FORTRA™

CASE STUDY (AGARI)

Los Angeles-Based Large Credit Union Eradicates Phishing Attacks

Executive Summary

Los Angeles Federal Credit Union (LAFCU) was in the crosshairs of email scammers. Its brand was constantly being spoofed, putting its members at risk of being defrauded. The CTO prioritized email security as part of his broader risk management strategy, and selected Agari as his partner. That was more than a decade ago. Today, domain spoofing is at near-zero.

> *"Our initial goal was to reduce phishing attacks down to the annoyance level, but in working with Agari we've eradicated it. And that allows me to focus on other strategic areas of my risk management strategy."*
>
> – Brian Todd, CTO, LAFCU

e-Branch Services

pple iPod inside e-Branch!

LAFCU Account #

e-Branch PIN

To access the below services, enter your Account #, PIN, click a Start Page from the drop-down menu, then click "Enter". If you do not click a Start Page, you'll access the "Welcome" page.

(call, fax, or e-mail LAFCU to request a free PIN)

Access Checking, Savings & Loan Accounts, e-Check Images, e-

Register for Wireless e-Branch

Online Account Statements

Pay Bills

View Card History

AT-A-GLANCE

Industry Financial Services

CHALLENGES:

- Brand domain abuse, including brand spoofing and executive impersonation

SOLUTION:

Agari DMARC Protection

POST-ENFORCEMENT RESULTS:

- *99.7% of emails are legitimate!*
- *95% reduction in phishing attacks on primary domain once at p=reject!*
- *A consistent trust score of 100!*

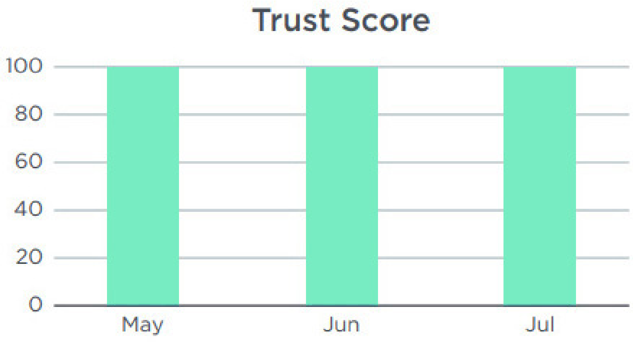
> *"DMARC should be a hard requirement during any vendor selection process. When your vendors have a DMARC set at p=reject, your brand and the whole ecosystem is protected, too."*

A question we often ask CISOs is: What was the compelling event that led you to prioritize your email security strategy? While the details vary, a constant theme exists and revolves around the fact that bad actors continue to bombard companies with phishing attacks and brand hijacking. Brian Todd, CTO at LAFCU, didn't pause when we posed the question to him. "We were getting a lot of phishing attacks against our brand – fake websites and emails," he said. "We were constantly getting phished and our brand was being compromised. We were trying to make it more difficult for the scammers to attack our brand, and they were constantly coming up with new attacks. It had become an unsustainable game of whack-a-mole."

And then in 2012, a crucible befell the company. Credit Union members, some of whom were elderly or less technically savvy, were under attack and falling victim to scammers; other non-members would receive the fake messages and start to engage with scammers and do their own investigations; and a scammer group set up different websites that looked like it was an official LAFCU website. The group spoofed the credit union's brand domain and emailed thousands of its people telling them a problem had occurred with their credit cards and/or account. Hundreds of people filled in their account information to the fake websites, handing over their credentials to the fraudsters. The victims' identities were stolen and many of them ended up losing money. "At the time, the only way we knew an attack had started was because our Credit Union's call center would get calls and questions from victims or members who were worried that something was wrong with their account. It was a perfect storm, an avalanche of phishing-related incidents that had to be stopped," Todd said. "We did extensive research and then received a recommendation for Agari. And that's made all the difference."

LAFCU began working with Agari immediately after these events to shore up its email channel, and ultimately protecting the company from highly sophisticated bad actors and restoring trust with its members. As one of the founders of the DMARC protocol that same year, Agari was a prime candidate to help LAFCU solve its spoofing woes. Todd elaborates, "When we switched over to Agari DMARC Protection, we were able to monitor more email traffic than ever before and sort out the scammers from our legitimate email quickly and easily." And Agari made a lasting difference. LAFCU completed its DMARC journey to p=reject within five months, and overtime, it has recognized a more than 95 percent reduction in the amount of phishing scams it has had to remediate.

With a DMARC record at p=reject, 99.7 percent of its email is legitimate. This improvement has enabled Todd to identify and focus on addressing emerging vulnerable areas to the company. "Today, I no longer spend hours dealing with e-mail scammers. Instead, I'm focused on secure communication for the members." Third-party risk management is critical in the current environment and companies need to ensure that their vendors are adhering to email security best practices, like a DMARC record with a policy set at reject. "When I started digging into potential exposure presented by various vendors, I was surprised at the number of email servers that sent emails on our behalf. We found more than 60 servers handling our email communications." And that's a real risk. While it can be challenging to hunt down all of those mail servers and IP addresses and determine whether they have DMARC, it's imperative in order to have member trust.



After years of leveraging Agari DMARC Protection, LAFCU has maintained a years-long Trust Score of 100, indicating a very healthy DMARC deployment.

Todd's risk management conversations with the LAFCU Board of Directors changed too, upon working with Agari. Email security has long been a forefront issue with the Board, but today, instead of just reporting the volume of constant phishing attacks or sharing the latest attack details, the conversation is more strategic in nature due to the analytics in Agari DMARC Protection. "Our Board pays attention to the heat map, which visualizes data clusters of where emails are sent from," Todd said. "This shows them levels of risk quickly and is the jumping off point I use for discussing on-going resilience of the business and the efficacy of our risk management strategy."

In summary, Todd shared these lessons learned in rolling out an email security strategy centered around email authentication using DMARC:

1. Conduct a thorough inventory quarterly of the vendors and the vendors' vendors that are sending emails on behalf of your brand. It's always changing, especially in a remote workforce operating environment. "Not all vendors understand DMARC and SPF, so finding the right contact at the vendor can be hard to do but necessary," Todd said.
2. Educate your internal department stakeholders on a rolling basis. Business is not static, and departments will continue to contract with new vendors that end up sending emails on a company's behalf.
3. Educate your customers on a rolling basis, too. By clearly communicating to customers what to expect from your company, they will be more alert when a scam comes in. "We regularly communicate to our customers our protocols. We tell them that we will never send an email which asks for their credit card number and PIN," Todd shared. "We communicate what we don't do, so now our customers will contact us proactively, if they see something that isn't right."
4. Ensure that you have enough lead time. Depending on who manages your DNS, the change-over process can be time consuming. Factor in lead time at the beginning of your DMARC journey for this important step.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.