



Trends in Scams Targeting Regional Banks & Their Customers Online



TexasBankersAssociation

Sam Bakken

DIRECTOR OF PRODUCT MARKETING
ALLURE SECURITY

June 20, 2024

AGENDA

1. Trends in Online Scams Targeting Regional Banks
2. Examples of Recent Schemes
3. Brand Protection 101: Online Brand Audit
4. The Problem With Traditional Approaches
5. FI Case Study: A Modern Approach to Brand Protection

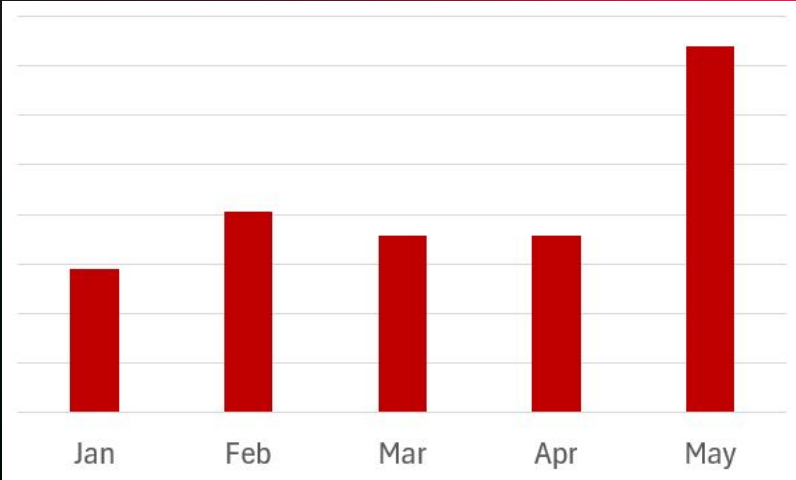
TRENDS IN ONLINE IMPERSONATIONS

Targeting Regional Banks

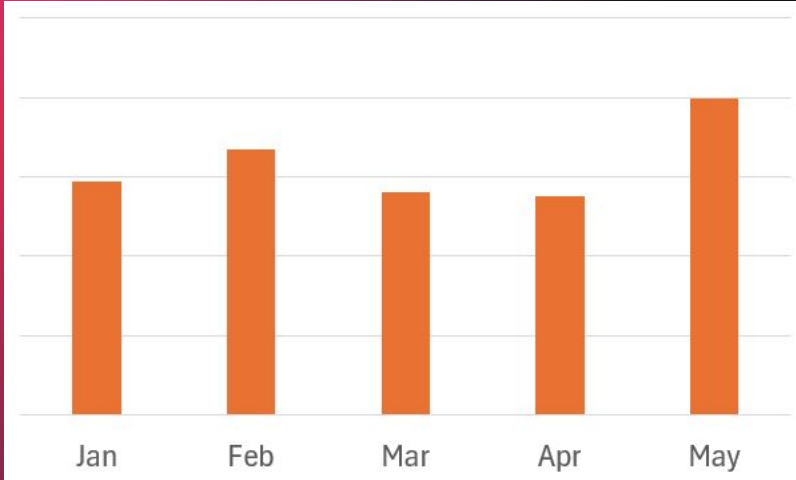


Regional Bank Impersonations Detected Jan. – May 2024

Impersonations



Brands Impersonated



Analysis of Rogue Mobile Apps Detected per Regional Bank

Minimum

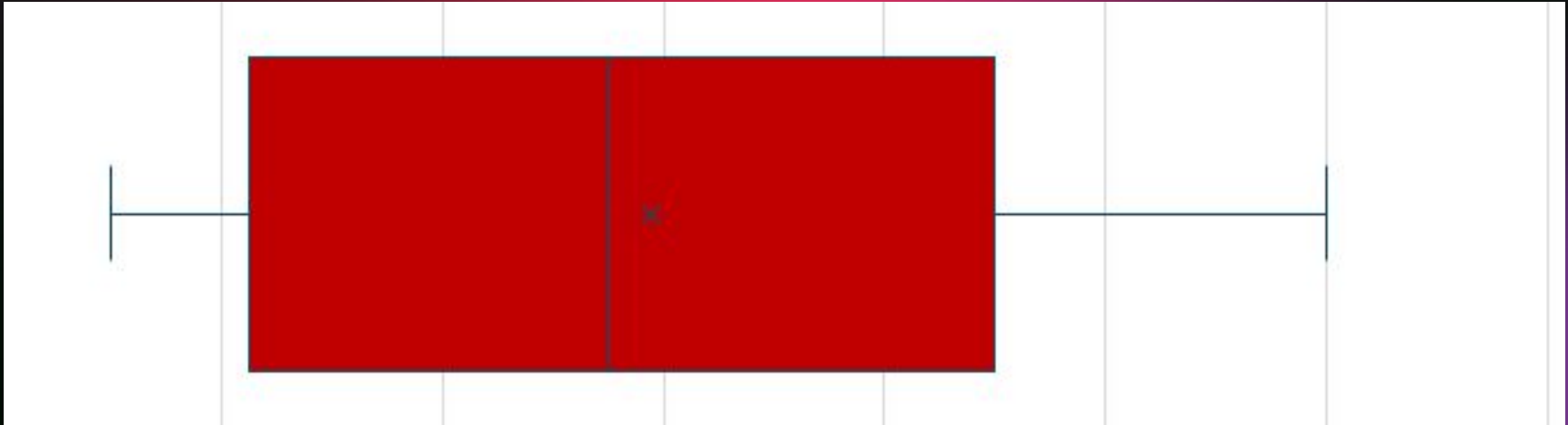
1

Median

5.5

Maximum

12



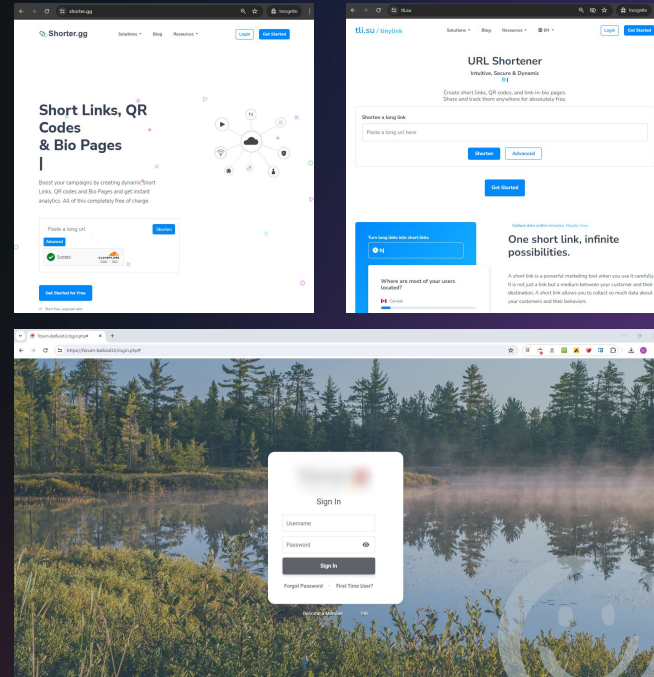
RECENT SCHEMES

Targeting Regional Banks



FRAUDSTERS USING THEIR OWN URL SHORTENERS TO EVADE DETECTION

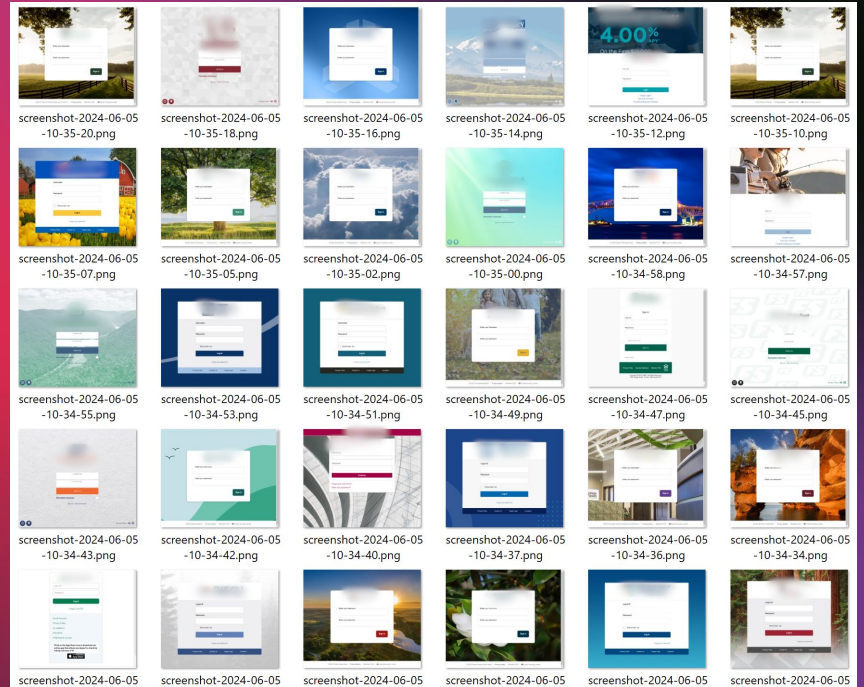
- **SMS phishing messages sent to credit union members in late May**
- **Used shortened URLs with domains including kn8[.]site, kv6[.]site, dx2[.]site, and dx5[.]site**
- **More mature link shorteners use vetting to prevent phishing**
- **Threat actors create their own link shorteners to evade vetting while still disguising links**



Screenshots of Suspicious URL Shortener Web Pages and Credit Union Impersonation

SCOURGE OF PHISHING KIT NESTS

- **Scourge of phishing kit nests targeting multiple FIs started in May**
- **Ready-made phishing page templates**
- **212 FIs targeted: regional banks & CUs**
- **10+ phishing nests detected a day**
- **Up to 40 phishing pages in any nest**
- **Impervious to typo-based detection**
- **Typical automated scanners can't find them**



Screenshots of 30 different credit unions and regional banks impersonated within one single phishing kit found June 5, 2024

FRAUD VIA ROGUE MOBILE APPS

**Growing portion of fraud:
5 percent of fraud attacks traced to
rogue mobile apps**

**Adversaries inject malicious code
into cloned apps**

**Older app versions lack
latest security features**

**Mostly Android apps, rogue iOS
apps will grow w/ new March 2024
EU rules**

“

Threat actors will weaponize our mobile banking app, put it on some third-party site and then send an email with a link to it.

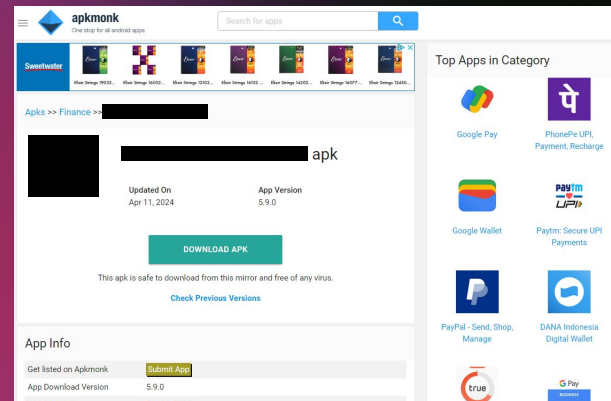
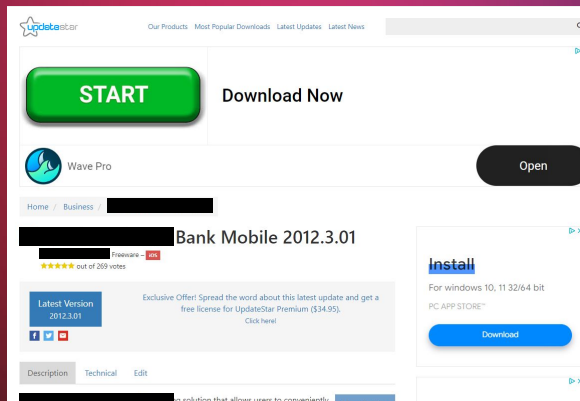
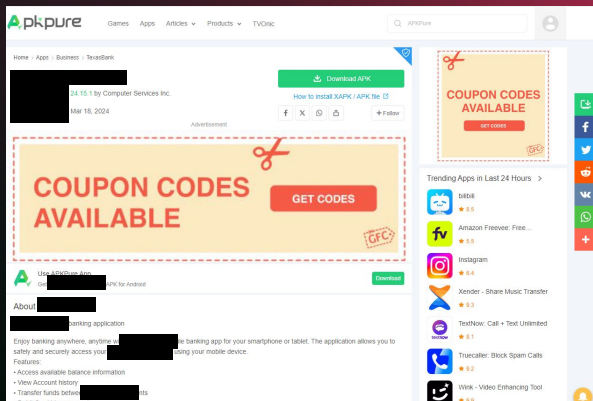
It's something I hadn't heard of before.

**VP Cybersecurity
Medium-Sized Financial Institution**

*“Ramp Up Protections as Mobile Fraud Grows” The Financial Brand
<https://thefinancialbrand.com/news/digital-banking/mobile-banking-trends/banks-must-ramp-up-against-multiplying-fraud-actors-173185/>*



ROGUE MOBILE REGIONAL BANK APPS



apkpure.com
3 mos. out of date
17 versions back to Oct 2016

updatestar.com
12 yrs, 23 mos. out of date
For iOS

apkmonk.com
Current version
7 versions back to Dec 2021

SEARCH ENGINE POISONING: PAID

About 560,000 results

Ad related to: [REDACTED] login

[REDACTED] | Your Trusted | [REDACTED]

<https://californiagamblers.com> ▼

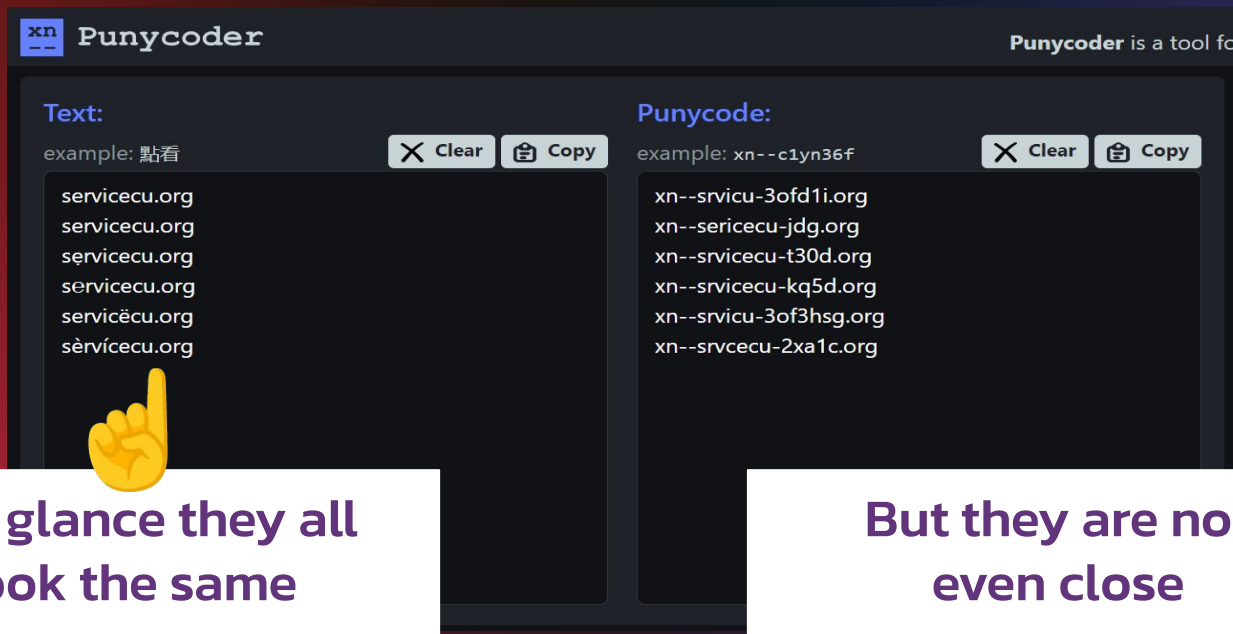
[REDACTED] is one of the largest locally owned and operated **financial** institutions. Convenient locations and free ATMs. [REDACTED] Credit Union offering savings, You have visited californiagamblers.com once in last 7 days.

Ad displays upon search for “[financial institution] login” (note irrelevant URL)

Clicking the ad directs the visitor to the malicious site

ADVERSARIES RELY LESS ON TYPOS

TYPOSQUAT-BASED DETECTION MISSES UP TO 94%



The screenshot shows the Punycoder tool interface. On the left, under 'Text:', the input is 'example: 點看'. Below it, a list of six typosquats is shown: 'servicecu.org', 'servicecu.org', 'servicecu.org', 'servicecu.org', 'servicëcu.org', and 'sèrvicecu.org'. A yellow hand cursor points to the first 'servicecu.org' entry. On the right, under 'Punycode:', the input is 'example: xn--c1yn36f'. Below it, a list of six corresponding Punycodes is shown: 'xn--srvicu-3ofd1i.org', 'xn--sericecu-jdg.org', 'xn--srvicecu-t30d.org', 'xn--srvicecu-kq5d.org', 'xn--srvicu-3of3hsg.org', and 'xn--srvicecu-2xa1c.org'. Each list has 'Clear' and 'Copy' buttons.

At a glance they all look the same

But they are not even close

LAYERS OF IMPERSONATION MEASURES TO EVADE DETECTION

The screenshot shows the FairShake website interface. At the top, there is a navigation bar with the FairShake logo and links for 'About', 'Consumer Complaints', 'Customer Service Help', and 'Legal Options'. A 'Login' link and a red 'Start a Claim' button are also visible. The main content area features a heading 'IS [REDACTED] A GOOD BANK?' and a sub-heading 'Reviews and Ratings for [REDACTED]'. Below this, there is a blue call-to-action box that says 'Having issues with [REDACTED] options. You may have legal options.' with a 'Share Your Complaint' button. The text below the box discusses the importance of researching banks before opening accounts and mentions that the website has gathered reviews and ratings for [REDACTED] to help users evaluate services and potential fees.

The screenshot shows a bank website interface. At the top, there is a navigation bar with a 'Disaster relief available for members. Learn More' notification. Below this, there are links for 'Locations', 'Join [REDACTED]', 'Rates', and 'Contact Us', along with a search bar. The main content area features a 'Personal' tab selected, with 'Business' and 'Student' tabs also visible. Below the tabs, there are links for 'Checking & Savings', 'Credit Cards', 'Loans & Lines', 'Mortgage', 'Investments', and 'Insurance'. The main promotional banner is for 'Certificates. Now in lofty (up to 2.70% APY*) or liquid (2.25% APY*)'. It lists '9-month certificate — up to 2.70% APY*' and '12-month liquid certificate — 2.25% APY*'. There are 'LEARN MORE' and 'OPEN ACCOUNT' buttons. Below the banner, there is a section titled 'We're here to help you build financial security.' with a sub-heading 'Find great features on checking accounts, low rates on home and personal loans, credit cards, and more.' At the bottom, there is a footer with a link to 'Manage Cookie Preferences' and an 'OK' button.

BRAND PROTECTION 101: BRAND AUDIT

For Regional Banks



BRAND AUDIT PLAN



TRADEMARKS / COPYRIGHT

Check your registrations



MOBILE APP DISTRIBUTION

Clarify approved app stores



WEB SITE INVENTORY

Build inventory of owned sites



ONLINE BRAND MONITORING

How will you spot fakes?



3RD PARTY PROPERTIES

Identify 3rd-parties' use of your brand



COLLECTING REPORTED FAKES

Who will collect reports?



SOCIAL MEDIA ACCOUNTS

Claim your brand accounts



INCIDENT RESPONSE PLAN

Who responds and how?

THE PROBLEM WITH TRADITIONAL APPROACHES



THE **PROBLEM** WITH OLD FASHIONED APPROACHES



69% of attacks can't be detected by domain monitoring

The old way misses most scams

75% of victims visit a scam site during the first 10 hours

The old way is too slow to help

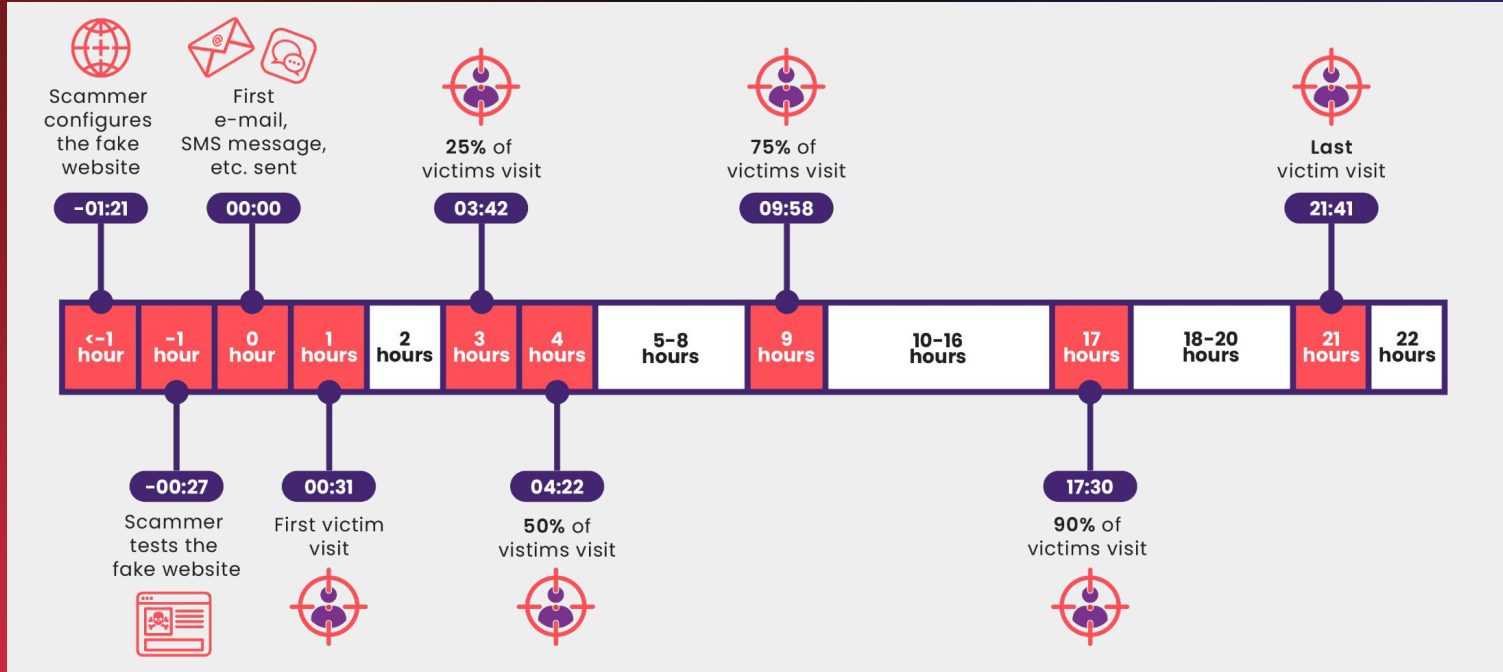
Up to \$14,700 cost of mitigating an impersonation (est.)

That's too much

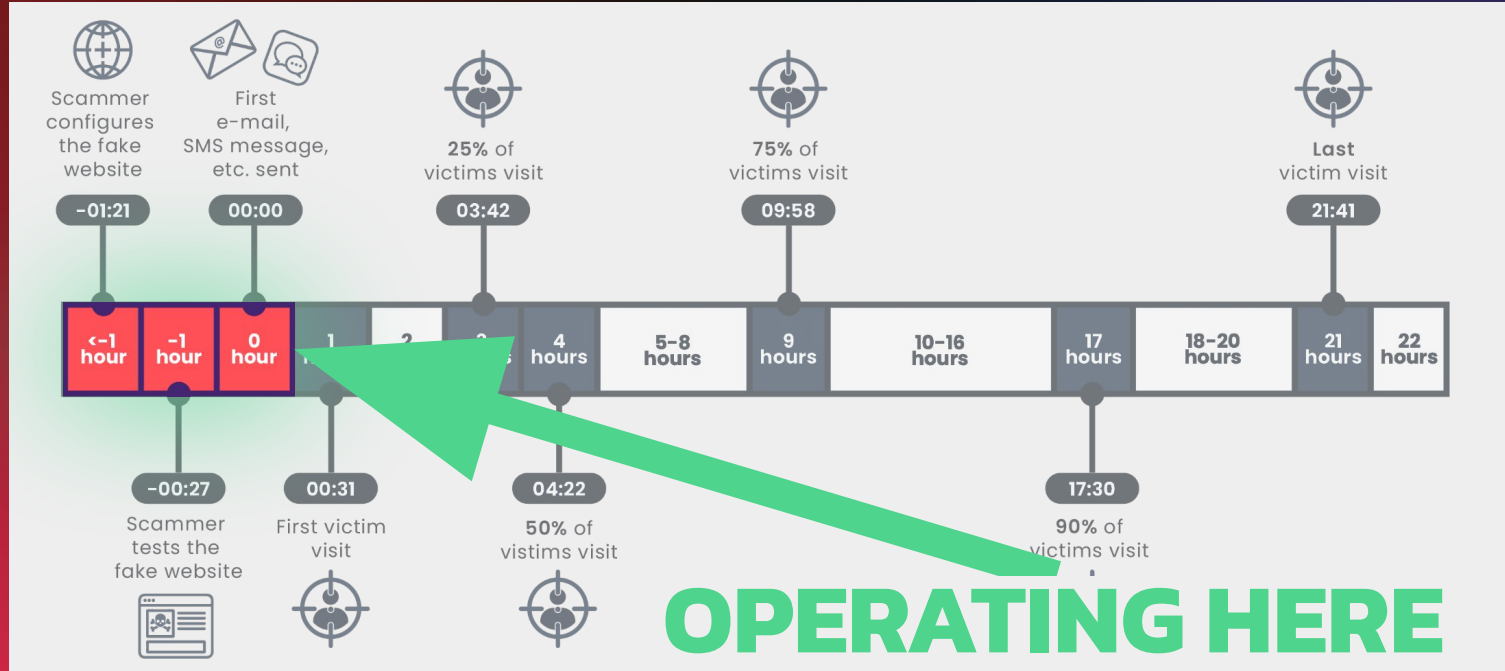
\$150,000+ cost of time (1.5 FTEs) hunting impersonations (est.)

Huge waste of time

BRAND IMPERSONATION TIMELINE



WHAT DOES IT MEAN TO STOP SCAMS BEFORE THEY STRIKE?



HOW A NORTHEAST REGIONAL STOPS PHISHING SCAMS BEFORE THEY STRIKE



FI CASE STUDY: HUNTING FOR BRAND IMPERSONATIONS

BEFORE

- Customers detected fraud first
- Takedowns were slow & expensive
- Blocking & takedowns took days, increasing the number of victims
- Internal IT security, fraud & customer support staff burdened with response in addition to other priorities



REACTIVE

FI CASE STUDY: PROACTIVE HUNTING FOR BRAND IMPERSONATIONS

AFTER

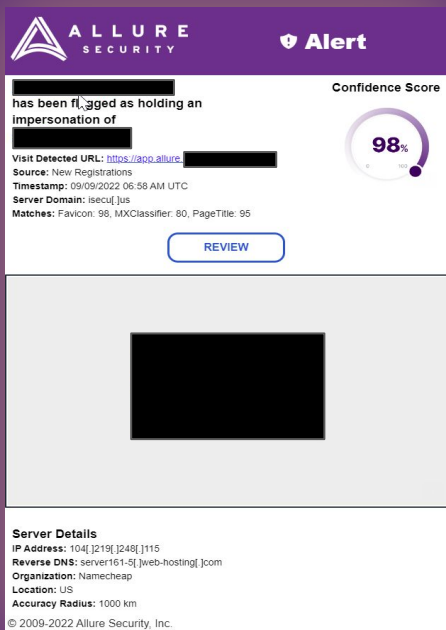
- Scams detected within minutes of being published, pre-empting fraud & complaints
- Visibility into 10+million new & updated websites each day
- Scams blocked & taken down in minutes, before customers visit the site
- IT security, fraud & customer support staff burden eliminated, but more importantly prevented customers' credential harvesting



PROACTIVE

PROACTIVE IMPERSONATION DETECTION & RESPONSE

Actual Results



ALLURE SECURITY **Alert**

██████████ has been flagged as holding an impersonation of ██████████

Confidence Score: **98%**

Visit Detected URL: <https://ago.allure.██████████>

Source: New Registrations

Timestamp: 09/09/2022 06:58 AM UTC

Server Domain: iseculjus

Matches: Favicon: 98, MXClassifier: 80, PageTitle: 95

[REVIEW](#)

██████████

Server Details
IP Address: 104.1219[.]248[.]1115
Reverse DNS: server161-5[.]web-hosting[.]com
Organization: Namecheap
Location: US
Accuracy Radius: 1000 km
© 2009-2022 Allure Security, Inc.



SEPT 9 06:42

Domain first observed on the Internet (DomainTools/Farsight)



SEPT 9 06:58

Alert on active impersonation attack by Allure Security



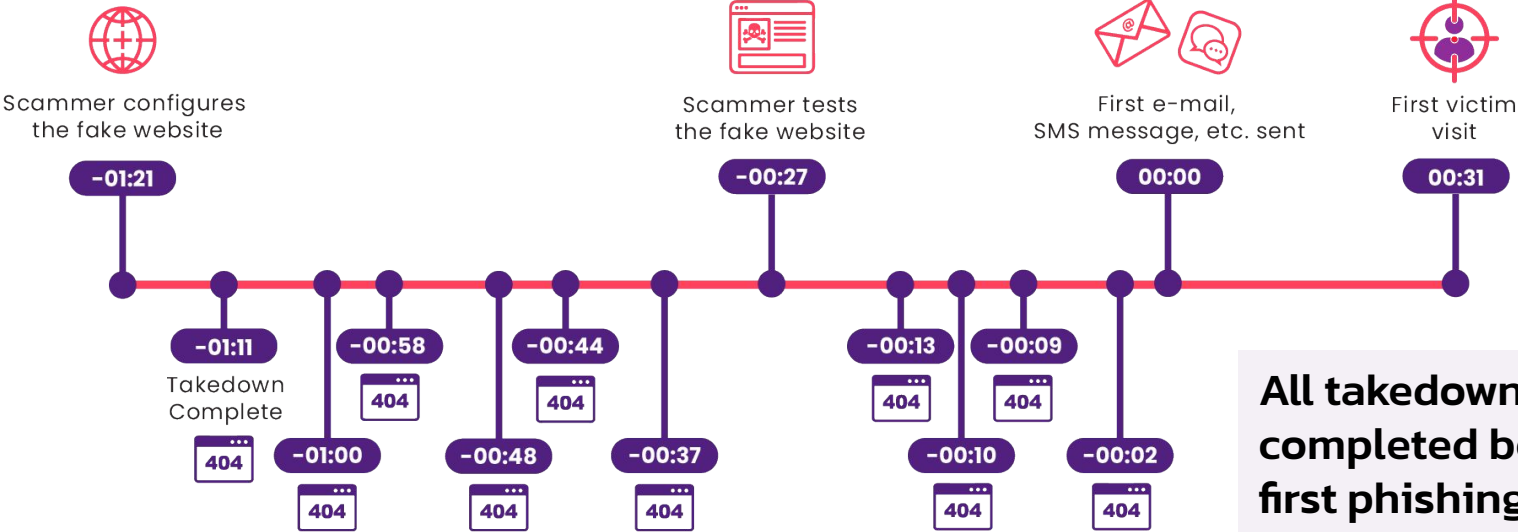
SEPT 9 07:03

Allure Security team completes site takedown

TOTAL ELAPSED TIME: 21 MINUTES

PROACTIVE DETECTION PROTECTS CUSTOMERS

Actual Performance (Sept. 1-9)



All takedowns completed before first phishing message sent

AVERAGE TIME: 40 MINUTES 54 SECONDS



THANK

YOU!

CONTACT

VISIT

alluresecurity.com

EMAIL

info@alluresecurity.com

CALL

877.699.8883