
REPORT

 BOLSTER

2024

State of Phishing & Online Scams



Table of Contents

Introduction	4
A Look Back at 2023	6
2023 Key Findings	8
Phishing Attacks Soar from 2022 to 2023	8
Attackers are Most Active in August	9
Fall of Freenom Gives Rise to Others	10
America Always Wins the Popularity Contest	11
GoDaddy? More Like No, Daddy	12
TL;DR Explosion of TLDs Means More Typosquat Attacks	13
Top Tactics Used by Scammers	13
Emergence of GPT-Powered Attacks in the Age of AI	23
2024 Predictions :	25
Old and New Worlds Collide	
Recommendations:	28
How to Protect Your Business in 2024 and Beyond	

INTRODUCTION

When we look back on 2023, one thing is going to stand out in the technology world

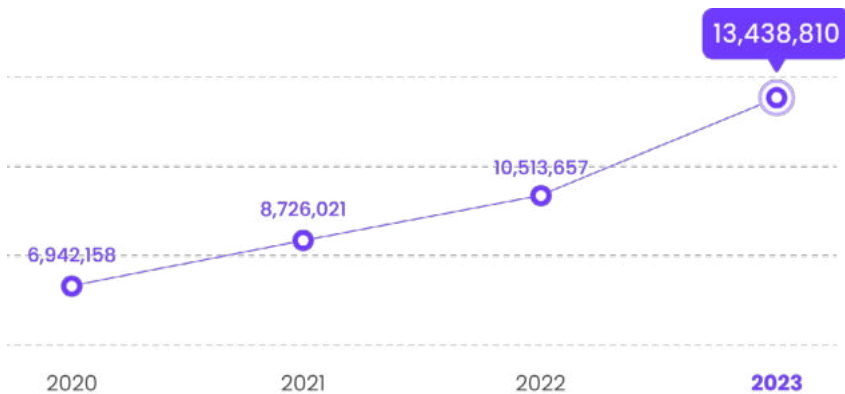


From prompt responses to self-driving cars, 2023 has witnessed a significant impact of Artificial Intelligence (AI) on the world, including the world of cyber threats. AI has revolutionized the capabilities of cybercriminals, enabling them to launch more sophisticated and targeted attacks. AI-powered tools have allowed cybercriminals to automate various aspects of their operations, including reconnaissance, attack execution, and evasion techniques. They can now leverage AI algorithms to analyze vast amounts of data, identify vulnerabilities, and exploit them with precision and speed.

Moreover, generative AI has enabled the development of advanced malware that can adapt and evolve in real-time, making it harder for traditional security defenses to detect and mitigate. Whether AI is solely responsible or not, our research team has identified new and evolving digital threats that have target

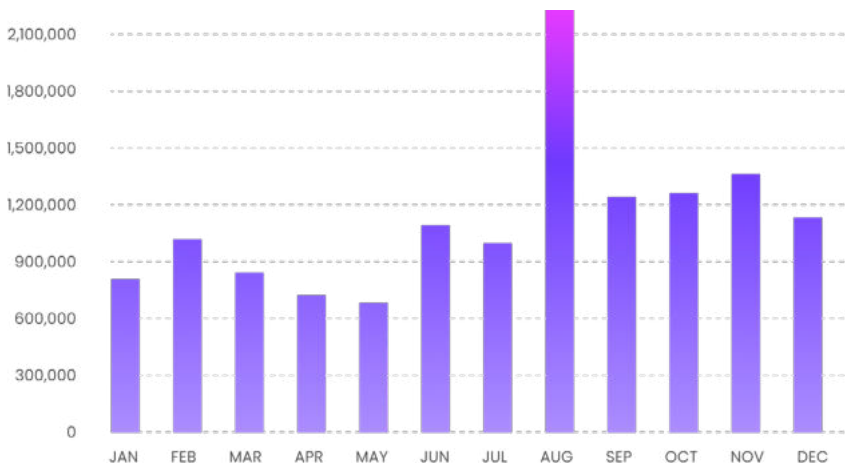
brands and consumers around the world in 2023. There may have been a heightened focus from security teams on optimizing their programs to defend against cyber attacks, but it was met with bigger and bigger attack waves from hackers.

Based on our world-class data, gathered daily from over 10 billion threat intel data points, the **2024 edition of our Phishing and Scam report highlights how our world was impacted by cyber threats**, including which industries were hit the hardest, what types of threats were the most common, and how we can prepare our businesses for the next year of cyber defense. With an over **94% increase** in phishing and scam pages since 2020, it's important to take note of cyber trends to better your defense. With over **2.2 million fraudulent sites** detected in just August alone, it's clear that threat actors are on the move going into 2024.



94% increase since 2020

Monthly Data 2023



2023 saw a 27.8% increase in activity since 2022

**A LOOK BACK AT
2023**

Emergence of AI-Powered Attacks

At Bolster, we've been tracking phishing scams and cyber fraud since 2019. We've seen the evolution of digital reliance brought on by the Covid-19 pandemic, and the resulting influx of cyber scams targeting consumers with the end goal of gaining access to their workplace network or financials.

This past year, cyber threats continued to evolve to make the most of AI technology adoption, making their impact more widespread and the attacks harder to take down. With phishing sites reaching record-breaking numbers in almost 20 countries

around the world, and some of the most well-known brands targeted more than ever before (we found over 1.3 million scams targeting Amazon alone), there's no doubt that generative AI lead to bigger threats.

This year's cyber attacks also highlighted the state of the market; whether it was the vulnerability of the workforce and widespread market strain resulting in layoffs, or shift to online shopping by consumers, wherever the targets went, fraud followed. Here are some of the 2023 key highlights:



1. **Financial Crisis gives ripe opportunity for largescale phishing attacks.** Phishing attacks directly target banks, startups, and impacted-consumers after the [collapse of banking giants](#) in March. Consumers and businesses already facing a high-pressure environment had to remain diligent against emotionally-driven cyber threats.



2. **Brand impersonations are now on a massive scale.** A major brand impersonation scam campaign [targeting over 6,000 well-known](#) brands with fake websites and sales. Our research team estimated that some of the scam sites had been active since 2020.



3. Holiday seasons is still peak months for new scams. During the busy 2023 holiday season, our research team identified a [USPS scam campaign targeting consumers with faking shipping notifications](#). Unlike 2022 where scammer were issuing fake gift cards en masse, 2023 showed a uptick in fake delivery service scams. By targeting a widespread service during the busiest time of year for online sales and shipping needs, hackers caught victims at a vulnerable time.



4. **Hackers prey on the waves layoffs in 2023.** Fake job postings targeted [our customers](#), and businesses globally, this year more than ever. With more people hitting the job search due to market impacts in 2023, hackers didn't hesitate to profit off individuals. With 2024 layoffs still riding high, we expect that this scam will continue well into the end of the year.



5. **GPTs are slowly becoming a hacker's favorite tool.** From conversational AI to malware creating GPTs, our research team uncovered a large amount of AI-empowered phishing and scam campaigns in 2023. We expect this to explode in 2024 as more hackers are getting more fluent in how to use AI in their nefarious activities

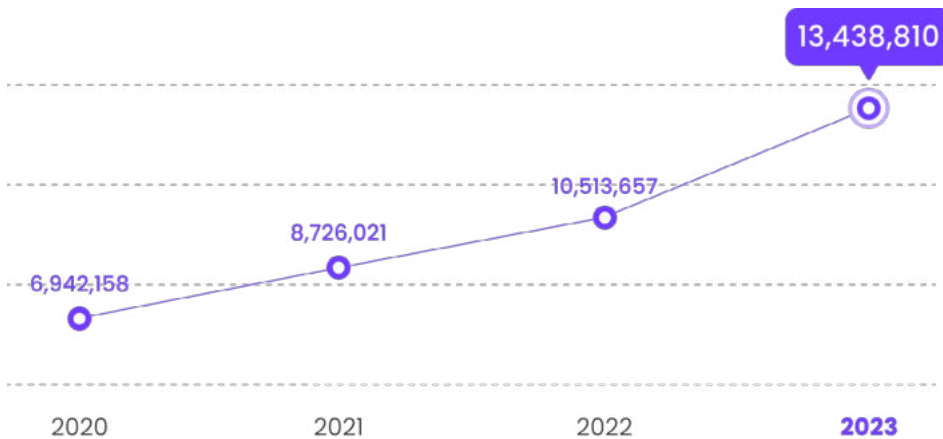
In this 2023 State of Phishing and Online Fraud report, we will walk you through the scam data we collected for the year, cover what it means for your business, and highlight how you can prevent attacks in 2024 and beyond.

2023 KEY DATA & FINDINGS

Phishing Attacks Soar From 2020 to 2023

Welcome to the summary of our latest survey on phishing and online fraud in 2023. The survey conducted over the past year revealed a significant increase in the total number of unique phishing pages, soaring from 10.5 million to 13.4 million - representing a **27.8% increase** in global phishing activities. These findings shed light on the alarming fact that phishing and online fraud continue to pose a persistent and growing threat to individuals and organizations worldwide.

Despite increased awareness and attempts to combat phishing, cybercriminals are continuously refining their tactics, resulting in an ever-expanding pool of malicious websites. This survey serves as a stark reminder that even in the face of extensive cybersecurity measures, phishing remains a pervasive problem that demands urgent attention and proactive countermeasures. Compare how the number of phishing and scam pages risen from the start of COVID (2020) to now (2023):



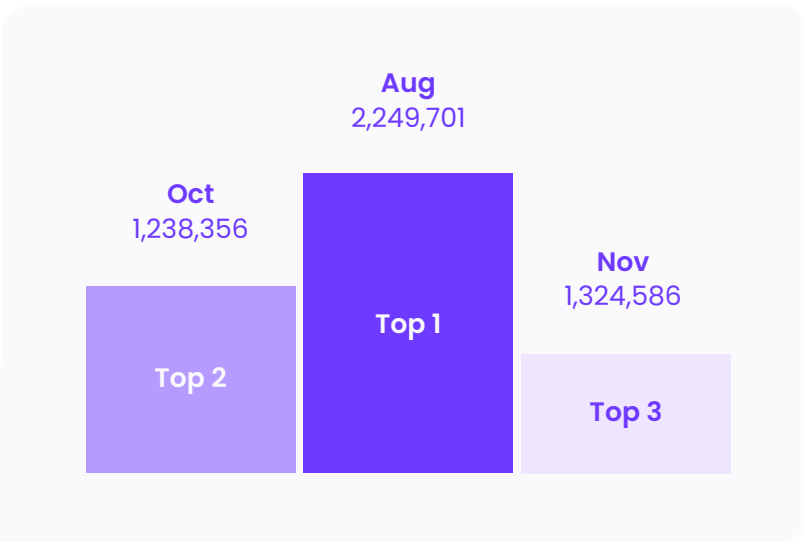
2023 saw a **27.8% increase** in activity since 2022

2023 Key Highlights

13M Phishing and Scam Pages Total

37K New Pages Created Per Day, on Average

TOP3 Months with Highest Daily Averages

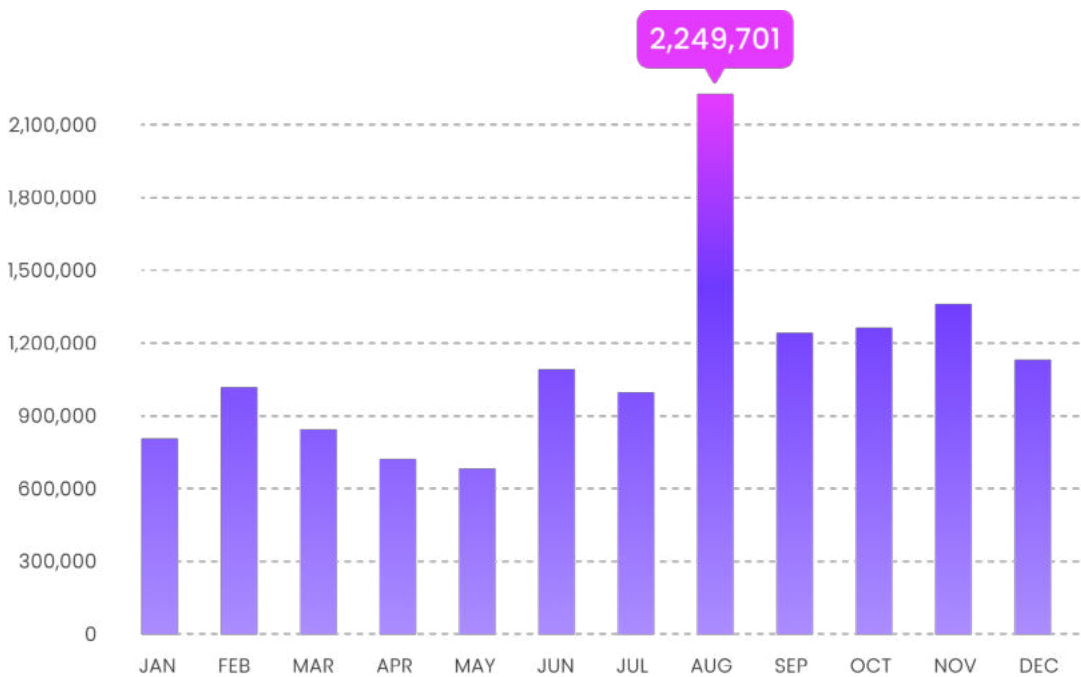


Attackers Are Most Active in August

The period from September to November has been identified as some of the busiest months for phishing attacks, coinciding with the onset of the holiday shopping season. Bolster research has found that the three months leading up to the holiday season account in December for 20% of all phishing and scam activity for the entire year of 2023. During these months, individuals and organizations are busy preparing for festivities and eagerly engaging in online shopping. Cybercriminals capitalize on this heightened online activity and employ various tactics such as phishing emails, fake websites, and social engineering techniques, targeting unsuspecting users for financial gain.

Interestingly enough, August of 2023 recorded a record high of 2.2M unique malicious websites when many Americans are off on summer vacation. Most notably, Bolster research uncovered a sharp increase in tax-related phishing campaigns in February 2023 such as fake tax refunds or have unpaid taxes that trick the unsuspecting user into clicking on a malicious phishing link.

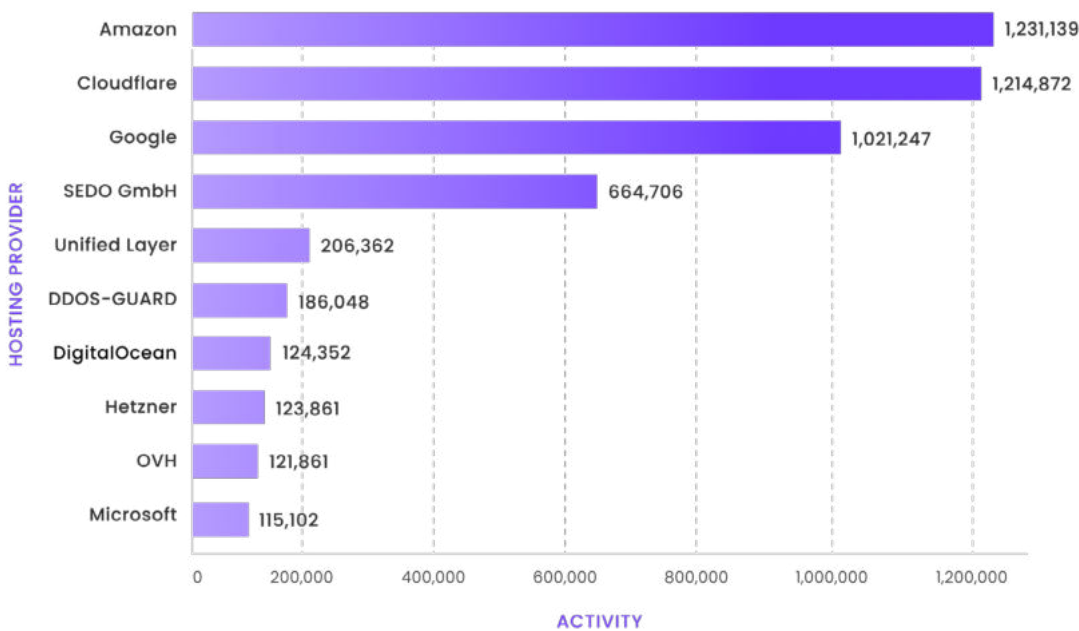
[Monthly Data 2023]



Fall of Freenom Gives Rise to Others

Phishing campaigns often exploit the infrastructure provided by top hosting providers, with notable names such as Cloudflare (1.2 million registrations), Amazon (1.2 million registrations), and Google (1 million registrations) being among the most commonly abused platforms. These providers, favored for their reliability and vast resources, inadvertently become conduits for cybercriminal activities. However, an interesting development occurred with Freenom, as since March 2023, when they ceased accepting new domain registrations, a significant decline in cybercrime related to this hosting provider was observed. Freenom’s decision appears to have dealt a blow to cybercriminals who heavily relied on their services.

Conversely, as Freenom faced legal action from Meta, there has been a noticeable rise in the usage of Unified Layer as a hosting provider by attackers seeking alternative infrastructures to carry out their fraudulent campaigns. This highlights the cat-and-mouse game between cybercriminals and hosting providers as they continuously adapt and shift tactics to exploit various platforms in their pursuit of illicit activities. Bolster analyzed data from over 9000 hosting providers across the world but listed the top 10 most abused hosting providers below:



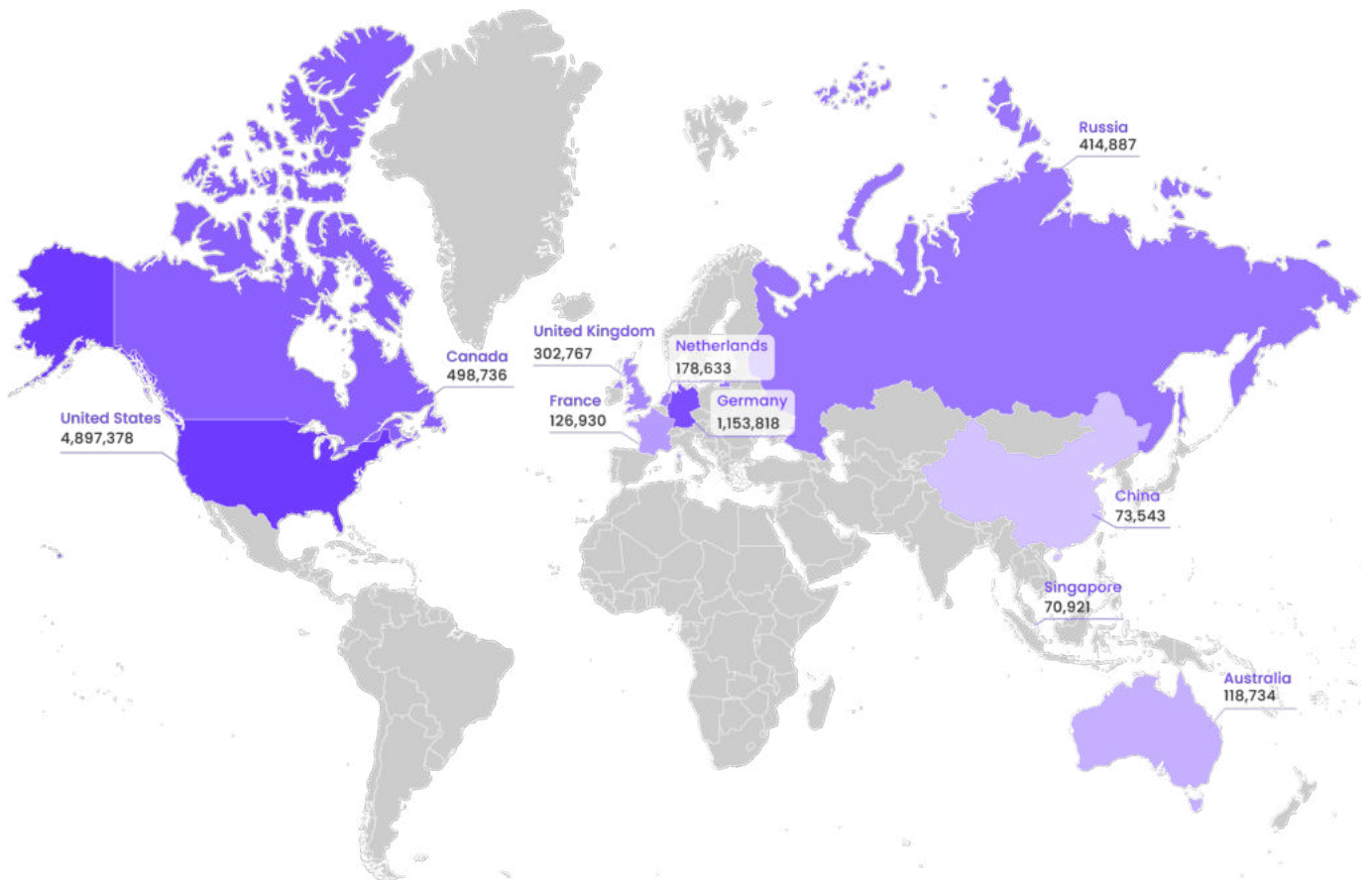
America Always Wins the Popularity Contest

Phishing domain registrations often originate from the very countries that attackers are targeting, demonstrating a concerning trend in global cybercrime distribution, with the only exception being Iceland. The top countries associated with hosting phishing domains include the United States (40.9 million registrations), Iceland (8.7 million registrations), China (5.7 million registrations), Canada (3.9 million registrations), and the United Kingdom (2.8 million registrations. The United States alone accounted for 47% of the world’s phishing and scam registrations.

It is worth noting that while many web security programs incorporate geo-location filters as part of their defense mechanisms, the choice of registering phishing domains in the same countries they intend to target can often bypass these security applications. Attackers take advantage of this loophole by strategically selecting hosting locations that align with their targets, effectively evading detection and mitigating the risk of being flagged by geo-location filters. This presents a significant challenge for cybersecurity professionals who must continually adapt their strategies and technologies to counter these tactics.

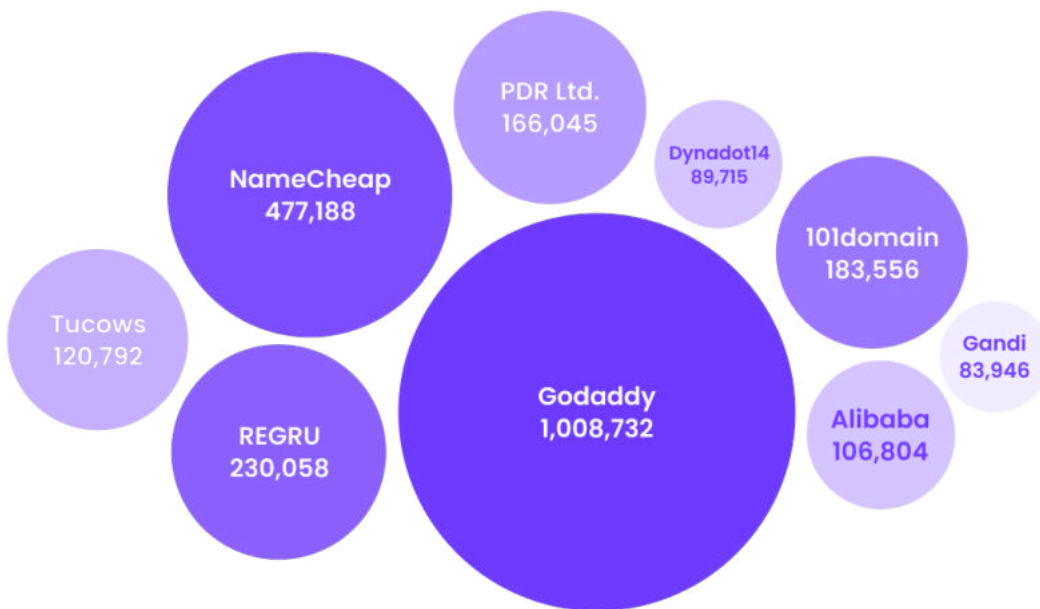
[Top 10 countries where phishing / scam is hosted the most]

Country	Activity	Country	Activity
Top 1 United States	4,897,378	Top 6 Netherlands	178,633
Top 2 Germany	1,153,818	Top 7 France	126,930
Top 3 Canada	498,736	Top 8 Australia	118,734
Top 4 Russia	414,887	Top 9 China	73,543
Top 5 United Kingdom	302,767	Top 10 Singapore	70,921



GoDaddy? More Like No, Daddy

Phishing attackers often rely on specific domain registrars to facilitate their illicit activities. Some of the top registrars frequently exploited by cybercriminals for phishing attacks include GoDaddy.com (1 million phishing attacks), Namecheap (447K phishing attacks), 101domain (183K phishing attacks), PDR Ltd. (166K phishing attacks), and NameSilo (151K phishing attacks). These registrars, while most are reputable and widely used, unfortunately attract malicious actors due to their ease of use, affordability, and large customer base. Attackers can exploit the anonymity and lenient registration policies offered by these platforms to create deceptive domains that closely mimic legitimate websites. Bolster saw phishing activity across 7000 registrars across the world with the top 10 registrars listed below:



TL;DR Explosion of TLDs Mean More Typosquat Attacks

In recent years, the internet has witnessed an explosion of top-level domains (TLDs), providing users with a wide array of options for website addresses. However, despite the proliferation of TLDs, a report on phishing trends in 2023 reveals that the .com TLD remains the most widely used for phishing campaigns at 4.1 million phishing and scam sites using a .com TLD. Bolster research finds that cybercriminals continue to leverage the familiarity and trust associated with the .com TLD to deceive unsuspecting victims. Despite the availability of numer-

ous alternative TLDs, such as .xyz and others, the enduring popularity of .com for malicious activities underscores the need for continuous vigilance and robust cybersecurity measures to combat phishing attacks.

The 18% rise in TLDs from 3307 TLDs in 2022 to 3914 TLDs in 2023 means more variations of typosquat variations that attackers can use to launch an attack. The below table shows the top 10 TLDs used in phishing attacks in 2023 versus 2022.

2022 Top 10 TLDs	Activity
Top 1 com	3,624,909
Top 2 net	946,897
Top 3 xyz	485,817
Top 4 com.br	289,311
Top 5 ru	229,660
Top 6 org	197,794
Top 7 de	161,569
Top 8 info	142,746
Top 9 co	115,003
Top 10 link	114,168

2023 Top 10 TLDs	Activity
Top 1 com	4,129,855
Top 2 net	739,111
Top 3 xyz	590,918
Top 4 ru	384,404
Top 5 com.br	291,498
Top 6 online	275,264
Top 7 top	272,589
Top 8 info	259,632
Top 9 site	240,314
Top 10 org	218,146

Top Tactics Used by Scammers

Phishing and scam activities encompass a diverse range of tactics employed by attackers to deceive unsuspecting victims. The top five categories of these attacks showcase the versatility of their techniques. Fake online stores or products are a prevalent form of phishing, where criminals create fraudulent websites or listings to trick users into purchasing non-existent or counterfeit goods. Credential theft is another common tactic, aiming to acquire sensitive user information, such as usernames and passwords, through deceptive methods like fake login pages or email scams. Fake app stores pose as legitimate platforms to distribute malicious apps that can compromise

user devices or data. Gambling sites often lure individuals into fraudulent schemes promising lucrative winnings or enticing rewards with no intention of delivering on their promises. Business Email Compromise (BEC) attacks specifically target companies, impersonating executives or partners to manipulate employees into transferring funds or sensitive information. These categories demonstrate the diverse tactics attackers leverage to exploit their victims, highlighting the importance of user awareness, cybersecurity education, and robust defense mechanisms to combat phishing and scam activities. t

Layoffs Give Rise to Fake Job Scams

Post-COVID-19 digitalization and a growth in remote work seekers, threat actors are often seen in cyberspace preying on individual job ambitions and the weaknesses in the job market. Cybercriminals construct sophisticated employment offers that often imitate well-known organizations to trick prospective

employees into providing personal information or completing financial transactions without the pretense of paying for training or application fees. The rise of fake job scams are quite intricate and often come in variations:



Case 1: Fake Emails

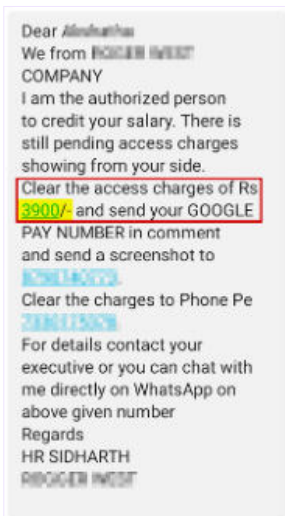
Specially crafted emails impersonating legitimate businesses are sent out to target people looking for an opportunity, often leading to financial loss or identity theft.

Threat actors usually buy a domain that looks like career <brand-name> / <typosquatted domain> etc to create a mail server.



Case 2: Fake Domain

Fake websites with testimonials claiming to earn \$6,000 per month online. Similar campaigns are extremely popular on social media platforms where multiple people reach out to others for online job requiring 1 or 2 hours every day to earn \$100 per day.



Case 3: Fake Jobs on Legitimate Platforms










Often on legitimate platforms like internshala or quikr jobs or social media platforms, fake openings/jobs are posted with handsome incentives to lure victims into either getting involved in financial loss or doing tedious work or working for free for some days in pretense of interview or sample work post which legal and identity documents are asked for legal purpose and offer letter. Once the task is completed, cybercriminals try to imitate legal authorities and asking for some sort of payment in order to get your name clear.

Top Targeted Verticals

Phishing attacks have become a prevalent threat across all industries, but technology companies, finance companies, and entertainment companies have emerged as the top targeted verticals. The technology sector is heavily targeted due to the valuable data it holds, including intellectual property, customer information, and financial data. Additionally, technology companies often develop cutting-edge products or services, making them attractive targets for cybercriminals seeking to gain a competitive advantage or trade secrets.

Finance companies are targeted for obvious reasons, as they hold vast amounts of sensitive financial information and are lucrative targets for theft or fraud. Moreover, the financial sector’s reliance on digital transactions and online services makes it more vulnerable to phishing attacks. Entertainment companies face being targeted due to the large consumer bases they possess and the personal data they gather. Cybercriminals exploit users’ trust in popular entertainment brands, aiming to deceive them into sharing personal information, financial details, or login credentials. As these sectors continue to thrive, it is crucial for organizations in these verticals to prioritize robust cybersecurity measures, employee awareness, and proactive threat detection to thwart phishing attacks and safeguard their valuable assets and user data.










Bolster analyzed over 25 verticals to show the top 10 most targeted verticals below:










Vertical	Number of Attacks
 Technology	4,194,764
 Financial Services	1,307,901
 Entertainment	1,260,478
 Travel	1,088,818
 Social Media	590,373
 E-Commerce	304,103
 Telecommunications	107,911
 Transportation	86,142
 Retail	56,521

Sensitive Still Reigns Supreme

Bolster has identified 19 categories of scams that pose the biggest threats to organizations and consumers. The top five scams identified by Bolster are login pages (2.9 million attacks), gaming scams (281K attacks), gift card scams (245K attacks), tech support scams (196K attacks), and fake online stores (175K attacks). Login page scams, used to steal sensitive information, involve luring users into giving away their login credentials through fake login pages. Gaming scams entice users with dubious offers, such as game hacks and cheats, to trick them into downloading malware or purchasing fake game credits.

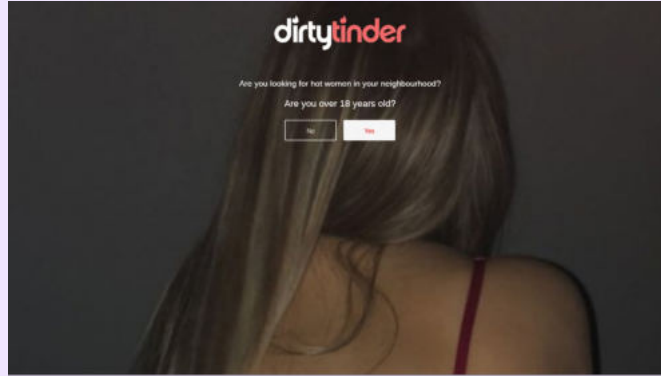
Gift card scams exploit users’ trust in legitimate retailers, offering fake gift cards or undeliverable gift card codes. Tech support scams use social engineering tactics, such as unsolicited phone calls, pop-ups, or messages, to trick users into giving away login credentials or installing malware. Finally, fake online stores mimic popular e-commerce sites, offering fake products or compelling deals that lead to financial fraud or identity theft. By understanding the various scams, individuals, and organizations can take proactive measures to protect themselves, such as staying vigilant, enhancing cybersecurity practices, and investing in digital risk protection solutions.

Intent	Number of Attacks
 Sensitive Data	2,936,542
 Gaming	281,364
 Gift Card	245,862
 Online Store	196,836
 Cryptocurrency	175,039
 Tech Support	133,639
 Banking	120,362
 App Store	96,781
 Promo Code	68,260

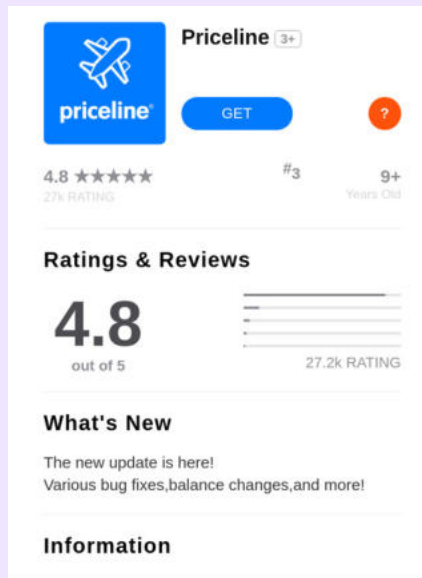
Intent	Number of Attacks
 Streaming	44,286
 Social Media	34,574
 Hacked Site	33,071
 Gambling	30,722
 Adult	16,138
 Drug	12,083
 Crypto Giveaway	10,941
 Contact	6,438
 Marketplace	4,528

Examples of the Scams Found and Analyzed by Bolster Are Shown Below:

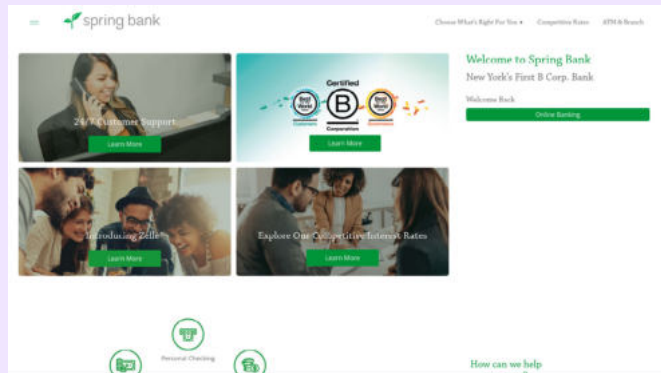
Adult :



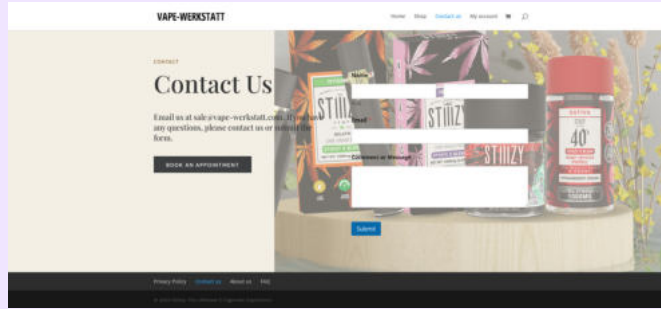
App Store :



Banking :



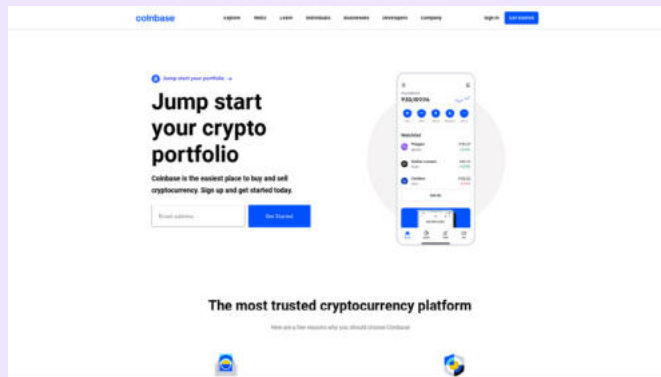
Contact :



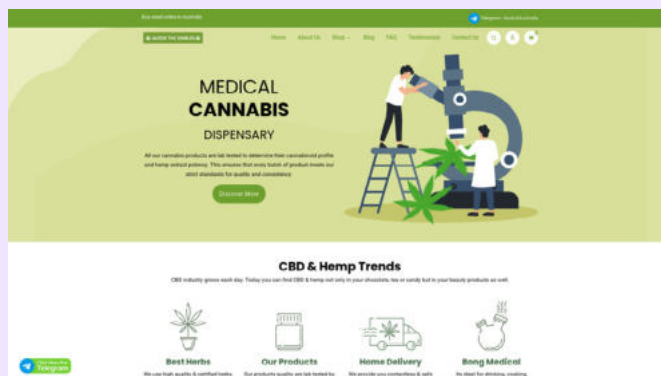
Crypto Giveaway :



Crypto Currency :



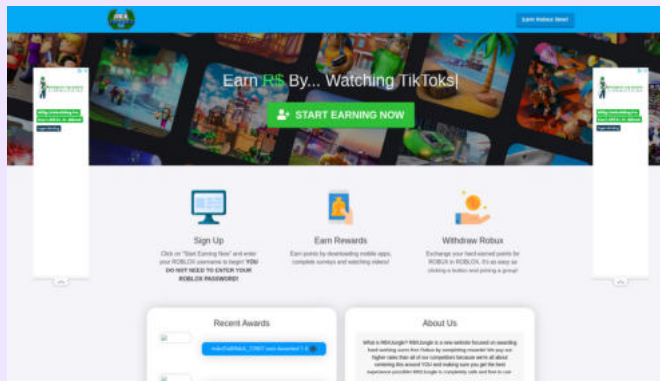
Drug :



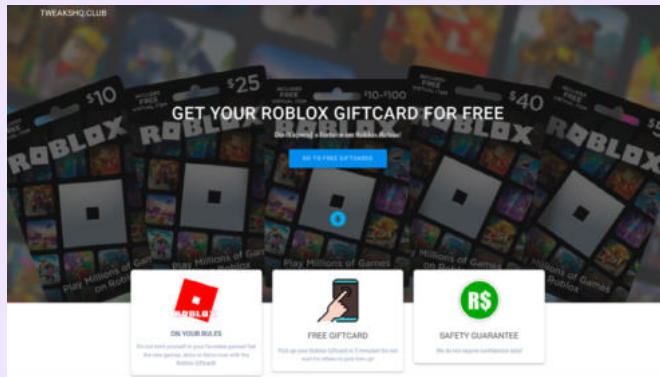
Gambling :



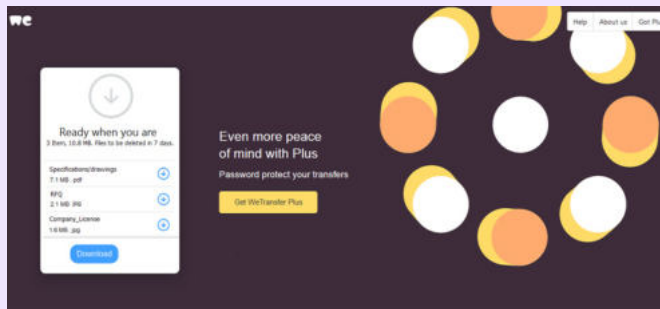
Gaming :



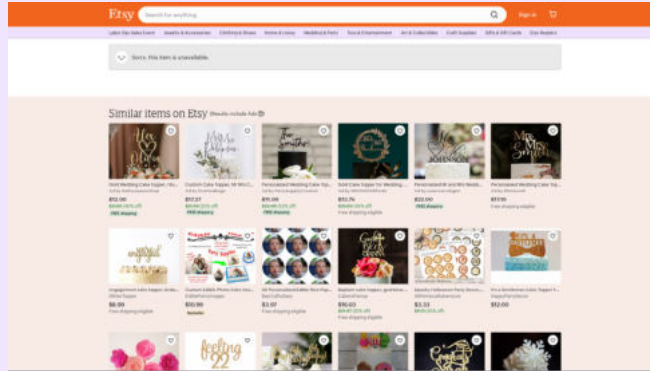
Gift Card :



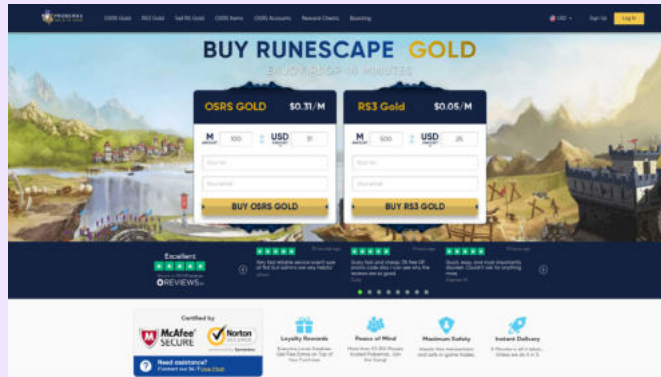
Hacked Site :



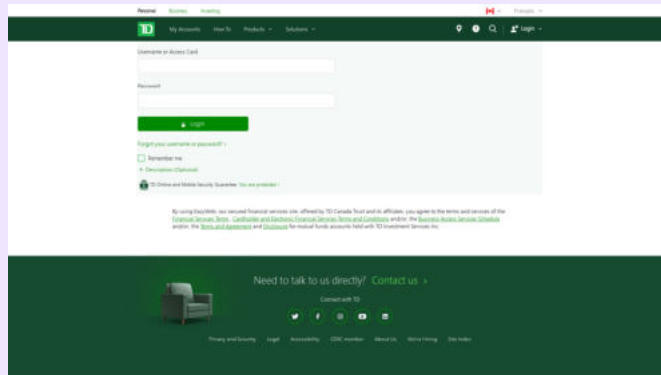
Marketplace :



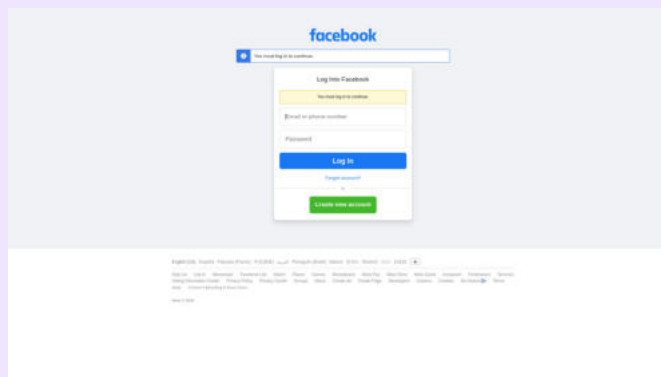
Promo Code :



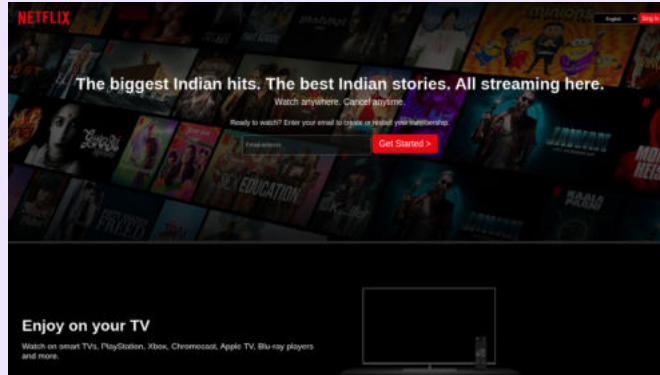
Sensitive Data :



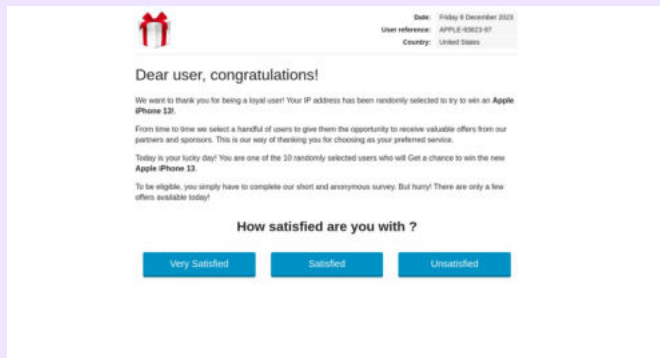
Social Media :



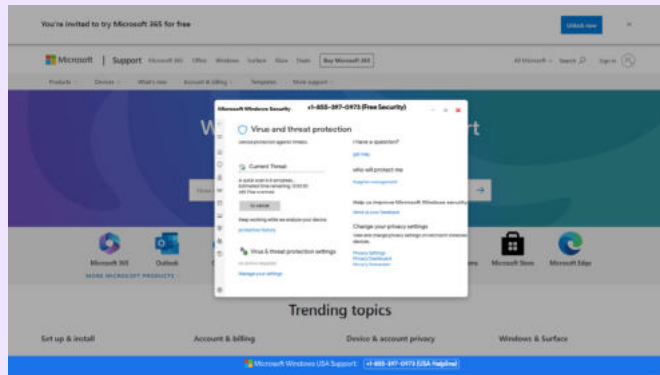
Streaming :



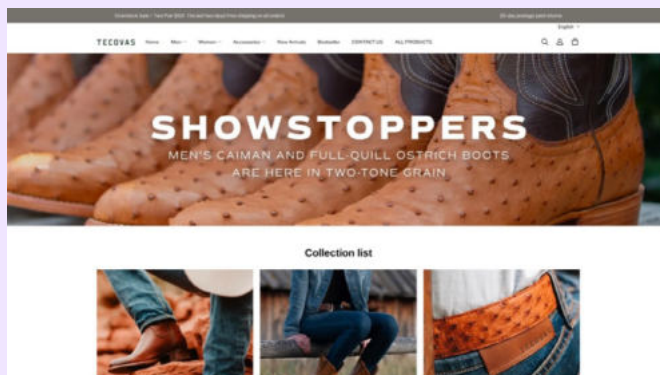
Survey :



Tech Support :



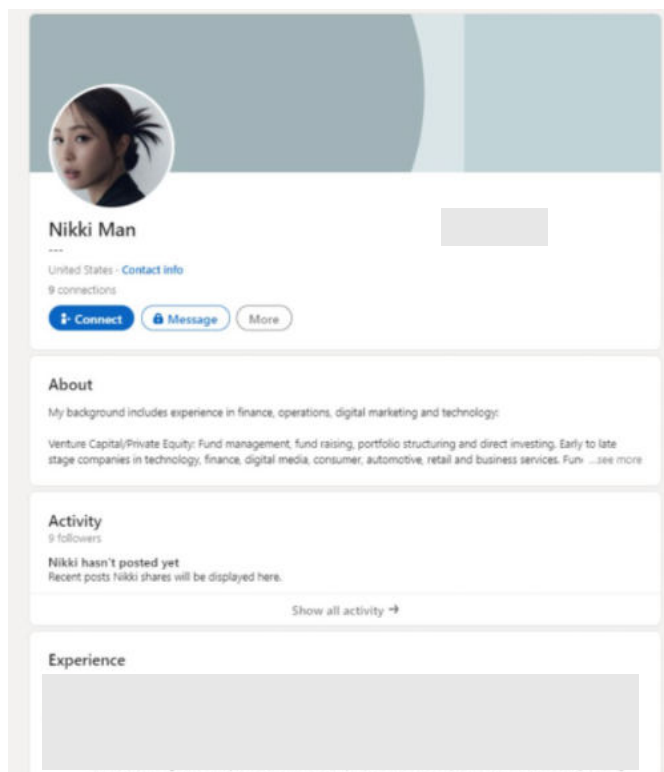
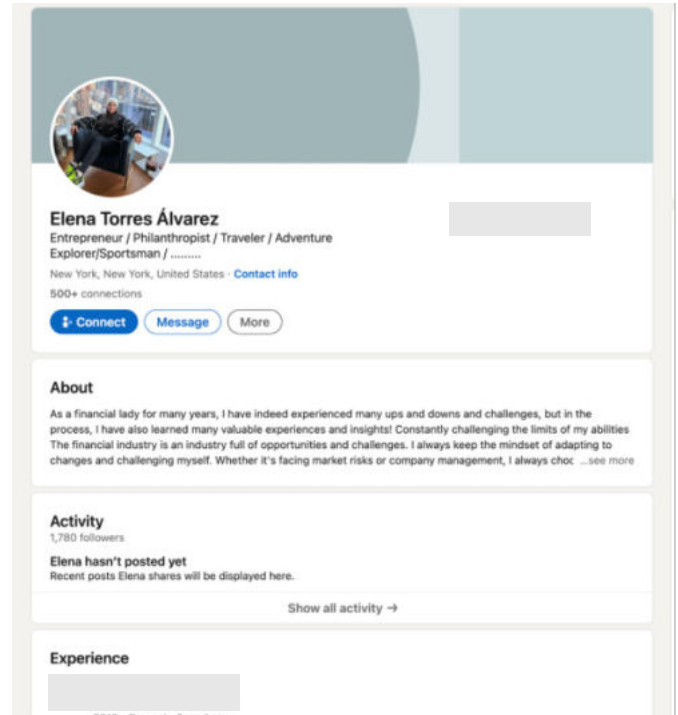
Online Store :



Impersonations are Reaching an All-Time High

Impersonation attacks have been on the rise in recent years, with cybercriminals exploiting the trust and authority of individuals to deceitfully gain access to sensitive information or funds. Executive impersonations, in particular, have skyrocketed in the past year, with criminals posing as executives and managers to trick employees into revealing confidential information, authorizing fraudulent transactions, or participating in false wire transfers. According to Bolster data, impersonation attacks have jumped **28x more** on LinkedIn in 2023 than in 2022 (For issues of privacy for our customers, we have kept the total count redacted from this report). Attackers often engage in social engineering tactics, such as creating fake email accounts, domains, or websites to closely resemble those of the targeted organizations.

Another emerging type of impersonation attack has been VC impersonations, where cybercriminals pose as venture capitalists to trick startup employees or executives into sharing confidential information or investing in fraudulent accounts. Because of the economic climate of rising interest rates, failing banks, and lack of funding for tech startups, the level of VC impersonations has been surging. Here are a few examples of VC impersonations in past year claiming to be high-level positions at famous VC firms:



The popularity and widespread use of social media platforms have provided scammers with ample opportunities to exploit unsuspecting users. Impersonation scams involve creating fake profiles or accounts that appear to belong to trusted individuals, brands, or organizations. These scammers often use various tactics to gain the trust of their targets, such as mimicking the appearance, content, and interactions of the genuine accounts. The implications of impersonation scams can be severe, as they can lead to financial fraud, identity theft, or the spread of misleading information. Additionally, social media platforms offer a vast pool of personal information about users, making it easier for scammers to create believable impersonations.

Emergence of GPT-Powered Attacks in the Age of AI

Artificial Intelligence (AI) has emerged as a double-edged sword, being wielded both by defenders and attackers in the realm of phishing and scam campaigns. Attackers are increasingly leveraging AI technology to enhance the effectiveness and sophistication of their attacks. AI algorithms can be utilized to automate various aspects of phishing campaigns, such as crafting convincing phishing emails or messages by analyzing and mimicking the language and writing style of legitimate senders. AI-powered chatbots can engage with victims in real-time, providing more realistic and personalized interactions to deceive users into sharing sensitive information.

Furthermore, AI can enable attackers to analyze vast amounts of data to identify potential targets, create highly targeted and personalized messages, and circumvent traditional security measures. As AI continues to advance, attackers will likely exploit its capabilities to create even more convincing and tailored phishing and scam campaigns.

In 2023, malicious actors have begun exploiting the capabilities of Generative Pre-trained Transformers (GPTs) to create and utilize malicious tools. The top 4 GPTs used for phishing attacks, as observed by Bolster's research, has been the following:

1. Fraud GPT, a subscription-based platform that generates malicious content for fraudulent purposes. This tool assists cybercriminals in generating convincing phishing emails, scam messages, and other deceptive content that can deceive unsuspecting victims into divulging personal and financial information.

2. Hacker GPT, a tool that operates similar to ChatGPT, serving as an AI assistant tailored specifically for hackers. This tool equips cybercriminals with a powerful resource to automate and streamline their malicious activities, providing them with real-time guidance and sophisticated attack strategies.

3. Worm GPT, which in 2023 seen a emergence that is worrisome. It is a rogue version of ChatGPT that lacks crucial guardrails and ethical guidelines. This unfiltered GPT variant can amplify the malicious intent of attackers, enabling them to create more dangerous and harmful content, such as hate speech, propaganda, or targeted manipulation campaigns.

4. Deep Voice Fakers, a tool used by malicious actors to deceive individuals over the phone. By leveraging GPTs, these voice fakers can mimic the voices of specific individuals, celebrities, or even trusted figures like company executives or family members. This tool enables scammers to carry out voice phishing attacks and impersonate others with remarkable accuracy, further complicating efforts to verify authenticity and increasing the risk of social engineering scams.

The emergence of these malicious tools highlights the need for robust security measures and proactive defenses. It becomes imperative for individuals, organizations, and technology providers to stay vigilant, continually upgrade their detection sys-

tems, and be aware of evolving threats. By investing in cybersecurity strategies and fostering a culture of awareness, we can mitigate the potential harm caused by these malicious uses of GPT technology in 2023.

WHAT TO EXPECT IN 2024

: Old and New Collide

Given the 2023 recap, you might be wondering how many of the trends will continue in 2024, and what new threats we are predicting. It might not be possible to completely predict the activity of hackers, we can make informed guesses based on the trends of recent years to help construct the best cyber risk defense.

While this past year saw a lot of new technology and threat trends, there were also a lot of familiar threats that we have grown accustomed to. Phishing sites pretending to be your business to confuse your customers for financial or informational gain are nothing new for cyber risk professionals to deal with, and their continued increase in frequency means we know they will continue to be a problem in 2024.

Here are our top phishing and fraud predictions for 2024:



1. An increase in multichannel attacks: Hackers are getting smarter and are continuing to test new and evolving avenues of attack. Multi-channel phishing attacks are predicted to increase in the coming years as consumers and businesses continue to improve their methods of defense. Individuals and organizations have become more aware of traditional phishing attacks and have implemented stronger security measures to protect against them. As a result, cybercriminals are shifting their strategies to include other communication channels to increase the chances of success. By utilizing multiple channels such as SMS, social media, messaging apps, and voice calls, attackers can further exploit human vulnerabilities and increase the reach of their phishing campaigns.

Furthermore, multi-channel phishing attacks allow cybercriminals to create a sense of legitimacy and urgency by presenting consistent messaging across different channels. By impersonating trusted organizations or individuals across multiple communication platforms, attackers can create a seamless and convincing narrative to deceive unsuspecting victims. This synchronized approach can make it difficult for victims to differentiate between genuine and fake communications, increasing the success rate of such attacks. Bad actors continue to be money-driven, and will evolve their attacks to hit on multiple fronts in 2024.



2. Explosion of TLDs means more challenges with detecting typosquats attacks. The explosion of top-level domains (TLDs) in recent years has inadvertently contributed to an increase in phishing attacks. With the introduction of numerous new TLDs beyond the traditional .com, .net, and .org, cybercriminals have gained greater flexibility in creating deceptive websites and email addresses that closely mimic legitimate domains. This allows them to carry out more convincing phishing campaigns, tricking unsuspecting users into disclosing sensitive information or performing fraudulent actions.

The abundance of TLD options provides scammers with a wider selection of domain names that can appear legitimate at first glance, making it more challenging for users to discern phishing attempts. As a result, organizations and individuals must exercise extra caution when dealing with unfamiliar or suspicious domains, double-checking the legitimacy of websites and email addresses before engaging in any online activities. Furthermore, deploying robust cybersecurity measures, such as email filtering and anti-phishing solutions, becomes crucial in mitigating the increased risk posed by the expanded TLD landscape.



3. Layoffs will continue the wave of fake job scams. The year 2024 witnessed widespread layoffs across various industries, leading to a surge in unemployment rates and a significant influx of job seekers. Unfortunately, this challenging environment has also given rise to the continued use of fake job scams, targeting vulnerable individuals in search of employment. Cybercriminals exploit the desperation and eagerness of job seekers by posing as legitimate employers or recruitment agencies, offering enticing job opportunities that turn out to be fraudulent.

These scams often involve tricking applicants into providing personal information, paying upfront fees for fake background checks or training, or even participating in illegal activities unknowingly. In such times of economic uncertainty, it is essential for job seekers to remain vigilant and adopt best practices, including thoroughly researching potential employers, avoiding suspicious job offers that seem too good to be true, and never sharing sensitive information or making financial transactions without proper verification. Additionally, organizations and authorities should actively work to raise awareness about these scams and implement measures to prevent the proliferation of fake job postings and protect vulnerable individuals from falling victim to such fraudulent schemes.



4. Impersonations will continue to rise. In 2023, attackers are increasingly utilizing social media platforms as a launchpad for their malicious activities, posing a greater threat than ever before. One prevalent tactic that has gained momentum is impersonation attacks, where cybercriminals create fake profiles or pages that mimic legitimate individuals, organizations, or brands to deceive unsuspecting users. These impersonation attacks are designed to trick victims into disclosing sensitive information, clicking on malicious links, or engaging in fraudulent transactions, exploiting the trust and connectivity that social media fosters.

It is crucial for individuals, businesses, and organizations to be vigilant and proactive in protecting themselves against such impersonation attacks on social media in 2024 and beyond. Implementing robust privacy settings, verifying the authenticity of accounts or profiles before engaging with them, and educating users on recognizing the signs of impersonation can help mitigate the risks posed by attackers leveraging social media platforms. By staying informed and exercising caution, users can safeguard their online presence and prevent falling victim to the increasingly sophisticated threats propagated through social media channels.



5. AI-powered cyber attacks: With the increasing adoption of artificial intelligence (AI) by cybersecurity professionals, it is anticipated that cybercriminals will also harness the power of AI to carry out more sophisticated and targeted attacks. AI-powered malware and botnets may become more prevalent, utilizing machine learning algorithms to evade detection and autonomously adapt to security defenses. These AI-driven attacks could exploit vulnerabilities, conduct reconnaissance, and employ advanced evasion techniques, making them highly challenging to detect and mitigate.

As much as we know now about the use of AI for both cyber protection and for threat actors, 2024 is shaping to be the year of the new and unknown in terms of hackers' use of AI. The opportunities continue to develop, meaning we won't be able to predict exactly how AI can be used in cyber attacks.

RECOMMENDATIONS

: How to Protect Your Business in 2024 and Beyond

We've outlined the threat trends from 2023 and summarized our biggest predictions for 2024 cyber attacks. The final step in our 2024 State of Phishing and Online Fraud report might be the most important: how can you protect your business from 2024 cyber threats?

Below are our 5 recommendations your business can take to protect from phishing attacks and online scams. While it's critical to protect your business from the predicted threats for 2024, it's also important to note the importance of over cyber-risk preparedness and proactive defense. Utilize cyber defense strategies and tools that can protect your business from both immediate and ongoing threats.

✓ 1. Utilize Automated Defense Tools

Automated cyber defense technology can help organizations continuously monitor their security posture, detect and respond to threats in real-time, and reduce the workload on overburdened security teams. Automated defense solutions, like [Bolster AI](#), leverage machine learning algorithms and artificial intelligence to continuously analyze vast amounts of data, detect patterns and anomalies, and respond to known and unknown threats with great speed and accuracy.

Automated cyber defense technology reduces the risk of human error and improves the overall efficiency and effectiveness of cybersecurity operations. By automating routine security tasks such as vulnerability scanning, phishing and typosquat and takedown practices, cybersecurity professionals can free up their time and focus on strategic initiatives that require human expertise and decision-making.

✓ 3. Create an Omnichannel Protection Program

To combat the increasing threat of multi-channel phishing attacks, individuals and organizations must adopt a holistic cybersecurity approach. This includes implementing robust security measures across all digital platforms and educating consumers and employees to be cautious and vigilant while interacting with different communication channels. Advanced technologies, such as machine learning and AI-powered security platforms, can help detect and mitigate multi-channel phishing attacks by analyzing patterns and anomalies across different channels.

✓ 5. Reduce the Time Hackers Go Undetected

In 2023, we detected cyber vulnerabilities that could be traced back to 2020, which means those hackers sat unnoticed for years, furthering their damaging activities to a truly undetermined extent. Moving into 2024, it's crucial to catch cyber threats as early as possible to prevent the prolonged damage of undetected threats. With the right automated detection technology that scans the internet, social media platforms, app stores, and the dark web without manual effort needed, you can trust you will catch cyber threats as soon as they go live, and limit the damage they can enact.

✓ 2. Lean on Community Defense Tools and Resources

Community tools play a crucial role in defending against cyber attackers by enabling collaborative efforts and information sharing among cybersecurity professionals and the broader community. Tools, like [Checkphish by Bolster](#), provide a platform for individuals and organizations to share threat intelligence and mitigation strategies, allowing them to stay updated on emerging threats and countermeasures. These tools help create a collective defense mechanism where the knowledge and experience of the community can be leveraged to identify and respond to cyber threats more effectively.

✓ 4. Use AI to Your Advantage

Traditional security measures often rely on static rule-based approaches, which may struggle to keep up with the rapidly changing tactics employed by cybercriminals. AI security solutions leverage machine learning algorithms to analyze vast amounts of data, detect anomalies, and identify patterns that indicate potential threats. By analyzing large datasets, AI can recognize subtle patterns and can automate routine security tasks such as monitoring domains, identifying vulnerabilities, and responding to incidents.

As cyber threats continue to evolve and become more sophisticated, AI security solutions offer a proactive defense mechanism, empowering organizations to detect and prevent attacks before they cause damage. By leveraging AI technology, organizations can strengthen their cybersecurity posture, mitigate risks, and stay one step ahead of cybercriminals in an increasingly complex threat landscape.

AI Security Platform Demo

Analyze phishing and scam threats to your business with securely trained LLM technology

[REQUEST A DEMO >](#)

Domain Risk Report & Acquisition Analysis

Determine current risk to your business and how to remove them

[DOWNLOAD >](#)



BOLSTER

www.bolster.ai

2880 Lakeside Dr ste#150,
Santa Clara, CA 95054