SLASHNEXT

The State of Phishing 2021

Phishing attacks are moving faster than defenses. With millions of dollars at stake, bolstering phishing protection is an imperative for all businesses in 2021.

INTRODUCTION

In 2020 phishing exploded as the world faced a 100-year pandemic and many people moved to remote working and learning. On March 15, 2020, when states implemented the first shelter-in-place orders, SlashNext researchers saw a +3000% increase in COVID-19 themed phishing URLs. Cybercriminals launched thousands of new phishing pages every hour to harvest personal information, steal corporate data, and commit credit card fraud with no sign of slowing down.

By mid-2020, SlashNext Threat Labs saw the number of daily phishing threats top 25,000 a day, a 30% increase over 2019 figures. By fall, the number had grown to 35,000/day and grew to 50,000/day by December.

Phishing is the number one cause of a cybersecurity breach, and with millions of dollars at stake, bolstering phishing defenses is an imperative for all businesses in 2021.

In this report, you'll learn:

- Why phishing exploded in 2020
- What has changed in the phishing threat landscape
- The new generation of evasive phishing threats
- Phishing beyond fake login pages with examples, and use cases
- Why a different defense approach is needed

THE EXPLOSION OF PHISHING IN 2020

Phishing has emerged as the most effective and far-ranging tool used to perpetrate cybersecurity breaches. While phishing has been growing exponentially for years, it increased 42% in 2020, over 2019 (Exhibit 1).

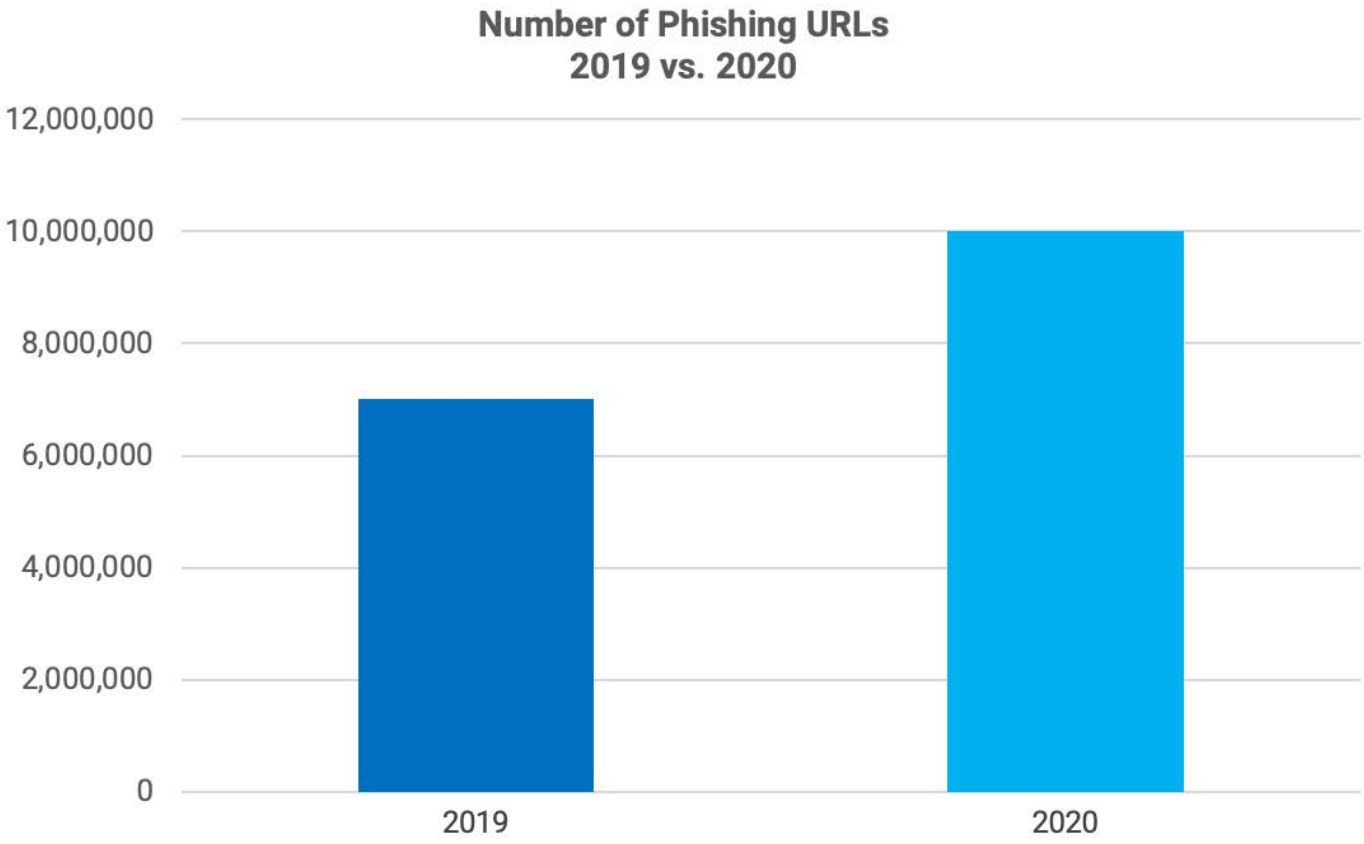


Exhibit 1: Phishing has increased 42% from 2019 to 2020

Throughout 2020, we've seen a litany of high-profile breaches that have created real damage. These included the Marriott International data breach that affected 5.2 million customers in April. In July, the Twitter spear-phishing attacks compromising several notable accounts, including Elon Musk, President Obama, and Bill Gates. Another spear-phishing attack began in September, targeting the World Health Organization's initiative for distributing COVID-19 vaccines to developing countries.

What do all of these breaches have in common? They started with a phishing attack. The number one cause of a cybersecurity breach is phishing, and this year the average

cost of a corporate breach was $2.8 million, making phishing a big business. Yet, many organizations do not see phishing as their biggest concern and do not use the latest technology to defend against this growth in phishing attacks.

By the middle of 2020, phishing threats grew to over 25,000 live threats a day, a 30% increase in phishing over 2019. As the year progressed, phishing grew at a record pace as SlashNext Threat Labs saw threats explode well above 50,000 live phishing domains a day; a trend we expect to progress at a steady pace. However, in the first few weeks of January 2021, SlashNext recorded a spike in phishing, with up to 80,000 live phishing domains a day. (Exhibit 2)

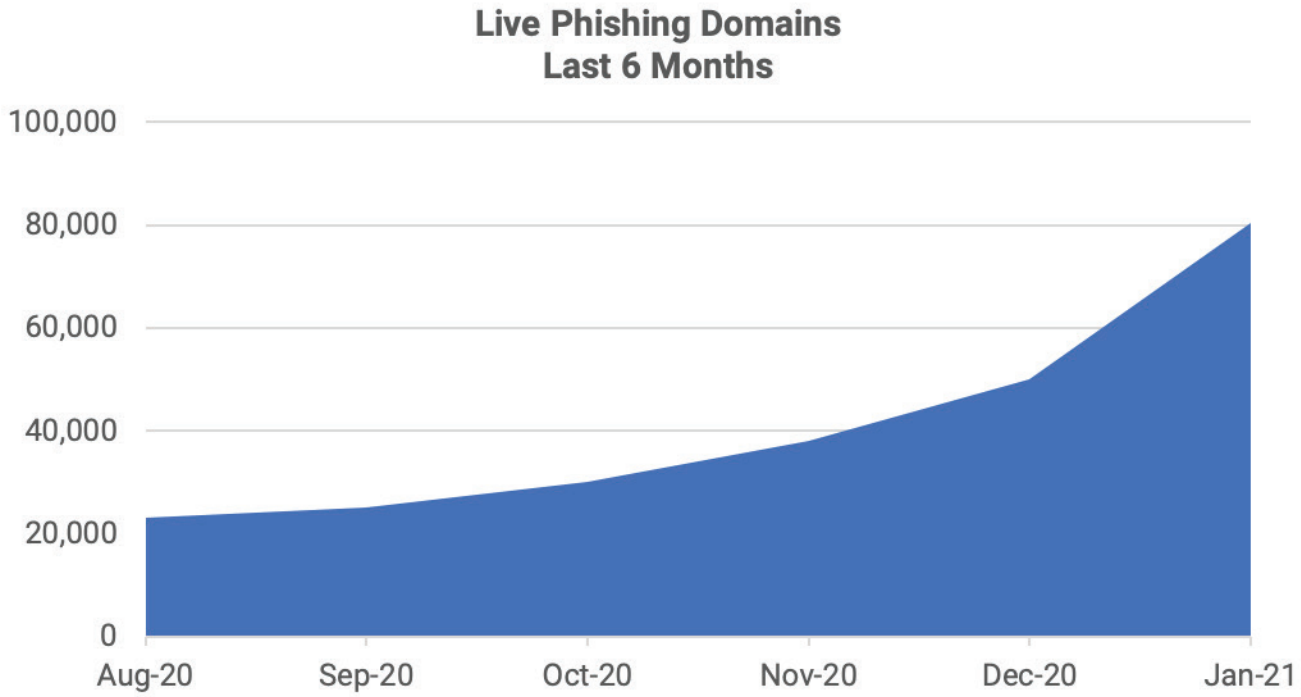


Exhibit 2: Chart indicates the growth of live phishing domains since August 2020

CYBERCRIMINALS HAVE REINVENTED THE PHISHING LANDSCAPE

Long ago, cybercriminals shifted their focus from malware to phishing. By the end of 2020, Google Safe Browsing reported over 2 million phishing sites and only 24,000 malware sites. Cybercriminals are going after the weakest link in security defense with intensified velocity as businesses and personal lives have merged with remote working and learning.

What precipitated the December spike in phishing?

A zero-hour phishing attack on Google's App Engine targeting Office 365 users pushed the holiday phishing spike. SlashNext Threat Labs witnessed an active attack on Google's App Engine service via Appspot.com designed to steal Office 365 user credentials. In its first 36 hours, the attacker created 20,000 subpages, a threat too fast for human forensics to stop.

The subpages are indistinguishable from an authentic login, and because the phish is hosted on Google Cloud Platform, it cannot be blacklisted. Over 70 anti-phishing services tested in VirusTotal showed Google App Engine remains clean.

As cybercriminals have shifted their tactics to phishing, they have also reinvented the phishing landscape. The rise in phishing attacks is directly correlated to the sophistication and effectiveness of these attacks. The classic phishing paradigm of an email linked to a fake login page easily detected with domain inspection and employee training is no longer how cybercriminals trap their victims. According to Gartner, a dramatic increase in phishing attacks and success requires a reevaluation of security controls and processes. A significant shift to remote working continues to fuel the adoption of cloud services and other collaboration tools beyond email. These are likely to become additional attack vectors.[1]

Email Phishing Protection is No Longer Enough

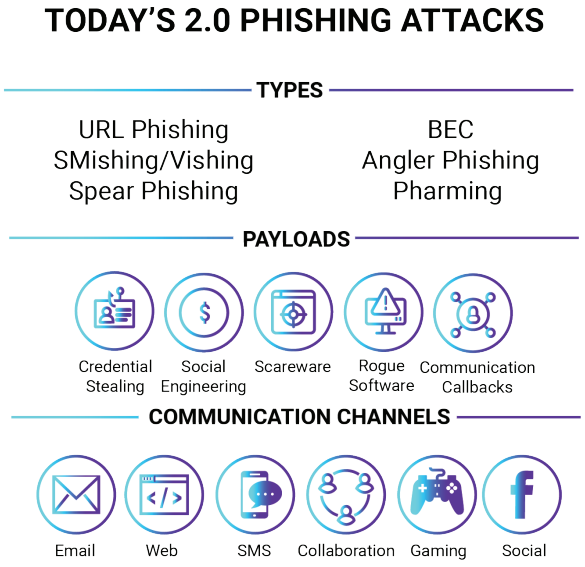


Exhibit 3: The phishing landscape has changed to include new attack vectors and phishing categories beyond email.

1: Gartner Market Guide for Email Security, Published 8 September 2020

Comprehensive Phishing Payload and Communication Channel Protection

Phishing attacks are growing because they are no longer just an email problem and have expanded to SMS/iMessage, social networks, collaboration platforms, videoconferencing, and gaming services. Cybercriminals have expanded their attack payloads beyond fake login scams to scareware, SMishing, social engineering, and rogue software. Mobile users are particularly vulnerable because of small screens, users' mistakes, and invisible URL strings hiding the address. According to the 2020 Verizon Data Breach report, iPhone users are 18x more likely to get phished than to download malware. (Exhibit 4).

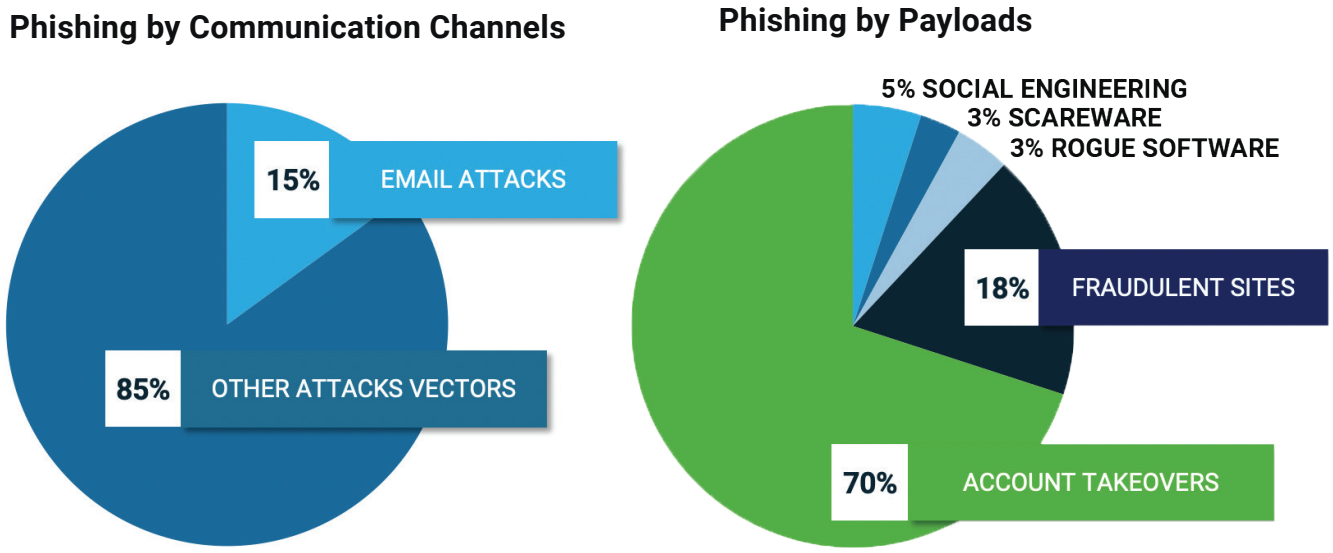


Exhibit 4: Phishing is happening outside of email more frequently and account takeovers/ credential stealing is the most common payload according to SlashNext Threat Labs.

Attacks are Moving Faster Than Defenses

Cybercriminals use automation and AI to increase the likelihood of compromising a target by leveraging legitimate infrastructure and matching data to build detailed lists of targets to increase their success. What was once spray and pray bulk phishing attacks are now mass quantities of highly target spear-phishing attacks. The low cost of computing and the availability of behavioral information make targeting effective by simulating trusted sources and launching attacks through new communication channels.

With unlimited global infrastructure and computing power, it's cost-efficient and easy to run short-lived but highly effective phishing campaigns. These short-lived phishing URLs gather valuable personal information and move on within 40-45 minutes to evade detection.

Cybercriminals are aware of how legacy 1.0 technologies are trying to catch them, and they see perfect opportunities to evade detection. They change domains and URLs fast enough so the domain reputation and blacklist cannot keep up. More often, malicious URLs are hosted on compromised sites that have a good domain reputation. People click, and within a few minutes, the cybercriminals have collected all the data they need, so they move on to the next site. By the time the security teams have caught up, that cool attack is already gone and hosted elsewhere.

Of the tens of thousands of new phishing sites that go live each day, most are hosted on compromised but otherwise legitimate domains. These sites would pass a domain reputation test, but they're still hosting malicious pages. SlashNext Threat Labs see up to 90% of the phishing URLs detected are either hosted on a compromised domain or hosted on legitimate cloud services like SharePoint, GoDaddy, and Amazon AWS. Bad actors know blacklisting Amazon or SharePoint isn't feasible, so any online services that provides HTML hosting are prey for these types of attacks, as bad actors attempt to evade domain reputation engines.

PHISHING BEYOND FAKE LOG-IN PAGES

Fake login pages are no longer the only game in town. HTML phishing can be delivered straight into browsers and apps, bypassing infrastructure (SEG, NGAV, AEP). Phishing protection that depends on domain reputation, URL inspection, and human forensics is not enough. You can't hire enough security experts to keep up with the growth in phishing attacks targeting people from multiple channels.

Phishing Types, Examples and Use Cases

The phishing type that everyone is familiar with is credential-stealing. Spoofing pages of various popular business applications like, PayPal, SharePoint, and Office 365, are all popular targets. The threat research team at SlashNext sees many phishing attacks that do not involve fake logins, including malicious browser extensions, rogue apps, social engineering scams, post-infection phishing C2s, and tech support scams leading to remote backdoor access.

Rogue Browser Extentsions and Apps

These attacks fundamentally try to exploit the user's trust with the end goal of wittingly (or unwittingly) installing malicious apps or extensions on their system with the promise of interesting or useful functionality. The typical types of apps and extensions include downloading fake system cleaners, anti-virus tools, private VPN, video players, or browser extensions. (Exhibit 5)

Common malicious characteristics include:

1. Snooping on browser sessions to sniff user's credentials
2. Actively parsing web page content (Man in the Browser)
3. Launching phishing pages within the browser

It's important to understand how rogue browser extensions and apps work to understand their sophistication and danger. Users think it's ok to use extensions that make their life easier, like logging into email faster or using a PDF Converter. These extensions have legitimate functionality, but they have a side business, which is why they are free. (Exhibit 6)

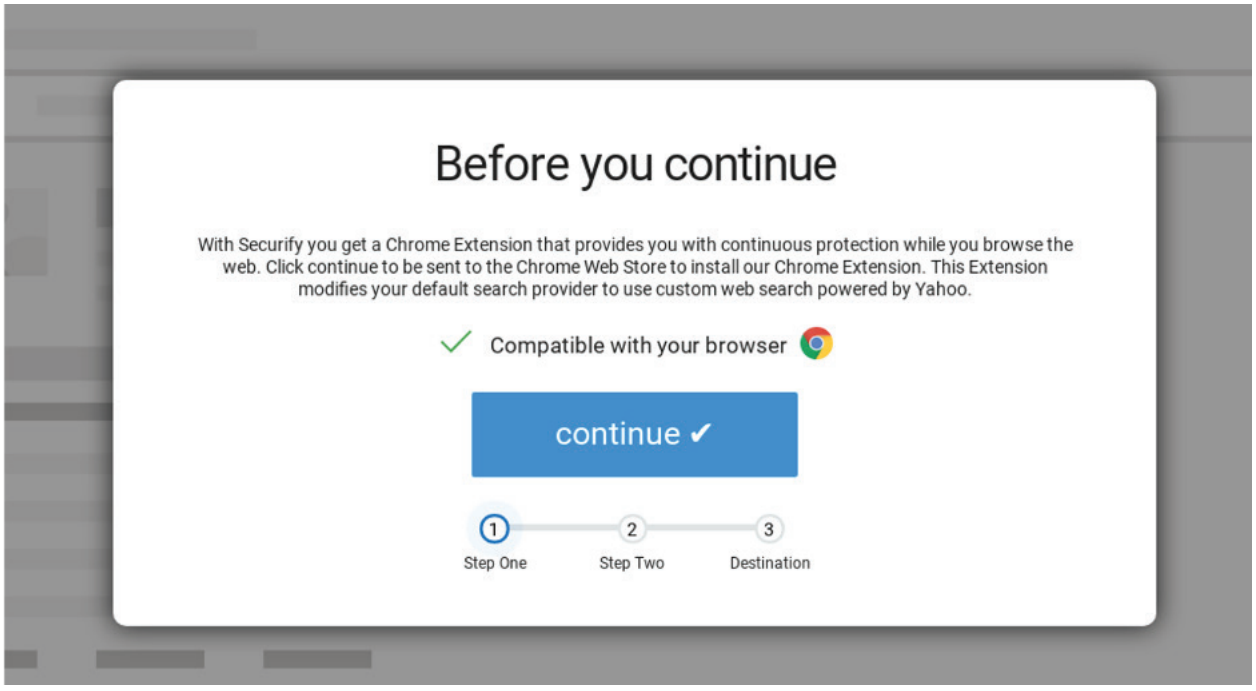


Exhibit 5: Example of malicious browser extension ironically offering browser security protection

Google runs security checks on Chrome extensions before they are available in their store, but cybercriminals design these browser extensions with legitimate functionality. However, once installed, the malicious script is downloaded from the web using a runtime code, once the browser is closed, it goes away. Since the code living inside the browser memory is JavaScript, the most common script inside a browser, there's no way to distinguish the malicious script collecting data from JavaScript that's being rendered by a legitimate page.

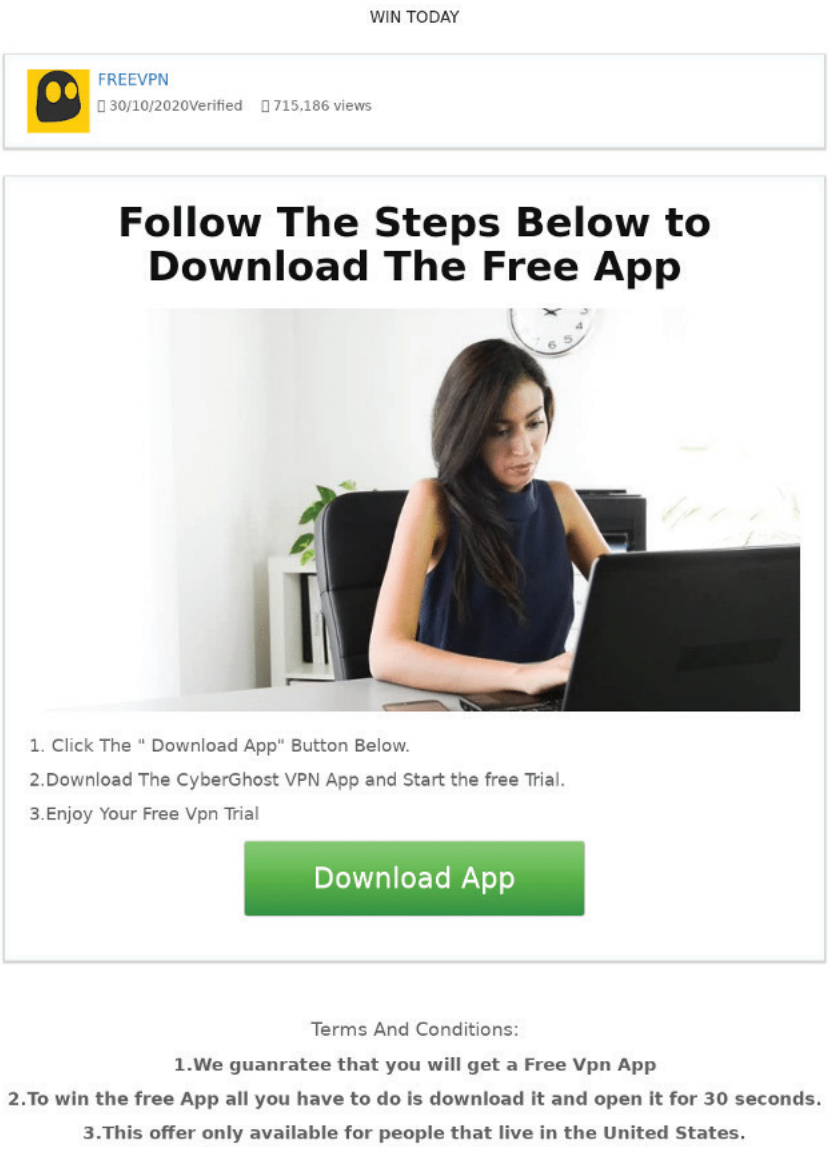


Exhibit 6: Example of a malicious browser extension for a private VPN app

Man-in-the-Middle Attacks

Now we see more phishing attempts that can bypass two-factor authentication (2FA) or multi-factor authentication, with Man-in-the-Middle attacks. Many with Two Factor Authentication (2FA) believe they're protected because the birth of 2FA grew from knowing that current security defense solutions were no longer working.

The exact functionality of Man-in-the-Middle attacks is collecting and selling data. These browser extensions offer cybercriminals the perfect workaround for organizations that rely heavily on 2FA. SlashNext Threat Labs have observed malicious browser extensions that merely wait for 2FA to complete before launching. By design, once a browser extension is installed, it can access the browser's complete canvas. Once logged in, the session is hijacked to capture whatever is being rendered on the computer screen. These extensions have the full power to do whatever the user is doing and seeing whatever is happening within that browser window.

SMishing

SMishing is phishing delivered through SMS text, and the threat types can be credential stealing, rogue software, apps, and extensions. These attacks are customized specifically for mobile delivery and designed to only work for Mobile iOS or Android. What makes them particularly dangerous is the attack vector is not email but ads and SMS, where most phishing protection is not effective. (Exhibit 7)

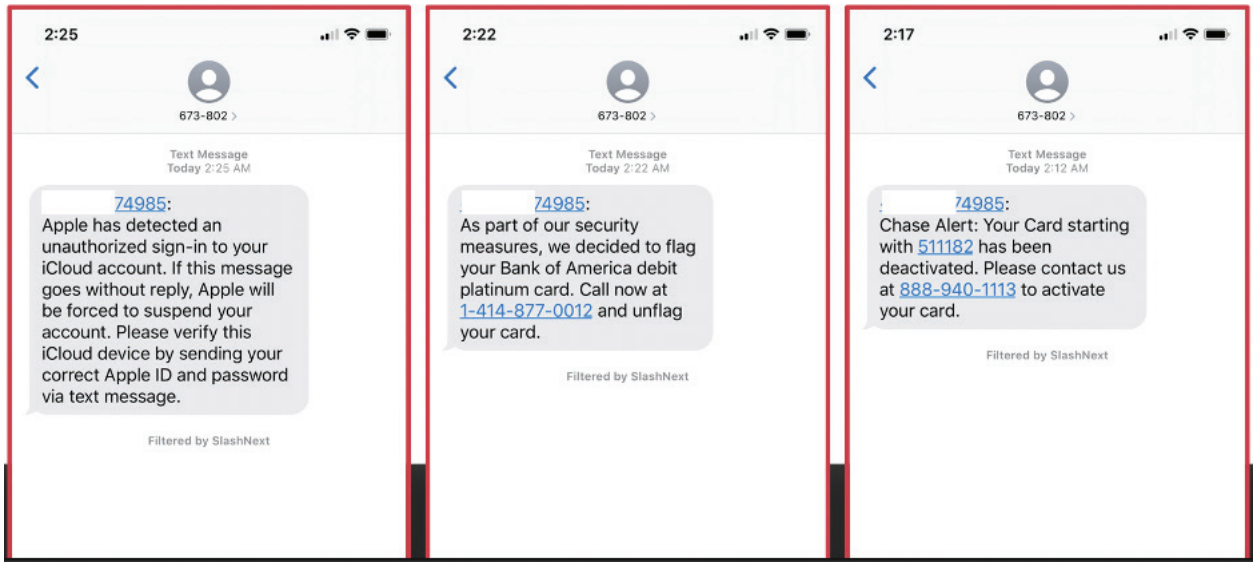


Exhibit 7: Example of a malicious SMS on mobile

Scareware

Scareware scams are designed to fool users. They are very dangerous because there are no exploits or malware that a phishing threat analysis would flag as malicious. A cyber-criminal is just trying to scare the user into giving them information and remote access, and then the real damage happens. One tactic is to ask the victim to install a legitimate remote support software like TeamViewer or LogMeIn, and once installed, there is a back-door. The credentials and license can be used for a breach or sold on the dark web. Now, whoever wants to attack your organization doesn't have to launch a spear-phishing attack; they can go to the dark web and buy the credentials. (Exhibit 8)

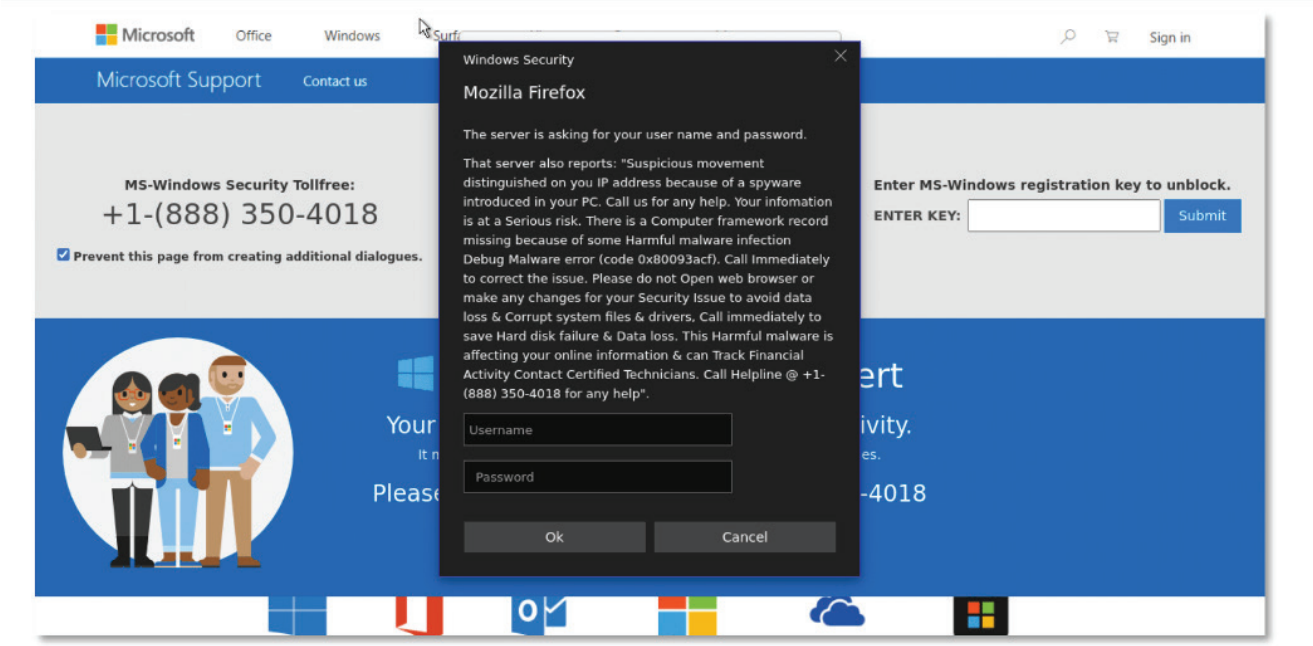


Exhibit 8: Tech Support Scareware scares users into creating a backdoor that can be sold on the dark web

Social Engineering Scams

Cybercriminals' motives are the same with social engineering scams as with other phishing attacks. The goal is to get a user to install, win or buy something to collect information. In 2020, a high-profile social engineering scam on Twitter received much media attention. As part of this breach, Twitter accounts of various celebrities were compromised to perform Bitcoin scams. Bitcoin transfer scams are not a new concept. SlashNext's Threat Lab sees dozens of Bitcoin phishing sites each day that use celebrity photos and names

to conduct similar cryptocurrency scams. Cybercriminals prefer stealing cryptocurrency because it can be used for nefarious purposes on the dark web, leaving no trail behind. (Exhibit 9)

With all of these phishing threat vectors, the purpose is exactly the same: installing a backdoor or collecting confidential information to sell on the dark web. The methods are different—They play on human desires and fears. Sometimes they scare, sometimes they pretend to be legitimate, or they merely create excitement.

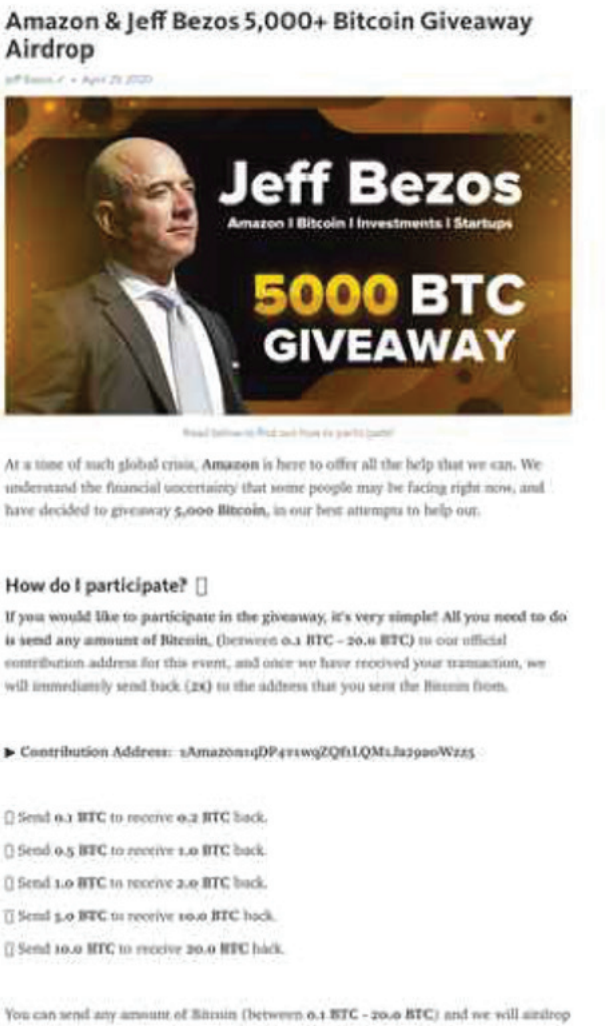


Exhibit 9: An example of the Twitter Bitcoin scam that promises to give away bitcoins only if you initiate a smaller transfer first—an easy way to make money.

Twitter Hack—Old Dog, New Tricks

There is an extensive list of TTPs (Tools, Techniques, Procedures) that attackers can use to conduct cybercrimes, but it boils down to only four fundamental motives, fun, money, information theft and extortion.

Money was the motive in the Twitter breach involving a Bitcoin transfer scams. Bitcoin scams are not a new concept. SlashNext's Threat Lab sees dozens of Bitcoin phishing sites that use celebrity photos and names to conduct similar cryptocurrency scams. Cybercriminals prefer stealing cryptocurrency because it leaves no trail behind.

These Bitcoins scams are just the tip of an iceberg. Phishing payloads have morphed into dozens of different payloads, including money transfer scams, scareware, rogueware, man-in-the-middle attacks.

Read more about the Twitter breach at www.slashnext.com/blog /twitter-hack-old-dog-new-tricks/

A DIFFERENT APPROACH IS NEEDED

Phishing is a Business, Built to Make Money

Most targeted attacks are happening when cybercriminals buy data from the dark web. Gone are the days where hackers or nation-states would actually send a phishing email and work hard to penetrate an organization. Today cybercriminals can go to the dark web to buy infected machines of almost any organization. Every organization has infected features and employees. Information is compromised. All hackers have to do is pay an intermediary for access. They don't have to go to lengths to try to scam you because the compromised machines with malicious browser extensions or TeamViewer are already available for sale.

We currently see tens of thousands of new phishing sites per day, but it varies day-to-day depending on cybercriminals' activity. For instance, on weekends, volume decrease by 50% because cybercriminals take weekends off too. By Sunday morning (PST), we see volume pick up again. By Monday and Tuesday, it's at full volume. Phishing is a business, much like any other, built to make money.

Moving from 1.0 Reputation Detection to 2.0 AI Phishing Defense

Even a tech-savvy user could miss phishing from different attack vectors, and most employees are not trained to detect the latest, sophisticated phishing attacks, and they merely fall victim.

Today cybercriminals are leveraging new AI phishing methods, while most of the industry is examining phishing URLs and domains. That process is often not accurate or fast enough to detect new, fast-moving phishing attacks. Organizations must start looking at 2.0 phishing defense methods that utilize AI and dynamic analysis to detect the latest generation of threats.

SlashNext exclusively focuses on 2.0 AI phishing defense by inspecting billions of URLs at cloud scale with virtual browsers that overcome sophisticated evasion techniques. Our patented SEER technology utilizes natural language processing, computer vision, and behavioral analysis to detect and block threats hours and sometimes days before vendors using 1.0 phishing techniques, resulting in:

- World's largest phishing intelligence network
- 99.07% Accuracy
- 1 in 1 million false positives
- 45,000 new phishing attacks daily

Zero-Hour Protection for All Phishing Types, Payloads and Channels

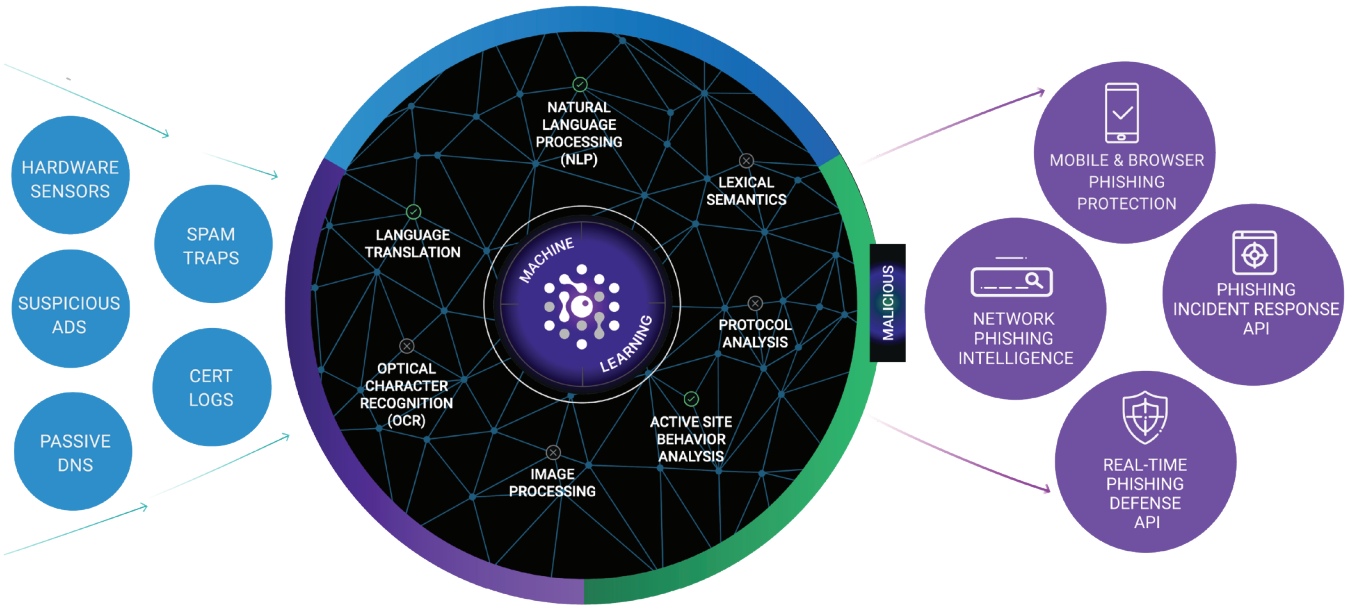
Our 2.0 AI Phishing Defense service provides the broadest range of protection against all phishing types, including URL phishing, spear-phishing, BEC, and more that deliver credential stealing, rogue software, and scareware across email, SMS, social media, messaging, collaboration, and gaming platforms.

World's Largest Phishing Intelligence Network

To successfully predict and protect users from phishing attacks, you must start with visibility. SlashNext global intelligence network provides insight into over 1 billion internet transactions and 7 million URLs inspections daily, using virtual browsers and AI. The source of intelligence includes:

- Spam Email and SMS Traps - Extensive honeypot network collecting suspicious emails and text
- Suspicious Ad Networks - Click redirect chain collecting suspicious ads
- Hardware sensors - Suspicious web links extracted from live web traffic
- Domains and certification logs - Newly registered domains and HTTPS certificates feeds are analyzed
- Passive DNS – Newly registered and observed domains are extracted from crawl throughs of suspicious IPs

SlashNext AI Phishing Threat Detection Technology



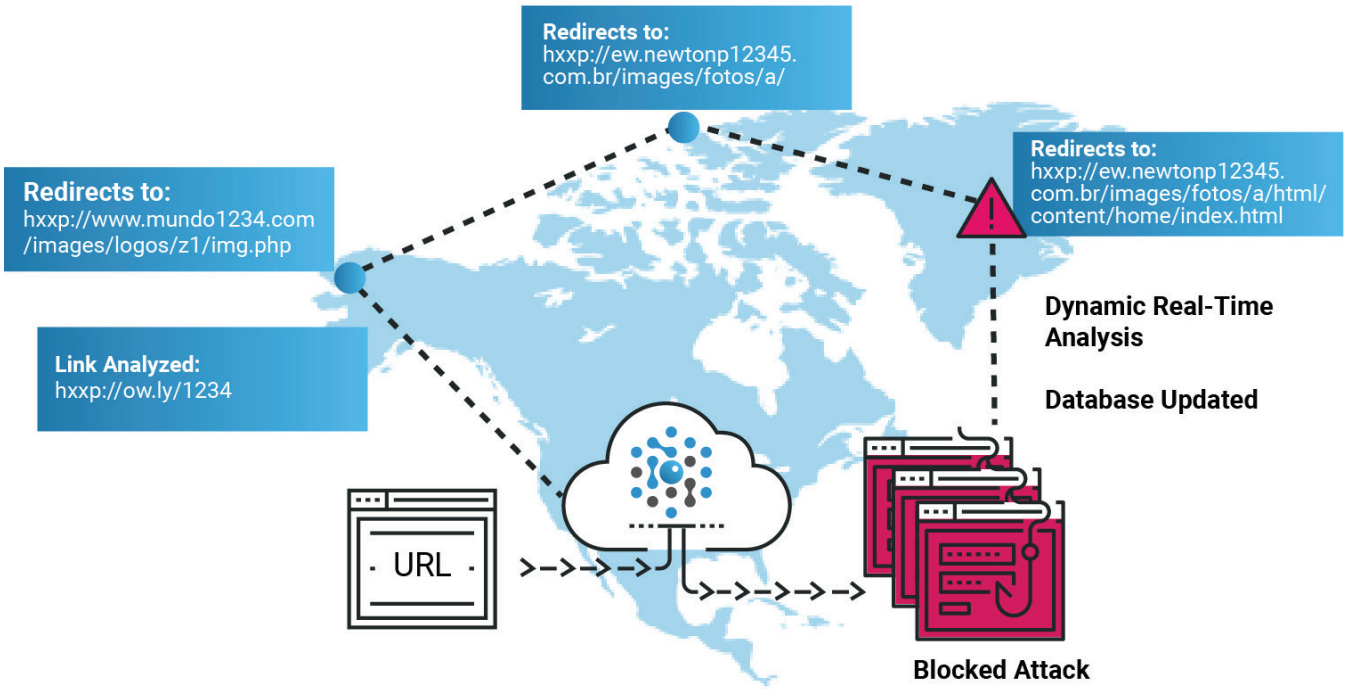
Overcoming Inspection Blocking

Many sophisticated attack pages apply defensive and offensive techniques to block inspection by security vendors.

These techniques include:

- CAPTCHA – SlashNext "injects" itself behind the CAPTCHA to access the attack page
- Access Control by IP – SlashNext uses dynamic residential IP addresses to mimic end-user browsing profile when the webpage is unreachable by using co-location IPs
- URL Redirection – SlashNext follows all URL redirections to analyze the destination webpage
- Using Shared Infrastructure – SlashNext applies a zero-trust-approach and applies the same scanning technologies to all webpages

SlashNext Follows URL Redirects



Virtual Browser and Progessive Machine Learning

As this paper discussed, most of the industry is using domain and URL reputation techniques to identify malicious URLs. That approach is often not accurate or fast enough to detect new and fast-moving phishing attacks. SlashNext's patented detection technology are purpose-built for phishing detection, and centers on the behavioral analysis of the content. The suspicious content is loaded into a virtual browser session and fully rendered, enabling our technology to analyzes the content using computer vision, natural language processing, and other machine learning classifiers to see exactly how it looks and understand the context of the page. SlashNext has viewed billions of websites that have been written historically for phishing or benign purposes. And just like a security education company that trains employees, our machine learning classifiers are trained to recognize a phishing site.

Progressive learning, a new form of machine learning invented by SlashNext, uses Artificial Intelligence (AI) techniques to emulate human cognitive reasoning and allow the system to learn and respond accurately without the need for human intervention. The AI layer allows the progressive learning machine to use dynamic features. This patented innovation allows the system to learn from its environment at run-time and become incrementally more accurate in its future detections without any human interaction. This process allows SlashNext to accurately inspect over 7 million URLs daily.

The core inspiration for progressive learning came from malware researchers. Progressive learning, replicates the analytical reasoning process a researcher goes through when manually analyzing a potential threat. Human researchers combine intuition, cognitive thinking, natural language analysis, and various other discovery methods to understand new, unknown threats. At SlashNext, we have succeeded in automating some of the world's best cyber researchers' thought processes and techniques and codified this knowledge into a cloud-based progressive learning AI.

About SlashNext

SlashNext is the phishing authority, leading the fight together with its partners to protect the world's internet users and brands from phishing anywhere. SlashNext 2.0 AI phishing defense services utilize our patented SEER technology to detect zero-hour phishing threats by performing dynamic runtime analysis on billions of URLs a day through virtual browsers and machine learning. Take advantage of SlashNext's phishing defense services using mobile apps, browser extensions, and APIs that integrate with leading mobile and endpoint management and IR tools. SlashNext is backed by Norwest Venture Partners and Wing Venture Capital and has customers around the world.

Contact Us

6701 Koll Center Parkway, Suite 250
Pleasanton CA 9456694588

Contact Sales 1(800) 930-8643

Request a Demo https://www.slashnext.com/request-a-demo/