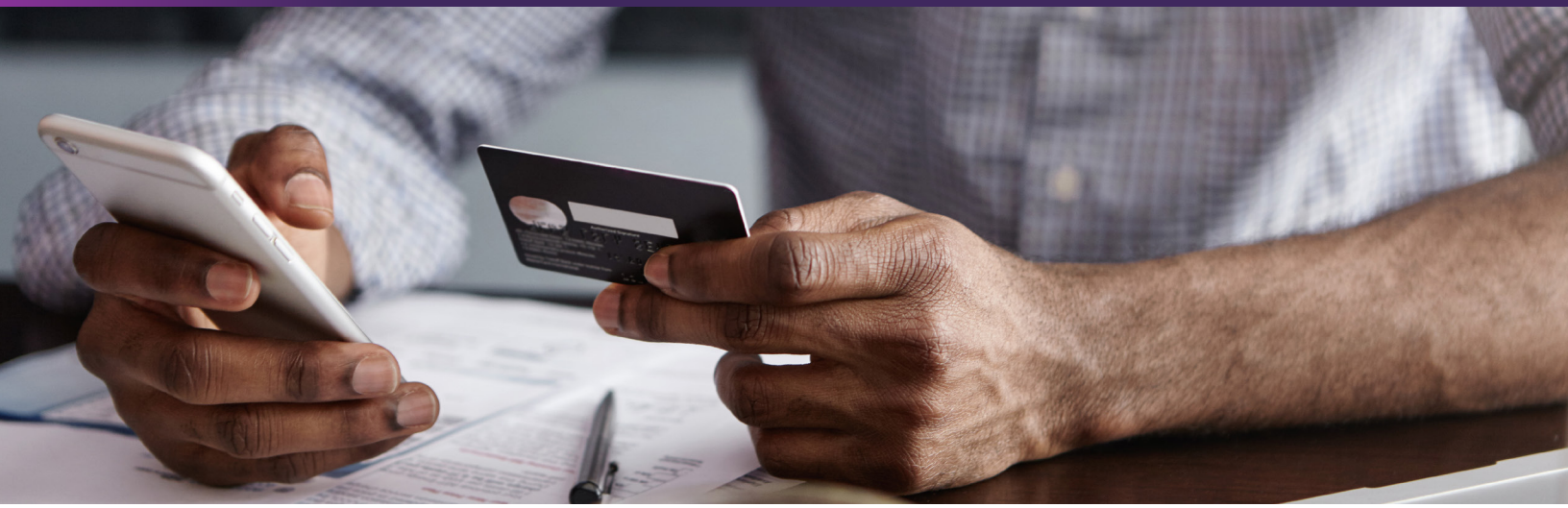
HOW SERVICE CREDIT UNION REDUCED ONLINE FRAUD & INCREASED MEMBER SATISFACTION WITH MODERN BRAND PROTECTION



AT A GLANCE

OBJECTIVE

- Fight fraud stemming from online brand impersonation
- Find and eliminate online scams more effectively and quickly

CHALLENGE

- Surge in fraud complaints burdened IT security, fraud, and member support staff
- Increase in call volume and wait time threatened member satisfaction
- Response was reactive, after fraud had already occurred
- Slow or unsuccessful takedowns allowed fraud to persist

SOLUTION

- Allure Security Brand Protection-as-a-Service for web and social media
- 100s-of-millions of digital assets inspected each day for impersonations
- Web beacons to immediately alert on cloned content
- Multi-pronged response including blocklisting and takedown

RESULTS

- Successful elimination of multiple, long standing scam websites hosted in Russia
- Mean time to detect and mean time to respond to online brand impersonations reduced from days/weeks to minutes/hours
- Significant decrease in wire transfer fraud and member complaints of fraud reduced to near zero

CHALLENGE

FAKE SITES & FRUSTRATED CUSTOMERS

Service Credit Union is an award-winning financial institution with more than 330,000 members, $5.1 billion in assets under management and 50 locations throughout the U.S. and Germany. The credit union began in 1957 with a mission to serve U.S. military, veterans, and U.S. Department of Defense employees but didn't think of itself as a top target of online scammers, at least in comparison to more well known financial services brands. A surge of frustrated members complaining of falling victim to fraudulent websites impersonating the credit union in early 2020 proved otherwise.

Assistant VP of Information Security Alex Laham and team tracked some of the fraud back to scam websites hosted in Russia. Unfortunately, the fake websites' registrars and hosts would not respond to the team's requests to shut the sites down.

SOLUTION

OFFLOADING BRAND PROTECTION TO AN EXPERT

Laham wanted to get ahead of these threats to reduce their impact and stop relying on members contacting customer service as their alert system. He needed proactive reconnaissance to find brand impersonation attacks quickly even before they could be launched. He also needed proven response capabilities that could make detected scam sites inaccessible to minimize negative impact on the brand and customers. And because these impersonations went beyond mere typosquatting, he needed sophisticated detection technology that went beyond just analyzing URLs for look-alike domains. The solution would require a combination of people, process, and technology he didn't have on hand, and so, he chose Allure Security's brand protection-as-a-service.

Allure Security's brand impersonation detection engine applies machine learning (computer vision and natural language processing) to automate the examination of images and text on websites (not only misspelled URLs) as soon as they're registered. As a result, it finds sophisticated, stealthy scam websites when traditional domain monitoring fails.

> *"Allure Security crushed the proactive detection…[within weeks] we observed a reduction in wire fraud and complaints to customer service about scams"*
>
> *— Alex Laham*
> *Assistant VP, Information Security*
> *Service Credit Union*

Allure Security evaluates hundreds-of-millions of websites a day. Something the credit union's security and fraud teams didn't have time for.

Along with the detection engine, the credit union has full disposal of Allure Security's expert threat research and response team. The team's proven response process repeatedly delivers results where other vendors and approaches have failed, bringing down more scam websites more quickly.

Finally, as an added layer of brand protection, the credit union deployed Allure Security beacons on their website. These beacons automatically alert when the credit union's web content is cloned and published elsewhere on the internet and take mere minutes to integrate into the genuine site.

RESULTS

To start, Allure Security's expert threat research and response team successfully facilitated the takedown of the counterfeit websites hosted in Russia. The credit union's takedown success rate now approaches 100 percent and mean-time-to-takedown has been reduced to less than an hour.

Next, within minutes of activating Allure Security brand-protection-as-a-service, the credit union received an alert on a brand impersonation - a scam they wouldn't otherwise have identified. Minutes later, Allure Security identified another website clone hosted on a completely different server. Best of all, because the credit union spotted these scams so quickly, they could be mitigated before members fell victim. In most cases, Service Credit Union can now identify a brand impersonation attack within minutes of the domain first being observed on the Internet. By detecting and mitigating impersonations during configuration and testing, the institution eliminates these threats before a single phishing message is sent.

In subsequent weeks, Allure Security detected and mitigated dozens of fake websites impersonating the credit union's brand. This reduced customer complaints of fake websites to near zero within a month. Along with the reduction in calls, Laham and team could demonstrate a significant reduction in wire transfer fraud and associated savings connected to the brand protection service. Today the credit union uses Allure Security to protect its digital presence across the web and social media — defending and maintaining their brand while reinforcing members' trust.