SPOOF 2023:

TRENDS IN ONLINE BRAND IMPERSONATION FOR CREDIT UNIONS

ALLURE SECURITY

TABLE OF CONTENTS

PREFACE

Welcome to Allure Security's second annual report on the pressing issue of online brand impersonations targeting credit unions and their valued members. This report holds a special place in our hearts, not just because of the effort we invested in its creation, but because it's truly one of a kind.

No other report in the market provides annual updates focused on online brand impersonations and spoofs targeting credit unions. The report's full name, "Summary of Patterns & Observations in Online Fakes 2023: Trends in Online Brand Impersonation for Credit Unions," is lengthy, but we've affectionately shortened the first half to "SPOOF 2023" for convenience (isn't that cute?).

The title does a good job capturing the report's singularity and purpose. It aims to raise awareness among credit unions regarding the drastic rise in online brand impersonations, nearly tripling the volume seen in 2022. Our report offers crucial insights into the latest threats while debunking outdated approaches that prove ineffective in combating this growing challenge.

We look forward to you diving deeper into the report. We think it's a valuable educational resource that will support you in implementing or enhancing proactive measures to truly protect your brand and members online.

JOSH SHAUL
CEO — ALLURE SECURITY

EXECUTIVE SUMMARY

This executive summary concisely summarizes Allure Security's unique report on the troubling rise in online brand impersonations targeting credit unions of all sizes.

This report analyzes online brand impersonation detection data from **August 2022** through **March 2023.**

- It highlights the pervasiveness of the threat and the vulnerability of credit unions of all sizes
- Our analysis reveals a significant surge in attacks during the first quarter of 2023 with triple the volume compared to the same period in 2022
- The UnFAIRSHAKE threat, discussed in the "Emerging Threats" section, played a role in this increase

The report also explores the relationship between a credit union's asset size and the frequency of online brand impersonations.

- Attacks targeted credit unions with assets ranging from $7 million to $150 billion
- Notably, 92 percent of credit unions targeted managed less than $10 billion in assets
- In terms of attack volume, 47 percent of brand impersonation attacks were on credit unions with $10-20 billion in assets and 41.3 percent of attacks were on credit unions with less than $10 billion in assets.

Our analysis highlights the continued growth of the online brand impersonation threat and exposes the limitations of outdated detection mechanisms.

- Many organizations and vendors still rely on outdated approaches such as generating a list of domain names similar to legitimate domains using tools like Dnstwist
- However, this permutation-based approach limits itself to an inadequate number of results by design based on what's referred to as "edit distance" which quantifies the dissimilarity of two strings of characters
- These legacy approaches failed to identify 94% of the attacks identified by Allure Security's AI-powered examination of 100+ million online assets every day

This year's findings accentuate the urgent need for organizations to adopt more advanced and effective online brand impersonation detection approaches to protect their brand and members from this rising threat.

INTRODUCTION

The failures of Signature Bank, Silicon Valley Bank, and First Republic Bank in 2023 fueled concern among consumers and businesses about their financial institutions' solvency and the safety of their deposits. Amid such uncertainty, reputation and clear, re-assuring communication is paramount in maintaining trust in your credit union (and attracting consumers that fled banks looking for institutions they felt more confident in).

This brings us to ***"SPOOF 2023: Trends in Online Brand Impersonation for Credit Unions,"*** our second annual report on the escalating threat of online brand impersonation. These scams – whereby adversaries pose as trusted brands online to defraud consumers – hold the potential to undermine faith in your credit union daily.

Each day from August 1, 2022 through to March 31, 2023; our AI screened over 100 million digital assets daily, detecting impersonations of credit union brands ranging from those managing $7 million to $150 billion in assets. Our report offers in-depth analysis of these threats that spare no credit union, regardless of size. We highlight growing trends, the inadequacy of traditional detection methods, and the urgency of adopting more modern, AI-driven strategies to confront this growing threat.

METHODOLOGY & DATA SOURCES

Allure Security's AI engine, harnessing computer vision and natural language processing, automates daily analysis of more than 100 million digital assets including websites, social media content, and mobile app marketplaces. For this report, we've extracted online brand impersonation detection data specific to credit union brands for the period of August 1, 2022 to March 31, 2023.

The sources ingested by our AI detection engine for digital assets to be analyzed include but are not limited to:

- All new domains & sub-domains (all global TLDs)
- Dormant domains & sub-domains
- Allure Security web beacon signals & customer referrer logs
- Social media profile pages
- Mobile app marketplace listings
- Online ad URLs
- Threat intel feeds
- Allure Security threat research team inputs

A differentiating feature of our online brand protection service, which also contributes to the uniqueness of this report, is the ongoing assessment of various digital assets. We don't simply examine an asset once. We continually monitor these assets, recognizing that online content could become a threat at any moment.

While our technology assesses online assets more frequently and in greater depth than any other option, the scale of the internet will constrain any relevant data set. As a result, this report likely underestimates the actual extent of the problem, particularly for non-customer credit unions due to reduced visibility. Allure Security customers, on the other hand, gain enhanced visibility through further training and refinement of our machine learning algorithms specific to their brand.

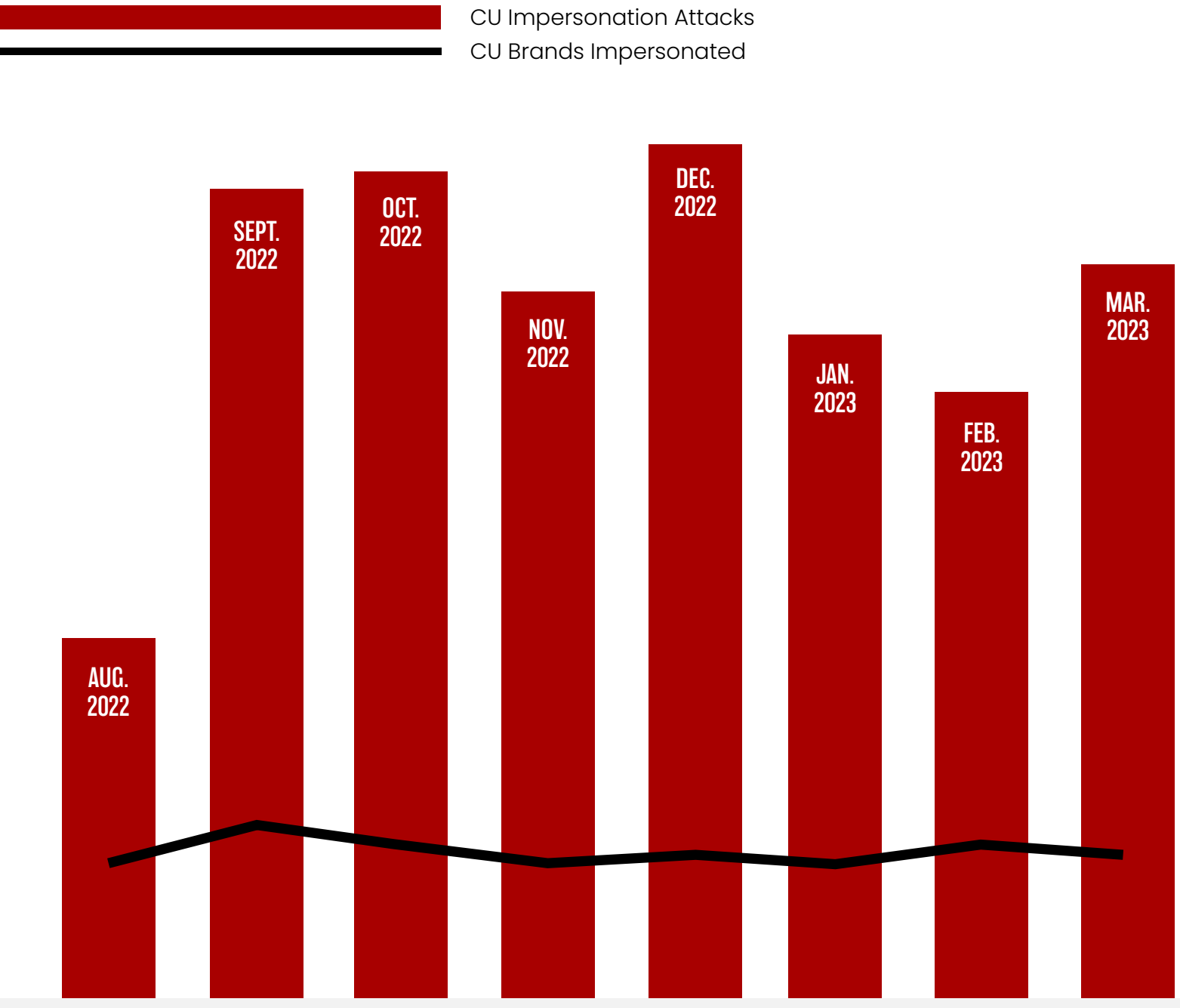
DUPED:
CREDIT UNION SPOOFS ONLINE IN 2023

ATTACK VOLUME OVER TIME

During an eight-month period, we detected thousands of online brand impersonations of hundreds of unique credit union brands.

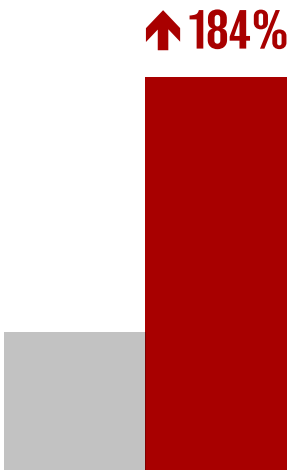
Adversaries impersonated credit unions with assets under management as low as $7.3 million and as high as $156.6 billion substantiating the fact that online brand impersonation problem affects credit unions of all sizes.

The figure below illustrates a timeline of online spoofs of credit unions from August 2022 to March 2023 that hit highs and lows. In September 2022 we see a significant surge in impersonations with the number nearly doubling over August. This wave continued through October with a slight drop in November, but it crested at an all time high in December 2022. Attack volume then decreased in January and February of 2023 but rose 56% in March. A campaign we've labeled UnFAIRSHAKE (see the "Emerging Threats" section of this report for more) contributed to the increase in March and accounted for 40 percent of the impersonations detected that month.

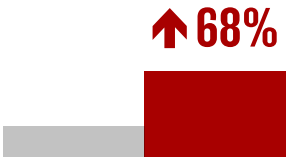


Comparing January, February, and March 2023 with a year earlier, we see that attack volume significantly increased in the first quarter of 2023 compared to the first quarter of 2022:

- Online brand impersonations nearly tripled, increasing 184 percent
- Credit unions targeted increased more than one-and-a-half times, growing 68 percent



ONLINE BRAND IMPERSONATION ATTACKS ON CREDIT UNIONS



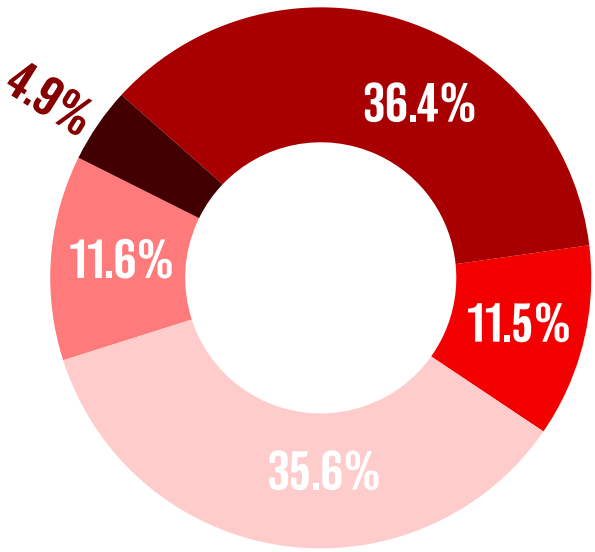
CREDIT UNIONS IMPERSONATED

ONLINE BRAND IMPERSONATIONS CHALLENGE CREDIT UNIONS OF ALL ASSET SIZES

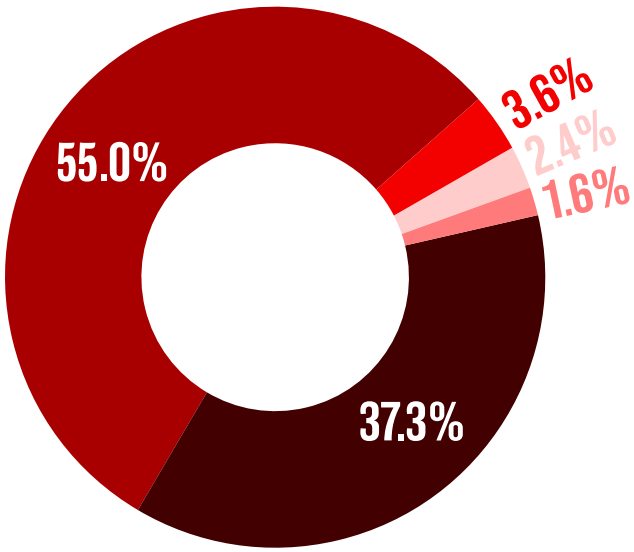
For our analysis, we sorted credit unions into five cohorts based on asset size with the three highest asset-bands aligning with the National Credit Union Administration's (NCUA) asset threshold tiers:

- $20 billion or more in assets (NCUA tier III)
- $15 billion to less than $20 billion in assets (NCUA tier II)
- $10 billion to less than $15 billion in assets (NCUA tier I)
- $1 billion to less than $10 billion in assets
- Less than $1 billion in assets

DISTRIBUTION OF ATTACKS ON CREDIT UNIONS BY ASSET SIZE



DISTRIBUTION OF UNIQUE CREDIT UNION BRANDS IMPERSONATED BY ASSET SIZE



$20 billion & above
$15 billion to less than $20 billion
$10 billion to less than $15 billion
$1 billion to less than $10 billion
Less than $1 billion

Slicing the data in this way can help credit unions better understand the threat to them and their peer institutions. Insights we've noted as a result of this breakdown of the data include:

- From August 2022 to March 2023, fraudsters focused efforts on credit unions with less than $10 billion in assets – 92 percent of the impersonations we detected were of credit union brands with less than $10 billion in assets under management
- No credit union is too small to attract fraudsters' attention – 24 percent of the credit union brands impersonated managed less than $500 million in assets, and in two cases credit unions at the $7 million in assets mark were impersonated
- One particular credit union in the $15 to $20 billion asset category found themselves the target of 32 online brand impersonation attacks each week on average

$20 BILLION OR MORE On average, credit unions that manage $20 billion or more in assets endured 11.6 percent of the brand impersonations we detected during the study. In one extreme case, a credit union in this category found itself the target of roughly 10 impersonations each week.

$15 BILLION TO $20 BILLION Overall, 35.6 percent of the online impersonations we detected mimicked credit unions with assets between $15 billion to less than $20 billion. One credit union came under particularly heavy fire experiencing nearly 32 brand impersonations each week on average.

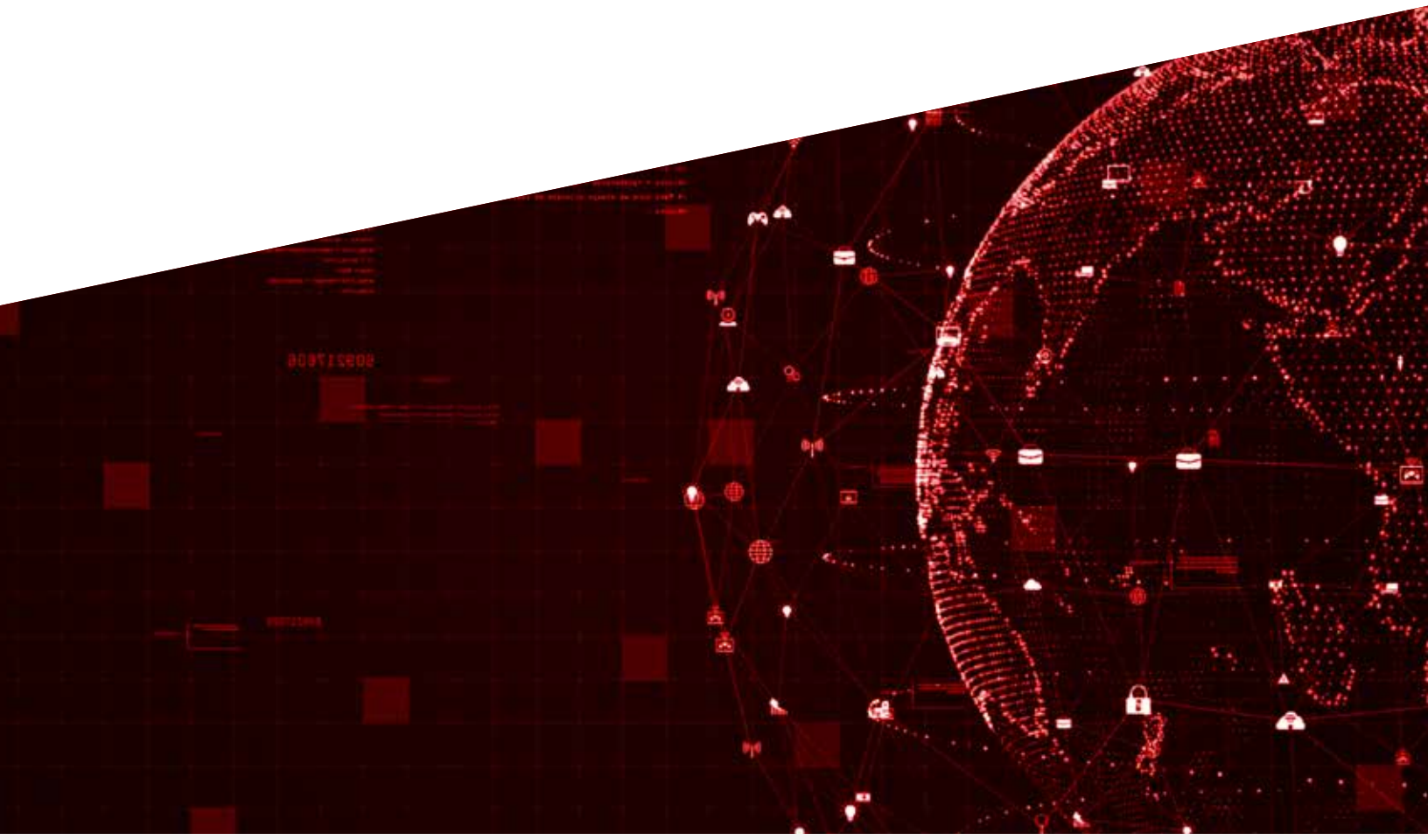
$10 BILLION TO $15 BILLION Credit unions with $10 billion to $15 billion in assets experienced 11.5 percent of the attacks detected during our study's timeframe. Two credit unions in this group shared the honor of more than one online impersonation targeting their brand detected each working day on average.

$1 BILLION TO $10 BILLION Of credit unions victimized by at least one spoof during the timeframe of this year's study, just over 92 percent of them managed less than $10 billion in assets. Of course there are simply more credit unions in this group than others, but it goes to show that the largest credit unions aren't the only targets. This asset category experienced more than a third of attack volume at 36.4 percent.

LESS THAN $1 BILLION Credit unions ignore the rising online brand impersonation threat at their own peril. To once again reiterate that scammers don't discriminate based on asset size, nearly 25 percent of the credit unions we found to be spoofed online manage assets of less than $500 million. In this cohort, we also detected impersonations of two credit unions with assets of just around $7 million.

EMERGING ONLINE BRAND IMPERSONATION THREATS

Here we explain four notable online brand impersonation threats that we observed in 2022 and the beginning of 2023. While some of these threats have appeared in the past, we include them here because we saw a material increase in their use by adversaries and staying informed of tactics used by fraudsters can help credit unions in taking action to protect their brand and customers online.



UnFAIRSHAKE

The scam we've named "UnFAIRSHAKE" accounted for 40% of online brand impersonations we detected in March 2023.

TIMEFRAME

UnFAIRSHAKE detections swelled beginning in mid-March 2023 extending into the first week of April 2023.

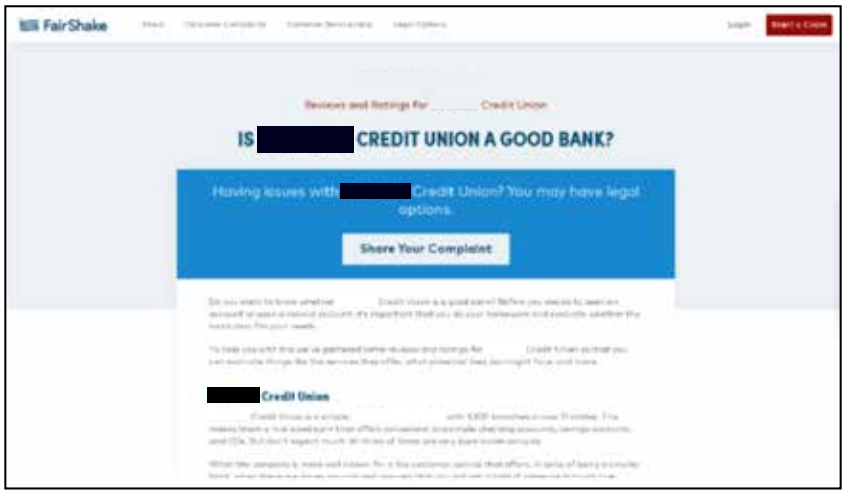
DESCRIPTION

Fraudsters began by impersonating a company called FairShake online. FairShake calls itself "the consumer rights service" and provides legal/arbitration services to consumers to help them settle disputes with companies. FairShake also publishes web pages on its fairshake.com domain that explain how to file complaints against certain companies and in some cases also collects those complaints.

With this particular scam, fraudsters cloned those FairShake complaint pages for a variety of financial institutions including credit unions, as well as, regional and community banks. Those cloned pages were hosted on domains using permutations of the financial institution's brand name or acronyms of that name. At any time, however, one of these cloned FairShake complaint pages would transition into a full-on phishing page that spoofed the target credit union's website including the credit union's log-in fields.

We speculate that the bad actors took this approach (first impersonating a FairShake web page and then transitioning to a spoof of the target institution) to avoid detection by traditional means for as long as possible. In addition, the scammers could have been hoping to improve the ranking of the FairShake spoof in search engine results for queries such as, "Is [insert credit union] a good credit union?".

UnFAIRSHAKE



EXAMPLE OF A FAIRSHAKE CLONE MENTIONING A CREDIT UNION THAT TRANSITIONED INTO A PHISHING PAGE TARGETING THE CREDIT UNION BRAND THE NEXT DAY.

UnFAIRSHAKE

POTENTIAL IMPACT

The UnFAIRSHAKE scam has potential financial, reputational, and operational impacts on a targeted credit union:

FINANCIAL

Stolen member credentials fuel account takeover fraud and the theft of member funds which potentially lead to both recovery and reimbursement costs.

REPUTATIONAL

A credit union member that falls victim to the UnFAIRSHAKE threat would likely hold the credit union somewhat responsible and lose some trust in the credit union or at least reconsider interacting with the credit union over digital channels. In addition, longer customer service wait times resulting from fraud complaints can tarnish members' perception of the credit union and affect customer satisfaction scores.

OPERATIONAL

Online scams targeting a credit union's membership can overburden security staff with reactive response activities taking them away from other more proactive security tasks. Such scams also result in increased call volume reducing quality of service provided to members.

PAY-PER-TRICK

At the end of December 2022 the FBI issued a public service announcement (alert number I-122122-PSA) about a threat that had bedeviled Allure Security customers and their peers for many months – fraudsters impersonating brands in search engine advertising to direct users to phishing sites. Google refers to their advertising services as pay-per-click (PPC), and so we've labeled the threat "Pay-Per-Trick."

TIMEFRAME

We've observed fake Google ads impersonating our customers and their peers throughout 2022 and 2023 and since as far back as 2020 with occasional flare-ups.

DESCRIPTION

Google allows nearly anyone to bid on advertisements based on whatever keywords they choose – even if those keywords are trademarked brand names. Because of this, scammers can bid on the names of financial institutions and other organizations and then display ads masquerading as the legitimate organization, but directing users to a phishing page seeking to steal their account credentials.

In a more sophisticated variant of this scheme, scammers initially set up a website that seems harmless when directly accessed through its URL to avoid detection. However, when the same website is reached through a Google ad, a Google Click ID (GCID) is generated. This GCID acts as a trigger, causing the website to redirect the visitor to a scam site that imitates the brand they originally searched for.

PAY-PER-TRICK

Searching for "notreal credit union login"
results in display of the following ad

Upon clicking the ad, the visitor is redirected to a malicious URL

A RECREATION OF AN OBSERVED GOOGLE ADVERTISEMENT DISPLAYED FOR A SEARCH OF A CREDIT UNION'S BRAND NAME WHICH THEN REDIRECTED TO A PHISHING PAGE.

PAY-PER-TRICK

POTENTIAL IMPACT

The Pay-Per-Trick scam presents financial, reputational, and operational impacts:

FINANCIAL

The theft of member credentials leads to account takeover and eventually the theft of member funds. In some cases credit unions will need to pay both recovery and reimbursement costs. In addition, with both criminals and competitors bidding on your brand name, the scam increases digital advertising and member acquisition costs.

REPUTATIONAL

Credit union members that click on a Pay-Per-Trick ad would likely blame the credit union for any resulting fraud, as well as, lose trust in the credit union and especially any digital promotions. Such a scam can also lead to increased customer service wait times and erode members' satisfaction and perception of the brand.

OPERATIONAL

Because not all users will necessarily be presented with Pay-Per-Spoof ads, these incidents can be especially costly to investigate. In addition, such scams can also flood customer service centers with complaints, keeping staff away from other, more valuable customer service tasks.

Learn more about this Pay-Per-Trick threat on the Allure Security blog at
https://alluresecurity.com/2023/04/20/trending-google-ads-as-phishing-hooks-understanding-the-threat-and-protecting-your-brand/

PUNYPHISH

Fraudsters use Punycode to create deceptive domain names that are strikingly similar to legitimate credit union domains.

TIMEFRAME

Fraudsters using Punycode to support their impersonation of credit union brands online wasn't a new technique in 2022 or 2023. Still, Allure Security observed an increase in PunyPhish-related impersonation attempts aimed at our credit union clients and their industry peers in late December 2022.

DESCRIPTION

ASCII, or the American Standard Code for Information Interchange, is a set of characters for computers primarily containing English-language characters. However, people in non-English-speaking countries require the use of non-English characters, a need addressed by Unicode. Punycode represents Unicode characters using ASCII.

At the end of 2022, we observed a marked increase in malicious actors using Punycode as a veil of deceit. Punycode allows them to craft URLs that the unsuspecting human eye can't distinguish from legitimate brand domain names.

PUNYPHISH

Examining the example illustrated in the image below, you'll notice a potentially malicious URL at left and Punycode on the right signaled by the "xn--" prefix, which instructs the computer system to interpret the Punycode included. The string "-w30d" inserts a lower-case "e" with a dot underneath it into the URL. It's strikingly similar to the domain notrealcu.com, making it nearly indistinguishable.

EXAMPLE DECEPTIVE URL CREATED TO MIMIC OUR IMAGINARY NOTREAL CREDIT UNION'S DOMAIN NOTREALCU.COM USING WWW.PUNYCODER.COM.

PUNYPHISH

POTENTIAL IMPACT

Detecting the use of Punycode in a URL, particularly on mobile devices, is challenging as many web browsers display Unicode (the deceptive URL) instead of ASCII (the real URL starting with "xn--"). As a result the PunyPhish threat is currently highly effective and can impact credit unions in several ways:

FINANCIAL

Scammers that have stolen online banking credentials can take over members' accounts and drain them of funds incurring recovery and reimbursement costs.

REPUTATIONAL

As with any scam involving brand impersonation, victimized credit union members will place some of the blame on the impersonated brand. As a result members and potential members may lose trust in the credit union, as well as, engage less with the institution digitally. Finally, longer wait times for customer service caused by a flood of fraud complaints may negatively affect customer satisfaction.

OPERATIONAL

These scams strain security staff with reactive tasks and increase call volumes, hampering service quality and proactive security work.

DYNAMIC DNSception

Dynamic DNS (DDNS) services help people and businesses manage the DNS (Domain Name System) and dynamic IP addresses which change over time. Unfortunately, scammers have also found a way to abuse these services to impersonate brands in order to deceive and defraud consumers. Therefore we've named this threat "Dynamic DNSception."

TIMEFRAME

For the most part scammers' abused dynamic DNS service providers rather steadily throughout the study's timeframe with a slight uptick in 2023.

DESCRIPTION

Some DDNS providers allow a user to create their own subdomain on a public DNS server – e.g., fakesite.[DDNSprovider].net – at no cost that then points to the IP address of their choice. Fraudsters will abuse such services offered by providers such as DuckDNS, ChangeIP, and No-IP to create URLs for free that direct to phishing websites that impersonate trusted credit union brands and include login fields that steal a victim's credentials.

Below are examples of URLs that abuse various dynamic DNS providers with the deceptive subdomains redacted:

- [deceptive_subdomain].duckdns.org/login.php (Duck DNS)
- [deceptive_subdomain].lflinkup.org/ (Change IP)
- [deceptive_subdomain].hopto.org (No-IP)

We estimate that at least 5 percent of our online brand impersonation detections for credit unions during this study's time frame were of the Dynamic DNSception variety (i.e., they created a URL with a deceptive subdomain and one of many possible free DDNS domains).

DYNAMIC DNSception

POTENTIAL IMPACT

The Dynamic DNSception threat poses financial, reputational, and operational risks to credit unions.

FINANCIAL

Stolen credentials can lead to unauthorized account access and the subsequent loss of member funds, resulting in potential recovery and reimbursement expenses.

REPUTATIONAL

Member victims of a Dynamic DNSception attack will likely hold the credit union somewhat responsible for ensuing fraud and lose trust in the institution. And a rash of such attacks can degrade customer service experiences and negatively impact the credit union's overall brand image.

OPERATIONAL

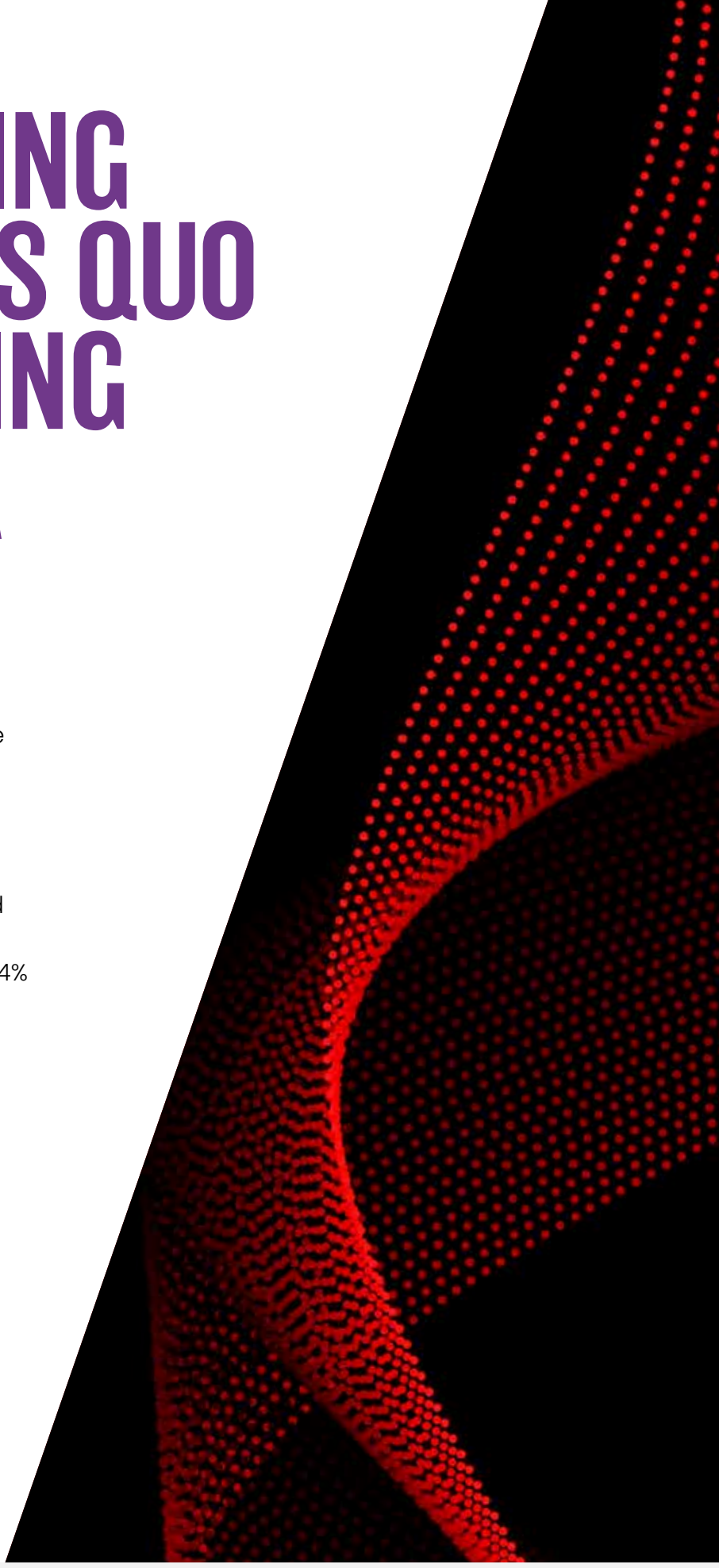
Similar to other scams involving online brand impersonation, the Dynamic DNSception threat affects business operations in the following ways: increased load on customer service staff, investigation costs, opportunity costs with staff focused on an incident rather than other value-creating tasks, and more.

Learn more about the Dynamic DNSception threat on the Allure Security blog at
https://alluresecurity.com/2023/02/10/trending-fraudsters-abuse-dynamic-dns-subdomains-for-phishing/

CHALLENGING THE STATUS QUO & EMBRACING A NEW ERA

Scammers have evolved past deceptive URL variations, knowing brands and brand protection vendors often check for permutations of their brand and domain names. As evidence, tools like Dnstwist could only spot 6% of the brand impersonations targeting credit unions that we detected, leaving a whopping 94% undetected. While Dnstwist and similar tools hold value, they only scratch the surface.

In light of the tripling of online brand impersonation threats to credit union members in 2023, traditional methods no longer suffice; especially considering the looming financial, reputational, and operational costs.



Many companies limit their own scope to avoid false positives, an approach which narrows their visibility and fails to capture the bulk of impersonations. The limitations stem from a lack of technology to cost-effectively process the daily deluge of online content.

To illustrate the shortcomings of this outdated method, let's use an example. Suppose you are Credit Union of Sam with a domain creditunionofsam.com. You might search for Dnstwist matches and even include common strings like "-online" or "-secure." However, you then ignore matches containing "creditunionofsam" with extra content before and after it to avoid excessive false positives, such as "creditunionofsamson." This approach, however, inherently restricts your visibility and overlooks variations such as "mycreditunionofsam" or "creditunionofsamdigital," among countless others. This becomes even more problematic when your domain is an acronym such as "abcu.com" which can appear in millions of hostnames. And then you're missing "secureabccu," "abcubanking," etc.

A well-trained and tuned AI begins to make daily internet-wide brand impersonation monitoring feasible. At Allure Security, we aim to scrutinize every new piece of public internet content, regardless of the URL. Instead we focus on indicators like the use of logos or specific brand language.

Our AI's capacity to handle their volume, a feat no other vendor could achieve, has even excited some of our data feed partners. Other parties only checked for name matches, missing out on 94% of the impersonations we spot. Unlike anyone else, we could evaluate the published online content itself for a more thorough analysis.

If you take nothing else away from this report, let it be that relying on traditional domain monitoring to look at permutations of your brand or domain name only addresses a very small fraction of the issue. With generative AI escalating the frequency and volume of online brand impersonations, countering this threat calls for an equally powerful AI-driven solution.

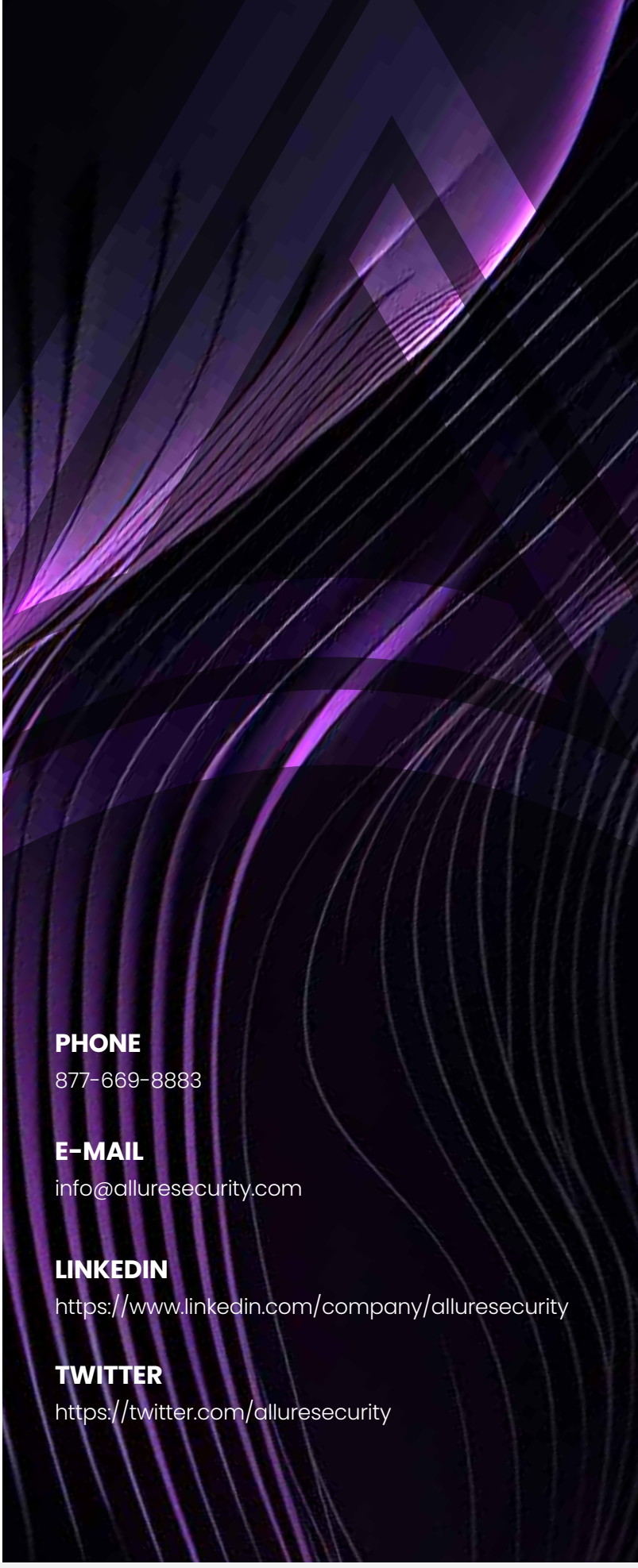
ABOUT ALLURE SECURITY

Allure Security online brand protection-as-a-service automates the examination of more of the digital world with AI — 100+ million digital assets a day including domains, social media posts, and mobile app product pages.

Consequently, and compared to alternatives, Allure Security identifies more online brand impersonations more quickly and closer to their first appearance on the internet — before a single human sees or falls victim to a digital imposter.

Finally, Allure Security's unique three-pronged approach to response — blocklisting, decoy data, and takedown diligence — increases takedown success rates and reduces time to takedown.

Deploying Allure Security allows brands to strengthen online reputation, customer trust, and customer satisfaction, as well as: reduce fraud, lost sales, customer churn, customer complaints, and staff burnout.

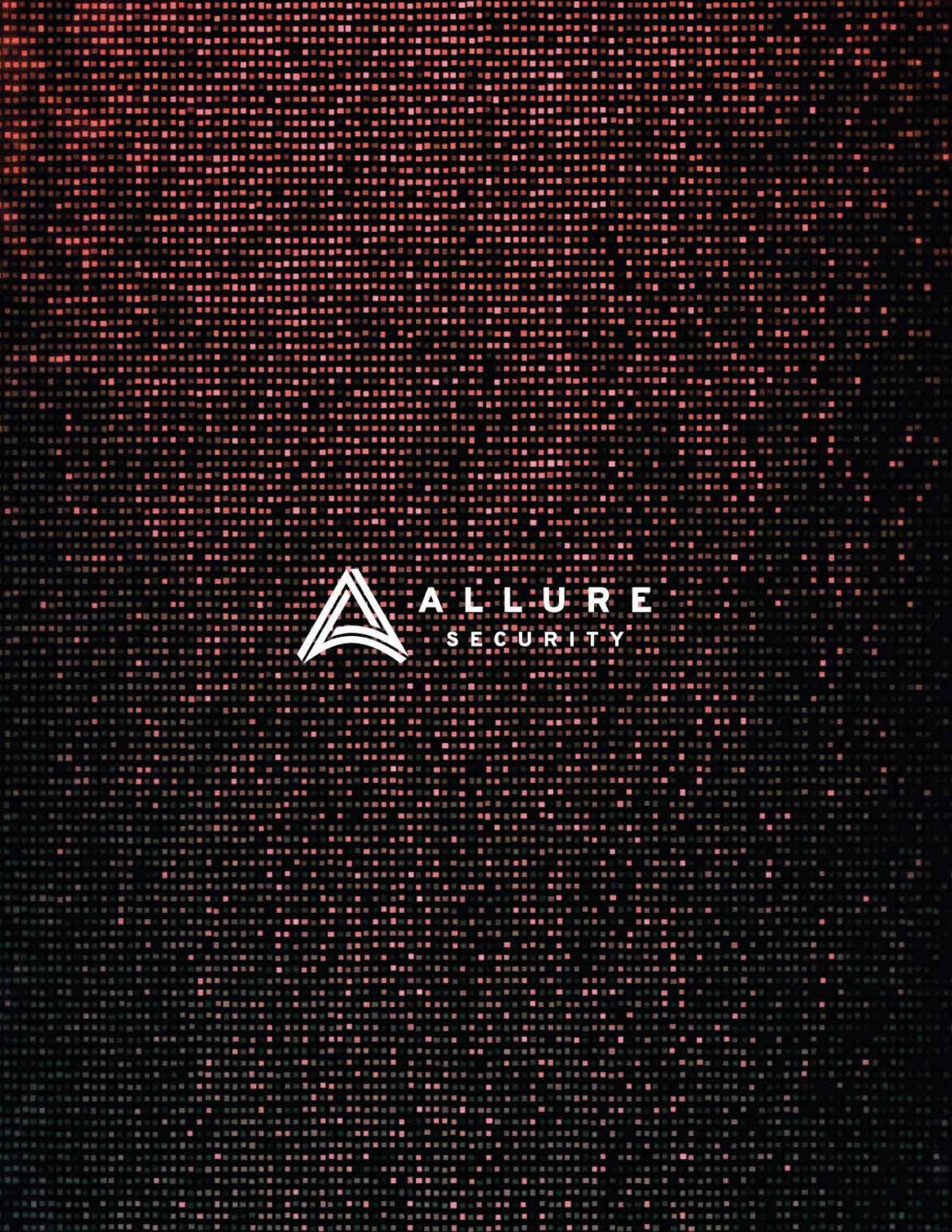


PHONE
877-669-8883

E-MAIL
info@alluresecurity.com

LINKEDIN
https://www.linkedin.com/company/alluresecurity

TWITTER
https://twitter.com/alluresecurity


ALLURE
SECURITY