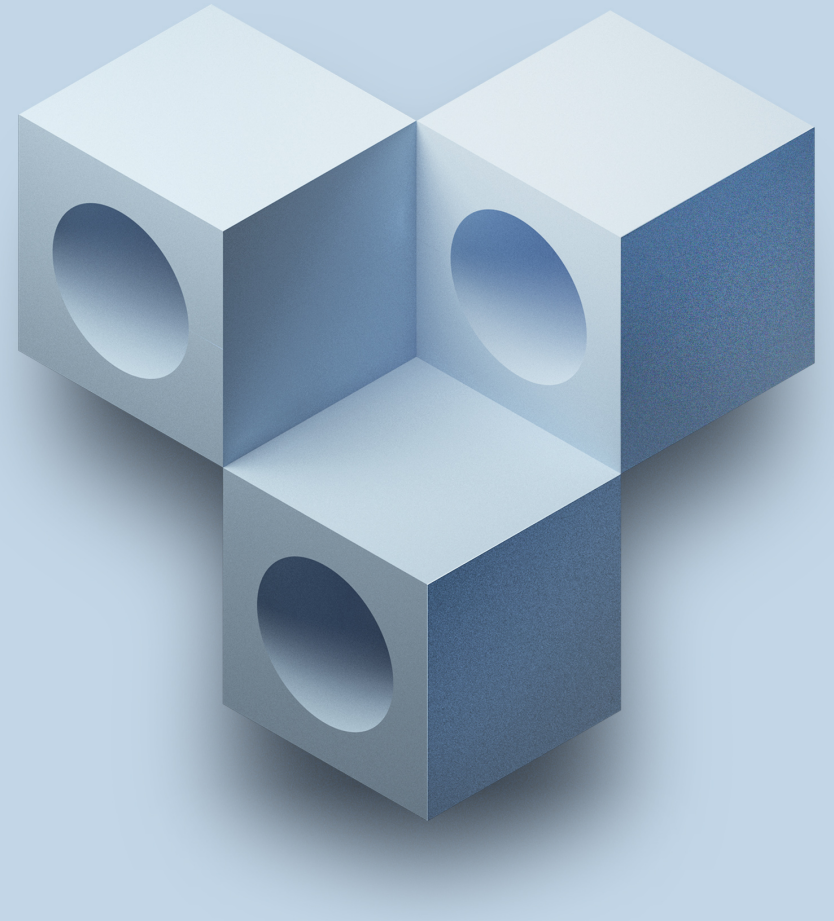
State of Phishing & Online Counterfeiting

Annual Report 2019



BOLSTER

Executive Summary

Online counterfeiting is on the rise. We detected a massive 4.2 million phishing and counterfeit pages targeting just across five major categories. From 2018 to 2019, online counterfeiting grew by 27%.

For most modern businesses, the menace caused by fraud and counterfeiting is inescapable. Hundreds of industries and thousands of brands were targeted in 2019. Finance and SaaS were the top-2 most targeted industries.

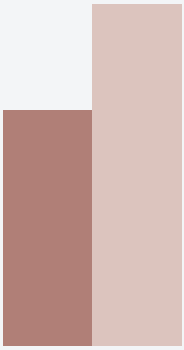
Despite the perception that most counterfeiting originates overseas, the vast majority of counterfeit sites are hosted in the United States of America. Most surprisingly, the vast majority of counterfeit sites were hosted on the popular ".com" top-level domain.

Though the online counterfeiting problem continues to grow, fast detection, timely reporting to hosting providers and their expedient action prove to be the best defense. Four hosting providers stand out as being the most responsive to takedown requests and the most effective in the fight against online scams.

Key Findings

In 2019, we detected 4.2 million phishing and counterfeit pages targeting just across five major categories. This is a 27% increase when compared to 2018. Threat actors spun up websites targeting the customers of a brand as well as its employees. We observed a 2200% uptick in the number of fake pages posing to be employee portals.

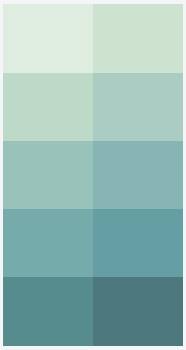
Finance and online banking remained to be the most impacted industry. We identified 1.8 million phishing and counterfeit websites targeting the finance industry worldwide. Over 11,000 phishing and counterfeit pages went live every day.



27%

INCREASE

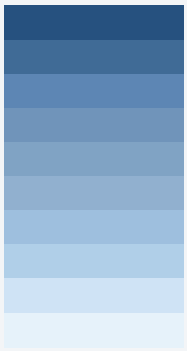
Total phishing and counterfeit websites in 2019 increased by 27% when compared to 2018.



1.8M

WEBSITES

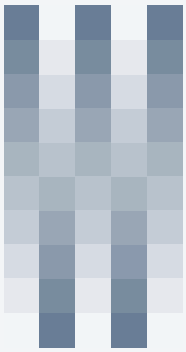
Finance was the most impacted industry with 1.8 million phishing websites detected in 2019.



100+

BRANDS

Brands across 100+ industries have been impacted by online phishing and counterfeiting.



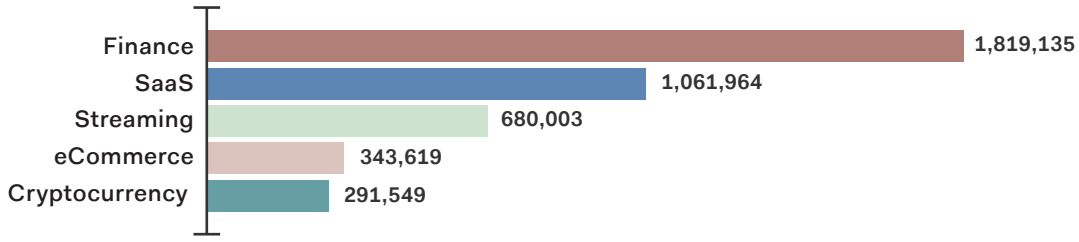
11K

WEBSITES/DAY

Over 11,000 phishing and counterfeiting websites went live per day.

Source: https://checkphish.ai

Top Targeted Industries



In 2019, we detected and analyzed counterfeit and phishing websites targeting over 100 industries. Almost 50% of these attacks were targeting brands belonging to Finance, Software-as-a-Service, Online Streaming, E-Commerce, and Cryptocurrency industries.

The cryptocurrency industry has seen the emergence of several fake ICOs (Initial Coin Offerings) while the scam pages offering cryptocurrency giveaways and discount scams displayed rapid growth (x10 increase). The problem for E-Commerce stores and platforms does not stop at phishing. Scammers spun up 32% more fake shopping sites than in 2018.

Online video and audio streaming services make up 6% of the phishing and counterfeiting websites we detected in 2019. This is a 40% increase over the previous year with the major problem being websites distributing pirated content for free and phishing pages.

Software-as-a-Service and Finance continued to remain the most affected industries. 43% of the phishing websites we detected in 2019 belong to brands from these industries.In 2019, we detected 4.2 million phishing and counterfeit pages targeting just across five major categories. This is a 27% increase when compared to 2018. Threat actors spun up websites targeting the customers of a brand as well as its employees. We observed a 2200% uptick in the number of fake pages posing to be employee portals.

Finance and online banking remained to be the most impacted industry. We identified 1.8 million phishing and counterfeit websites targeting the finance industry worldwide. Over 11,000 phishing and counterfeit pages went live every day.

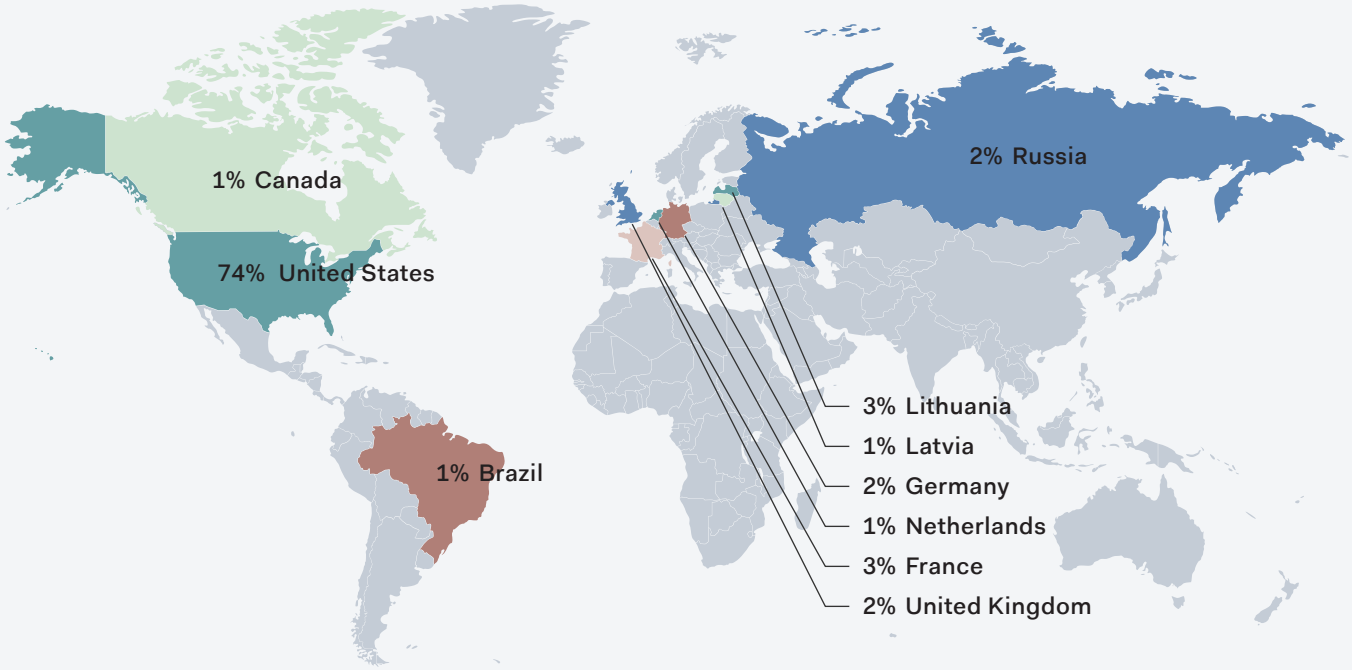
Source: https://checkphish.ai

Countries Hosting Phishing and Counterfeit Websites

1% of the phishing and counterfeit websites in 2019 were hosted in 10 countries. In comparison to 2018, scammers hosted twice the number of phishing and counterfeit websites in the United States. While most of the countries displayed a steady increase in the number of phishing and counterfeit websites hosted, Japan and Russia have seen a 50% reduction.

Countries in North and South America hosted 76% of the phish followed by European countries (12%), Asian countries (7%), Africa (4%) and Australia (< 1%).

These numbers do not imply that the scammers belong to these countries. A scammer can host a phishing web site anywhere in the world (including compromised networks).



Source: https://checkphish.ai

Most Active Scammers

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.

Every time a victim enters his/her credentials, their credentials are sent to a drop email. Drop emails belong to the scammers carrying out the phishing attack. Here is a list of the most active scammers associated with the phishing kits we found in 2019. We analyzed these actors to be hosting phishing and counterfeit websites targeting several brands. Almost all these hosted online banking and software-as-a-service scams during 2019.

Drop Email	Kits
kingrabitu111@gmail.com	403
aimeemiller165@gmail.com	390
joanndradelozano@gmail.com	333
aoljnr001@gmail.com	241
newlogwater@gmail.com	233
usermaintenance@outloutlook.com	214
Lvrxdnona@gmail.com	212
casualonakoya@gmail.com	210
mouoman.sa33d@gmail.com	182
whizkossy@gmail.com	171

Source: https://checkphish.ai

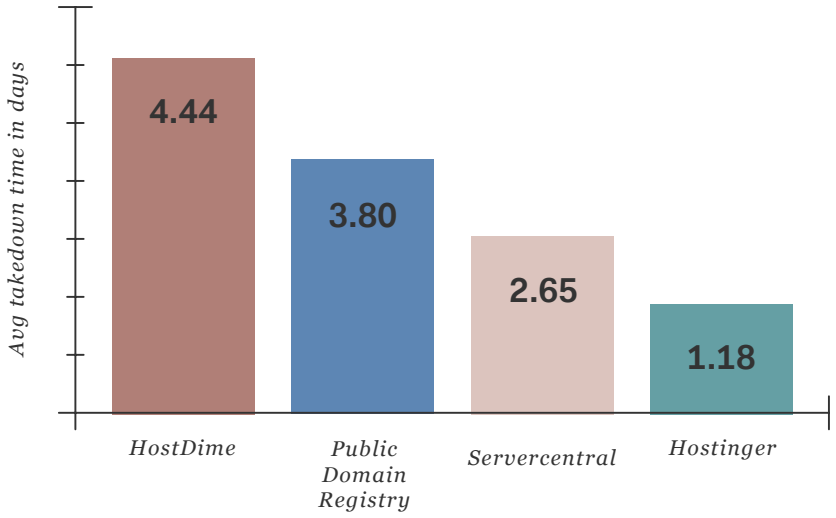
Most Responsive Hosting Providers

In 2019, we worked with several hosting providers worldwide to takedown over 25,000 phishing and counterfeit websites. In this section, we talk about the most responsive hosting providers who took immediate action to bring such websites down.

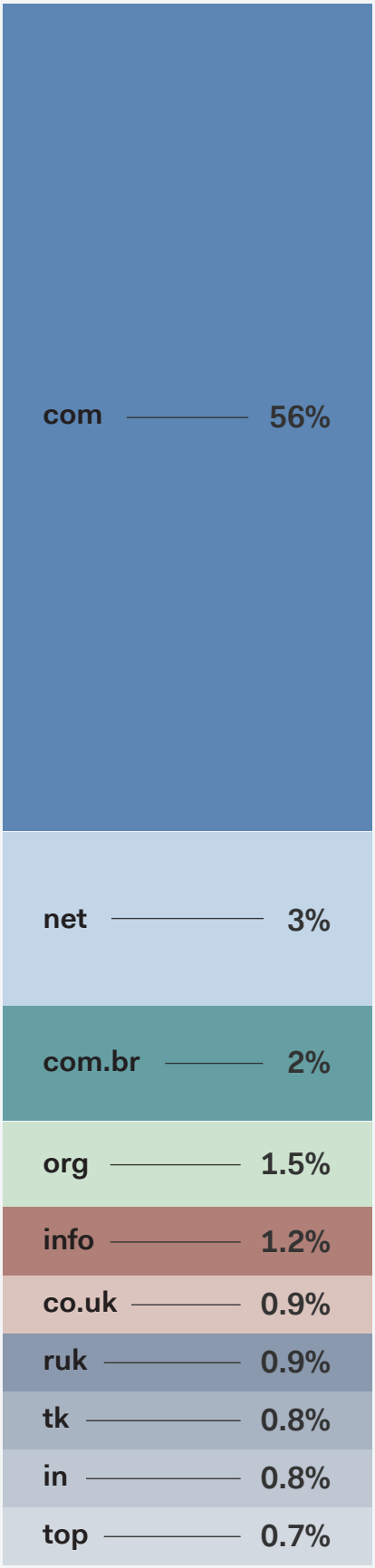
Hostinger has been the most responsive hosting provider in 2019. On average, they took down websites within 30 hours of reporting them. Servercentral, Public Domain Registry, and HostDime follow closely behind with an average takedown time (in days) of 2.65, 3.80 and 4.44 respectively.

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.

Hosting Provider Response Time



Source: https://checkphish.ai



Most Common TLDs

Top-Level Domains

'.com' continued to remain the most commonly used TLD. In 2019, 56% of the total counterfeit websites we detected were hosted on '.com' top-level domain. The number of phishing/counterfeit websites hosted on '.com' increased by 200% when compared to 2018.

'.net' remained in the second position with an increase of 130% when compared to 2018.

'com.br' is the only addition to the top-10 when compared to 2018. It replaces 'win'.

Source: https://checkphish.ai

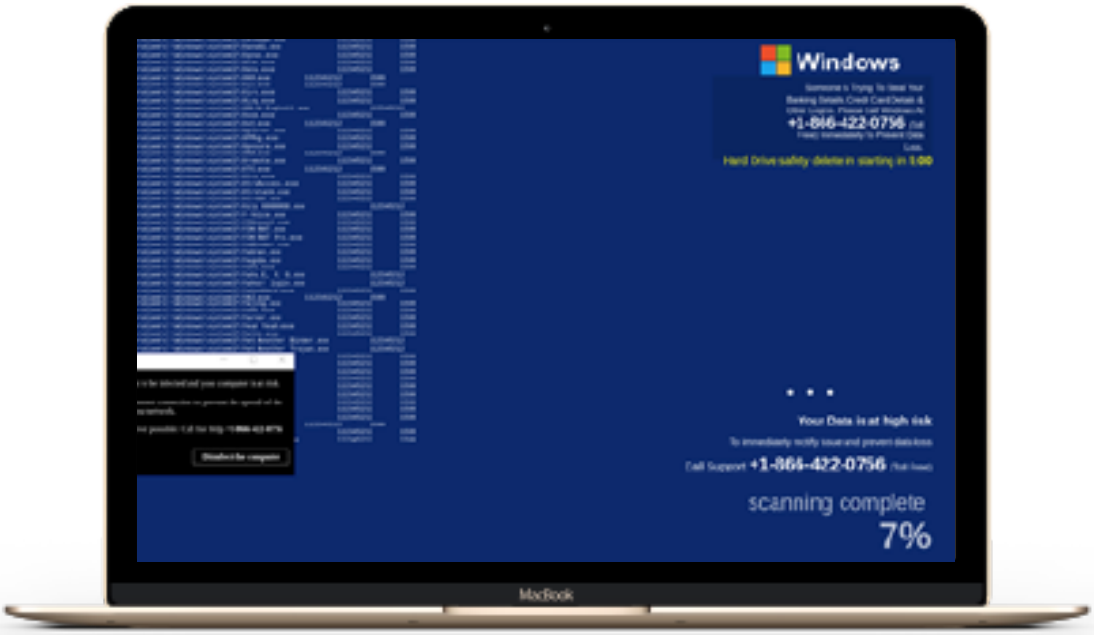
Popular Scams of 2019

In this section, we talk about some of the most popular and interesting phishing / scam websites we detected in 2019. 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 2019.

Tech Support Scams

In 2019, we observed tech support scams impacting online and offline businesses alike. Scammers set up web pages with fake customer support phone numbers of a targeted brand. When a victim calls the number, the scammer tricks them into giving away their credit card and other banking details. Some of the major industries affected by these scams include Online Technology Services, SaaS, Travel, and E-Commerce stores. We observed an increase in these scams by 18% when compared to 2018.

MICROSOFT CUSTOMER SUPPORT SCAM



URL: hxxp://www[.]trzdfxgchgxfdzsfx[.]ga

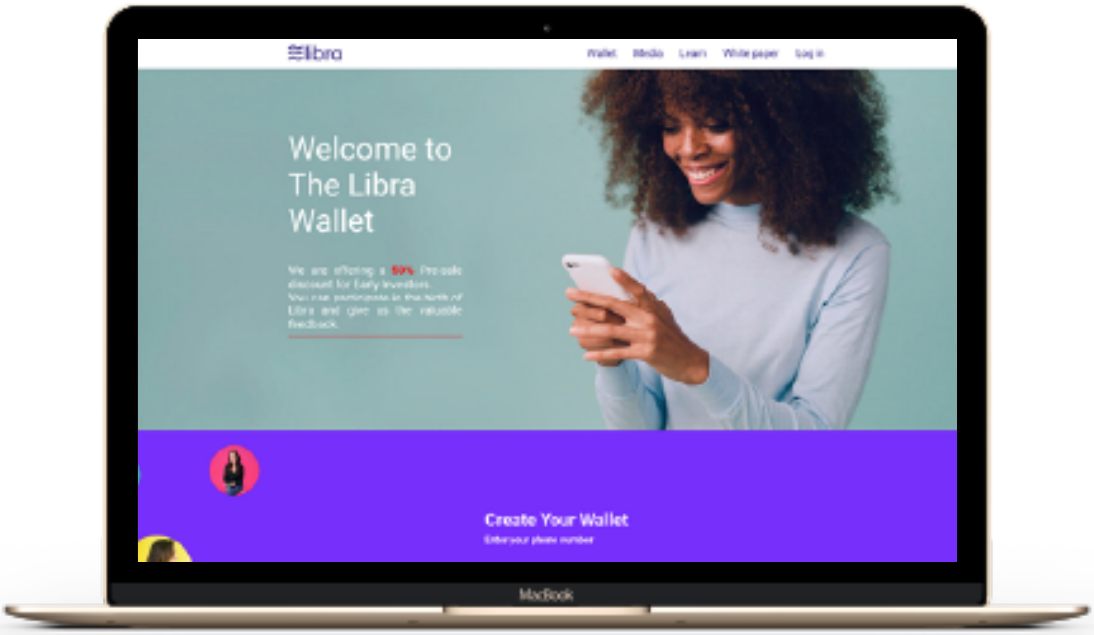
Whats new? We identified several industries including SaaS, Travel, Transportation and Online Streaming to be impacted by this problem.

Source: https://checkphish.ai

Cryptocurrency Scams

Cryptocurrency scams continued to show rapid growth with a 24% increase over 2018. When compared to 2018, scammers adopted innovative ways to lure crypto enthusiasts. In 2019, we observed the emergence of Libra (Facebook's cryptocurrency) and Cybertruck giveaway scams. In the case of Libra, scammers promised 50% discounts for early investors. In the Cybertruck giveaway scams, they tried to lure customers by promising a free Cybertruck in return for bitcoin.

LIBRA EARLY INVESTOR SCAM



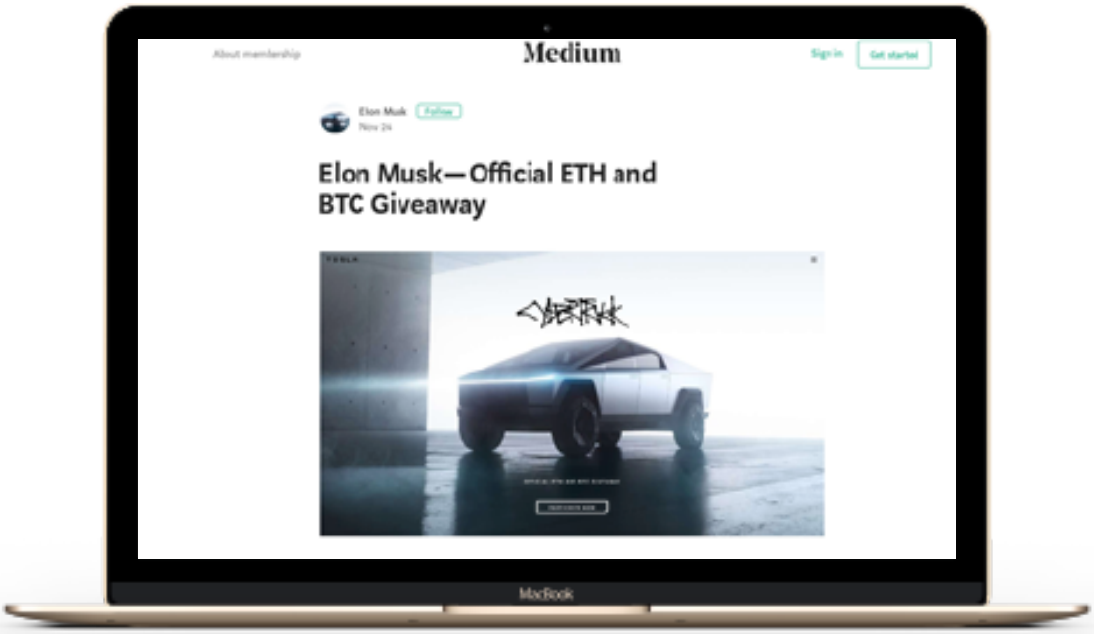
URL: hxxps://librawallet[.]today

Whats new? Libra is set to make its debut in 2020.

Source: https://checkphish.ai

Tesla Scam

TESLA CYBERTRUCK GIVEAWAY SCAM



URL: hxxps://cyberelon[.]com

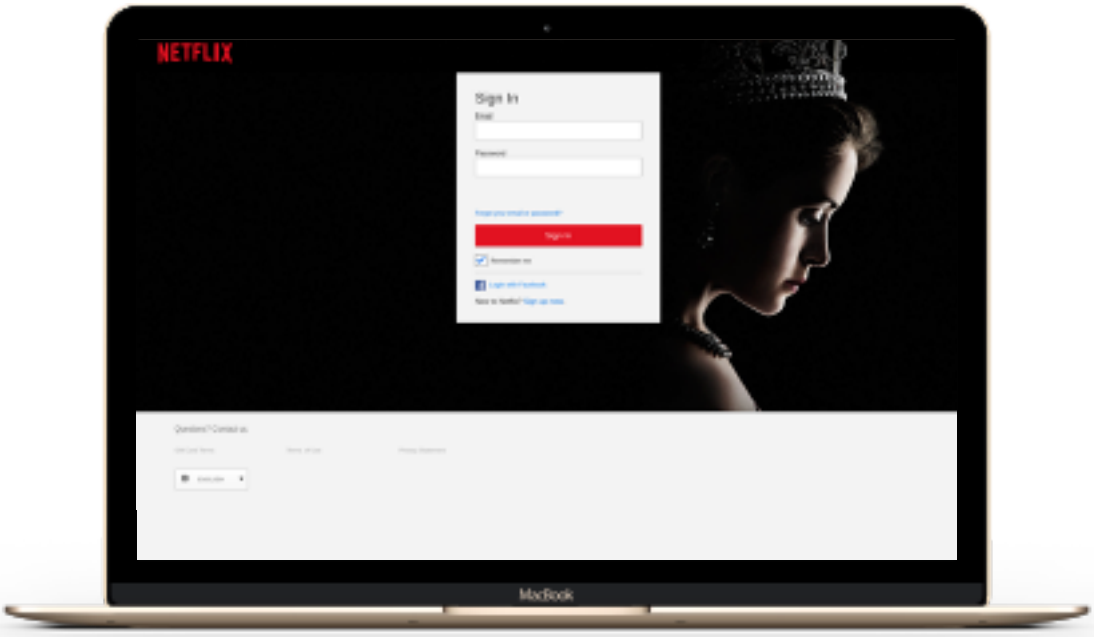
Whats new? Scammers are adapting at a rapid pace. This scam surfaced within 2 days of the Cybertruck announcement.

Source: https://checkphish.ai

Streaming Scams

2019 has seen an increase in the volume and variety of counterfeiting websites targeting the streaming industry. Almost every streaming service including Netflix, HBO, and Disney+ were affected. We saw a 40% increase in the number of pirated websites while phishing for credentials continued to grow steadily. We also observed audio streaming services including Spotify, Pandora, and Audible being targeted.

NETFLIX PHISHING SCAM



URL: hxxp://settings-update[.] com

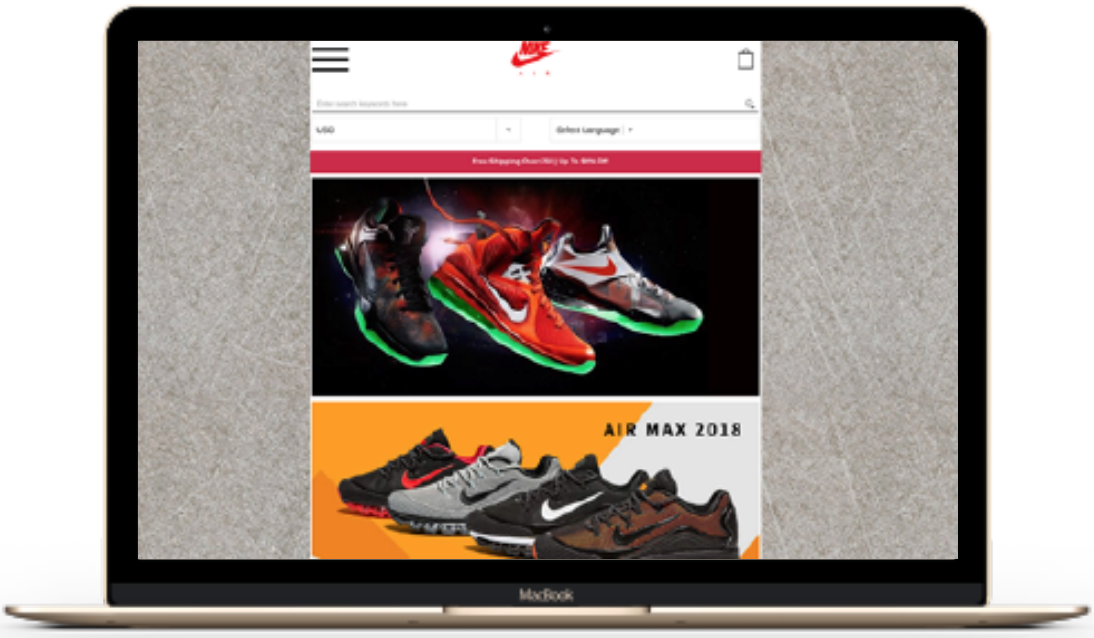
Whats new? Threat actors have included audio streaming services to their list of phishing and pirated streaming.

Source: https://checkphish.ai

Fake Online Stores

Scammers spin up fake e-commerce websites and offer steep discounts in order to lure customers into paying for products that do not exist. Almost all brands selling online including e-commerce platforms have been affected. We observed these counterfeit pages to increase by 32% when compared to 2018.

FAKE NIKE ONLINE STORE



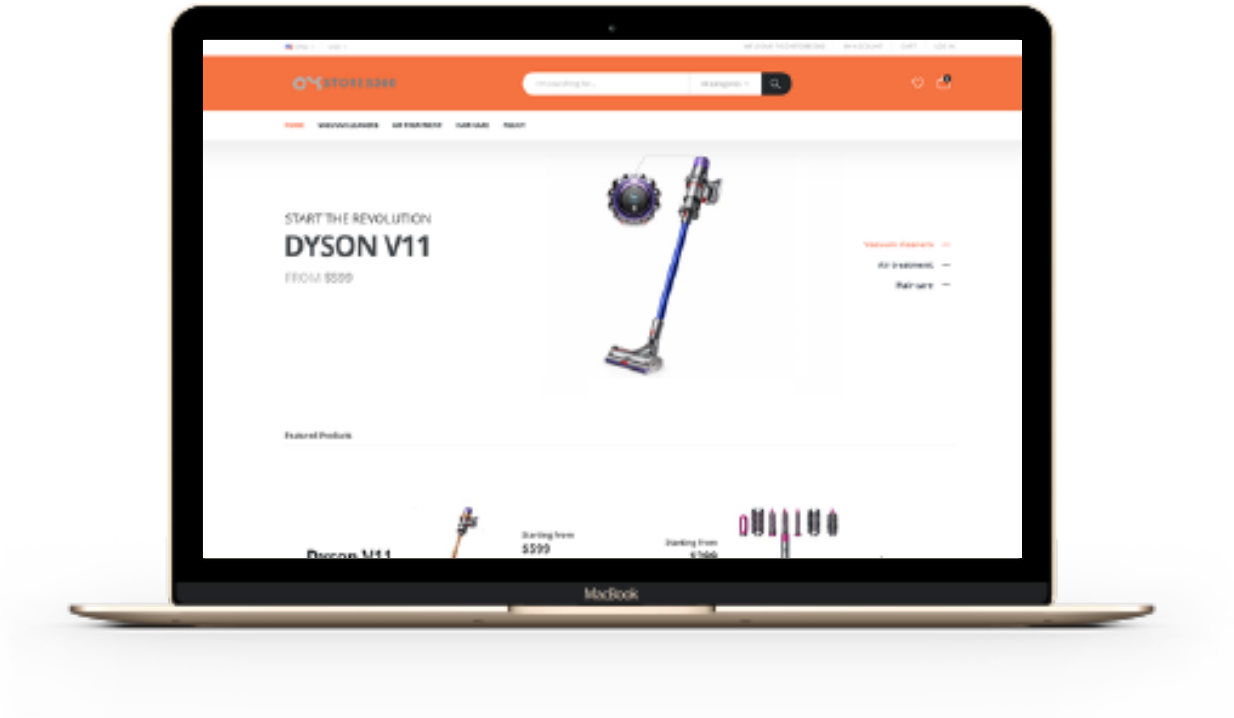
URL: hxxp://www[.]nnktrw[.]com

Whats new? The volume of these pages around the holiday season has grown threefold.

Source: https://checkphish.ai

Fake Online Stores

FAKE DYSON ONLINE STORE



URL: hxxps://dystores360[.]com

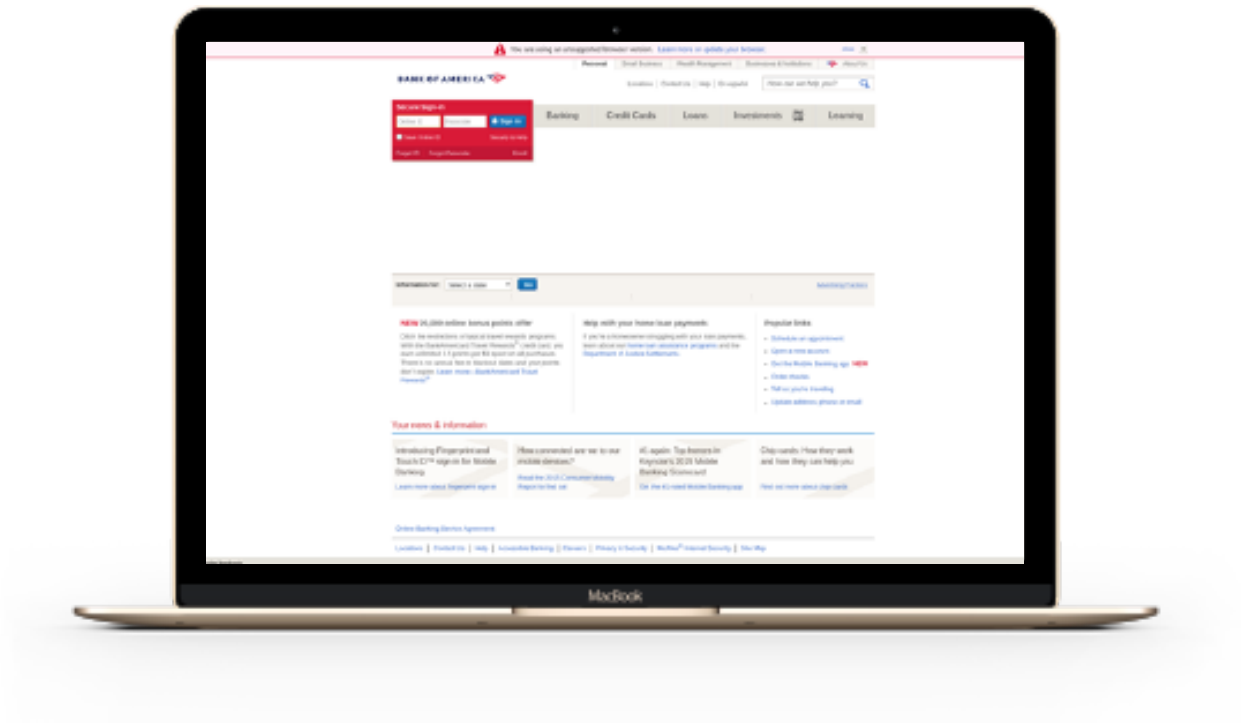
Whats new? We identified Dyson being targeted by online threat actors for the first time in 2019.

Source: https://checkphish.ai

Online Banking & Payments

With almost 26% of the total counterfeit websites in 2019 targeting online banking and payments services, they continue to be the most targeted industry.

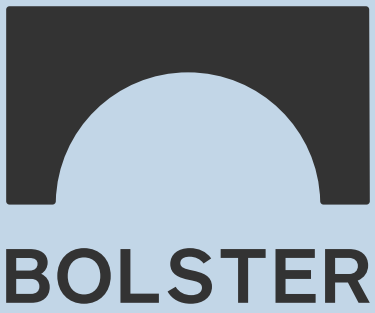
BANK OF AMERICA COUNTERFEIT



URL: hxxps://predioservices[.]com/[.]well-known/adsadsadsads

Whats new? We observed domains to be appearing on different IP addresses after being taken down.

Source: https://checkphish.ai



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

CHECKPHISH

Data Source:
https://checkphish.ai