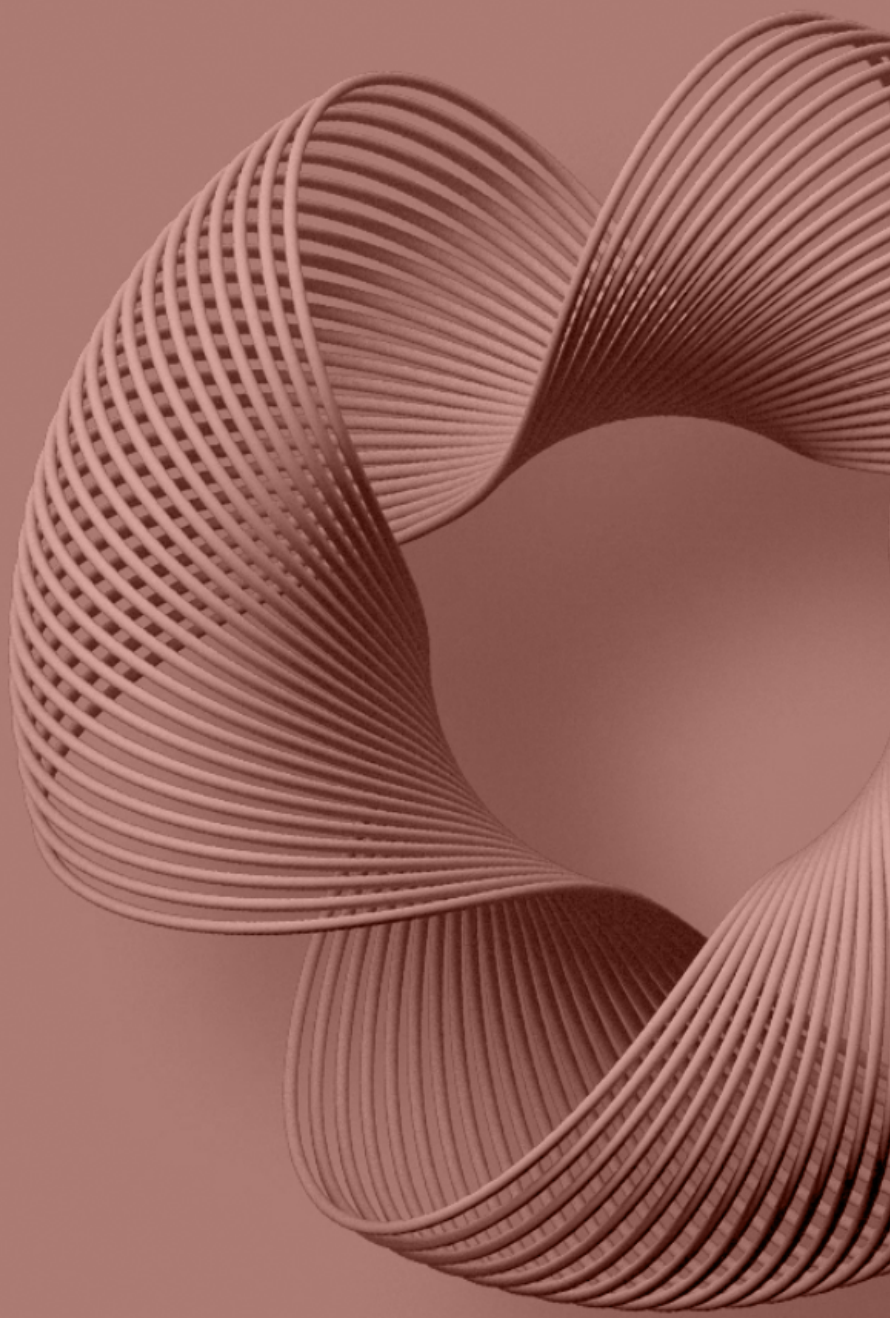
State of Phishing & Online Fraud

Q2 and Q3 2020 Report



BOLSTER

Executive Summary

Cybercriminals continue to use the Internet as a playground, creating new ways to deceive and steal from users and businesses every day.

The pure scale of their activity is alarming. Our Q2 2020 research reveals a 13% increase in phishing and scam sites over Q1 2020. Major brands once again felt the sting of these scams, as did this year's presidential candidates and their campaigns. We are facing a crisis of scale that demands a paradigm shift. With an average of 18,000 scam sites created every day, businesses must fight scale with scale using the power of artificial intelligence, machine learning and automation.

Introduction

The Internet is a cesspool of fraud and theft of information, data, and wealth. Criminals operate in the open with impunity, violating copyrights, misrepresenting brands, and peddling deceit overtly. They do not hide in the shadows of the dark net. Instead, they use mainstream ISPs, hosting companies, and free Internet services – the same ones that are used by legitimate businesses every day.

Cybersecurity is facing a scale crisis. Criminals are creating thousands of phishing and counterfeit pages every single day. Their weapon of choice is deception. Victims are tricked; believing they are interacting with a legitimate business, they offer up their corporate login credentials; personal information like a social security number, address, or phone number; financial details like banking and credit card information, and more. In turn, cybercriminals use this data to impersonate the victim and apply for credit cards or loans, open bank accounts, steal corporate information including private customer data, and for other fraudulent activity.

Based on our latest findings from Q2 2020, these numbers are only getting higher, and cybercrime continues to spiral into chaos as criminals take control of the Internet. There are more than 4 million suspicious pages live today. Businesses are falling victim to these cybercriminals due in part to the sheer scale of the attacks. The traditional security paradigm is to wait for an attack to happen and then either try to prevent it or mitigate the associated risks. Rather than playing defense all the time, Bolster plays offense.

Like looking for and de-activating land mines, we go out to the Internet and remove, neutralize and de-weaponize the threat so it cannot do harm. We fight scale with scale through a combination of AI, natural language processing, and automation to identify criminal intent on millions of web pages every day. And then we work with hosting providers to shut those sites down fast—often within minutes from discovery. The automation works so well our average time to take down from detection is only three minutes.

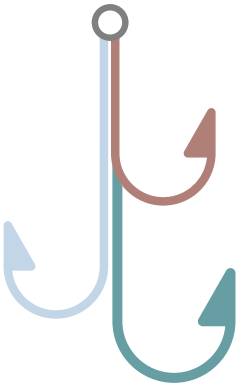
AVERAGE TIME IN MINUTES FROM BOLSTER DETECTION TO TAKEDOWN

3

In this quarterly report, we provide a summary of the most recent trends in phishing and scams, offer insights into the scale, breadth and scope of these attacks, and finally take a deeper look into examples of recent attacks and how organizations can protect themselves.

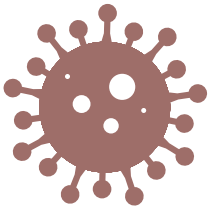
Quick Look: How Data Changed from Q1 to Q2

Overall, 13% increase in phishing and scam sites, peaking in June



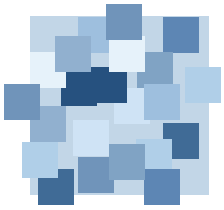
45%

of phishing attacks use free Gmail accounts to collect user and compromised data



COVID-19 related scams rose more than 22%

Telecom moved from the third to the second most targeted vertical



US remains the host to most of the phishing and scam sites, though the number of US sites dropped from 61% to 37%

Turkey moved into the top 10 list of countries hosting the most phishing sites in Q2

OVHcloud

was the most responsive hosting provider, appearing on our list for the first time

.info

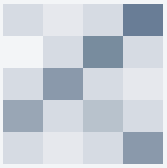
replaced .net as the second most common TLD used for hosting phishing and counterfeit websites

Q2 Trends and Findings

Cybersecurity is facing a scale crisis

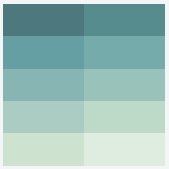
The Internet gets more and more dangerous every day. Many users are lulled into a false sense of security, assuming they won't be targeted or victimized – confident they could spot a phishing or fraud scam a mile away. But companies like Twitter, Amazon, PayPal, Microsoft and Apple know better; all felt the sting of phishing and fraud scams in Q2.

Criminals are operating at scale, flooding the Internet with thousands of new phishing and counterfeit pages daily. In Q2, we saw an alarming, rapid increase of new phishing and fraudulent sites being created, detecting 1.7 million phishing and scam sites – a 13.3% increase from what we detected in Q1 2020. Phishing and scam sites continued to increase in Q2 and peaked in June 2020 with a total of 745,000 sites detected. On average, there were more than 18,000 such sites created each day.



17M

NEW PHISHING AND SCAM SITES DETECTED IN Q2



13.3%

INCREASE FROM Q1 2020

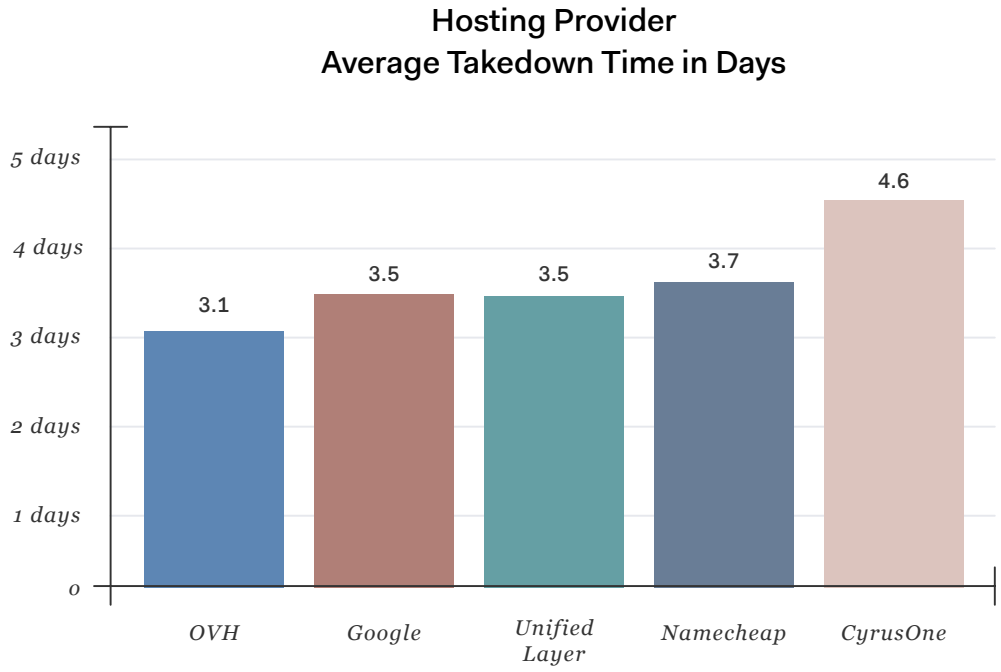
18,000

AVERAGE NUMBER OF FRAUDULENT SITES CREATED DAILY

One of the most startling trends we found is a rapid increase of new phishing and fraudulent sites without an extraordinary event. Extraordinary events, such as a global pandemic, major retail sales, or government aid announcements can cause large spikes in phishing and online fraudulent campaigns. However, our data found that the number of new malicious sites being created is now at a higher level, with no extraordinary shocks. The sheer volume means that an attack will inevitably succeed, and why ridding the cesspool of phishing and fraudulent activity is essential.

As businesses continue on their journey to digital transformation, the opportunities for cybercriminals to exploit vulnerabilities will only increase. The most effective way to respond to these cybercriminals is by shutting down their phishing and scam sites. It's more important than ever for hosting providers to step up and help mitigate the impact from online threats. The faster a hosting provider takes those sites down, the less damage to everybody: businesses, employees, and customers.

In Q2 2020, we continued to work with several hosting providers worldwide who took immediate action to bring down tens of thousands of phishing and counterfeit websites. Appearing on our list for the first time, OVH is the most responsive hosting provider, with an average takedown time of 3.1 days. Google, Unified Layer, Namecheap and CyrusOne follow closely behind with an average takedown time (in days) of 3.5, 3.5, 3.7 and 4.6 respectively.



Source: https://checkphish.ai

New scams are targeting remote workers

In the spring and summer of 2020, employers had little choice but to quickly enable remote working capabilities for the majority of their employees. Projects that would normally have taken months or years to plan and execute had to be implemented in a matter of days and weeks. This rushed approach inevitably created new vulnerabilities, providing cyber criminals with new opportunities to target users and infiltrate businesses. Scammers quickly shifted their attention to developing new phishing attacks targeting work-at-home employees.

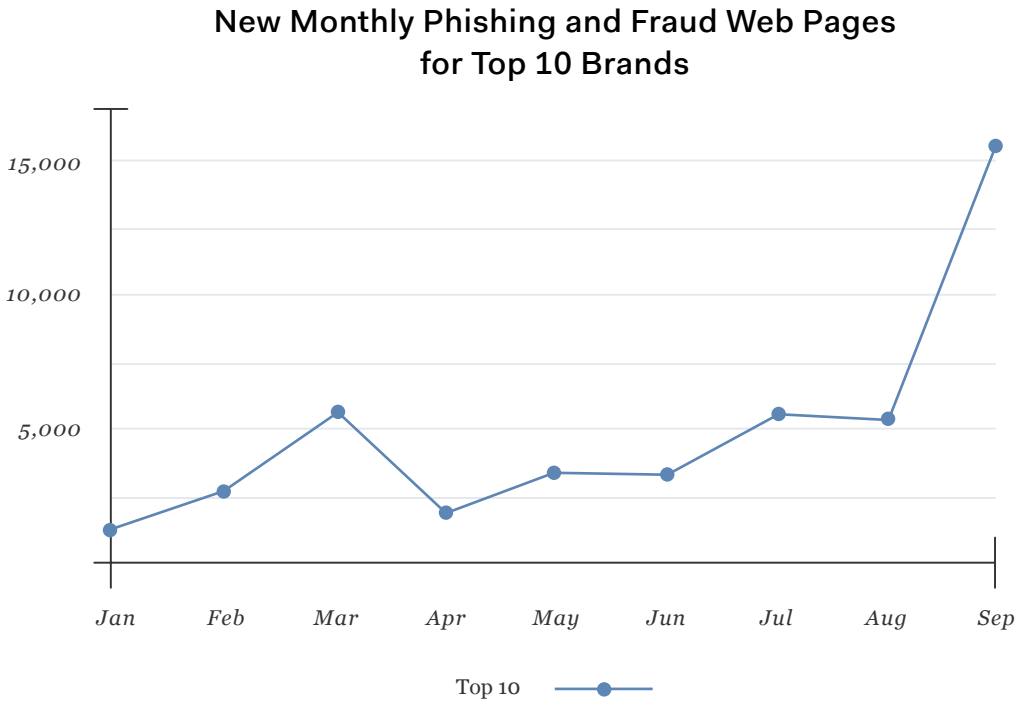
Threat actors took advantage of the new remote working experience for users, by sending urgent, company-related messages that require immediate action. Cybercriminals posed as corporate IT Support asking users to take action, for example, entering their login information to update their VPN access. The link in the email then took the user to a seemingly branded, legitimate website where they were asked to provide their credentials. Upon doing so, they exposed that account and any others that use those same credentials for signing in.

Another common type of attack on the remote worker is an urgent email from the employee's boss or another executive, requesting that they make payments to a vendor, possibly to fill an invoice or pay for office equipment and supplies. Cyber criminals are banking on the fact that new remote workers will fall victim to scams that prey on their need to access corporate assets remotely to be productive or their instinct to please a person in a position of power.

Brand impersonation continues to escalate

Cybercriminals continue to strike at the heart of organizations' identities and reputations; the consequences can be devastating. A recent report from Ponemon Institute found that the average cost to an organization due to a cybersecurity attack in 2020 is $3.86 million. Those costs can span years and cost centers, impacted by audits, crisis management, loss of customers, reputation and revenue, regulatory fines, outreach to affected customers, and much more.

Our data reveals that the top 10 brands are responsible for nearly 44,000 new phishing and fraudulent websites from January through September in 2020. Every month, there are approximately 4,000 new phishing and fraudulent websites created for just these 10 brands alone. September saw a near tripling in volume, with more than 15,000 new phishing and fraudulent sites being created for these top brands. The sharp increase is likely due to criminals preparing their campaigns for the upcoming holiday season.

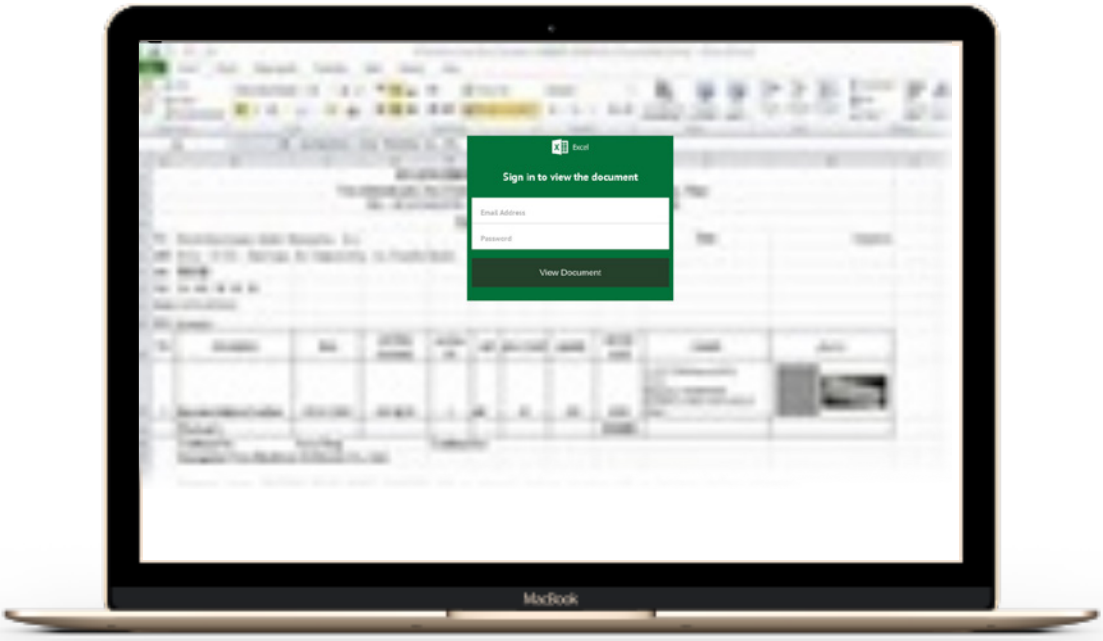


Source: https://checkphish.ai

Microsoft

Among the three brands driving the sharpest increase, Microsoft accounts for almost 50% of the total number of phishing and fraudulent web pages. Detailed analysis shows that the attack focused on credential phishing through the creation of fake login pages for the company's leading SaaS services. The pages were crafted with a high level of attention to detail, indicating the threat actors are highly sophisticated. Phishing and fraudulent websites related to Microsoft continue to increase, and in the first half of September they surpassed the number of malicious web pages created in March.

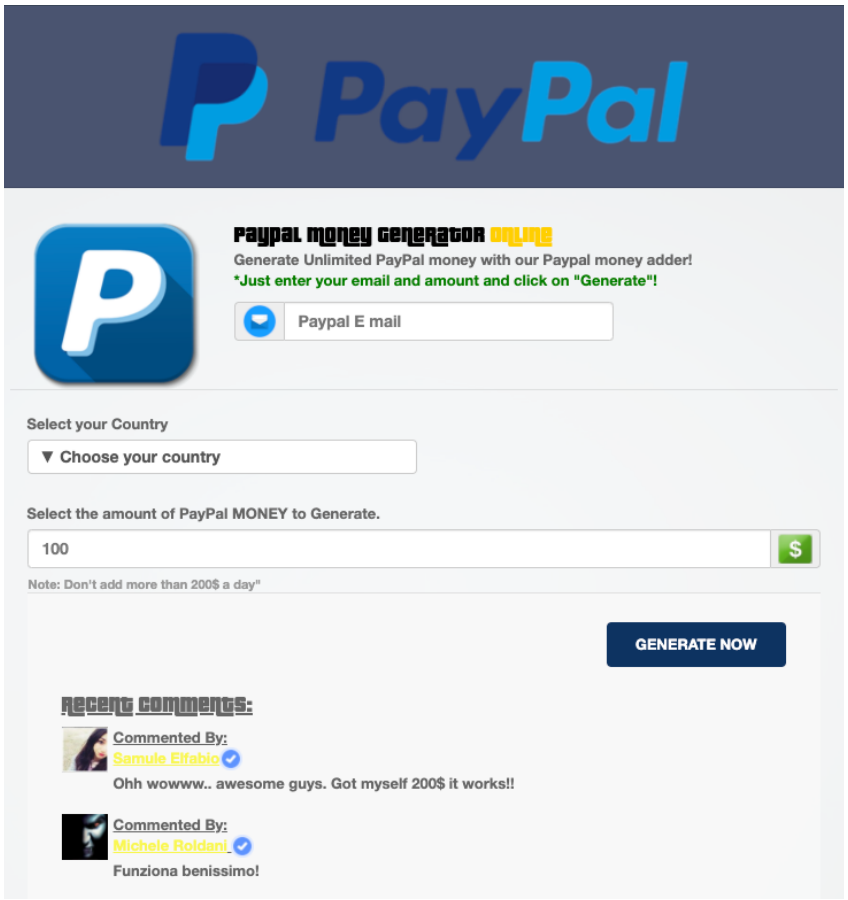
MICROSOFT PHISHING SITE



PayPal

Our data finds that most of the attacks on the online payment giant were instances where PayPal was used to collect fraudulent payments or harvest user credentials. One novel campaign purported to add money to an account by only providing credentials. To make the site look authentic, the fake site added numerous endorsements from people whom supposedly made hundreds of dollars.

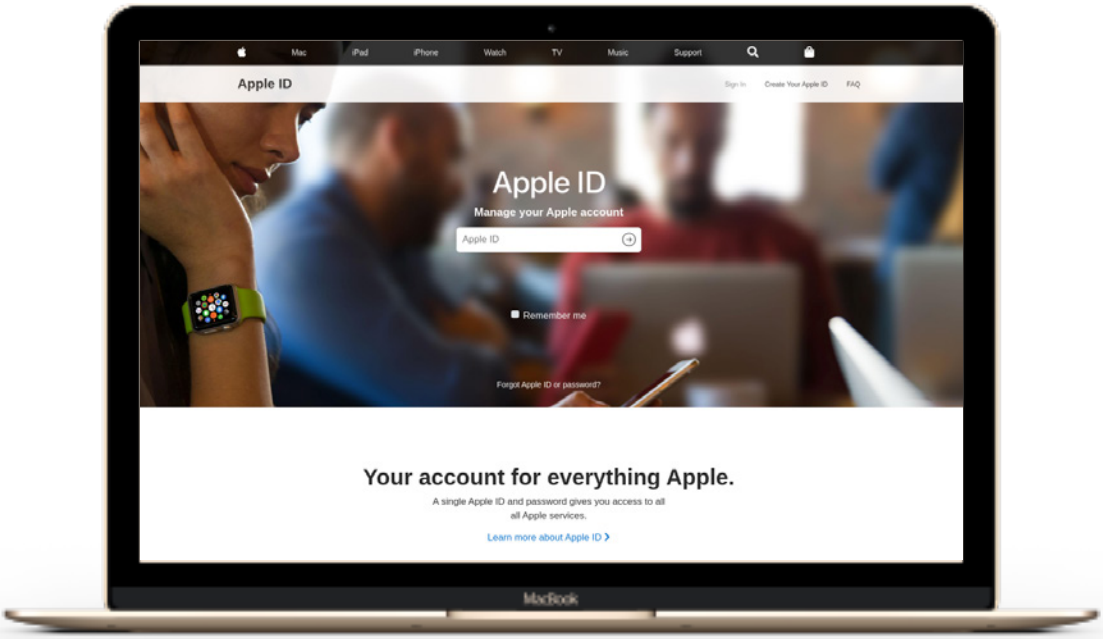
PAYPAL PHISHING SITE



Apple

Apple experienced a very large spike in July, with more than 10X its usual volume of phishing and fraudulent websites, and returned to normal levels in August. The Apple campaign attempted to gain user's Apple ID login and password information. The threat actor created multiple domains that displayed a fake Apple ID login page. The URL used was designed to trick users into thinking it was a legitimate Apple domain by using "secureupdate.appleID.com." However, upon closer inspection it was clear the domain was actually "duilawyeryork.com."

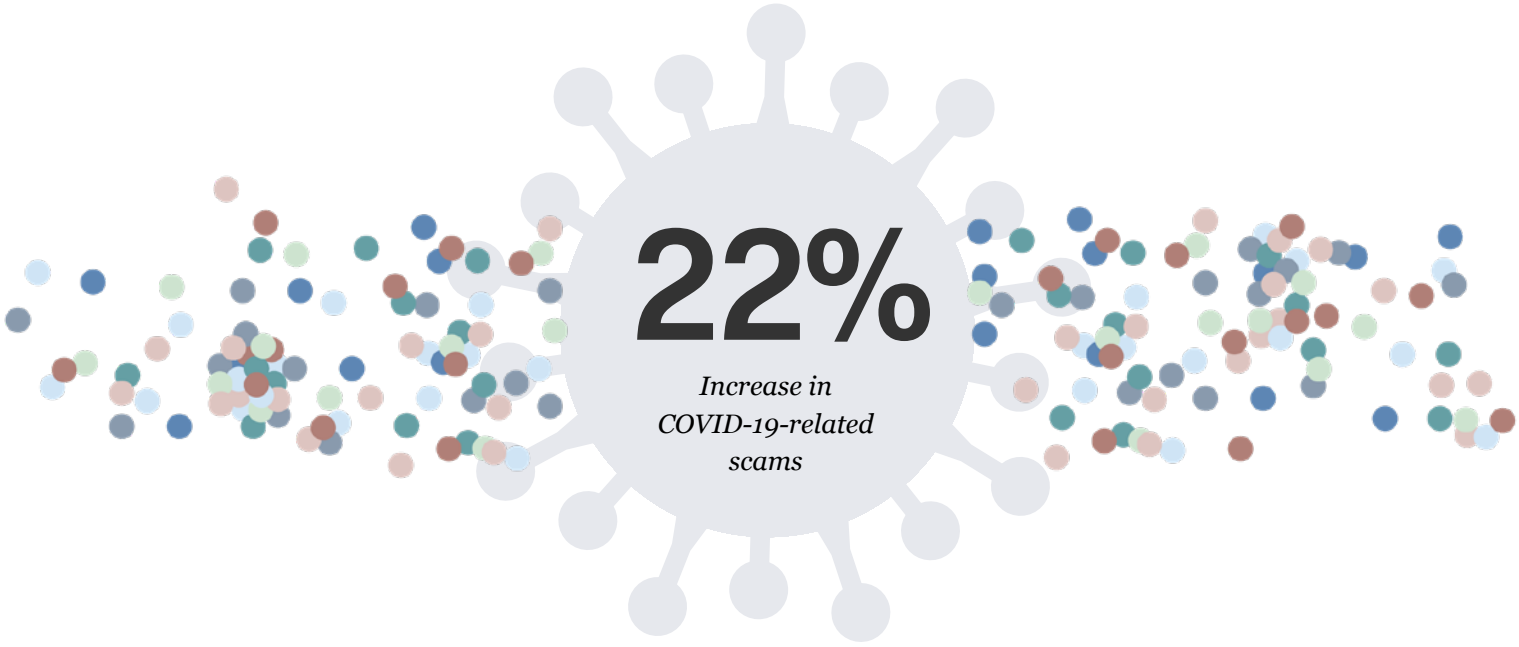
APPLE PHISHING SITE



COVID-19 is still a target, but less so

Since the World Health Organization (WHO) declared a worldwide pandemic in March, life as we knew it changed. Much of the world is still sheltering in place, and virtual-everything has become the norm. Cyber criminals adapted quickly, and the Internet was immediately flooded with online phishing and fraudulent websites. The campaigns covered everything from fake local government COVID-19 updates to offers to help with the U.S. Government Paycheck Protection Program.

COVID-19 related phishing and scam sites continued to increase in Q2 following the trend of the global pandemic. Compared to Q1, these scams increased by 22%. In Q2, scammers followed the dynamic news headlines to change their strategies to defraud people in new and creative ways. From fake coronavirus drugs, N95 masks and government stimulus checks to fake employer, charitable and community-related cons, the sheer variety of phishing and fraud scams we detected was something we had never seen before.



There is one good piece of good news to share. Although COVID-19 related scams increased overall in Q2, they were on the decline month-over-month.

Cybercriminals use common, free email services

The most active phishing scammers are using the very same services most of us use – free email accounts from trusted providers like Google and Yahoo. Most phishing attacks utilize something called a drop email to collect the information that is collected from a phishing site. We analyzed more than 78,000 phishing kits and found that 66,000 of those used a drop email address. Among the kits with drop emails we found 16,321 unique email addresses, meaning that many scammers were using multiple – many times hundreds – of phishing sites. The top two most active drop emails we found being used were team_pbg@yahoo.com and resultpage2020@gmail.com, followed by threat actors using Yandex, Hotmail, Protonmail and Outlook accounts.

Phishing Kit Analysis

No. of Phishing Kits	78,607
No. with Drop Emails	66,0751
No. of Unique Email Addresses	16,321

Email Service

Among all the email services being used, Gmail was by far the most popular with over 45% of email address. Yandex, from Russia, was the second most popular service with 7.3% followed by Yahoo! With 4.0%.

Email Service	% Phishing Drop Emails
Gmail	45.3
Yandex	7.3
Yahoo	4.0
Hotmail	2.8
Protonmail	1.6
Outlook	1.5
Other	32.5

How it works:

A phishing kit is a collection of code and tools that helps scammers carry out a phishing attack. Once a phishing kit is created for a particular brand it can be deployed anywhere, by anyone, and at any scale. Each phishing kit is associated with a drop email, i.e. an email account created by the criminals. Every time a victim enters their credentials, the information is sent to a drop email belonging to the scammers carrying out the phishing attack.

Q3 Phishing & Scam Website Examples

Cybercriminals continue to be highly creative, leveraging new methods and technologies to get what they want. Though phishing and fraud campaigns outside of extraordinary events are on the rise, cyber criminals continue to demonstrate their agility to profit from major events. Scams connected to Amazon Prime Day and the presidential election offer up examples of just how clever these criminals can be.

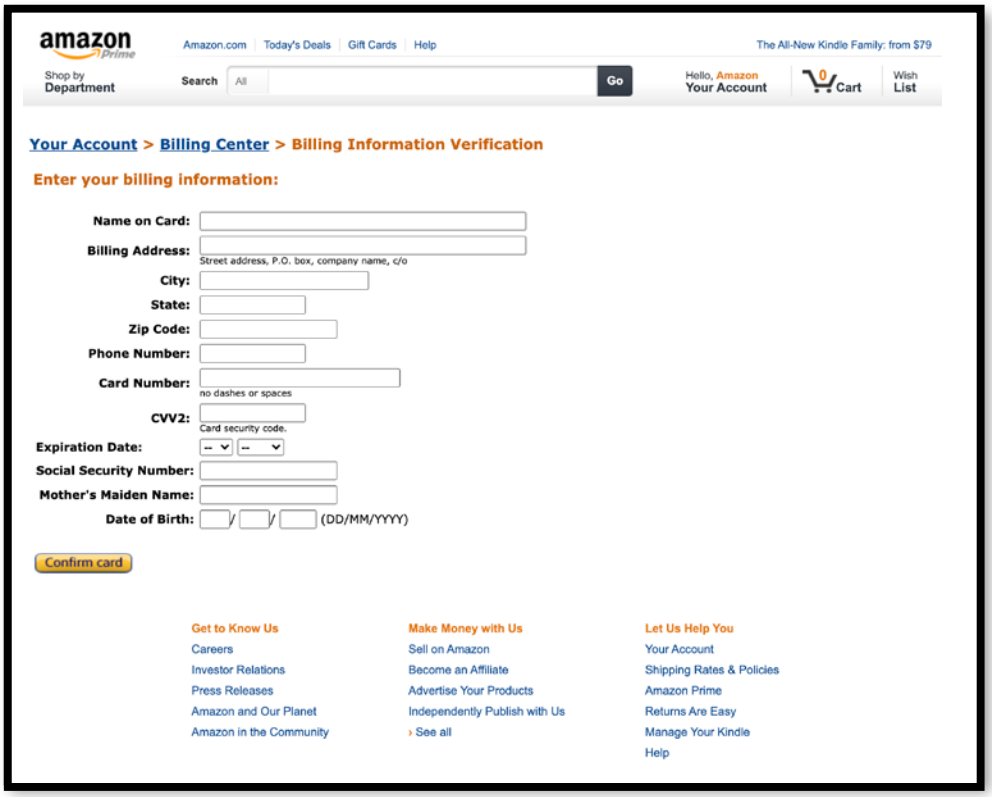
Fall Amazon Prime Day Scams Run the Gamut

Prime Day is Amazon's largest, most highly anticipated retail event, bigger than Cyber Monday and Black Friday combined. As shoppers geared up for two days of great deals, threat actors were prepping to prey on the unwary, taking advantage of those who let their guard down to snap up bargains.

We analyzed millions of web pages and tracked the number of new phishing and fraudulent sites using the Amazon brand and logos. We identified a sharp spike in August, with another 2.5X increase in September. The obvious spike was a strong indication that cyber criminals were gearing up for a profitable Prime Day to take advantage of unsuspecting victims, excited to secure the best deals. These criminals demonstrated the depths of their deceit and creativity through a number of campaigns.

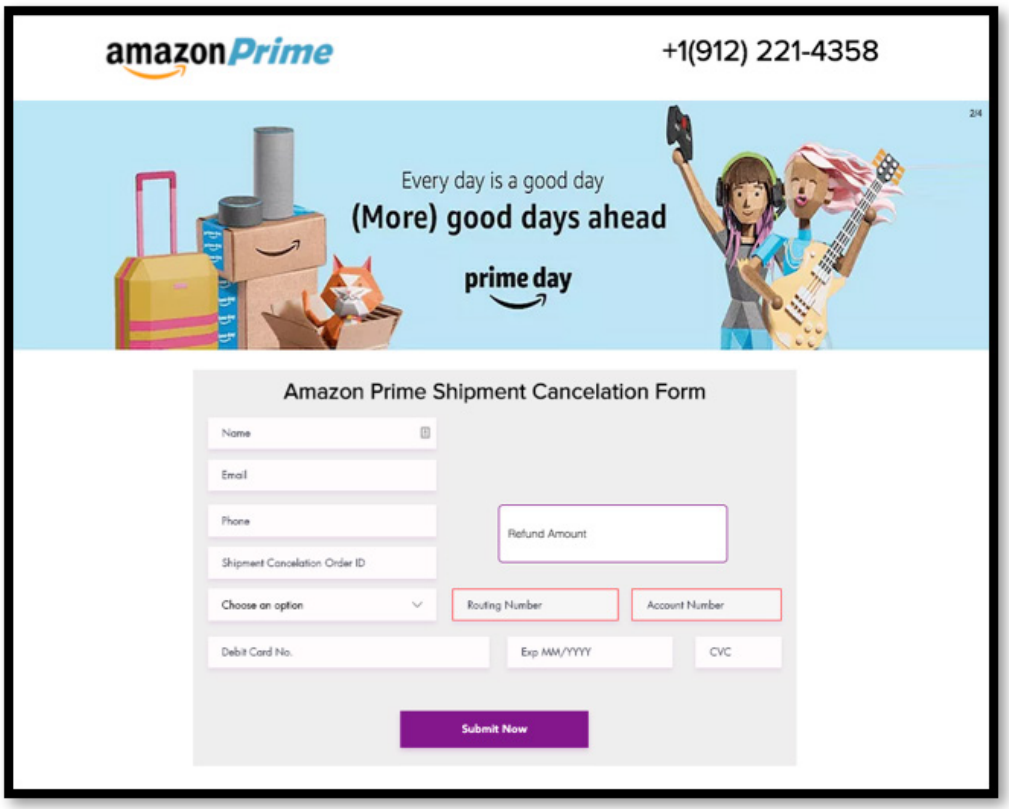
Payment confirmation: One fraudulent campaign discovered the day before Prime Day looked very authentic. The criminals took the time to actually copy elements of the Amazon website in great detail. The page asked the user to confirm payment details for their purchase and even promoted "The All-New Kindle Family: from $79." The page copied the header and footer layouts, fonts, and dimensions to really deceive the shopper. But, on closer inspection, there were clear warning signs the site was a fraud. For example, only the form itself worked; the other links went nowhere. The information requested on the form was far more than what Amazon usually asks for, such as a social security number, date of birth, mother's maiden name, or even the CVV number.

AMAZON PRIME DAY PAYMENT SCAM SITE



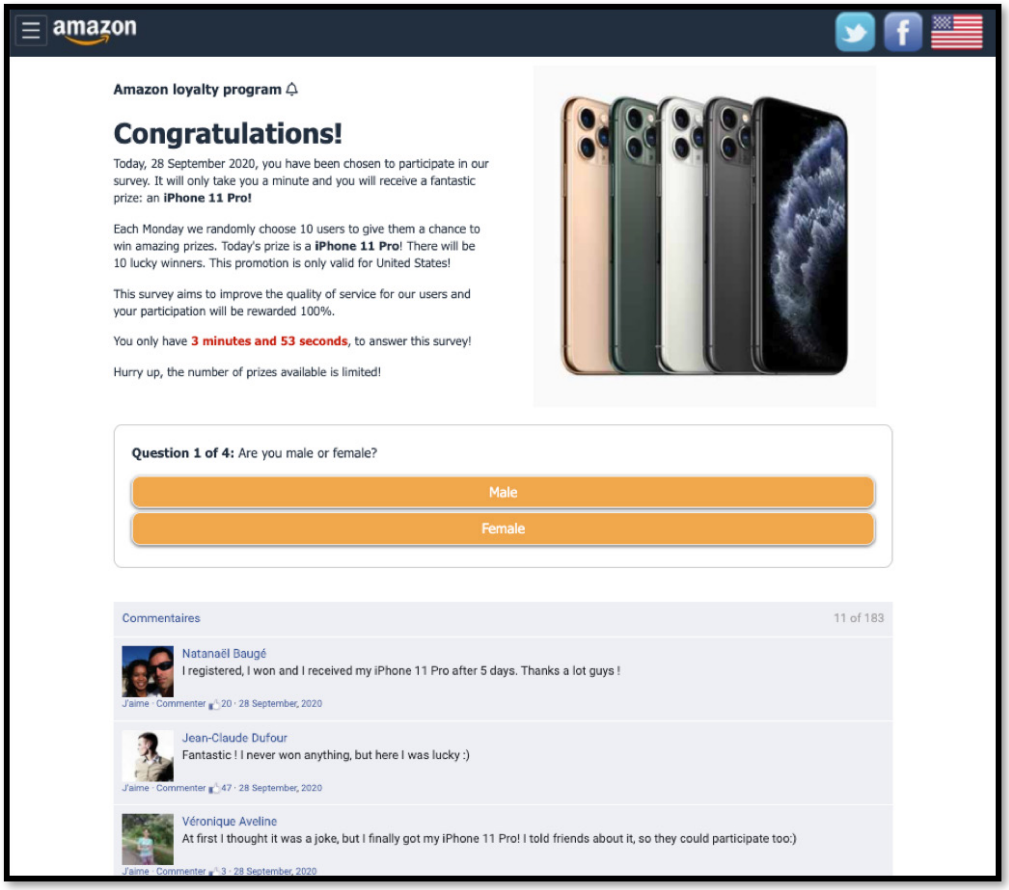
Returns and cancellations: Another campaign targeted "returns" or "order cancellations" related to Prime Day. The URL www.amazoncustomersupport[.]net was designed to mimic an authentic Amazon site, and the webpage could easily fool an unsuspecting shopper. However, a closer look clearly indicated the site was not legitimate. For example, the form requested bank or credit card information – Amazon always offers refunds to original form of payment or gift cards. Also, no password was required – Amazon always requires an Amazon account to make purchases and returns.

AMAZON PRIME DAY RETURNS SCAM SITE



Survey for free merchandise: Another fraudulent site promoted an Amazon loyalty program and offered a free iPhone 11 Pro for answering a few survey questions. The user was asked four easy questions and then directed to a simple game that looked like they would likely lose. Of course they won, and were required to enter credit card information for a $1 to receive the iPhone 11 Pro. On the website, glowing customer reviews validated the offer. The site claimed the phone would be delivered in 5-7 days. But the $999 phone would never arrive, and the shopper likely began to see strange charges on the credit card number provided.

FAKE SITE OFFERING $1 IPHONES



2020 Presidential Campaign Welcomes Counterfeiting and Internet Trolling

Cyber security is a critical issue for the 2020 Presidential Campaign, dominating news headlines. Along with the typical election crimes including voter and campaign finance fraud, today's campaigns are also fraught with nation state cyber attacks. Microsoft recently reported that nation state criminal groups from China, Iran and Russia are actively interfering with the campaign and government officials.

To date, attacks include a range of techniques from spear phishing, where targeted emails trick users into disclosing confidential information or user credentials, to brute force password spraying, a tactic hackers use to access accounts through common passwords.

Bolster Research recently discovered the Trump and Biden campaigns are dealing with online issues beyond traditional cyber attacks. The Trump campaign faces a rampant counterfeit paraphernalia problem, where unofficial merchandise is being distributed and sold through various websites – impacting the campaign's ability to raise funds. For example, one site, https://officaltrumpgear[.]com, looked legitimate but misspelled the word "official."

The Biden campaign is dealing with Internet trolling, not financially destructive, but disconcerting. The Biden campaign has only two websites that are suspicious. One seeks a $20 donation, but never claims the money will go to the Biden campaign. The other leads to a parody site that promotes negative and disturbing news about Biden.

Like any other brands, the Trump and Biden campaigns should be more diligent in protecting their public perception. In the commercial world, it is common practice to remove phishing and fraudulent sites by contacting the hosting company. Companies like Bolster leverage a combination of deep learning, computer vision, and natural language processing to complete this process without human intervention. Given the scale at which the criminals operate, this automated takedown process is realistically the only scalable solution to the problem.

Actionable Learnings

Be Proactive

Organizations need active threat elimination that removes the threats that endanger their customers and employees. This approach is the antithesis of cyber defense, which is waiting for an attack to happen and then trying to prevent it or mitigate the ensuing damage.

Our approach: we find them before they find you. Bolster turns the security paradigm upside down and removes threats and digital risks before an attack occurs. Bolster has developed AI technology that evaluates more than 1 million web pages per day. The combination of deep learning and natural language processing results in a 99.999% accuracy in determining whether a web page is designed for malintent. Leveraging AI and automation, Bolster is able to remove these sites within hours of discovery with zero human intervention. We empower companies to proactively take back control of the Internet by stopping cybercriminals before they can even attempt an attack.

Find and stop attacks as quickly as possible

In 2020, the average time to identify and contain a data breach is 280 days. Every day an attack goes unnoticed, the potential damage to a business increases, eroding revenue, customer trust, brand equity and so much more.

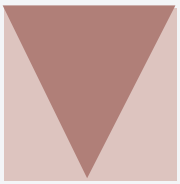
Using AI and natural language processing, Bolster can scour the Internet in real time, quickly identifying and taking down phishing and fraudulent sites in minutes at scale. We also tirelessly monitor known and suspicious sites to monitor for any malicious activity. The minute we detect malintent on a site, our technology automatically takes the site down—no human intervention needed.

As the COVID crisis was spiking in the United States, Zoom, the leader in modern enterprise video communications, took steps to bring on Bolster swiftly. Within the first 24 hours, the Bolster Detection Engine discovered and took down 1,476 sites with a 99.3% takedown rate. The near-instant takedown ensured that the vast majority of users were never exposed to Windows and Android malware, various phishing sites, and tech-support scams.

Zoom Case Study

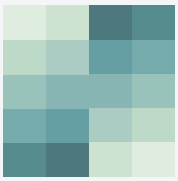
1,476

SITE TAKEDOWNS
IN THE FIRST 24 HOURS



99.3%

TAKEDOWN RATE
IN THE FIRST 24 HOURS



14,012

SUSPICIOUS SITES
IDENTIFIED AND MONITORED
IN THE FIRST MONTH

Fight scale with scale using automation, AI and machine learning

Fight scale with scale using automation, AI and machine learning Technology advances created these problems, but they also offer a potential solution: automation at large scale. Corporations do not have the manpower to monitor millions of websites and thwart malicious sites, but artificial intelligence and machine learning solutions do.

Bolster has developed artificial intelligence that delivers human intelligence at machine scale. It combines deep learning, computer vision, and natural language to understand the intent of a page rather than static criteria. Trained on the world's

largest data set of phishing and fraud sites in the world, Bolster algorithms are so sophisticated that they recognize minute differences between a legitimate brand logo and a highly sophisticated illegitimate one. They also recognize how a site is handling sensitive information, like a username and password, and flag cases of potential fraud.

With AI and machine learning, accuracy rates are vital, especially for automation. Bolster has developed the industry's most accurate algorithm with a false positive rate of 99.999 % (1 in 100,000). The automation results in a takedown rate of over 99% within 24 hours – all without requiring manual intervention.

1 in 100K

FALSE POSITIVE RATE

99%

TAKEDOWN RATE WITHIN 24 HOURS

Neutralize the threat. Hit the bad guys where it hurts.

Aside from jail time, the worst-case scenario for phishing and fraud cyber criminals is having their websites shut down. Doing so immediately stops the flow of information and money. Leveraging AI and automation, Bolster is able to identify and remove these fraudulent sites within hours of discovery with zero human intervention. Free scanning of suspicious URLs or sites can be done using our community product available at checkphish.ai.

Conclusion

With the holiday shopping season kicking off, the results of the presidential election, and the New Year approaching, we anticipate the number of phishing and fraud attacks will continue to rise through the end of 2020 and into 2021.

Similar to the Amazon Prime Day scams, threat actors will inevitably prey on our holiday excitement and stress as we look for the best deals, scour the Internet for that sold out toy, or panic over getting our gifts on time.

The outcome of this U.S. presidential election may be unprecedented in its social, emotional and psychological affects on citizens. Cybercriminals will no doubt prey on our passions and heightened emotions.

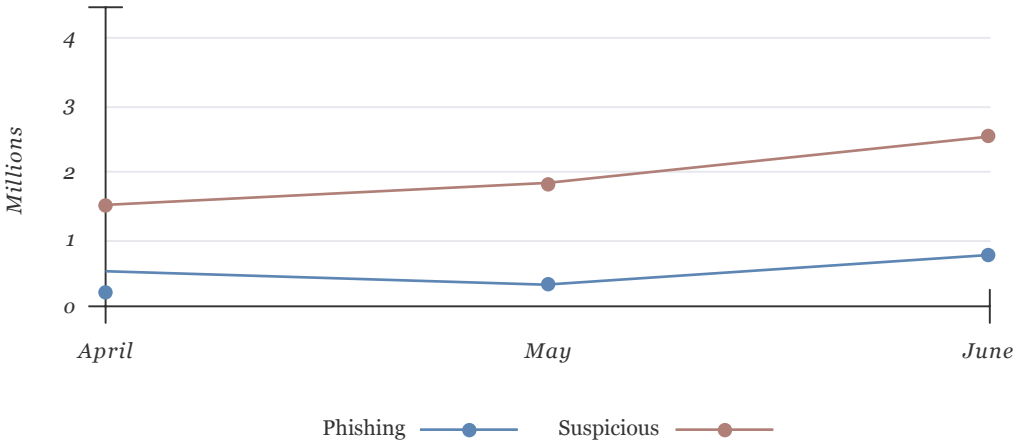
Finally, the New Year will come with its inevitable affect on the corporate world – ringing in new processes, strategies, technologies and more. Workers, particularly remote workers, will likely be targeted with dull messages urgently requesting that they update or download an app, change their credentials or pay outstanding invoices. But the consequences for organizations will be anything but dull.

In anticipation of these events, phishing and fraud cyber criminals are sharpening their knives of deception, planning new and creative ways to dupe victims into divulging important information. To match the scale of attacks, organizations must fight fire with fire, using the power of AI, machine learning and automation to continuously find these sites and shut them down, before an attack ever takes place.

Complete Findings

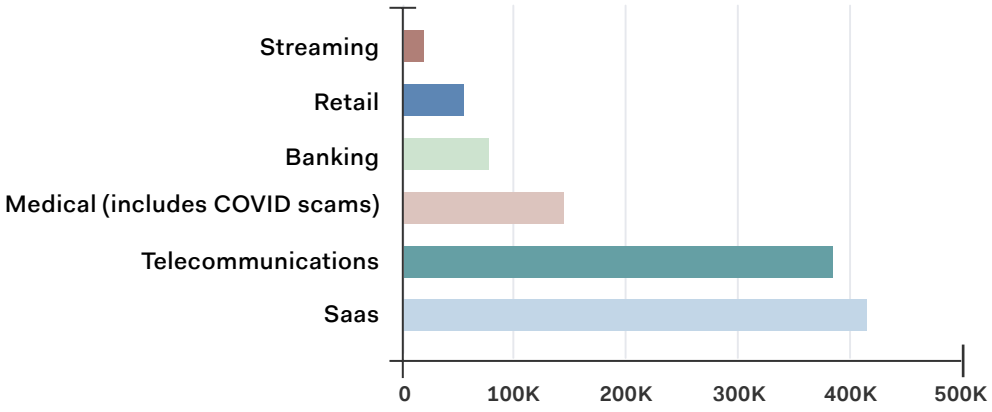
Growth of Phishing

Overall, in the first half of 2020, we've seen total of 2.56M phishing sites, an increase by 7.1% compared to first half of 2019.



Phishing by Industry

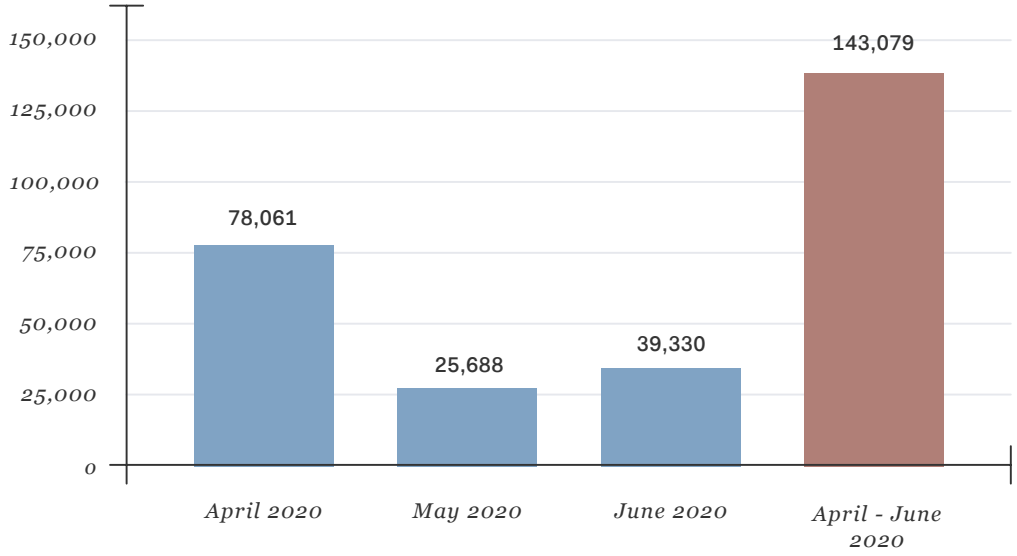
The top three targeted verticals in Q2 continued to be SAAS, Telecommunications and Medical.



Source: https://checkphish.ai

COVID-19 Scams

Suspicious Domain Registrations
Number of COVID Phish & Scams Per Month



Suspicious Domain Registrations
Per Keyword

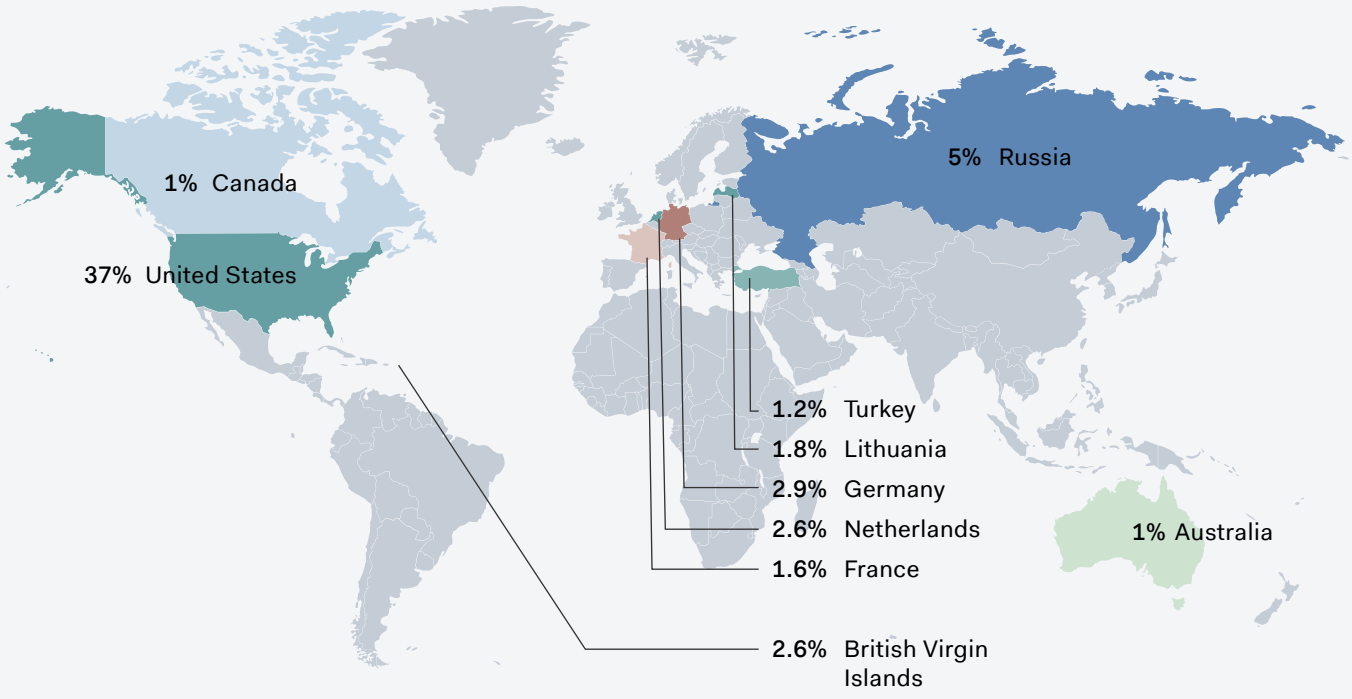
Keyword	*Apr 2020*	*May 2020*	*Jun 2020*
COVID	114,329	31,669	44,990
Corona	96,172	13,440	30,426
n95	3,121	904	976
Mask	44,659	19,751	23,627
Vaccine	2,230	887	955

Source: https://checkphish.ai

Countries Hosting Phishing & Counterfeit Websites

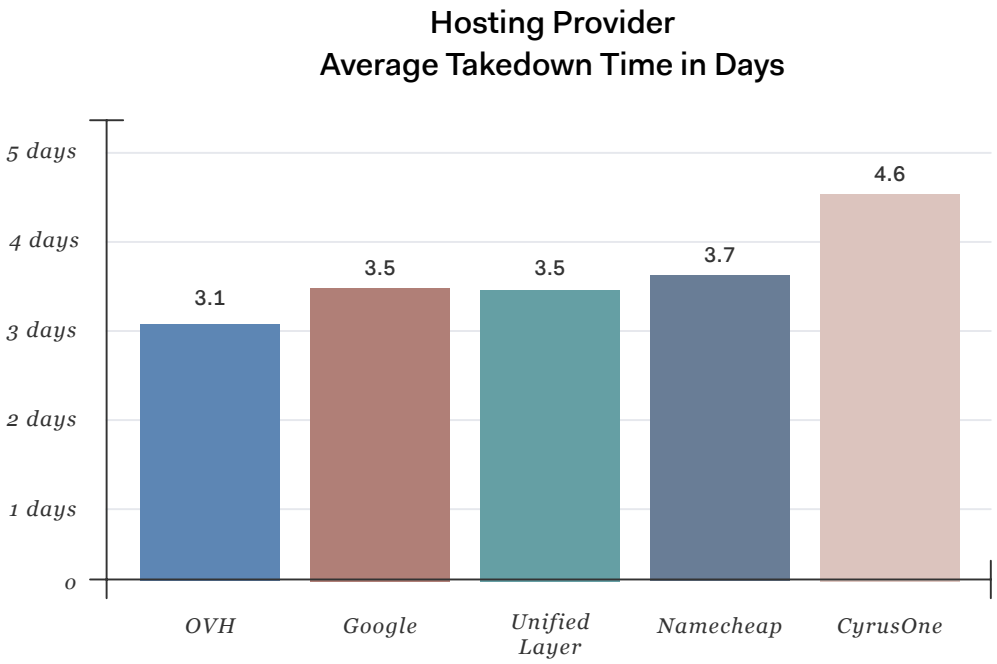
% of Phishing and Conterfeit Websites

Country	*%*
United States	37.0
Russia	5.0
Germany	2.9
Netherlands	2.6
British Virgin Islands	2.6
Lithuania	1.8
France	1.6
Turkey	1.2
Canada	1
Australia	1



Source: https://checkphish.ai

Most Responsive Hosting Providers



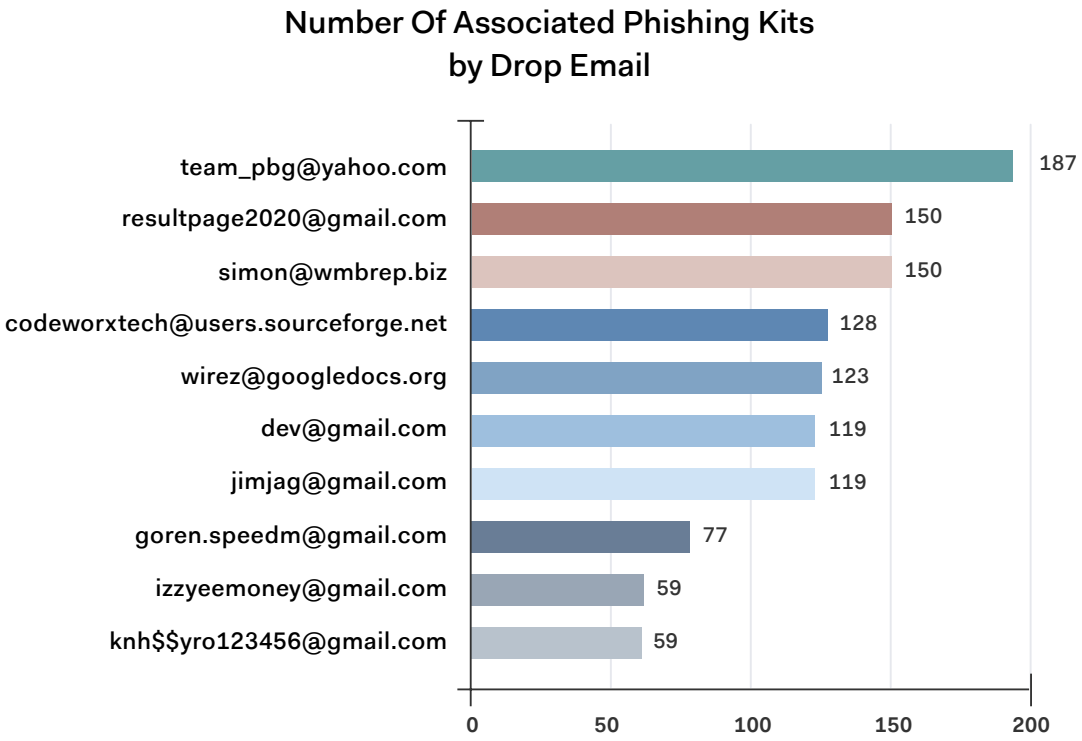
New Monthly Phishing and Fraud Web Pages for Top 10 Brands by Month

(January through August)

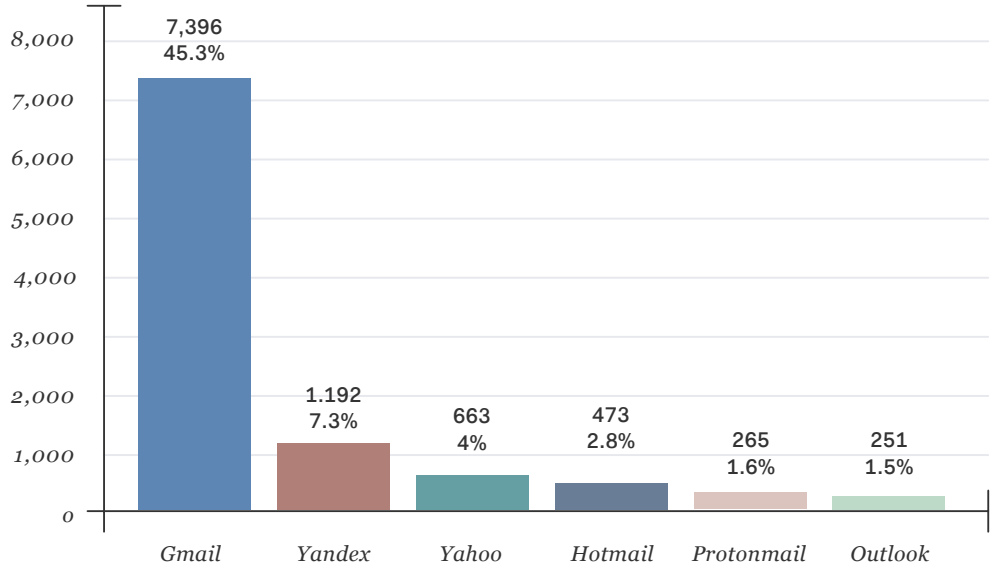
	Jan	*Feb*	*Mar*	*Apr*	*May*	*Jun*	*Jul*	*Aug*
Microsoft	431	957	*2,559*	589	949	1,441	1,754	2,613
PayPal	126	244	*570*	294	1,567	1,020	938	592
Facebook	103	245	*249*	141	199	285	299	414
Adobe	46	166	*409*	163	214	294	329	216
Ray Ban	20	23	*75*	117	236	187	417	408
Apple	76	97	*112*	14	169	76	987	146
Chase Bank	14	106	*929*	105	60	86	119	112
Google	66	112	*303*	94	159	111	136	163
Amazon	39	77	*113*	46	119	167	153	322
AT&T	39	156	*121*	76	115	49	325	175

Source: https://checkphish.ai

Most Active Scammers

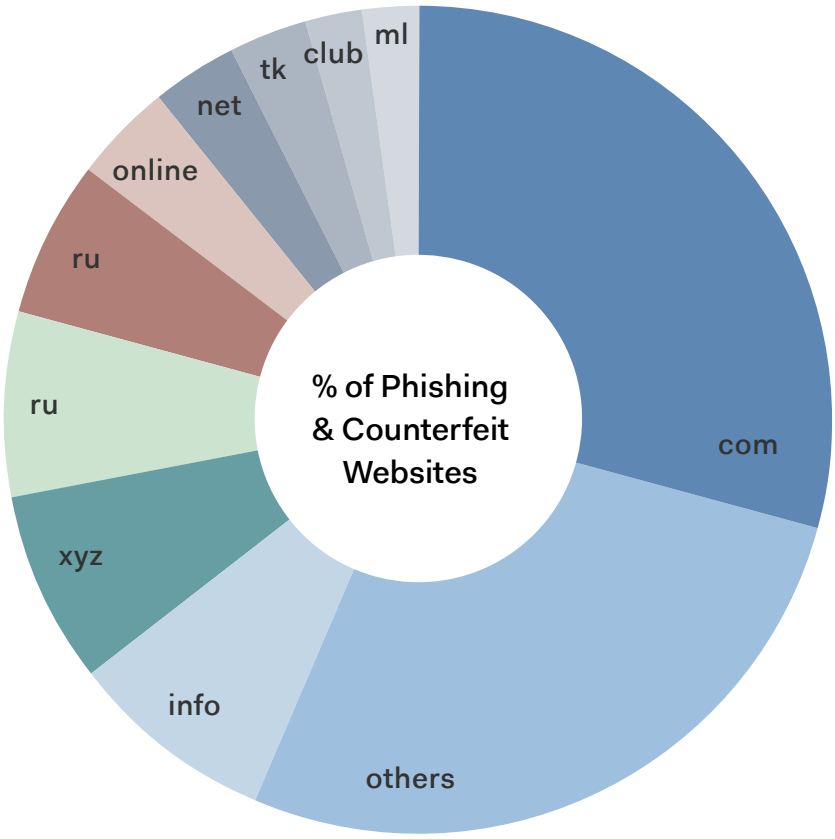


Most Common Email Providers for Phishing Kits



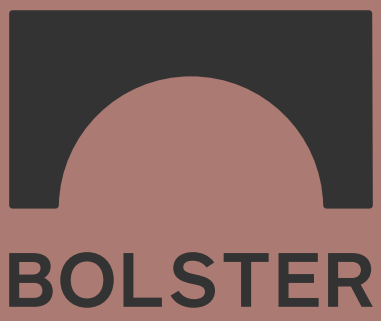
Source: https://checkphish.ai

Most Common Tlds Used For Hosting Phishing & Counterfeit Websites



- com.....29.3%
- info 8.2%
- xyz..... 7.5%
- ru..... 7.2%
- link..... 6.0%
- online.....3.8%
- net.....3.4%
- tk.....3.1%
- club..... 2.3%
- ml.....2.0%
- Others.....27.2%

Source: https://checkphish.ai



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