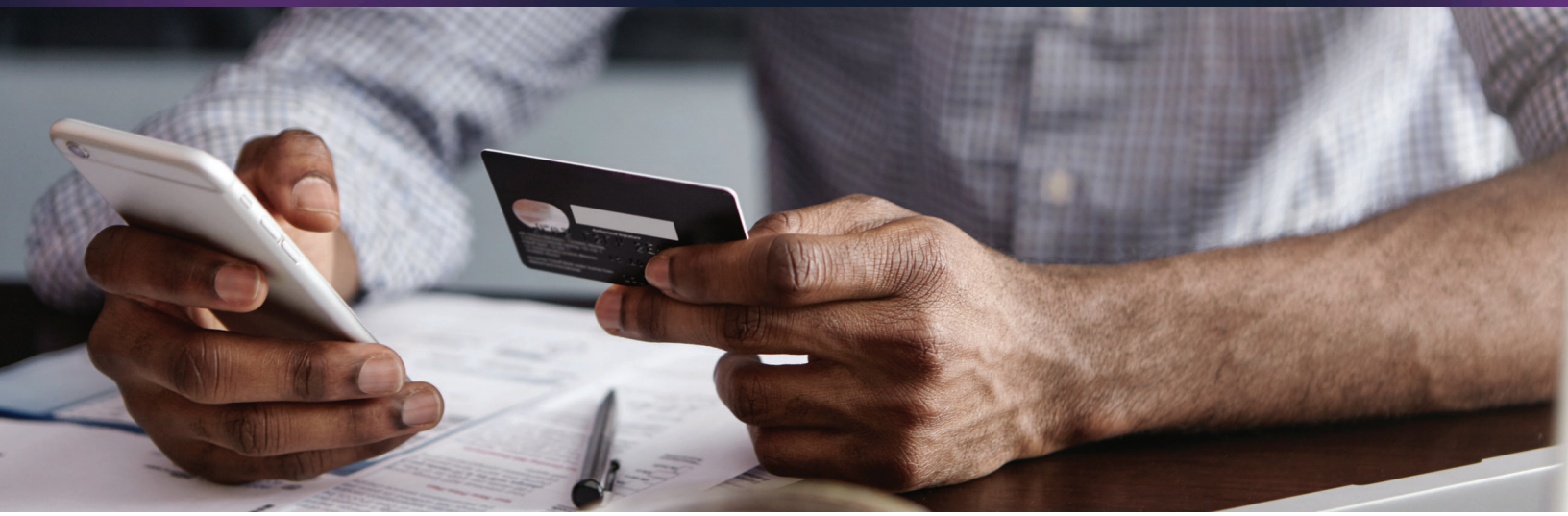
ALLURE SECURITY

HOW A CREDIT UNION REDUCED ONLINE FRAUD & INCREASED MEMBER SATISFACTION WITH ALLURE SECURITY BRAND PROTECTION



AT A GLANCE

OBJECTIVE

- Eliminate scam websites targeting the credit union's members

CHALLENGE

- A surge in member complaints of scam websites impersonating the credit union's brand
- Unsuccessful attempts to take down a cluster of scam websites hosted in Russia
- Lack of visibility into the scope of the problem

SOLUTION

- Allure Security brand protection-as-a-service detected more fake websites, deceptive social media profiles, and rogue mobile apps. And then more quickly rendered them inaccessible. The credit union also deployed web beacons as an added protection against spoofing of their website content before customers fell victim

RESULTS

- Successful elimination of multiple, long standing scam websites hosted in Russia
- Identification of multiple previously unknown brand impersonation attacks within minutes
- Dozens of fake websites mitigated
- Significant reduction in member calls complaining of scams, as well as, instances of wire transfer fraud

CHALLENGE

FAKE SITES & FRUSTRATED CUSTOMERS

An award-winning credit union with $4.5 billion in assets and 50 locations throughout the Northeastern U.S. found itself, and its 293,000 members, targeted by a ring of online scams. 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 in frustrated members calling to complain of falling victim to online fraud impersonating the credit union proved otherwise.

As part of investigating these instances of fraud, for example, the credit union's VP of Information Security and his team tracked some of the fraudsters back to a number of scam websites impersonating their brand and 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

The VP of Information Security 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 lookalike 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 combines 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"*
>
> *— VP Information Security, Northeastern U.S. Credit Union*

It also evaluates tens-of-millions of websites a day. Something the credit union's security and fraud teams couldn't achieve.

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. This was a relief to the team after having expended significant effort in the past with little to show for it.

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 subsequent weeks, Allure Security detected and mitigated dozens of fake websites impersonating the credit union's brand. This resulted in call volume from customers complaining about fake websites decreasing to zero within a month. Along with the reduction in calls, the Information Security VP could demonstrate a significant reduction in wire transfer fraud and associated savings correlated with the brand protection service. Today Allure Security protects the credit union's entire digital presence from web to social to mobile - helping them protect and maintain their brand and reinforcing their members' trust.