphish.ai/coronavirus-scams-tracker

CheckPhish is our free community site scanner. It provides all the real-time accuracy of the Bolster Detection Engine - at no cost. Feel free to scan one-off suspicious URLs or integrate our free API for programmatic real-time detection.

Are you a brand or company representative? Learn more about our fully automated online customer protection or brand protection at bolster.ai/online-customer-protection

Are you a representative of a non-profit or social benefit corporation? Visit bolster.ai/for-good to learn more about our social good program. We're offering at-cost online customer protection services to approved organizations.



www.bolster.ai
4966 El Camino Real, Suite #101
Los Altos, CA, USA 94022
info@bolster.ai

CHECKPHISH by BOLSTER

Data Source:
https://checkphish.ai