SLASHNEXT

The Human Hacking Report

Phishing is a human problem across all digital channels

TABLE OF CONTENTS

INTRODUCTION

Humans are the most porous cybersecurity entry points into an organization. By moving completely to the cloud, apps and browsers are all humans need to communicate with work, family, and friends. While most of us are aware of the cybersecurity guardrails, we are not infallible. We can be lured into providing personal information, credentials or installing malicious apps that can undermine even the most sophisticated cybersecurity defenses.

For the cybercriminal, it's much more straightforward to launch an attack against a human because personal targeting, automation, and the availability of free legitimate domains have increased the speed and success of their attacks.

In fact, humans don't stand a chance against sophisticated, targeted phishing attacks coming at them from all digital channels. Once reliable security strategies, including secure email gateways (SEGs), firewalls, and proxy servers, are not enough to stop these new cyber threats. Security training, which is the last means of defense, is useless against these well-crafted attacks. All the clues humans use to detect these attacks are not present, and expecting human intervention is not a practical solution.

In this report, you'll learn:

- How human hacking is growing across email, text, web, social, gaming, collaboration, and search apps
- Why human hacking is not just an email problem and how cybercriminals have moved on to unprotected communications channels
- How security leaders can better understand the threat of human hacking and take proactive measures to improve their security posture
- How the future of anti-phishing lies in stopping human hacking with AI and machine learning

In the first half of 2021, SlashNext Threat Labs analyzed millions of domains and URLs for phishing attacks targeting humans at work and in their personal life. These key findings use data collected from those attacks and are intended to present the current threat landscape to the security community to better understand the evolving phishing threat landscape.

"Phishing is anything malicious that reaches a user to steal credentials, data or financial information."

PHISHING REDEFINED

Anyone who thinks phishing is email-only might be living in 2005

The term phishing was coined in 1996 by hackers who were sending out email lures to steal passwords and financial information from AOL users. Hackers replaced the letter f with ph, as a tribute to the first form of hacking, called phreaking (phone system hacking from the 1970s).

By 2005 the Oxford dictionary added phishing to its list of definitions. Defining it as "the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers." This definition clearly defined phishing in 2005 since email was the number one form of digital communication, but today delivering "lures" through email is not the only game in town. In fact, hackers have employed a multi-touch strategy. While there has been an attempt to categorize phishing, with terms like Smishing (SMS phishing) and SMP (Social Media Phishing), it's still phishing, and the more digital channels evolve, the longer and more complicated the list becomes. So with the growth of digital channels and the multitudes of ways hackers can reach a user, wouldn't it be better to redefine phishing as "anything malicious that reaches a user to steal credentials, data or financial information."

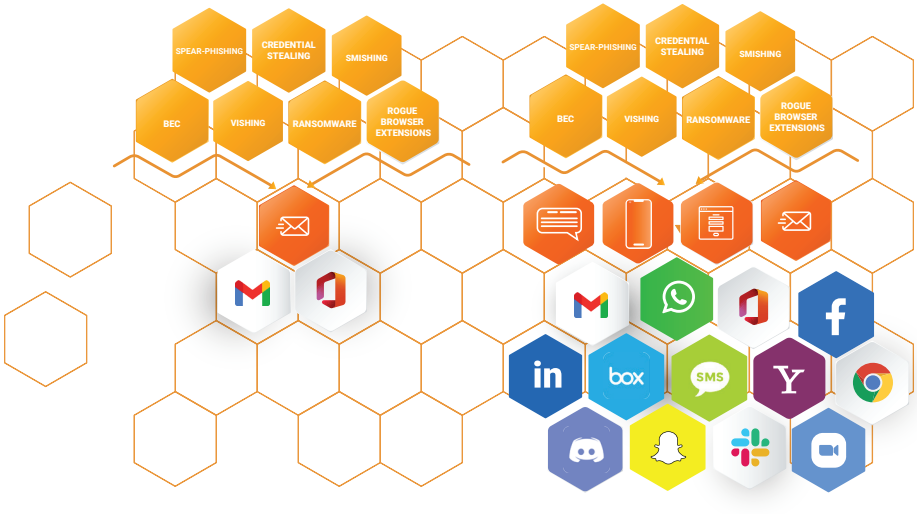
By thinking phishing is an email problem or a spam problem gives the hackers the upper hand. Only protecting against email phishing in your organization is like using security protection from 2005. You wouldn't do that, right? Because that would be like having no protection at all. Today, only protecting email and leaving other digital communication channels unprotected from phishing is enabling hackers to target your high-value users with increased success.

Again, let's think about phishing in its entirety as multi-channel phishing. "Anything malicious that reaches a user to steal credentials, data or financial information."

The Shift to Multi-Channel is Happening Now

Yesterday:
Email Phishing
Only protecting email and leaving other digital communication channels unprotected from phishing.

Today:
Multi-Channel Phishing and Human Hacking
Users working from anywhere on any device are susceptible to multi-channel attacks in email and all digital channels.



Now that it's established that anti-phishing needs to protect users from multi-channel phishing, the only way to know if you have a phishing problem outside of email (and trust me, you do) is to assess the phishing attack surface.

Here are a few questions to get started:

- Where are your employees protected from phishing?
- What phishing attacks are you missing on mobile, browsers, collaboration apps, gaming, or search?
- Are your users protected from zero-hour threats in real-time?
- Are they protected when accessing URLs on their browser or their mobile device?
- Do they have on-app or extension protection from zero-hour phishing threats?

Keep the answers to these questions in mind while reading this report to better understand the threat landscape and the phishing attack surface you need to protect.

KEY FINDINGS

By the Numbers

Eighty-five percent of data breaches involve human interaction, according to the Verizon Data Breach Investigations Report (DBIR) 2021. Phishing is the most pervasive way to initiate human interaction. It is the most effective tool to perpetrate data breaches, and it has moved to the number one position for ransomware attacks. While phishing has been growing exponentially for years, 2020 was a record-breaking year, but the triple-digit spike was not an aberration. SlashNext Threat Labs saw a 51% increase in 2021 vs. 2020. The peak in July 2021 showed a 40% increase, more than 1M malicious URLs taking advantage of humans, including their love of watching the Olympics. (Exhibit 1).

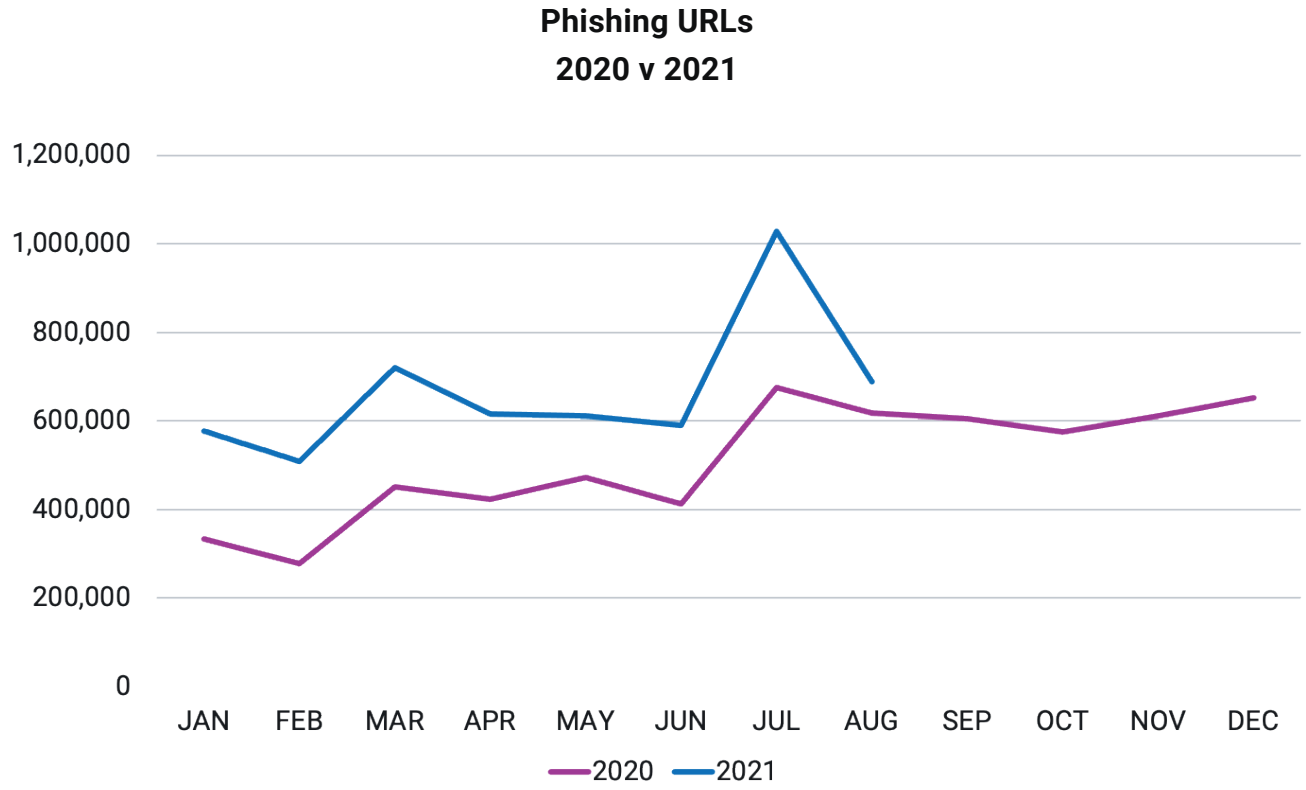


Exhibit 1: *SlashNext Threat Labs detected over 14 million malicious domains and URLs with a 51% increase in 2021 from 2020.*

Credential stealing is leading the charge in phishing attacks. More than 60% of breaches involve credential data and 95% of organizations experience credential stuffing attacks, according to the Verizon DBIR 2021.

SlashNext Threat Labs saw 82% of all phishing attacks were credential stealing attacks in 2020, and in the first 8 months of 2021 59% of all phishing involved credential theft. Social engineering rose 270% in 2021 vs. 2020, mainly fueled by scams for fake streaming sites and adware for the Tokyo Olympic Games. (Exhibit 2)

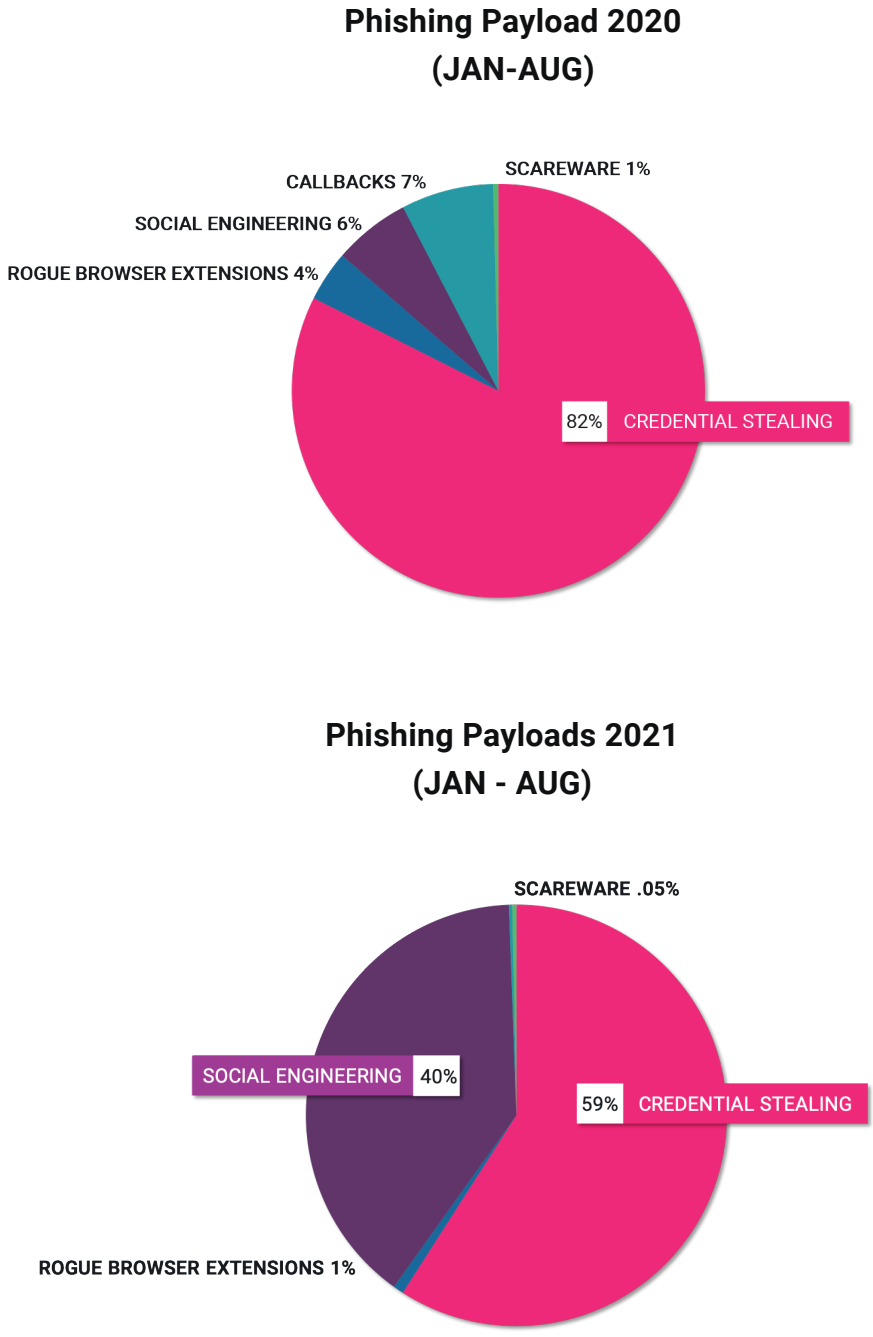


Exhibit 2: *The growth of live phishing URLs 2020 - 2021 grew by 59%*

Spear Phishing and Human Hacking Across Digital Channels

The changes in cybercriminal tactics, specifically an increase in spear phishing velocity vs. old school spray and pray phishing, led to an increase in the speed of attacks and their success. These factors have supercharged the growth in spear phishing, and we expect this growth to continue due to the advancement of these tactics. Understanding what has changed to increase success is critical in mounting a defense. (Exhibit 3)

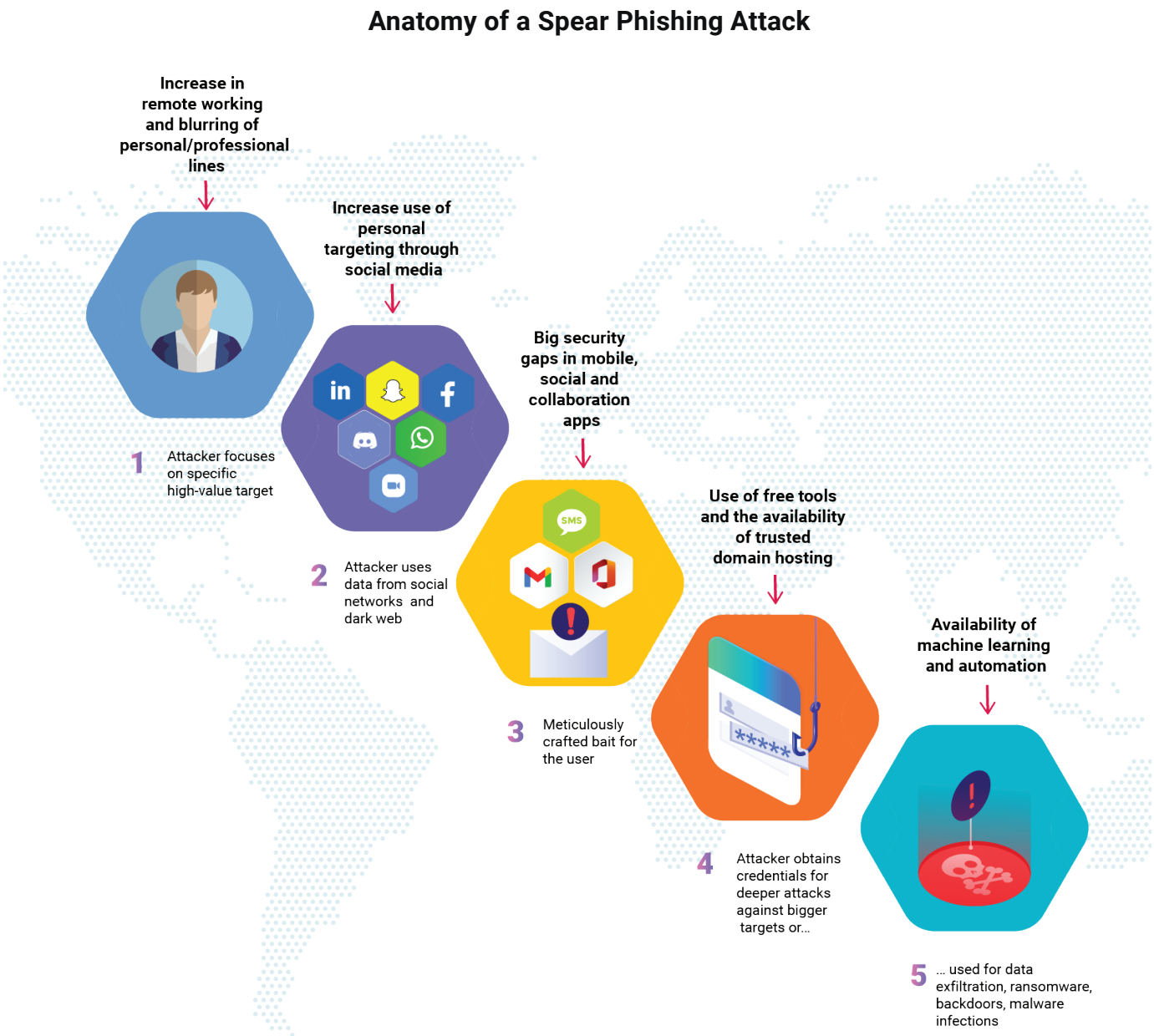


Exhibit 3: *The phishing landscape has changed with the weaponization of cloud and social tools to the success of spear-phishing attacks.*

Cloud, Apps and Browsers Are All We Need

Humans only need apps and browsers in the cloud to communicate at work and in every other aspect of life – video meetings, health charts, social life -- every digital channel is susceptible. Fake login pages are no longer the only game in town; phishing can be delivered straight into browsers and apps, bypassing infrastructure (SEG, NGAV, AEP). You can't hire enough security experts to keep up with the growth in phishing attacks targeting humans in multiple channels.

In 2021, SlashNext Threat Labs identified 2.5 million phishing attacks that did not involve fake login pages but malicious browser extensions, rogue apps, and social engineering scams leading to remote backdoor access.

Rogue Browser Extensions and Apps attacks fundamentally try to exploit the user's trust with the end goal of installing malicious apps or extensions on users' systems by promising useful functionality. The typical types of apps and extensions include free streaming services, fake system cleaners, anti-virus tools, private VPN, video players, or browser extensions. Users think it's ok to use extensions that make their life easier, like streaming content or using a PDF Converter. These extensions have legitimate functionality, but they have a side business, which is why they are free, so it's important to understand how they work to understand their sophistication and danger.

These malicious apps and extensions can be much more dangerous than email phishing. The malicious nature of these threats involves snooping on browser sessions to sniff user's credentials and actively parsing web page content (Man in the Browser) to launch phishing pages within the browser. Security checks are run on Chrome extensions before they are available in their store. However, hacker design browser extensions with legitimate functionality, and once installed, malicious JavaScript is downloaded from the web using a runtime code. Since JavaScript is the most common script inside a browser, there's no way to distinguish the malicious script collecting data from JavaScript being rendered by a legitimate page.

Man-in-the-Middle (MIM) Attacks

The most successful Man-in-the-Middle attacks are used to bypass two-factor authentication (2FA) or multi-factor authentication. The exact functionality of Man-in-the-Middle attacks is collecting and selling data, which is often used for ransomware and data exfiltration. 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 to 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. (Exhibit 3)While these attackers appear to be nation-states, they demonstrate how spear-phishing has evolved from small campaigns to very large but highly targeted attacks. Spear phishing typically targets employees working in finance with a monetary motive. These spear-phishing attacks are targeting specific, high-value individuals working on Covid-19 vaccines or therapeutics with access to lab technology and intellectual property in an attempt to steal sensitive account credentials, including executives working in innovation, clinical research, patents, and manufacturing. (Exhibit 4)

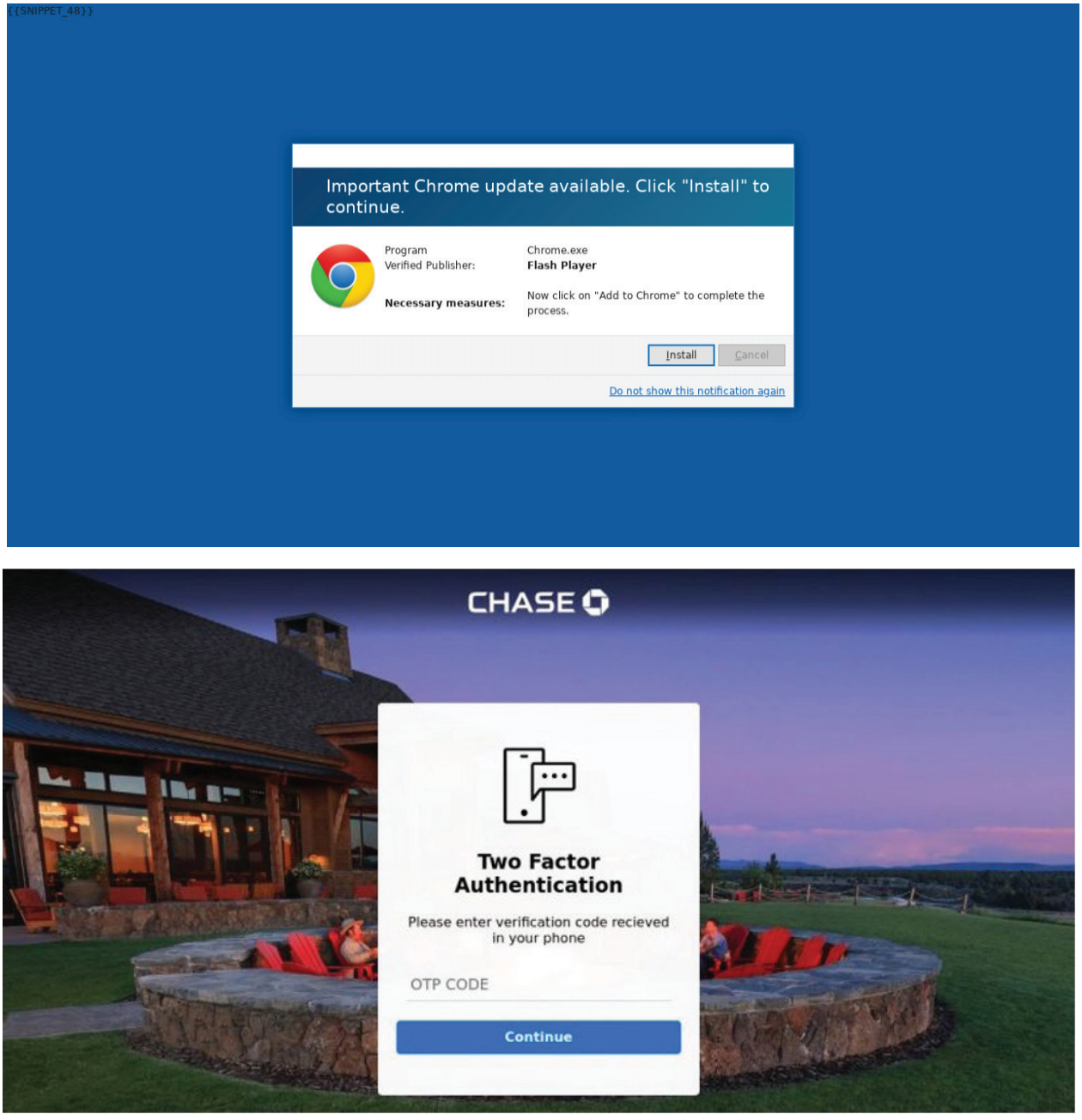


Exhibit 4: *Chrome Rogue Browser Extension asking to install malicious content and Chase Bank Reverse Web Proxy MIM to hijack session cookies*

TRUST, AUTOMATION, AND PERSONALIZATION TARGETING HUMANS

Spear Phishing at Scale: Mass Personalization Automates Lures Too Good to Resist

The tried and true Microsoft 365 log-in page was virtually indistinguishable from the real thing in a massive spear phishing attack in March 2021. SlashNext Threat Labs first observed these spear-phishing attacks three days before the end of 2020. Over 60 days, more than 1,000 spear phishing domains belonging to the same threat actors were launched in a flurry, targeting companies working to deliver Covid-19 vaccines and therapeutics. In all cases, these attacks point to Microsoft 365 log-in pages hosted on legitimate domains, including Azure websites.(Exhibit 5)

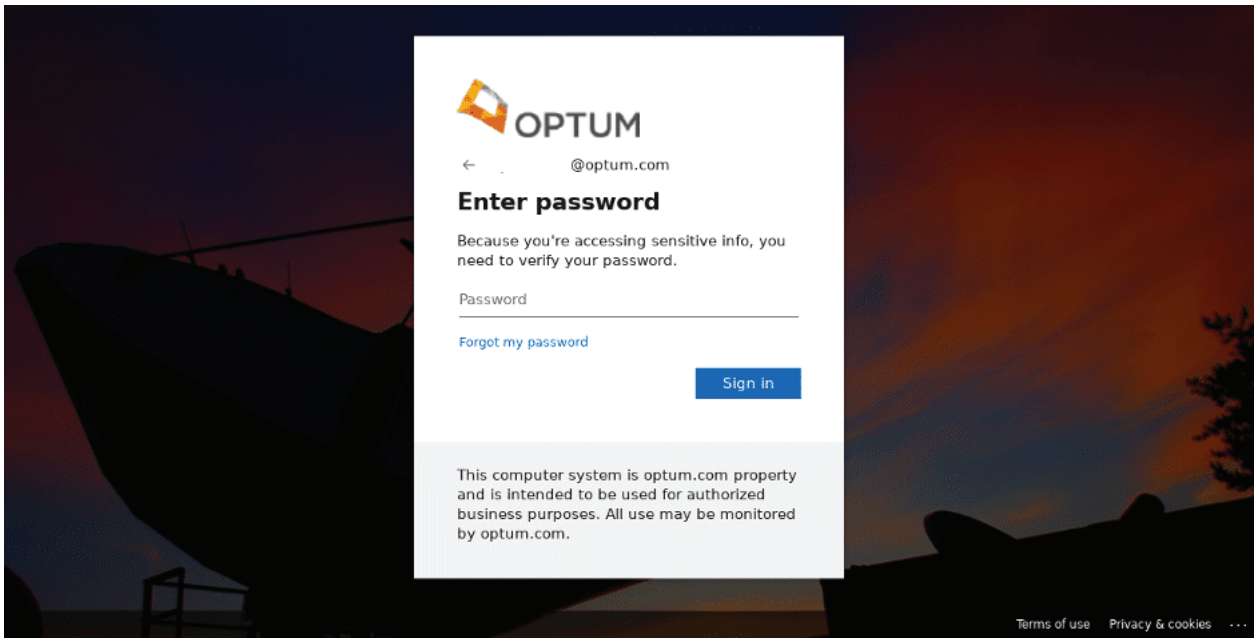


Exhibit 5: *Example of spear-phishing attack targeting employee during first quarter of 2021.*

While these attackers appear to be nation-states, they demonstrate how spear-phishing has evolved from small campaigns to very large but highly targeted attacks. Even though These spear-phishing attacks are targeting specific, high-value individuals working on Covid-19 vaccines or therapeutics. Spear phishing typically targets employees working in finance with a monetary motive. These attacks target high-value employees with access to lab technology and intellectual property in an attempt to steal sensitive account credentials, including executives working in innovation, clinical research, patents, and manufacturing. (Exhibit 6)

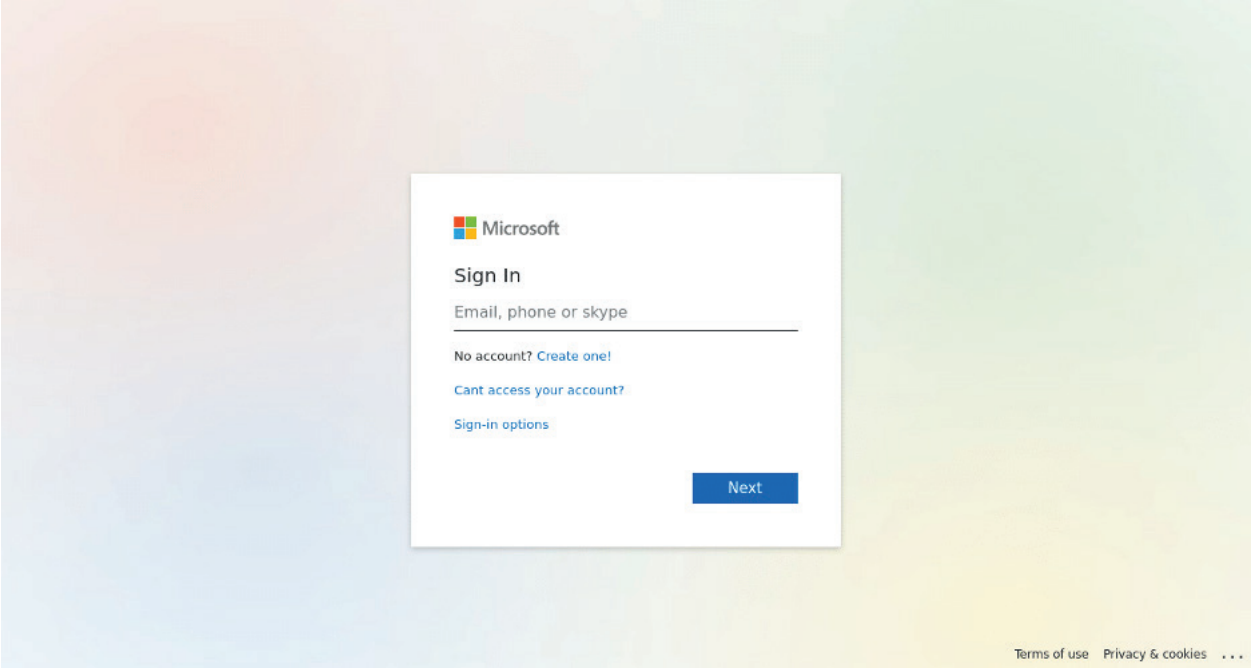


Exhibit 6: *Example of spear-phishing attack targeting employee during first quarter of 2021.*

The Use of Trusted Domains

The phishing landscape truly changed in 2020 and continues to evolve in 2021, and cyber-criminals are celebrating their success with even more targeted human hacking campaigns. SlashNext Threat Labs observed an increased volume of malicious URLs from trusted cloud services. In August 2021, 12% (or 79,300) of all malicious URLs identified by SlashNext Threat Labs were from legitimate cloud hosting infrastructure. (Exhibit 7)

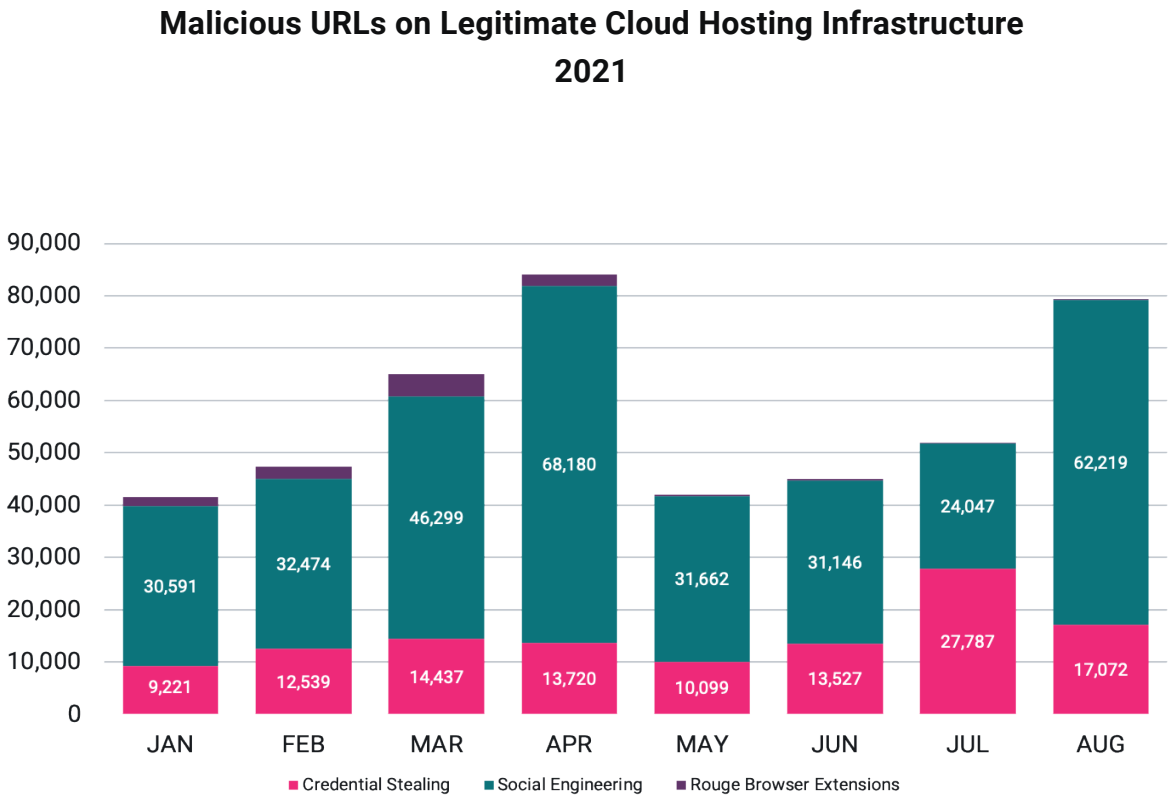


Exhibit 7: *In August alone, 12% (79,300) of all malicious URLs identified by SlashNext Threat Labs were from legitimate cloud hosting infrastructure.*

The trusted reputation of these domains, including AWS, Azure, outlook.com, and share-point.com, enables cybercriminals the opportunity to easily evade current detection technologies using domain reputation and blocklists like SEG, proxy, SASE, and endpoint security tools. Attackers are using shared services to get around domain reputation technologies with increased frequency. (Exhibit 8)

How Cyber Attacks Bypass Detection Technology

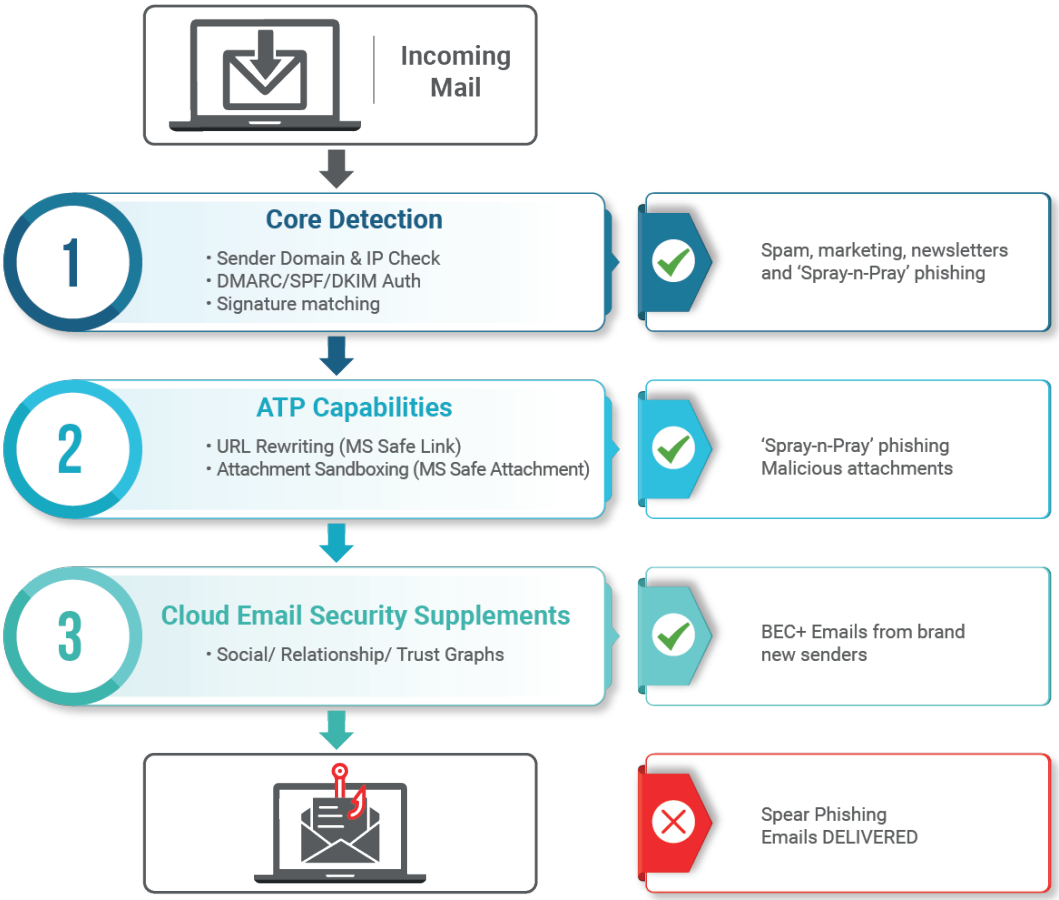


Exhibit 8: *How cyberthreats are bypassing SEG, proxy, SASE, and endpoint security tools*

Social Engineering Goes Mobile

With the rising popularity of iOS and Android devices for everything from sending a client an SMS to attending a Zoom call, it was only a matter of time before cybercriminals seized the opportunity to target users through the least protected and most popular communication medium. (Exhibit 9)

SlashNext Threat Labs sees a multitude of mobile-specific phishing attacks daily. 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 as effective.

Let's review the most popular types of mobile-specific phishing attacks, which include:

- Business Text Compromise
- SMS based Money Transfer & Gift Scams
- Rogueware, including Fake VPNs, used to conduct Man-in-the-Middle attacks
- Account Take-Over (ATO) or multi-stage phishing including, SMS, voice and links for fake fraud alerts or technical support scams (Exhibit 9)

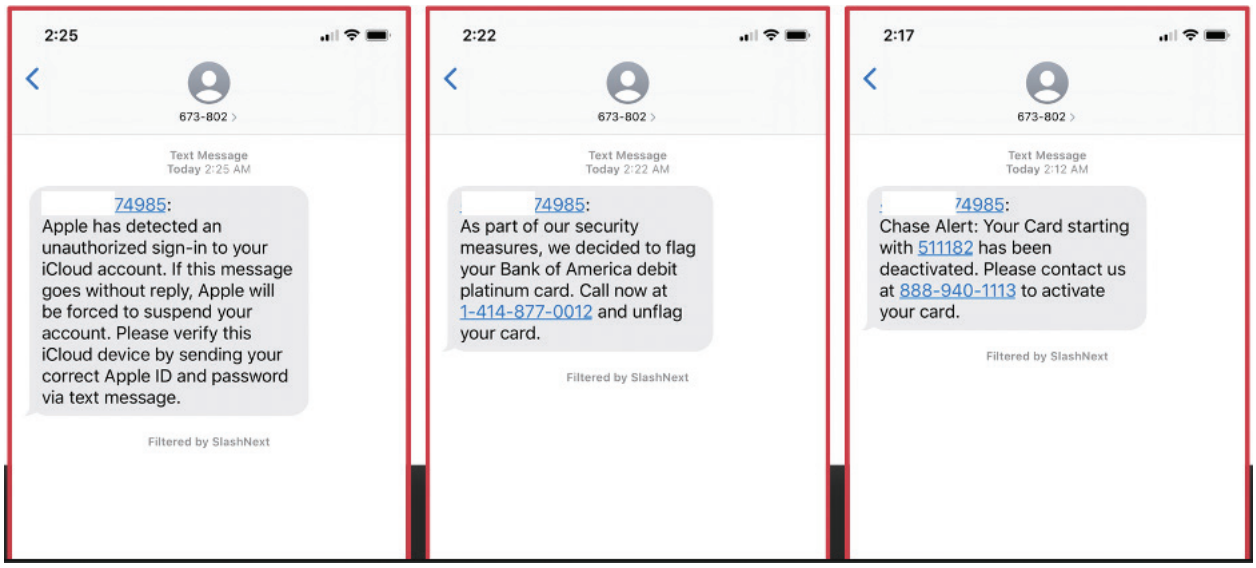


Exhibit 9: *Example of a ATO attempts on SMS mobile*

Spear Phishing and Other Targeted Attacks in Social Media and Collaboration Tools

Sophisticated well-craft spear-phishing campaigns have almost become an art form. Crafty cybercriminals are using automation and personal targeting to see who can be lured, convinced, and manipulated—and what better place than social media, where everyone, even your employees, are sharing their personal information, looking for a better photo filter, and clicking on news and ads.

Using fake blogs, fake email accounts, and fake profiles on social media platforms like LinkedIn, cybercriminals create elaborate fake profiles to trick high-value targets. They connect to the target's friends and colleagues, "like," and comment on content with the goal of building the illusion of being a real contact. They will send a connection request, which makes the cybercriminal seem trustworthy, and the target is more likely to participate in a spear-phishing attack.

In 2021, one billion Linkedin profiles were compromised and important personal information, including full names, gender, email addresses, phone numbers, and industry information became available for cybercriminals. They can use this information to automate targeted attacks. They can trick users into sharing more sensitive information, as

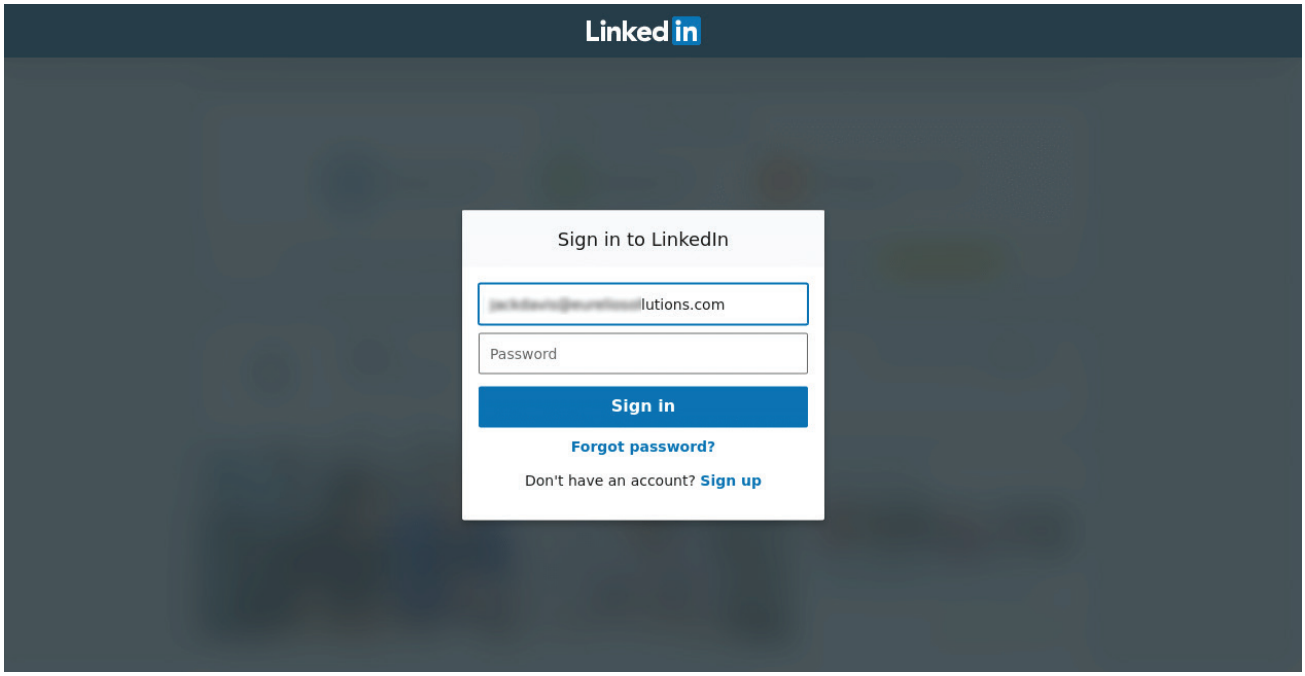


Exhibit 10: *Spear-phishing attacks with fake Linkedin log-in pages hosted on legitimate cloud infrastructure.*

seen in a recent spear-phishing attacks with fake Linkedin log-in pages. This spear-phishing attack is most dangerous because it's hosted on legitimate cloud infrasture, in this case Weebly, and will bypass most phishing detection tools. (Exhibit 10)

With access to millions of profiles, an expert cybercriminal can share malicious URLs between connected users or through Linkedin in-mails, luring the target to provide credentials that could later be used to for ransomware, exploit money or to be sold on the Dark Web for later use. (Exhibit 11)

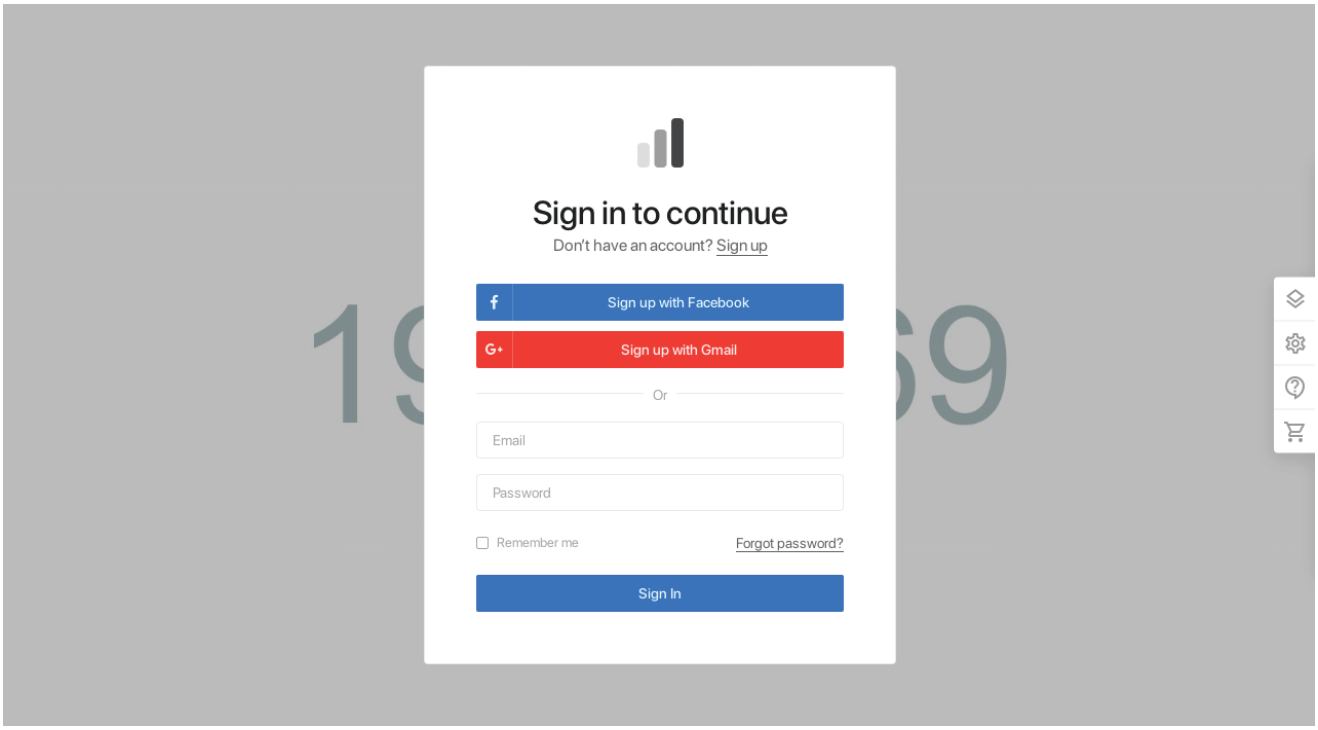


Exhibit 11: *Fake log-in page served through Linkedin*

CONCLUSION & RECOMMENDATIONS

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.

Most of the industry is using established security tools like SEG, proxy, SASE, and endpoint protection to minimize phishing threats. But they are often not accurate or fast enough to detect new and rapid attacks — But using AI is different. It centers on behavioral analysis of the content and can detect threats missed by human forensics, URL inspection and domain reputation analysis used by established security tools.

AI is the only really effective tool to counter well-crafted spear phishing attacks, because it emulates human cognitive reasoning to learn and respond accurately without the need for human intervention. Machine learning uses computer vision, natural language processing and other classifiers to see, examine and understand the context of a threat. AI examines billions of URLs and domains to determine if they are malicious.

SlashNext 360° Defense-as-a-Service offers continuous, zero-hour spear-phishing human hacking defense against targeted user attacks across all digital communication channels by exclusively focusing on AI phishing defense. Our patented SEER technology utilizes natural language processing, computer vision, and behavioral analysis to detect and block

Approach for Protecting your Organization

1 IDENTIFY
The risks you need to manage

2 PROTECT
Create safeguards to ensure delivery of critical services

3 DETECT
Define continuous ways to monitor potential cyber incidents

4 RESPOND
Activate an incident response program

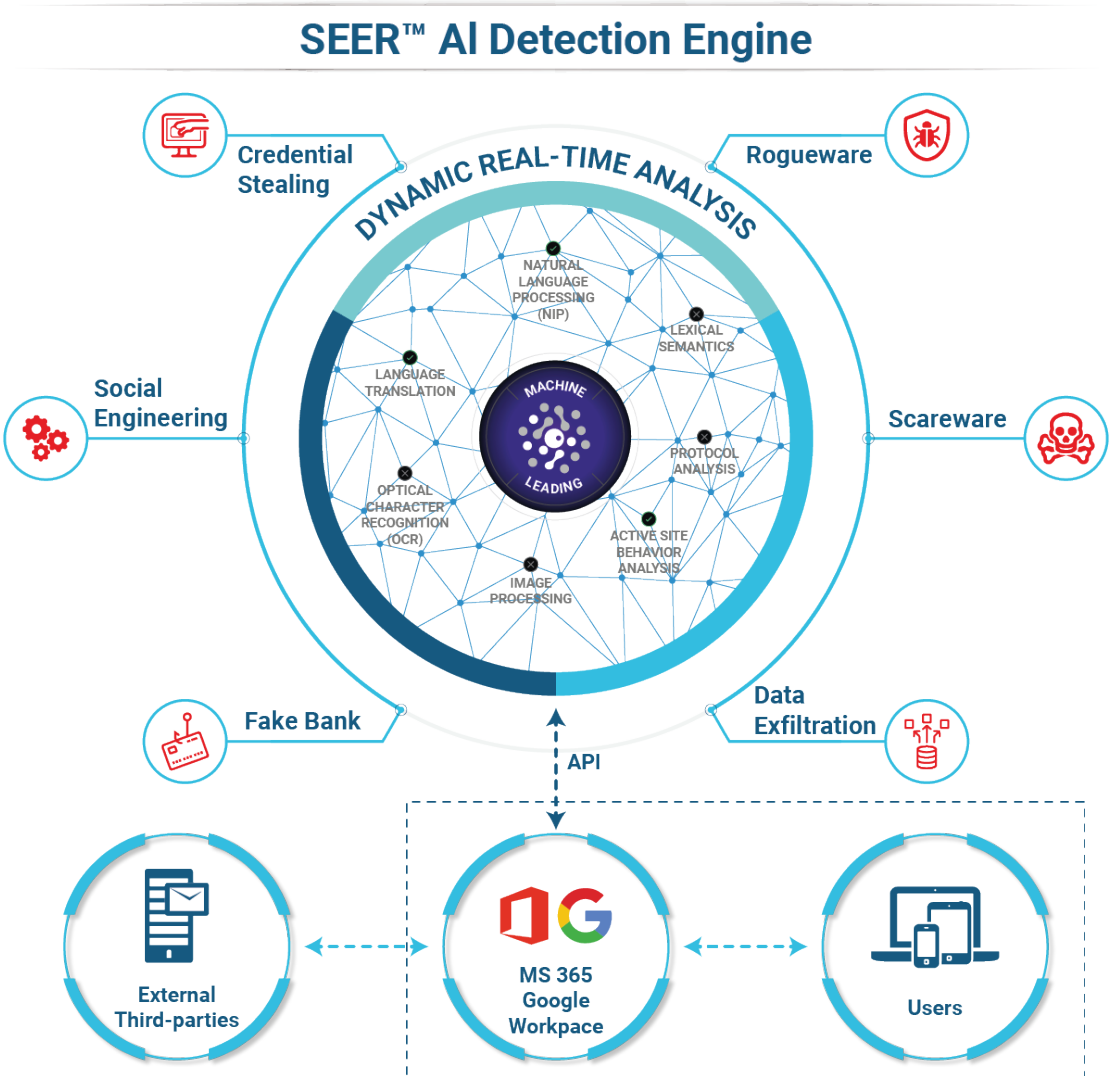
5 RECOVER
Build a cyber resilience program

threats hours and sometimes days before other vendors, resulting in a phishing intelligence network six times larger, with 99.9% accuracy and 1 in 1 million false positives.

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

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



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

Virtual Browser and Progessive Machine Learning

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.