






Table of Contents

2	Introduction
3	A Look Back at 2020 - The COVID-19 Effect
4	2021 Key Data and Findings - Threat Actors Step it Up in 2021
5	Phishing & Scams by Vertical - All Industry Verticals at Risk
6	Brands Phished - Top Brands Remain Targets, New Trends Emerge
7	TLDs, Hosting, and Mail Services - Online Fraud has no Boundaries
9	What to Expect in 2022
10	Actionable Insights



Introduction

We are living in a very different world than we were pre-pandemic. Forced into isolation, people, schools, and businesses have had little choice but to adopt a digital-first mindset. Companies accelerated their digital transformations. People, many for the first time, are working and studying from home, while realizing the convenience of digital services they'd never previously used. At the time of this report, we continue to live, work, and find entertainment largely within the confines of our own homes. Thankfully, digital technologies have enabled us to do so with relative ease. But they've also provided a growing opportunity for fraudsters.

It's no secret that modern cyberattackers go where the money is, so it should be no surprise that when digital business exploded during the height of the COVID-19 pandemic, so too did phishing and cyberfraud attempts. In this, our third year of tracking phishing and scam sites, we can see with no uncertainty how the pandemic has impacted digital adoption and cyberfraud.

Using data gathered from analyzing more than one billion sites, our **2022 State of Phishing and Online Fraud Report highlights the trends that drove digital scams**. In 2021, the total number of phishing and counterfeit pages increased 153% over 2020 levels to a total of more than 10.5 million—and it continues to grow. The average number of phishing and counterfeit pages detected per day increased to over 29,000. While no one can predict where the next fraud campaign will come from, it's clear that threat actors are ready to pounce whenever and wherever an opportunity arises.

2020

6.9 million

Total # of phishing & scam pages

19,000

Daily average

2021

10.7 million

Total # of phishing & scam pages

29,000

Daily average

In 2021, the number of phishing and counterfeit pages increased over 2020 by **153%**




A Look Back at 2020

Bolster has tracked phishing and scam attempts for over three years, providing in particular a view into COVID-19's impact on cyberfraud and digital-first experiences.

THE COVID-19 EFFECT

In 2019, Bolster detected 4.2 million phishing and scam/counterfeit pages. **In 2020, that number increased by 166% to nearly 7 million pages.** It's interesting to note that the World Health Organization declared COVID-19 a pandemic on March 11, 2020. In the same month, the scams detected (406,319) nearly doubled those detected in February (219,804) or January (229,111).

Digital first became the new norm in 2020 as employees grew accustomed to working from home and adopted new digital services. All of this resulted in the explosive growth of digital-based services:

- *With indoor dining shuttered in mid-March of 2020, meal delivery services like those from DoorDash, GrubHub, and UberEats experienced a surge in customer base. According to credit card data from research firm Second Measure, spending on meal delivery services was up 70% year-over-year in the last week of March 2020.*
 - *Online retailers also experienced business growth. By the end of June 2020, Amazon's stock price was nearly \$1,000 higher than it was at the start of the pandemic.*
 - *Tech companies like Zoom that enable distributed teams to remain productive also saw their subscriber base grow astronomically.*
 - *Grocery stores and brick-and-mortar retailers embraced buy online, pick-up in store—or curbside pick-up all facilitated through digital means.*
 - *Streaming media services became a primary form of entertainment for many. Netflix, for example, added nearly 16 million new subscribers during the first quarter of 2020, more than doubling the quarterly growth it had predicted at the start of the year.*
- 

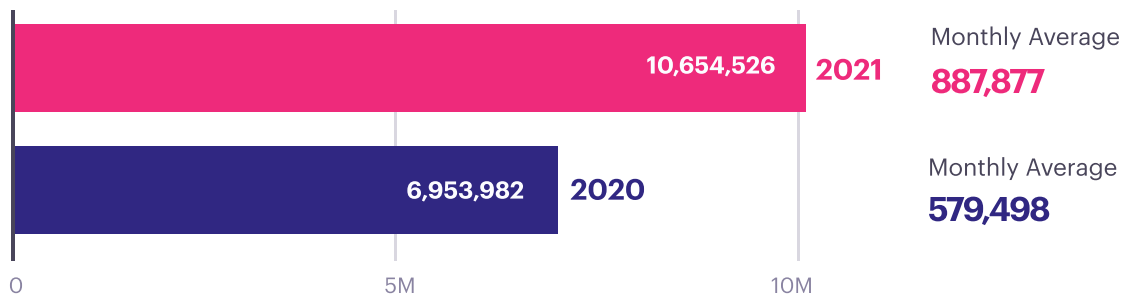
THREAT ACTORS STEP IT UP IN 2021

By 2021, the viability of working from home full-time was proven. Employees had become accustomed to having no commute and when it appeared that companies might begin sending employees back to the office, there was push back from those who at least wanted the option to work remote part-time. Meanwhile, people continued to social distance and isolate—and rely on digital technologies to help keep them safe.

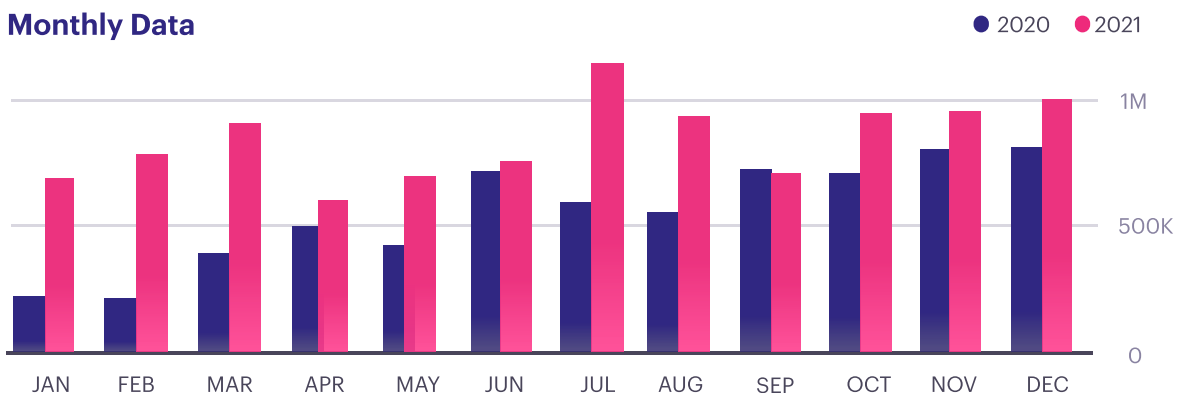
2021 Key Data & Findings

Seemingly, threat actors also settled in with heightened activities. In total for 2021, our systems detected nearly 10.7 million total phishing and scam pages, a 153% increase versus 2020's 6.9 million. The monthly total broke one million in July as summer hit with COVID still in full force. November and December also broke the one million mark each. **The average number of phishing and counterfeit pages detected per day in 2021 increased to over 29,000.**

Total Phishing and Scam Pages



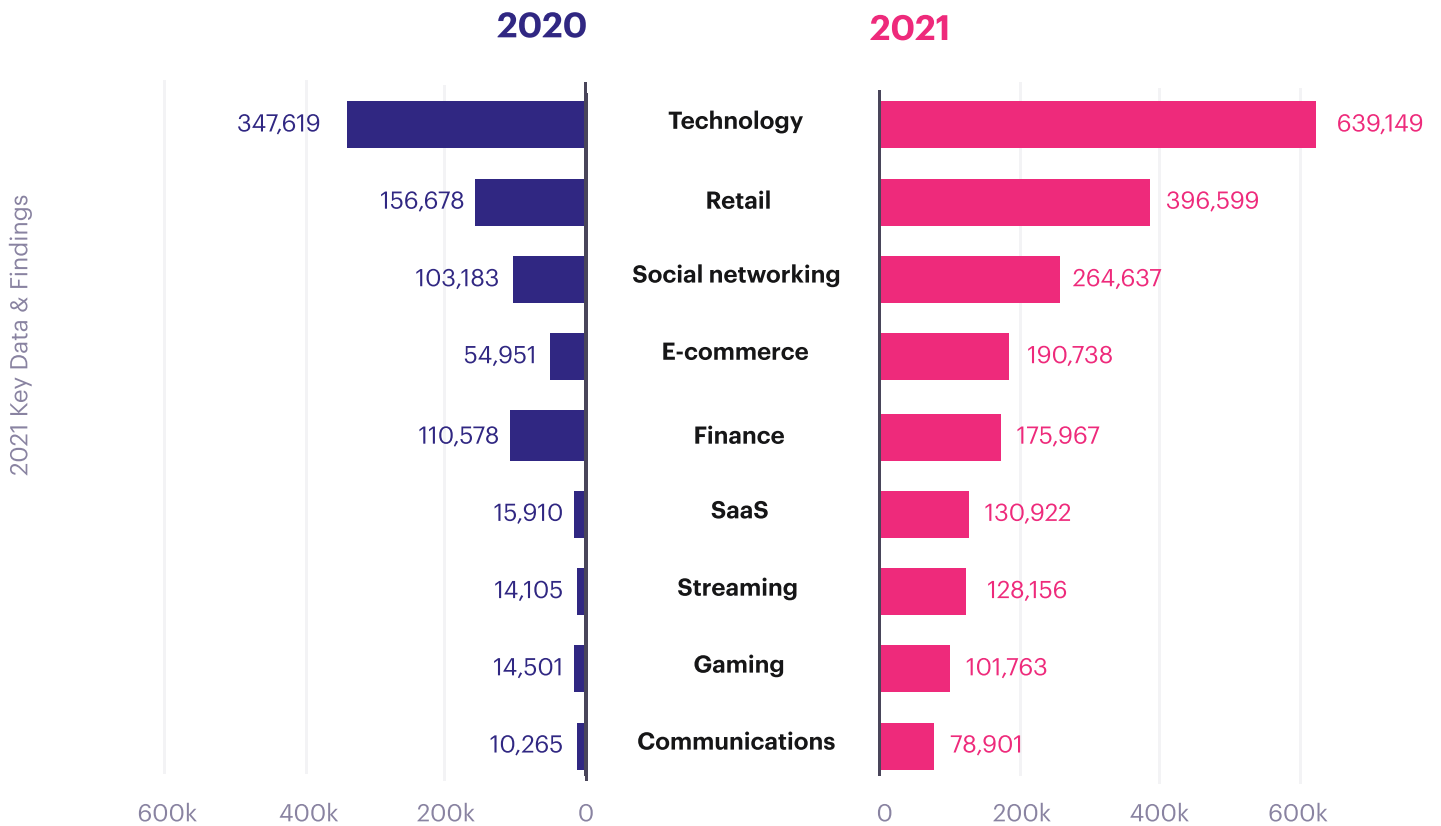
Monthly Data



ALL INDUSTRY VERTICALS AT RISK

None of the verticals we track were left unscathed by the increase in phishing and scam attacks in 2021. In fact, they more than doubled for retail and social networking, more than tripled for e-commerce, and more than quadrupled for the SaaS, communications, gaming, and streaming industries.

Annual Phishing & Scams by Vertical



The increase in phishing and scam attacks in these industries substantiate:

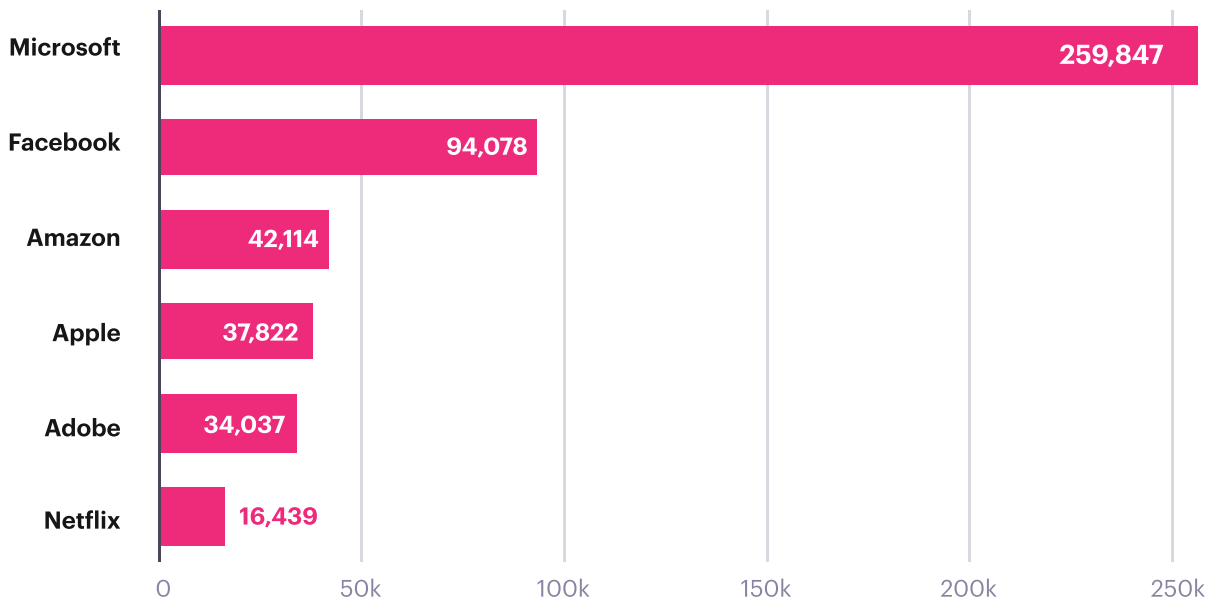
- The continued/protracted COVID effect
- The accelerated move to online entertainment and services
- The broader ongoing digital transformation across virtually all industries

TOP BRANDS REMAIN TARGETS, NEW TRENDS EMERGE

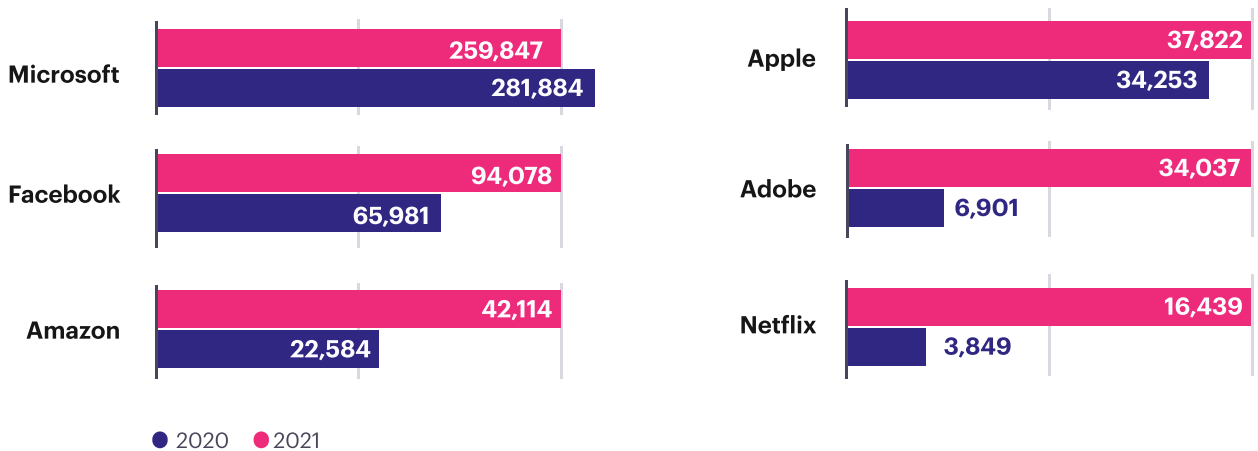
The most targeted brands were perhaps the most telling in terms of where attackers expected to find success during the COVID pandemic. Microsoft continues to be a perennial target but notice the upticks observed for Adobe, Amazon, Facebook and Netflix. This is a direct reflection of people doing more digitally from signing documents, to buying products, to socializing with colleagues and friends, to streaming content. And evidently, the threat actors are right there ready to pounce.

2021 Key Data & Findings

Top Brands Phished in 2021



Top Brands Phished 2020 vs 2021



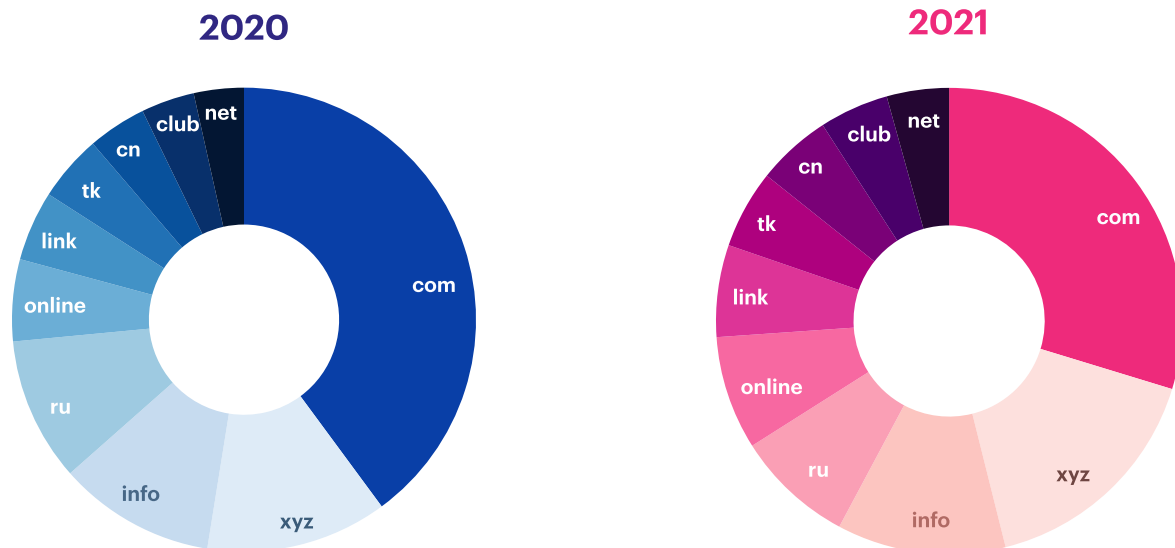
ONLINE FRAUD HAS NO BOUNDARIES

Fraudulent activity also grew in scope in 2021 as the top countries hosting malicious sites expanded. The United States, Russia, Germany, and Netherlands made both lists but were accompanied by an additional six countries in 2021 versus just one in 2020.

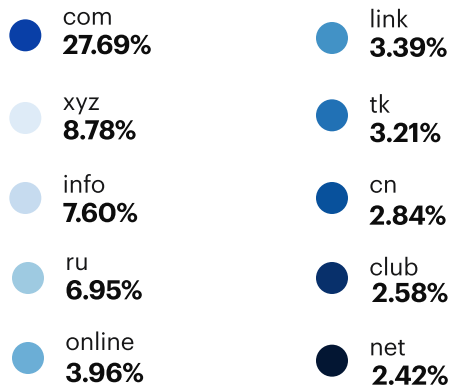
There was little change in the top-level domains represented year over year. Com, xyz, ru, info, and online remained the top five in both 2020 and 2021 with ru and info swapping places.

Most Common Top-Level Domains Hosting Fake Sites

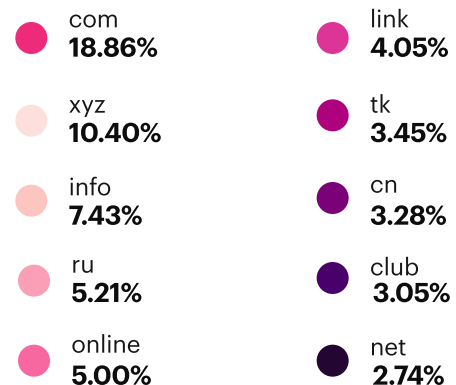
2021 Key Data & Findings



These 10 top-level domains accounted for **69.28%** of all phishing and scam sites

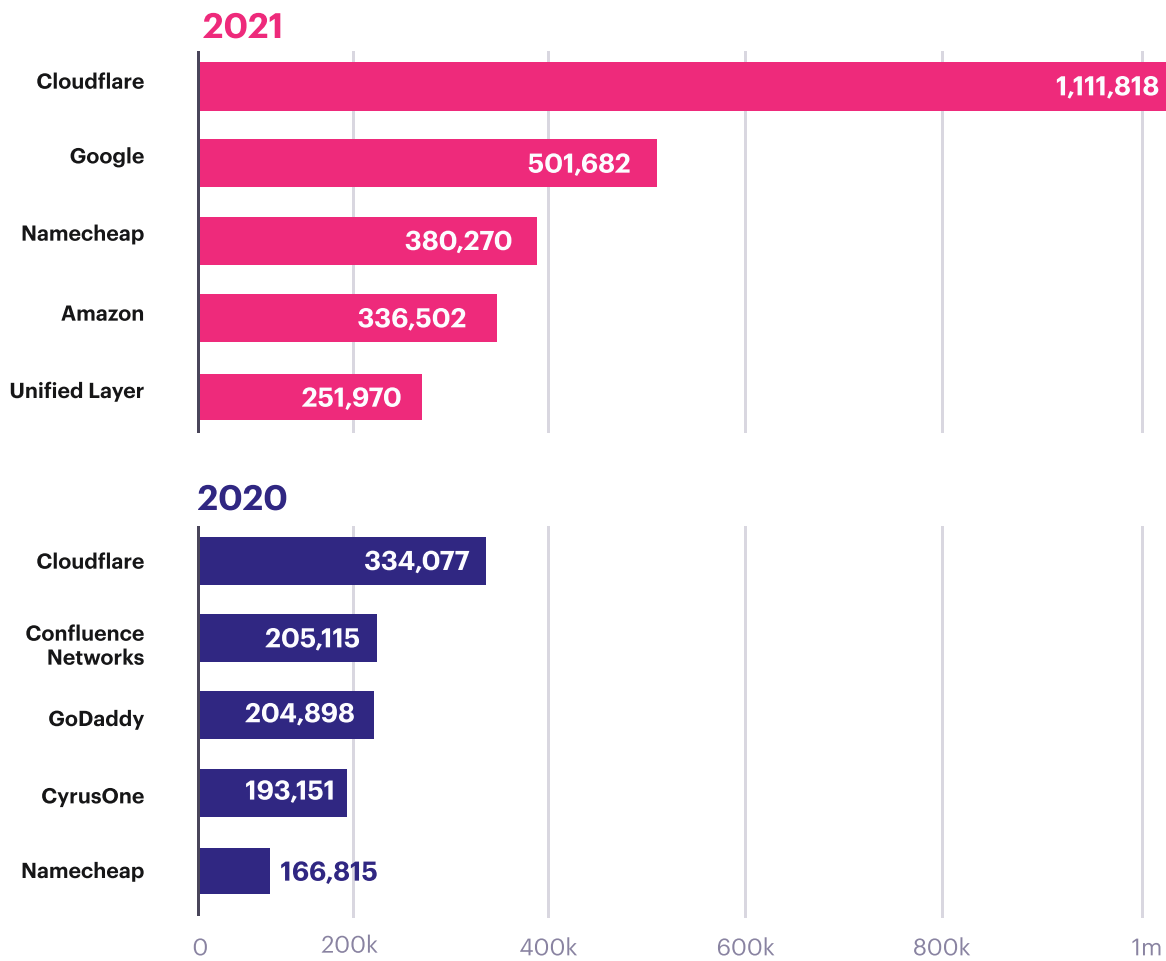


These 10 top-level domains accounted for **63.5%** of all phishing and scam sites



We also saw new entrants on the list of top hosting providers used by fraudsters. Cloudflare continued to be the preferred provider, and Namecheap moved from fifth place in 2020 to third place in 2021. Google, Amazon, and Unified Layer were new to the list in 2021, bumping Confluence Networks, GoDaddy, and CyrusOne.

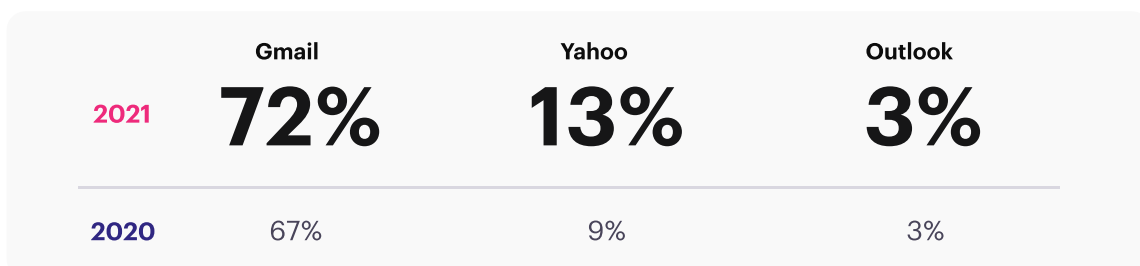
Top Hosting Providers for Malicious Sites



2021 Key Data & Findings

There was no change in the top email services in use from 2020 to 2021. Gmail took the lead both years, followed by Yahoo, and then Outlook.

Top Email Services Used





What to Expect in 2022

The world is settling into a new norm—one that's digital first. But the explosion of phishing and cyberfraud is far from over. People will continue to grow increasingly dependent on the digital innovations and services that make life safer and more convenient. Eventually, digital first will become digital only.

As we continue down this path, it's imperative that we understand the risk and practice vigilance. Companies must take the lead. The expanded and more complex risk ecosystem calls for a cohesive strategy that enables them to approach both fraud prevention and brand protection 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 because while the pandemic will eventually become history, digital and cyberfraud are here to stay.



Actionable Insights

1 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.

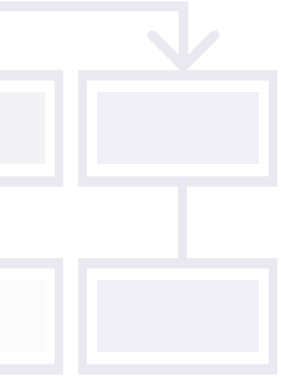
2 Reduce your time-to-respond window.

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 time and minimize impact by accelerating both the detection and remediation processes.

3 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.





4 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 including Internet domains, social media platforms, marketplaces and app stores, must be ongoing and in real time to keep pace with, or get ahead of, scammers.

5 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.

Actionable Insights

 **Domain Risk Report & Domain Acquisition Analysis**

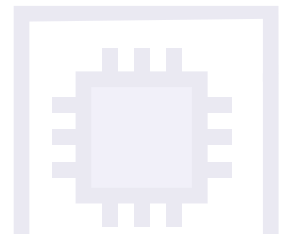
Determine risks to your business and brand for free.

www.bolster.ai/domain-risk-report

 **Bolster Global Fraud Index**

Stay current with the latest phishing and scam data.

www.bolster.ai/global-fraud-index



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.