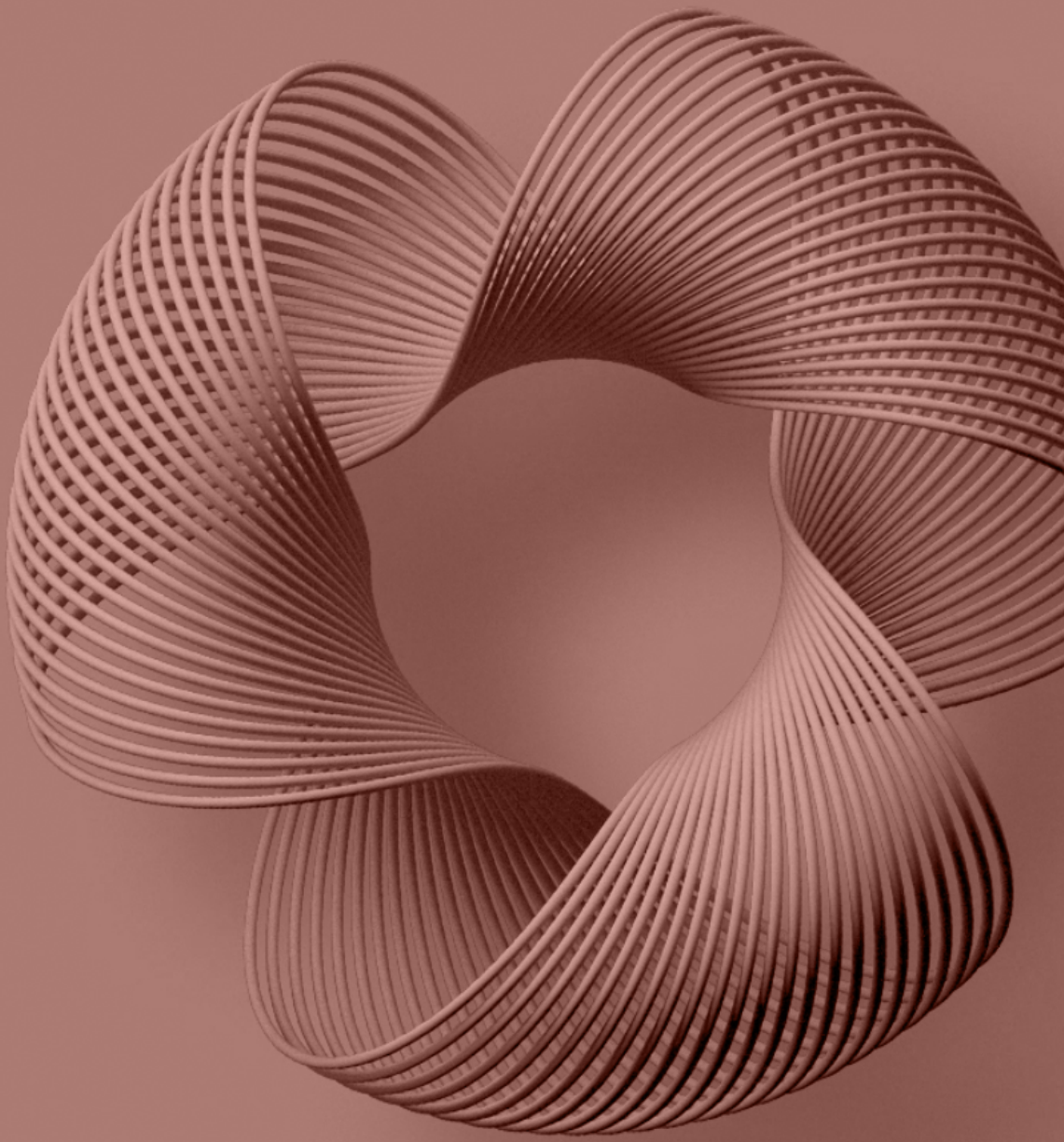
State of Phishing & Online Fraud

2021 Report



BOLSTER

03 Executive Summary

04 Introduction: The Explosion of Digital Business

05 Digital Business = New Threat Vectors and Opportunities for Fraud and Risk

07 Fragmentation = Higher Risk

08 Emerging Trend: Security Plays a Central Role in Trust and Safety

09 Looking Ahead: What to Expect in 2021 and Beyond

09 Key Findings

10 Top Targeted Industries

12 Other Key Trends

14 Trend 1: Escalating Threats

16 Trend 2: Protecting Brand Reputation Gets Harder

19 Trend 3: The 5 Most-Popular Themes

27 Actionable Insights

28 What's Next

28 About Bolster

29 Appendix

Executive Summary

Attacks are Growing Faster than Ever Fueled by COVID-driven Digital Explosion.

Our 2021 State of Phishing and Online Fraud Report highlights the key trends that drove digital scams using data gathered from analyzing more than one billion sites. A multitude of factors drove record growth in fraud campaign activity in 2020 with an increase of 185% from what was observed in 2019.

2020 saw an explosion of digital business as companies accelerated their digital transformation projects and transitioned to remote working and online distribution and sales channels. As digital business exploded, so did the online phishing and fraud activity, averaging more than 19,000 new threats being created daily.

> *"COVID was not the only pandemic in 2020, and unfortunately, there is no vaccine for phishing and online fraud," said Shashi Prakash, chief technology officer and co-founder at Bolster. "Our data shows that the fraudsters seem to be increasing their activity with unabated vigor, and the companies are at risk of damaging their online initiatives unless they rethink their approach to protecting their digital perimeter not just for their employees but also for their customers, partners, and supply chains."*

The report provides insights into the volume of phishing and scam attacks with examples of real phishing and fraud campaign sites being used to steal credentials.

Among the examples of scam sites identified are:

- Online sales of a COVID-19 vaccine with free shipping
- Counterfeit Ray Ban sunglasses being offered for 90% off retail
- Applications to become a mystery shopper for Walmart and Kroger grocery stores

Key findings:

- 6.95 million new phishing and scam pages created
- Key themes used for scams: COVID, gift cards, gaming hacks
- Highest number of new phishing and scam sites in one month: 206,310
- Top three industries targeted: technology, retail, finance
- Top three countries where scams were hosted: USA, Russia, British Virgin Isles
- Top email service used for phishing kits: Gmail

Introduction

The Explosion of Digital Business

Digital business is booming. In today's customer-centric world, brands are interacting with customers through an increasing number of digital touchpoints. This extensive contact enables businesses to be nimbler and more responsive to their customers' needs. But it also magnifies the risks, making fraud detection and security more complex.

The COVID-19 pandemic compelled many businesses to fast-track their digital transformation projects in 2020. Employees needed to work remotely, and consumers increased their online activity and spending almost overnight as many countries enacted restrictions to limit the spread of the virus. A global survey of more than 4,300 leaders across multiple sectors found that 80% have successfully accelerated their digital transformation initiatives, according to Dell Technologies 2020 Digital Transformation Index. Reinventing the delivery of digital experiences for customers and employees was among the top five priorities.[1]

The focus on the digital touchpoints is not surprising. More consumers are interacting with brands digitally, and this trend accelerated during the pandemic as people shifted their activities online.

In just a few months after COVID-19 restrictions came into effect, eCommerce in the United States saw 10 years' worth of growth, according to an analysis by Accenture.[2] Consumers also increased their use of multiple shopping channels—45% shopped more on their mobile phones while 23% shopped more via smart digital assistants, according to a global survey of nearly 4,500 consumers by PwC.[3]

While these digital trends were sparked by the pandemic, they're here to stay. Brands will need to maintain their omnichannel focus.

An Accenture global survey of more than 8,800 consumers found that[4]:

85%

Planned to maintain their increased usage of in-app ordering

80%

planned to sustain their increased shopping via social media channels

77%

said they would continue shopping more on company websites

[1] Digital Transformation Index 2020, Vanson Bourn Research, Dell Technologies, September 2020
[2] "How is COVID-19 changing the retail consumer?" Accenture, August 2020
[3] "The consumer transformed," PwC, 2020
[4] "How is COVID-19 changing the retail consumer?" Accenture, August 2020

This digital business explosion comes at a time when security threats and fraud are escalating. We found that the number of phishing and fraudulent sites going up daily increased by nearly 73% from 2019 to 2020, to a total of nearly 7 million. We also saw an 185% growth from the first to the fourth quarter of 2020 in the number of newly created malicious sies. As Bolster's data shows in this report, the scale of the threat continues to grow—while the environment is becoming increasingly more complicated.

Increase in Phishing and Fraudulent Sites

73%

INCREASE FROM 2019 TO 2020
TO 7 MILLION TOTAL SITES

185%

INCREASE FROM
1ST TO 4TH QUARTER IN 2020

Digital Business = New Threat Vectors and Opportunities for Fraud and Risk

Digital business has amplified risks and created new ones that many companies did not have to consider in the past. Traditionally, fighting fraud was defined primarily as screening payments and securing digital commerce transactions. This is no longer enough in today's landscape, and businesses need to focus on the wider customer interactions for every digital touchpoint, or, as Gartner calls it, the business-to-consumer (B2C) perimeter

Gartner defines the B2C perimeter as comprising eight touchpoints, each susceptible to a range of threats. The perimeter is continuously expanding, and the proliferation of touchpoints will lead to even higher risks. Understanding the nature of this evolving threat landscape, and the connections therein, is critical.

Checkout: Fraudulent activity in this area is common and the prevention mechanisms are mature; however, fraudulent payment methods and stolen or synthetic identities remain a concern.

Login: This is another mature target that businesses have been actively addressing, yet credential theft and account takeovers via phishing campaigns are a constant concern.

Fake domains: Fraudsters can copy entire websites at scale for illicit profits and fraud, and use look-alike domains to steal credentials or syphon business from brands—and grappling with this problem is a tough undertaking for companies.

Search engines: Scammers use various tactics to get counterfeit and phishing sites to show up in organic search results, but many companies overlook this touchpoint, leaving unsuspecting customers vulnerable.

App stores: Brand infringement and impersonation doesn't stop at websites—fake branded apps that pop up in app stores are a growing concern, yet finding them and removing them is a challenge for many digital businesses.

Third-party sites: The digital business ecosystem relies on numerous partners, and companies need to not only understand this ecosystem but also monitor for unauthorized brand use and sale of goods on third-party sites and affiliate sites.

Social media: From fake brand accounts to account takeovers, social media opens up new avenues for fraud; however, this is a less urgent area for many digital businesses since content is highly controlled on those platforms.

User-posted content: Comments, reviews, and other content generated by users can threaten brand trust; getting ahead of this problem requires monitoring online communities and other platforms for harmful posts and malicious links.

Many digital businesses typically take a siloed approach to address these touchpoints. Risk mitigation therefore becomes fragmented among various business functions, each team having a limited view of attack vectors and threats.

For example, a phishing page designed to gain credentials for account takeovers may be viewed as a fraud issue. In reality, that site also impacts customer service and security. Yet the cybersecurity team doesn't get involved unless a corporate account is breached, and customer service is hands-off unless there is a direct customer complaint. Oftentimes, customers do not even know they have been compromised, and by the time they complain to customer service, the fraud has usually already taken place. This causes a negative experience with the company's brand and over time trains the consumer not to trust the brand.

While one phishing attack could impact different areas of the company, the lack of central coordination among the teams prevents businesses from both seeing and solving these problems holistically. Coordination among the groups would allow companies to use the data across the functions and solve problems that impact other departments. Given the speed and scale that cybercriminals operate at today, it is becoming critical that businesses expand their focus on the wider customer interactions and monitor activities wherever the customers interact with the digital brand.

Fragmentation Means Higher Risk

Why is fragmentation of such concern? Because opportunistic threat actors exploit the cracks and the silos. To perpetrate their schemes, they adapt their tactics to leverage more B2C touchpoints.

In the typical organization, different teams and functions have their own objectives. Brand protection is often a legal issue. But ultimately an attack that impersonates a brand can lead to fraud as well as cybersecurity incidents if, for example, the perpetrators take over the email accounts of a high-level executive to initiate a fraudulent financial transaction or steal credentials.

To close the security and risk gaps, businesses need to:

- *Adopt proactive strategies* that enable them to anticipate challenges.
- *Fight scale with scale,* employing artificial intelligence and machine learning for rapid fraud detection.
- *Adopt a customer-centric approach* that accounts for and catalogs the various customer digital touchpoints and threats.

Emerging Trend: Security Plays a Central Role in Trust and Safety

One of the ways organizations can shift to a customer-centric approach is by adopting a "trust and safety" framework. Trust and safety is a cross-functional model that goes beyond fraud detection and brand protection to create a safe and secure environment for customers as part of the overall customer experience.

Security is at the core of a trust and safety framework, which encompasses all the touchpoints where customers interact with the brand. All the teams—from IT, marketing and legal, to finance, customer experience, and fraud analysis—are working in tandem to secure the B2C perimeter. This model builds off the understanding that interconnectivity is increasing and creating new attack vectors, whether customer touches the brand on or off the corporate infrastructure.

Gartner forecasts that 30% of banks and digital commerce businesses will have trust and safety teams by 2023, an increase from fewer than 5% in 2020.[5] Leading companies such as Google, Airbnb, eBay, and TaskRabbit have already adopted the model, setting the example for this next evolution of the market. For brands, trust and safety doesn't just serve to protect customers and employees—it can become a business differentiator.

Trust and safety initiatives require a fine balance between the competing priorities of the different business units or functions. This is where companies struggle, because historically each of those functions had a fragmented view of fraud and security, relying on piecemeal solutions. To succeed, cross-functional teams need tools that are designed to work across the touchpoint ecosystem and provide them a unified view of the company's fraud risks.

[5] "Market Guide for Online Fraud Detection," Gartner, May 2020

Looking Ahead: What to Expect in 2021 and Beyond

The data in this report demonstrates that the scale of fraud and risk is growing faster than today's patchy, reactive approaches can keep up. While no one can predict where the next fraud campaign will come from, it's clear that threat actors are ready to pounce whenever an opportunity arises.

The major 2020 themes were COVID-19, remote work, and technology. In 2021, who knows? Already, we're starting to observe some dramatic shifts. One thing is certain: The scope and scale will not get any smaller, and protecting brands—and customers—will not get any easier without more predictable and scalable strategies

Key Findings

While much of the world plunged into chaos in 2020, the scammers stayed the course. The pandemic did not slow down fraud activity. On the contrary, it provided new kindling for fraud schemes.

Bolster detected more than 6.9 million phishing and scam pages in 2020. New activity grew every quarter, with a 185% increase in the new number of pages from Q 1 to Q 4. The daily average for the year eclipsed 19,000. Although the averages fluctuated down on some months, they grew steadily every quarter—starting with 7,391 average new phishing and fraudulent sites in January, and peaking at 28,158 average daily in November.

6.9M

MILLION PHISHING AND SCAM PAGES TOTAL

19,000

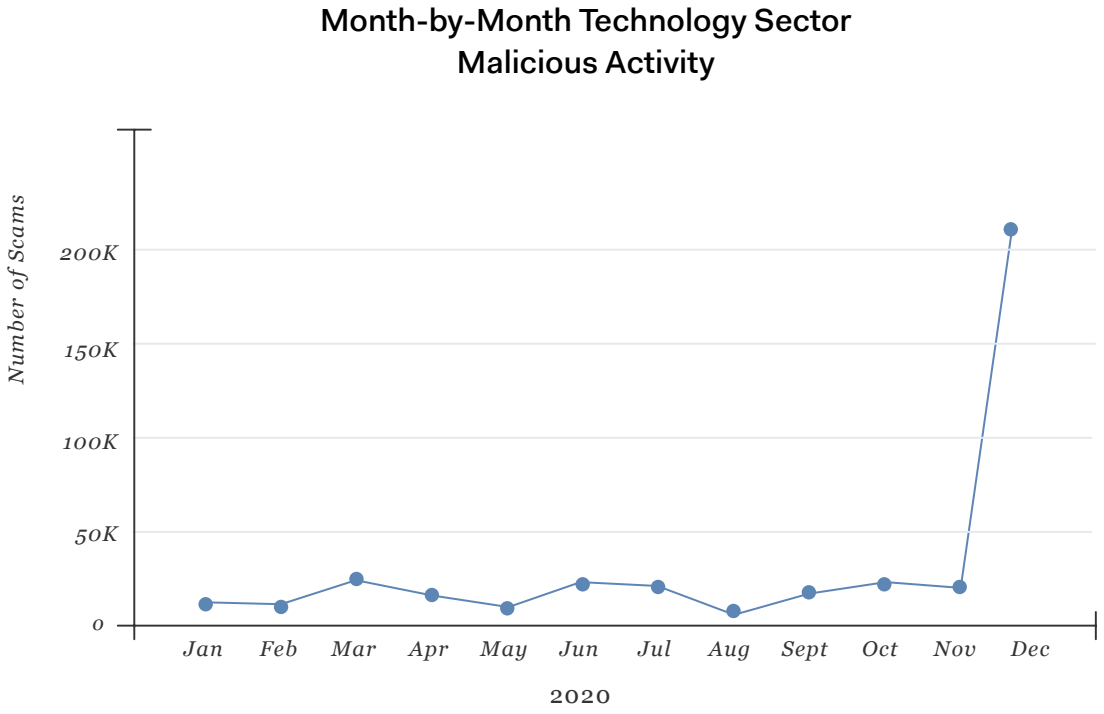
NEW PAGES CREATED PER DAY, ON AVERAGE

TOP 3 MONTHS WITH HIGHEST DAILY AVERAGES

November — 28,158
December — 27,374
June — 24,068

Top Targeted Industries

Many sectors experienced a lot of economic uncertainty in 2020, but the technology industry saw a boom. Perhaps that explains why scammers targeted the technology sector the most, with nearly 347,619 new phishing and fraudulent pages total and about 5% of the daily average. December was an especially busy month for scammers—more than half of the malicious pages targeting technology sector went live that month, surpassing the total of the previous 11 months combined.

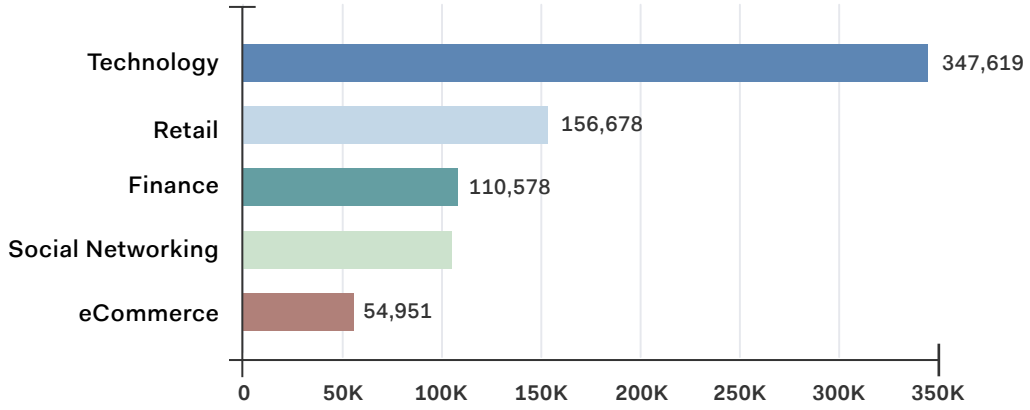


Cybercriminals stake their bets on current events—unleashing new campaigns themed around topics that are top of mind for consumers and businesses. The COVID-19 pandemic was no exception. Considering the major shift to online shopping, we weren't too surprised to see retail climbing to second place among the top-targeted sectors, with 156,678 new malicious sites. Consequently, the finance sector dropped from No. 1 spot in 2019 to No. 3 in 2020, with 110,578 new phishing and fraudulent sites.

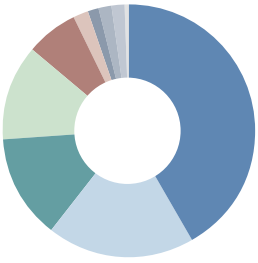
Another industry that was more targeted in 2020 was social networking, with 103,183 new pages. Again, scammers' activity was a reflection of the real-time world—people flocked to social media to stay in touch and to follow the news, and threat actors zeroed in on that channel for their own, nefarious, purposes.

The eCommerce sector also dropped one spot from last year, coming in at No. 4 with 54,951 new phishing and fraudulent sites. This doesn't mean cybercriminals moved on. They simply diverted some of their focus to those themes that were the hottest at the moment.

Top 5 Targeted Sectors in 2020



Breakdown by Industry

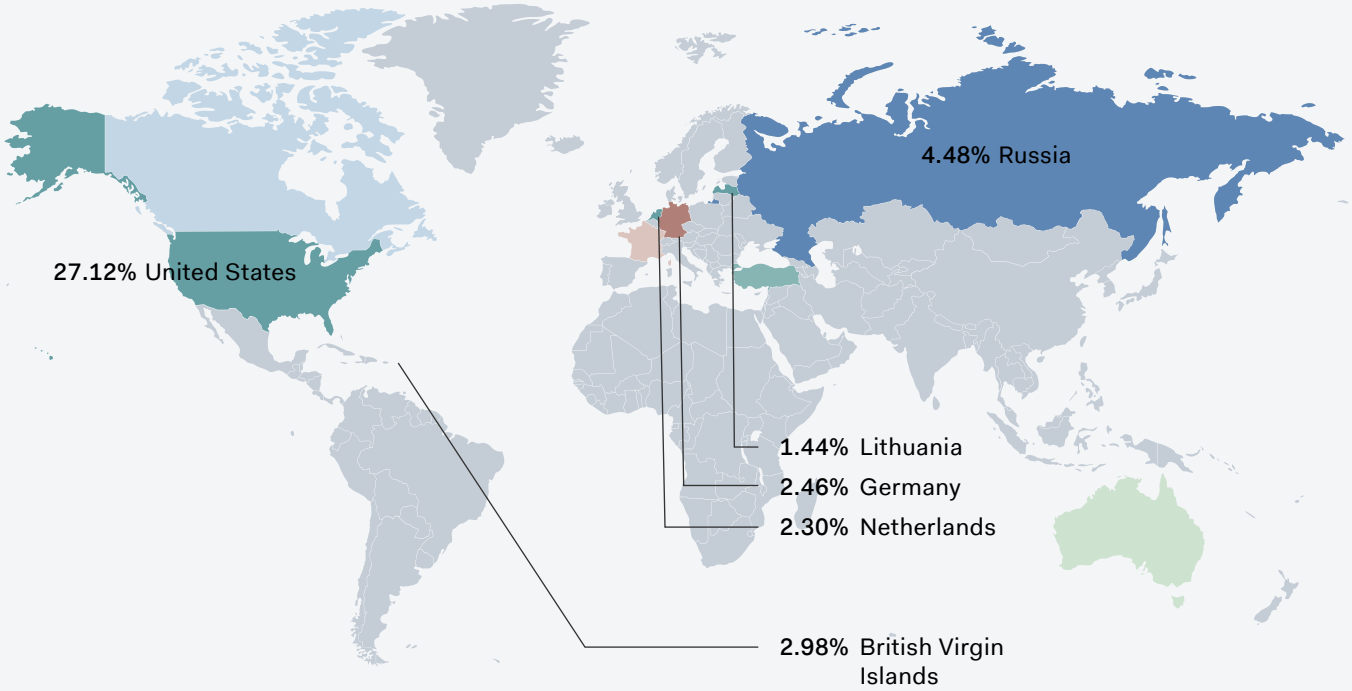


technology	347,619	SaaS	15,910
retail	156,678	communications	10,265
finance	110,578	gaming	14,501
social networking	103,183	streaming	14,105
eCommerce	54,951	logistics	3,474

Other Key Trends

Top Countries Hosting Malicious Sites

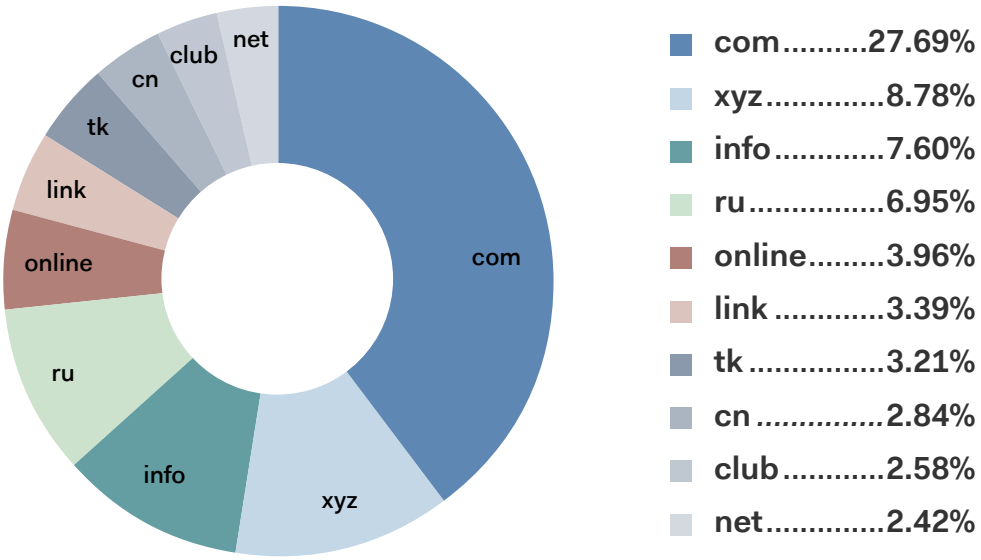
Country	*%*
United States	27.12
Russia	4.48
British Virgin Islands	2.98
Germamy	2.46
Netherlands	2.30
Lithuania	1.44



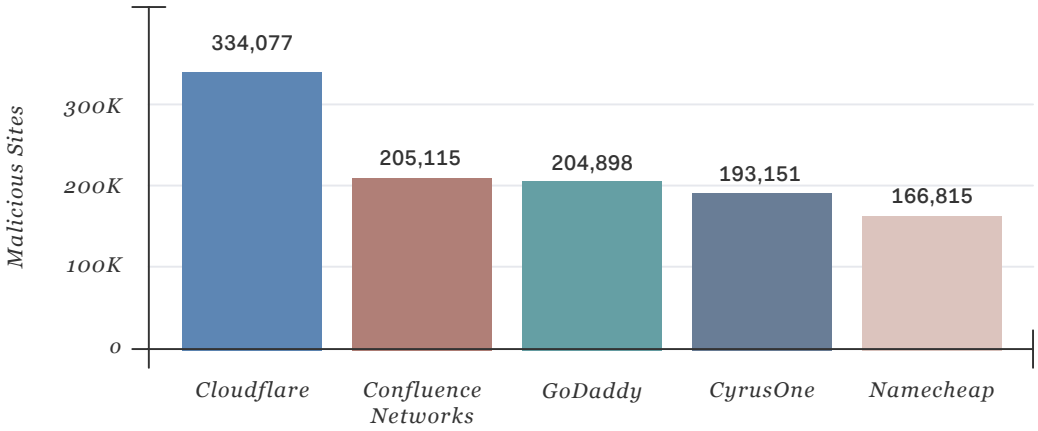
Source: https://checkphish.ai

Most Common Top-Level Domains Hosting Fake Sites

These 10 top-level domains accounted for nearly 70% of all phishing and scam sites



Top Hosting Providers for Malicious Sites

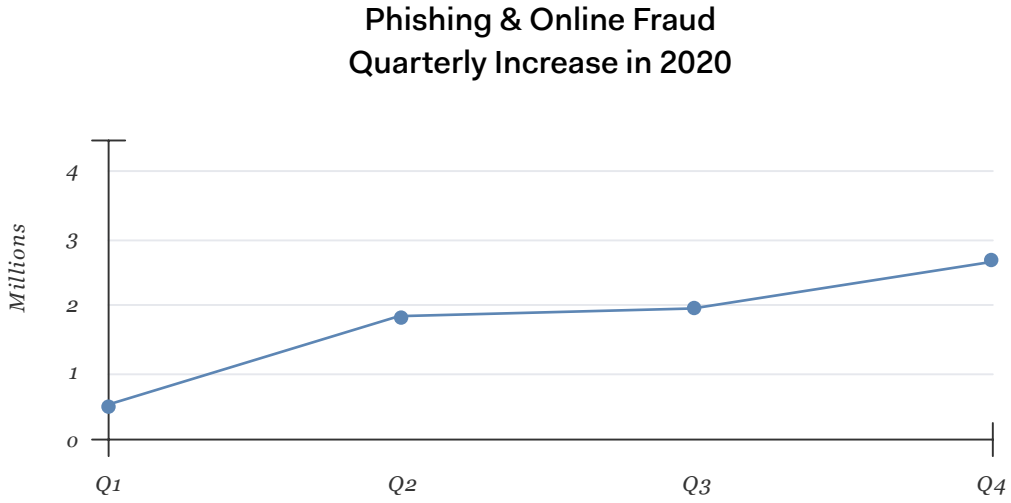


Top Email Services Used

gmail.com	yahoo.com	outlook.com
66.99%	9.35%	2.63%

Trend 1: Escalating Threats

Year after year, we see the scale of threats continuing on the upward trajectory. The number of new average phishing and scam pages that went live each day increased by nearly 73% in 2020, compared to 2019. And in 2020, each quarter saw more malicious activity than the previous one.

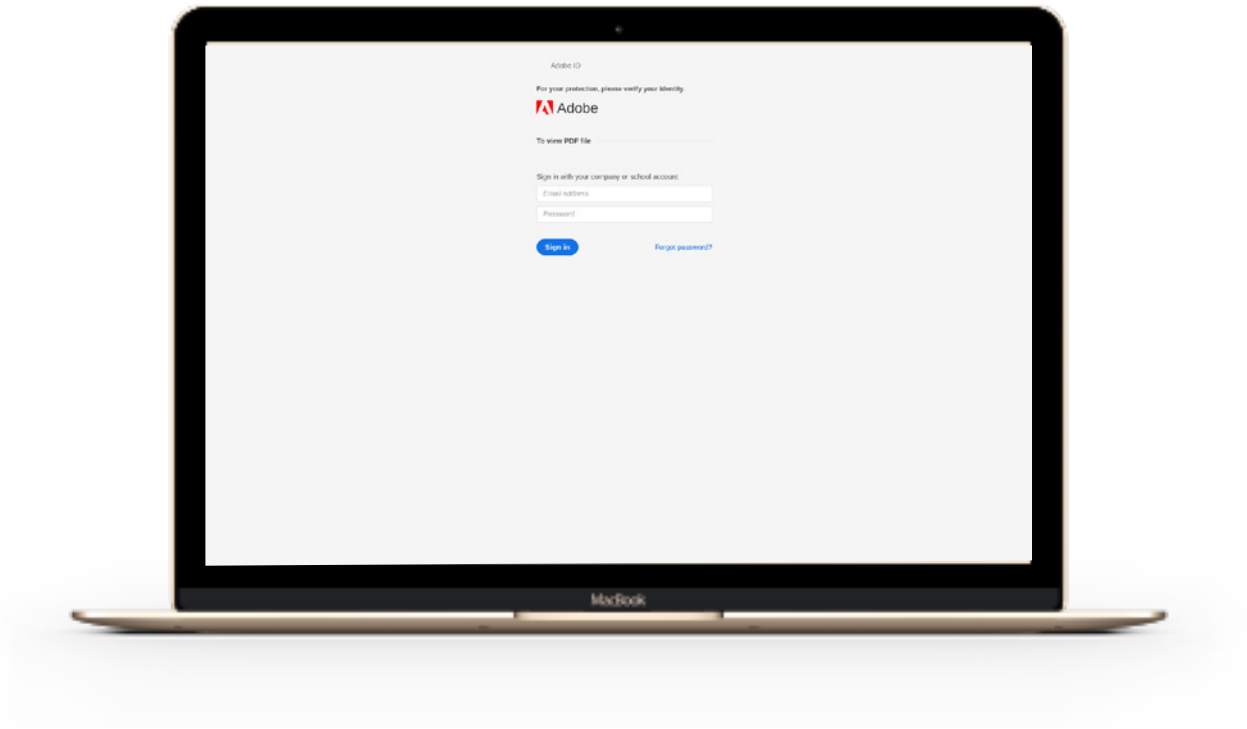


What's alarming is not just the sheer scale of fraud. The ingenuity of the cybercriminals is also extraordinary. And it's not just because they follow current events in search for new areas to exploit. They're growing more sophisticated as well. Of all the new phishing and scam pages in 2020, nearly 20%—or more than 1.37 million pages—were on sites that used SSL certificates. Since the https in a URL signals that the site is secure, criminals know that visitors are more likely to click on an https link.

Fake Adobe login page

Scam URL: hxxps://cssnf[.]gq/?login=do
View CheckPhish Insights page

This fake Adobe login page, designed to harvest login information, is asking users for their corporate or educational institution credentials, obviously taking advantage of remote school and work during COVID. Given the growing scale and sophistication of the attacks, fast detection and takedown of malicious sites is critical. Every day and week that each fraudulent or phishing site is live—and chances are that there are dozens if not hundreds and even thousands of sites per brand—the company's exposure grows.



Trend 2: Protecting Brand Reputation Gets Harder

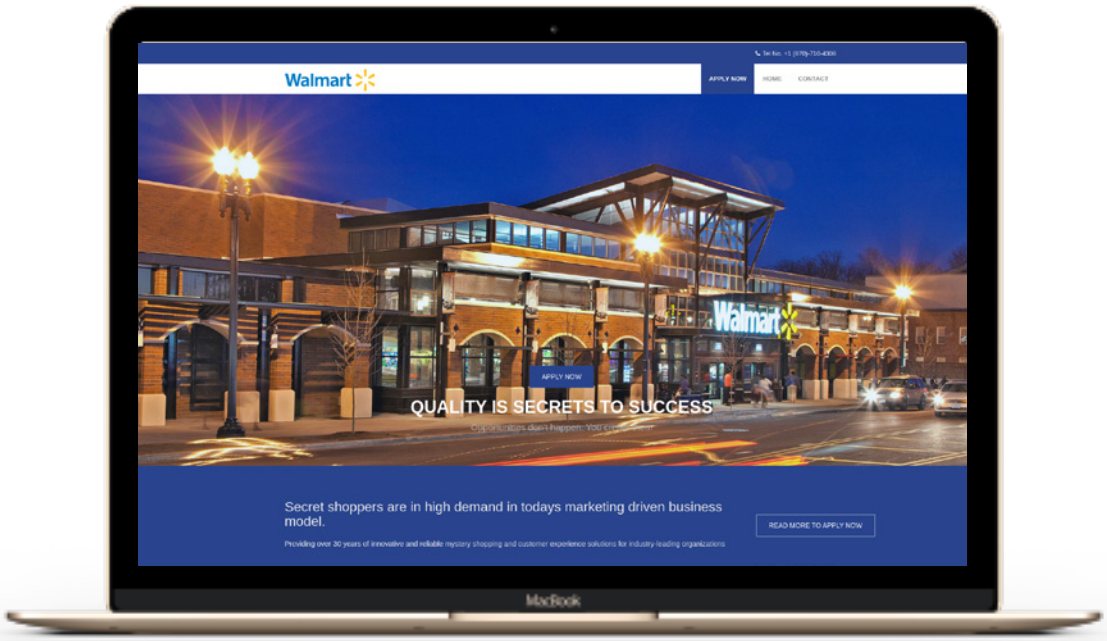
The growing speed and scale of threats means protecting brand reputation gets harder every year. Threat actors use spoofed websites for everything from harvesting employee credentials to stealing customers' financial data.

Our analysis shows that the top 10 most-phished brands span across industries, from technology and retail to social media and financing. Nearly 700,000 phishing pages impersonate those brands alone. Phishing is of special concern because fraudsters have become quite good at brandjacking—assuming a brand's online identity—to create flawless emails and websites to lure customers and trick them into revealing their credentials, buying fake goods, and taking other harmful action.

Walmart mystery shopping scam

Scam URL: hxxps://freshinsightshopper[.]com/Walmart
View CheckPhish Insights page

This page is an example of how fraudsters use brandjacking to lure unsuspecting consumers—in this case, getting them to apply for a mystery shopping gig in a fake recruitment for Walmart. Typically, these scams defraud the victims of money, often by getting their banking information. Walmart, however, doesn't use a secret shopper program, and warns about these and other scams on its website.



Phishing Across All Brands

10,061

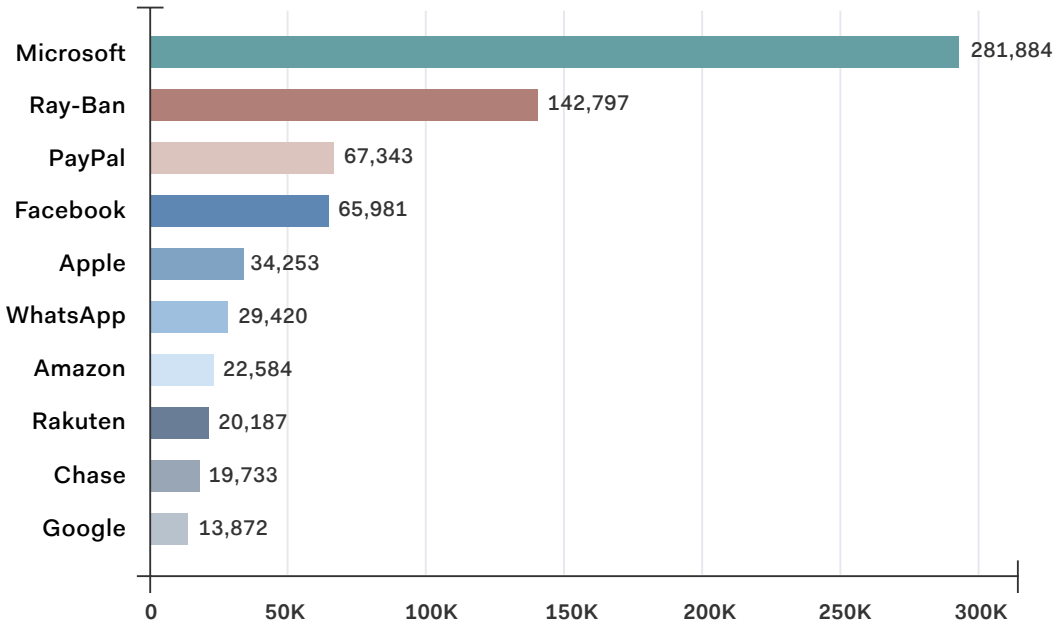
AVERAGE NUMBER OF NEW PHISHING PAGES PER DAY

53%

OF ALL PHISHING AND SCAM PAGES

Top 10 Phished Brands

Totals of new phishing pages in 2020



Phishing, scam, and fraudulent sites are at the heart of brand losses. Brand impersonation is no longer a brand or marketing problem. And regardless of company size, any brand is at risk—and the consequences can be devastating since mitigating a breach can take years and cost millions of dollars.

Trend 3:
The 5 Most-Popular Themes

The world changed in 2020, and the threat actors' attention changed with it. Although they continued to use phishing and other scams as their tactics, cybercriminals pivoted throughout the year to themes that were more likely to resonate with their potential victims. The topic of COVID-19, along with related themes—remote work, eCommerce, retail, and gaming—rose to the top of phishing and scam campaigns.

1. COVID-19

The World Health Organization declared COVID-19 a pandemic on March 11, and threat actors saw their opening. Although there were only 33 new domain registrations and 203 malicious COVID sites in March, those numbers skyrocketed in the next quarter to 34,066 and 143,085, respectively.

In total for the year, we detected 61,316 domain registrations and 244,309 phishing and scam pages. The top schemes were fake pharmacies selling hydroxychloroquine and other drugs, stimulus check scams, and fake vaccines. For example, this one:

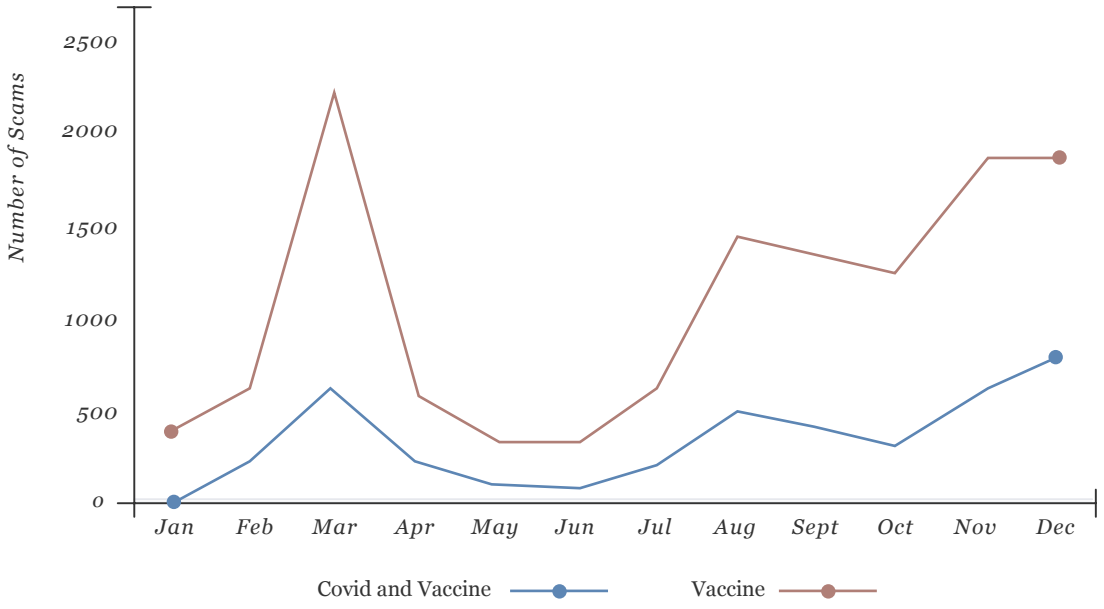
Sinovac vaccine scam

Scam URL: hxxp://xenoninitiative[.]com/
View CheckPhish Insights page

This fake site is impersonating Sinovac, a real-life sciences company in China that developed a vaccine approved by the Chinese government. Registered in Panama, the domain uses a service the keeps the owner's name private and lists a shared address and phone number. The site advertises free shipping, even though the vaccine must be refrigerated to specific temperatures to maintain efficacy—and it is impossible to meet that requirement without an expensive, specialized shipping container.

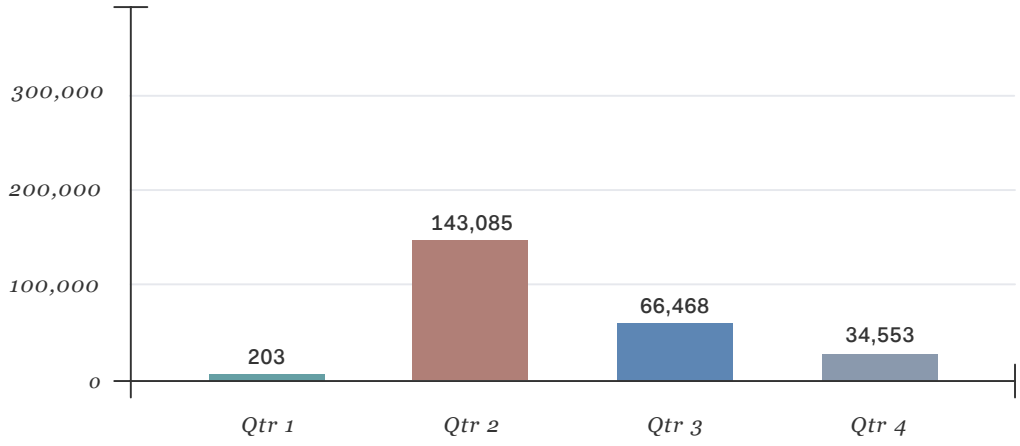
Things got even more interesting as various pharmaceutical companies ramped up vaccine research and availability. In the US, Pfizer and Moderna—top companies that made significant progress on vaccine—became popular with scammers. In August, Moderna confirmed it agreed to supply the US government with vaccine, and announced discussions with other governments. As a result, the number of new fake Moderna domain registrations more than doubled between August and September.

New Domain Registrations Containing "COVID" and "Vaccine" in 2020



As the world grew weary of the pandemic toward the end of the year, so did scammers. COVID-related activity waned in the third quarter, and further decreased in the fourth quarter.

COVID-Related Phishing and Scam Activity in 2020



2. Remote Work

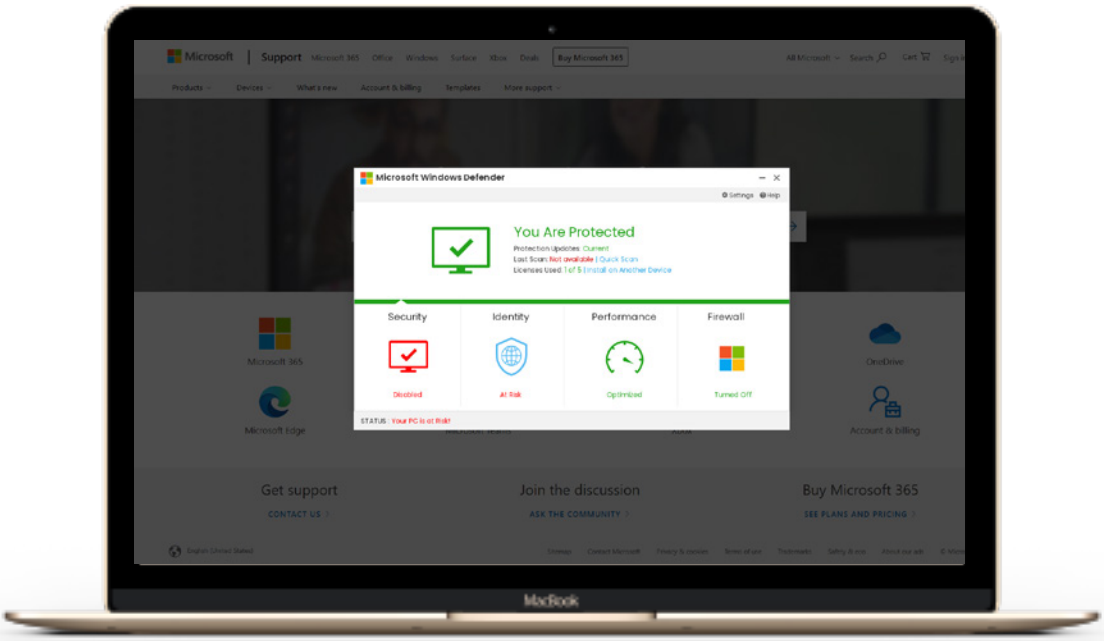
Remote work became the new normal during lockdowns, creating a major disadvantage for many businesses: They had little time to prepare for the massive shift to working from home. Threat actors didn't lose a beat, going to work to harvest login credentials for VPN and remote access, as well as for Microsoft 365 apps.

Frequently, the scammers posed as corporate IT support personnel, emailing employees links to what looked like legitimate corporate websites, like this one here:

Microsoft Defender scam

Scam URL: hxxp://micro201asdcfv[.]gq/3955/WinFhelpxcodexwin444CHerrorxxdc/#
View CheckPhish Insights page

This fake Microsoft Defender site is likely part of phishing campaigns targeting employees with tech support scams. These types of sites typically take potential victims to a fake Microsoft "Support" page that includes a phone number. Users who call that number get scammed over the phone by making payments for obtaining the tech support.



3. Retail Stores

Retail was the new kid on the block in 2020, drawing threat actors' attention like never before. They launched close to 430 new phishing pages a day, on average. Similar to COVID scams, the second quarter had the highest activity, coinciding with the peak of lockdowns, but declined in the third quarter. However, we saw an increase again in the last quarter, as retail shopping was on consumers' minds during the holiday season.

Top Retail Brands Targeted

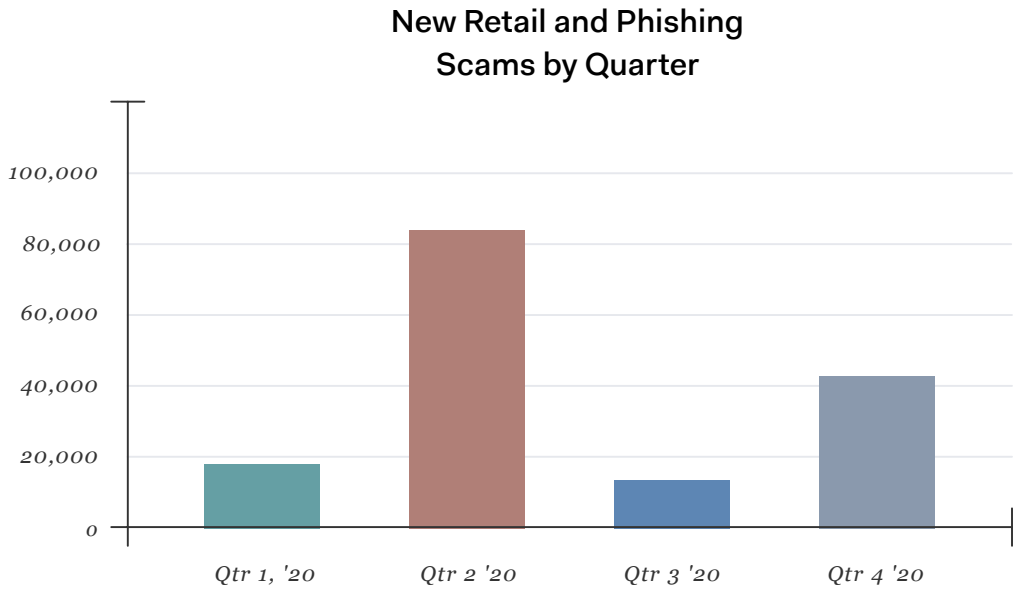
Ray-Ban, Nike
Pandora Jewelry
UGG, Gucci

Total New Retail Phishing and Scam Pages

156,678

Common Types of Scams

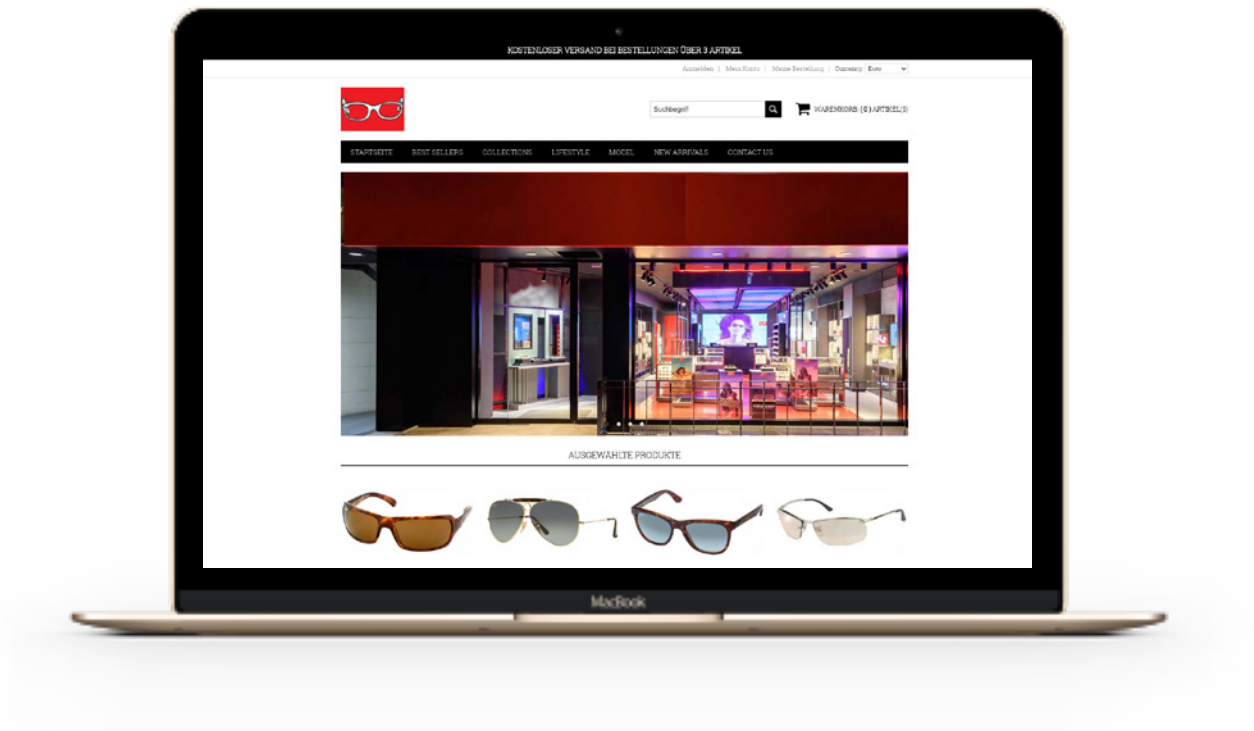
Counterfeit goods
Phishing
Fake promo codes



Counterfeit Ray-Ban products

Scam URL: hxxps://www[.]rbgde[.]net
View CheckPhish Insights page

This is a typical online storefront for forged goods. The German website is selling counterfeit Ray-Ban sunglasses at highly discounted prices. Except for the generic image used as the logo, the website looks legit, even mimicking the right product names and styles and posting user reviews.



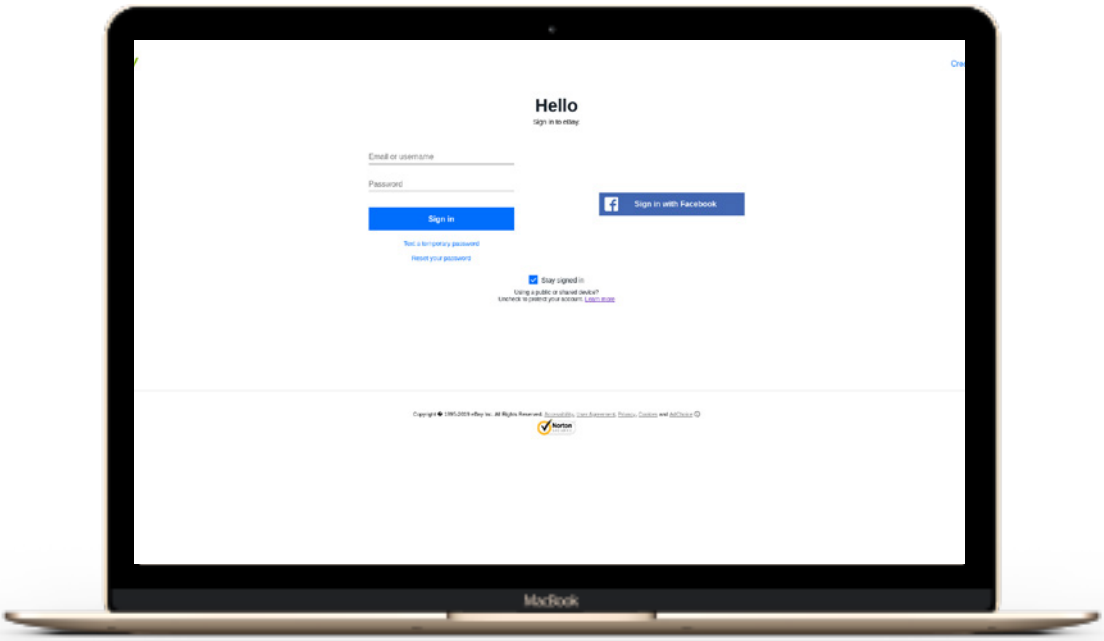
4. eCommerce

In 2020, eCommerce dropped from the fourth most-targeted category to the fifth. Perhaps the novelty of the retail sector commanded more of the cybercriminals' focus, or perhaps their attentiveness was divided with so much else going on. Even so, we observed that eCommerce activity was among the highest in September-November, coinciding with the ramp-up in the holiday shopping season. Amazon, eBay, Alibaba, Rakuten, and Made in China were the top targeted brands, with fake gift cards as the fraudsters' favorite type of scam.

eBay login scam

Scam URL: htxxps://ghheksgiusshodjs[.]com
View CheckPhish Insights page

This site was likely a redirected email link used to steal login credentials. It's noteworthy that cybercriminals are piggybacking off single sign-on (SSO) authentication trend, as many users choose social media and other sites, like Facebook shown here, to log into their online accounts.



5. Online Gaming

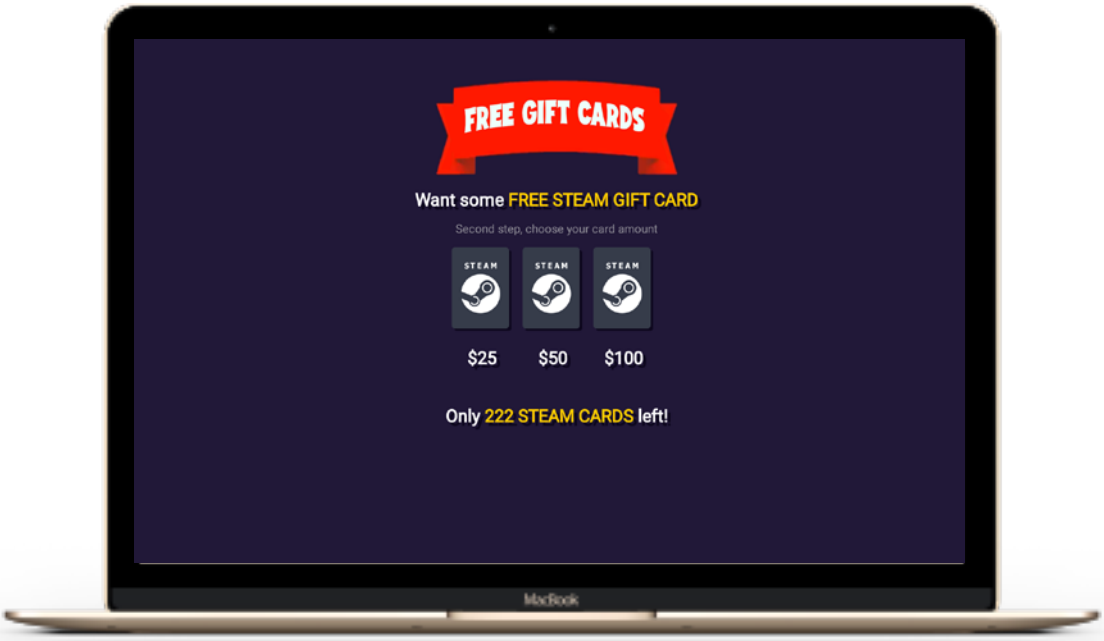
The home became the hub of entertainment during the pandemic, creating yet another offshoot theme for fraud: online gaming. Many consumer surveys showed more people diving into online gaming and streaming at home during lockdowns—and the scammers followed those breadcrumbs.

We detected 14,501 new phishing and scam sites targeting gaming companies, with Steam, Roblox, and Epic Games among the top brands. Fake promo codes and online point generators were common scams—proving, once again, that threat actors know their stuff.

Steam gift cards scam

Scam URL: hxxps://gifthubs[.]xyz/steam/index.html
View CheckPhish Insights page

This site is offering fake gift cards for Steam, a popular game-purchasing platform, just in time for holiday shopping. Scammers are catering to gamers looking for free Steam Wallet codes; however, there are very few legit sources for those free gift |cards in reality. We also detected that the IP address previously hosted 30 other phishing pages.



Actionable Insights

Solve machine-scale problems with machine-scale solutions.

Human-driven detection and takedown strategies are slow and ineffective against the tsunami of daily threats that your business faces today. Cybercriminals are using machines to launch and scale their attacks, and you need technologies to match—like artificial intelligence and machine learning—to fight back at scale.

Reduce your time-to-respond window.

The longer a fraudulent or phishing site stays live, the more damage your business and brand will incur. By applying AI and automation technologies, you can drastically reduce your response window and minimize impact by accelerating both the detection and remediation processes.

Automate response as much as possible.

Leverage APIs or automated emails with hosting providers to automate your response to fraudulent sites. Bolster, for example, can take down a fake site in as little as two minutes via API, and take down 95% of all fraudulent sites detected without human intervention.

Monitor continuously.

Fraud detection will never be “one and done,” given that scammers move incredibly fast from one scheme or hosting provider to the next. Monitoring all the customer touchpoints must be ongoing and in real time in order to keep pace with, or get ahead of, scammers.

Seek out the best threat intelligence.

Threat intelligence is critical to your understanding of the overall fraud landscape and how conditions are changing. Look for fraud prevention platforms powered by rich, multi-point threat intelligence feeds to provide you with maximum context and insights.

What's Next

In a customer-centric world, maintaining a competitive edge as a digital business doesn't just mean meeting and interacting with customers in one single place or in one manner. Customers expect brands to create a safe and trustworthy environment wherever and however they choose to engage, regardless of the digital touchpoint.

Bolster has already been observing the rapid growth of fraud and risk every year—but we expect the boom in digital business to create a scale of risk not seen before.

The expanded and more complex risk ecosystem calls for a cohesive strategy that enables companies to approach fraud detection and prevention holistically. Visionary brands can innovate by bringing together cross-functional teams that work from a single source of truth. This will ultimately serve as the only way forward.

About Bolster

Bolster builds artificial intelligence and machine learning technology to protect consumers and businesses from threat actors on the internet. Top favorite brands from technology to eCommerce trust Bolster's software to detect and take down threats that might attack their customers, employees, or partners. Learn more at: www.bolster.ai.

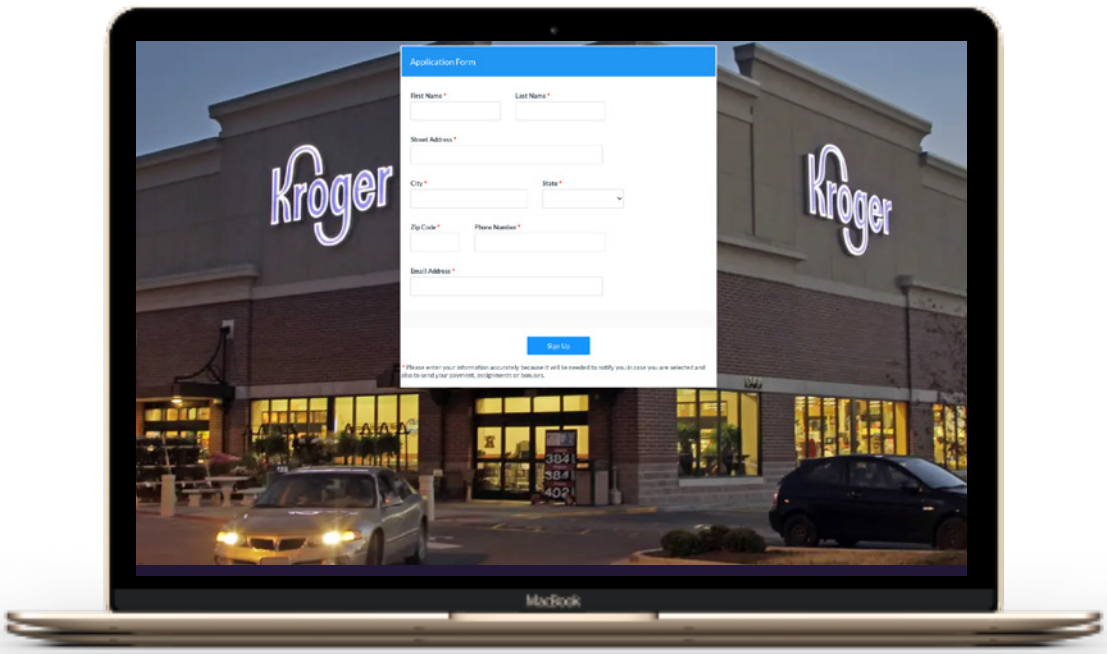
Appendix

These are select examples of the types of scam and fraud sites that Bolster detected and feature the major themes of 2020.

Kroeger mystery shopping scam

Scam URL: hxxp://offlinecapi[.]com/offer
View CheckPhish Insights page

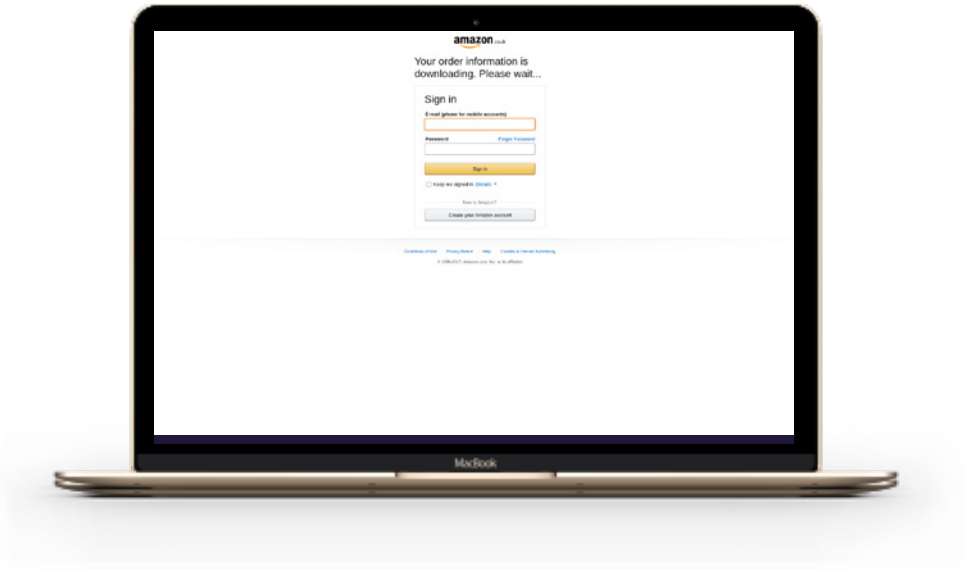
This is another instance of mystery shopping scams, which typically perpetrate financial fraud.



Amazon login scam

Scam URL: hxxp://thegritchens[.]com/AmazonSignIn[.]html
View CheckPhish Insights page

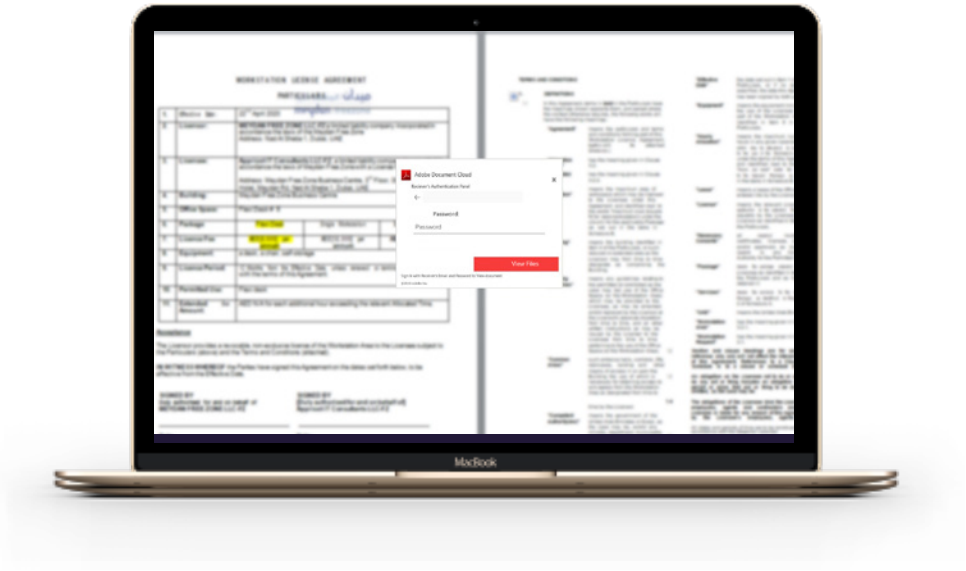
This is a typical phishing site for an eCommerce brand, generally propagated via email. The campaigns usually involve many variants, so the content changes over time.



Embedded Adobe Document Cloud scam

Scam URL: hxxps://contract-849394[.]web[.]app/
View CheckPhish Insights page

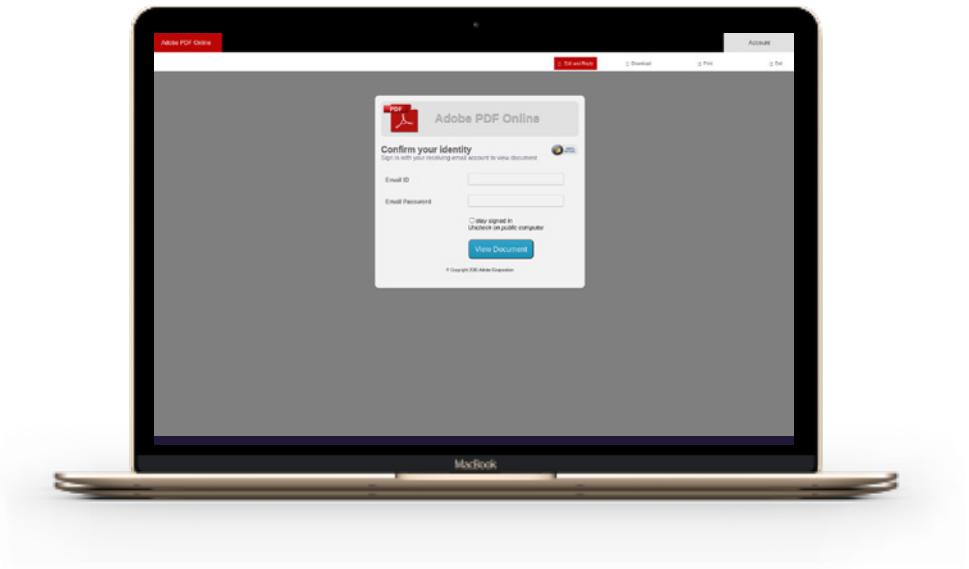
This is another example of a phishing page that tries to steal login credentials for corporate users of popular software and other products.



Adobe PDF login scam

Scam URL: hxxp://deluxeinternationalschool[.]co[.]zw/s43f/PDFFILE

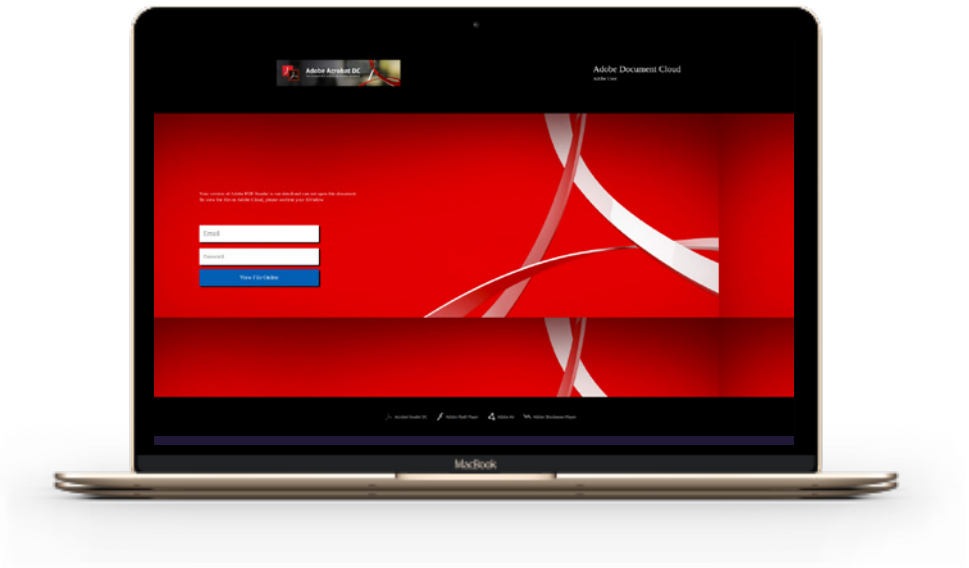
View CheckPhish Insights page



Adobe Document Cloud scam

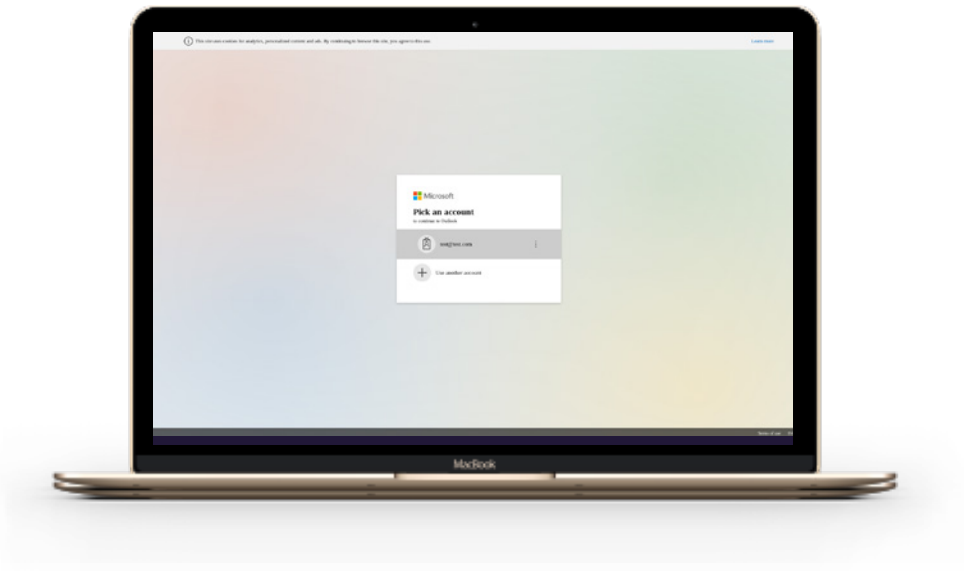
Scam URL: hxxp://creativecombat[.]com/wp-admin/network/acct/login[.]php

View CheckPhish Insights page



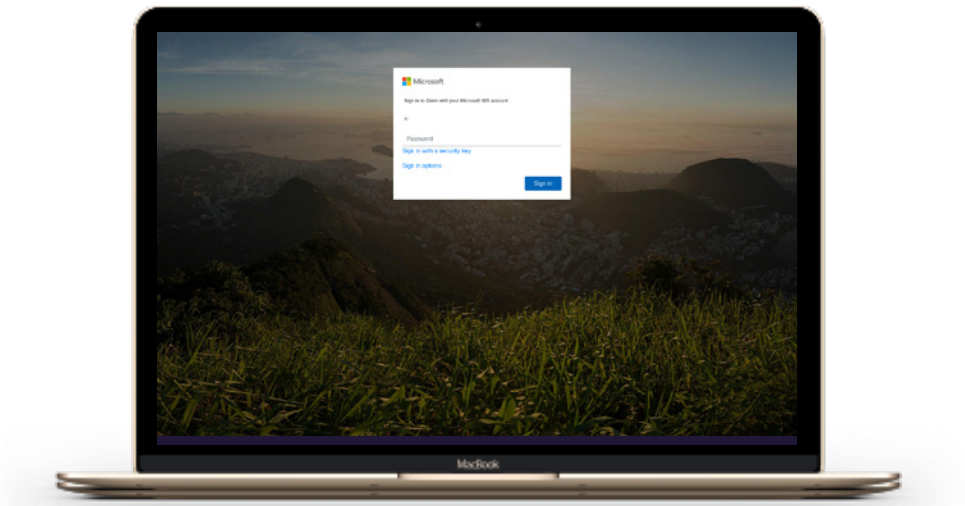
Microsoft 365 login scam

Scam hxxp://gehe[.]blurmask[.]ga/test@test[.]com
View CheckPhish Insights page



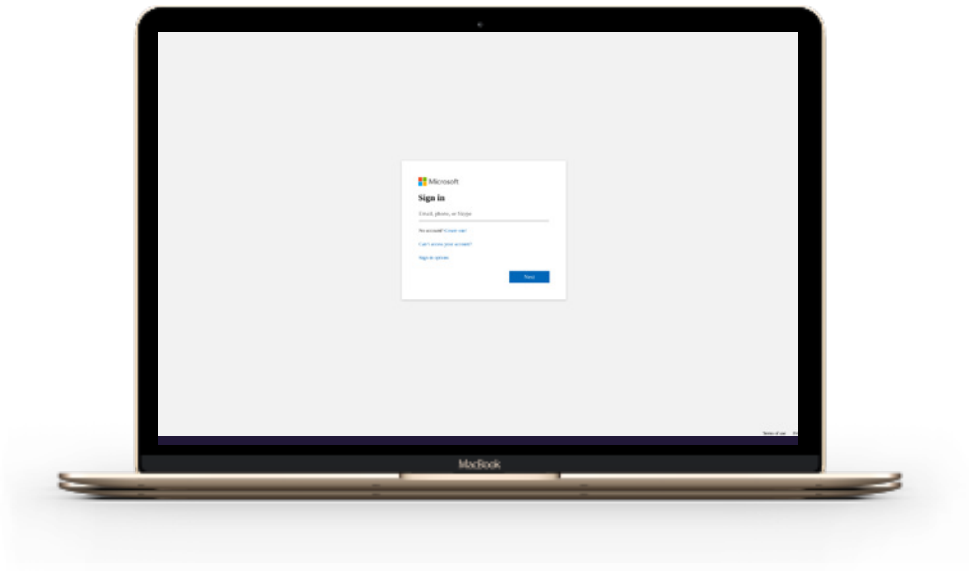
Zoom/Microsoft 365 scam

Scam URL:
hxxps://fra1[.]digitaloceanspaces[.]com/wemmmmzooooomomommom/77ofz0ormi9823[.]html
View CheckPhish Insights page



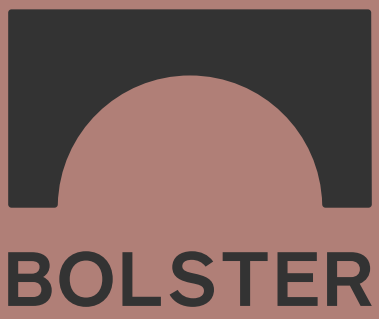
Fake Microsoft 365 login site

Scam hxxp://Microsoft[.]77zrgrta[.]com/
View CheckPhish Insights page



Sony PlayStation gift card scam

Scam hxxp://freeonlinenew[.]com/free-playstation-store-gift-cards[.]html
View CheckPhish Insights page



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