

CITY OF NAPA DEFEATS PHISHING WITH COMPLETE EMAIL IDENTITY SOLUTION

CASE STUDY



THE BUSINESS

Founded in 1847, the City of Napa is the seat of California wine country's most famous county and home to more than 76,000 residents. This arm of local government employs hundreds of full- and part-time employees, as well as managing a staff of volunteers. Departments include city police, fire, housing, utilities, parks and recreation, public works, water, and planning and development. For an organization that serves city residents with many employees and volunteers working from the field, not in an office, email is the main mode of communication. As such, email security is an important part of the City of Napa IT team's scope and charter.

CHALLENGE

City of Napa was looking for a partner to help them prevent spoofing and phishing attacks.

SOLUTION

Valimail Enforce and Valimail Defend give City of Napa domain protection and zero-trust inbox protection from phishing attacks.

RESULTS

The organization is protected with a solution they can rely on and that gives them time and resources back.

THE CHALLENGE

The City of Napa IT team accomplishes a lot because they know how to maximize resources. They find efficiencies and vet the most effective solutions to keep the organization running at top speed, securely. One area they thought they could optimize further was in email security – particularly domain spoofing and domain and user impersonation.

First up was protecting the cityofnapa.org domain from being spoofed – used without permission – to send email that appears to be from the City of Napa but isn't. The solution to domain spoofing is to implement DMARC with a policy of enforcement (p=reject or p=quarantine). Garrett Brown, Network Systems Administrator at City of Napa, is very familiar with the DKIM, SPF, and DMARC standards and was looking for a solution that could give his team some time back and get the job done while not disrupting email in the process.

Brown also wanted to protect employees from phishing attempts. Phishing attempts continue to rise and evolve, and the recent COVID-19 pandemic hasn't helped matters.

As he set out to evaluate potential services and products, Brown looked for a solution that would:

- Reduce staff workload and align with his budget
- Streamline the initial DMARC deployment job
- Provide ongoing DMARC management and protection
- Not disrupt legitimate email delivery
- Complement / integrate with the City's existing Microsoft 365 implementation.

"Users' inboxes are cleaner and we're protecting them from malicious actors trying to trick them. We worry a lot less about phishing now."

Garrett Brown,
Network Systems Administrator

SOLUTION

As a Microsoft customer, Brown began his research among the resources available to him through Microsoft. In doing so, he found a [blog post](#) on the Microsoft Security blog describing DMARC and offering a free Valimail DMARC Monitor account to Monitor 365 customers. He signed up for a free account and began his evaluation.

The instant visibility provided to him by DMARC Monitor prompted a conversation with the Valimail team about the company's fully-automated solution, Valimail Enforce. And, since protection from inbound phishing was also a priority, it made sense to look at Valimail Defend at the same time.

Using both Enforce and Defend, Valimail provided City of Napa with a custom domain analysis for cityofnapa.org which revealed suspicious email, including messages sent "from" City of Napa that actually originated from foreign countries; messages sent on behalf of the City from legitimate services the City was using, but which failed to authenticate correctly; and hundreds of inbound emails that had been sent from unverified domains.

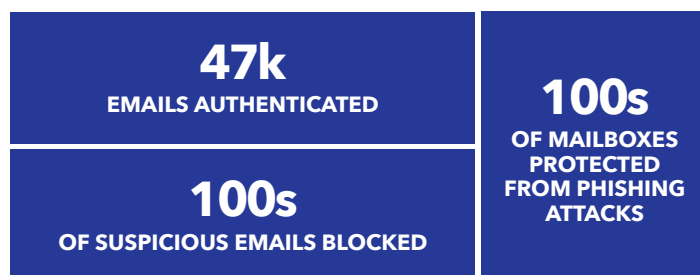
Brown and his team selected Valimail Enforce and Valimail Defend to complement their Microsoft 365 environment with a zero-trust sender identity layer. Throughout the evaluation, they found that the Valimail technology outperformed the competing solutions. In addition to the technology itself, Valimail's partnership with Microsoft played an important role in the decision. The Valimail products integrate with Microsoft 365 and Office ATP to work seamlessly together in the City of Napa's layered defense / defense-in-depth approach to security.

In doing so, the City of Napa team found they could fine-tune the anti-phishing policies in Office ATP enabling them to get false positives to near zero and optimizing employees' inboxes.

RESULTS

With Valimail Enforce implemented, the City of Napa achieved its goal of DMARC enforcement (p=reject) in five days. And with Valimail Defend, it has additional inbox protection from untrusted domains and untrusted senders.

Results delivered by Valimail since implementation:



Cityofnapa.org is protected from spoofing, which means that employees, volunteers, and residents can trust that email from the domain is legitimate. Employees are also protected from inbound phishing attacks. And the City of Napa IT team can focus on other priorities that keep the organization performing at top speed.



"Valimail buys us
back a lot of time."

Garrett Brown,
Network Systems Administrator



Valimail is a pioneering identity-based anti-phishing company that has been ensuring the global trustworthiness of digital communications since 2015. Valimail delivers the only complete, cloud-native platform for validating and authenticating sender identity to stop phishing, protect and amplify brands, and ensure compliance. Valimail has won more than a dozen prestigious cybersecurity technology awards and authenticates billions of messages a month for some of the world's biggest companies, including Uber, Fannie Mae, Mercedes Benz USA, and the U.S. Federal Aviation Administration. For more information visit www.valimail.com.