City National Bank Keeps Phishing Attacks At Bay Through Automated Email Authentication

The Business

Based in Los Angeles, City National Bank is the 30th largest bank in the United States, offering a full complement of banking, trust and investment services through 72 offices, including 17 full-service regional centers, in Southern California, the San Francisco Bay Area, Nevada, New York City, Nashville, Atlanta and Minneapolis. The bank was founded in 1954 and today has $43.8 billion of assets under management. Its 4,200 colleagues deliver highly personal service and complete financial solutions to entrepreneurs, professionals, their businesses and their families.

The Challenge

In addition to corporate email, City National Bank sends marketing emails and transactional notifications, such as banking alerts, to clients. It uses a number of third party services that send such messages on its behalf. These messages are essential for communicating with clients, building relationships, and cultivating loyalty and trust.

Phishing attacks put that critical communication at risk. Every day, City National was experiencing hundreds, if not thousands, of attacks from bad actors who impersonated its brand or misused its domain.

These attacks were intended to extract sensitive financial information, and some resulted in attempts at fraud on the bank. City National was concerned about data security, as well as the reputational damage that such phishing attacks could inflict. However, efforts to prevent the attacks through user education and awareness proved insufficient. “We had struggled for years, focusing on training users what to look for, what to click, what not to click, when not to download files, and that struggle really had limited results over time,”

In Brief

CHALLENGE: Stop email impersonation attacks and domain abuse directed against City National Bank and its clients and protect the brand by preventing damage to CNB’s reputation from phishing attacks.

SOLUTION: ValiMail’s Email Authentication Service automated the implementation, maintenance, and ongoing monitoring of DMARC authentication for City National Bank.

RESULTS: Fraudulent emails are completely blocked from employee and client inboxes, email deliverability to customers is improving, and the IT and security teams have greater visibility into its ecosystem of email senders and receivers. ValiMail has blocked 700k+ suspicious emails and authenticated more than 2M+ since getting to enforcement.

180 Montgomery St., 18th Floor
San Francisco, CA 94104

info@valimail.com
www.valimail.com

says Karl Mattson, Chief Information Security Officer for City National Bank. "It was over a decade that we were focused primarily on user education, with only marginal results."

> *"It's rare that cybersecurity enforcement, IT control, and business benefit are actually aligned and working together towards the same goal."*

City National was interested in a technical solution to phishing attacks that would provide better, more reliable results than a decade of training had done.

The Solution

ValiMail performed a complimentary analysis for City National Bank to better understand the extent of the problem. ValiMail put just one of the bank's many domains into monitoring mode and after 30 days, produced a domain visibility report that enumerated a large volume of suspicious emails emanating from a range of international locations.

"We had no idea," says Mattson. "We had no visibility to this activity happening." The report also revealed that many of the bank's third party email providers were not using DMARC-based email authentication and needed to be addressed.

"During this onboarding process, we noticed spikes in suspicious emails," says Steve Whittle, ValiMail's Head of Customer Success.

Faced with those numbers, City National Bank knew it had a problem and needed to take action. It extended the monitoring to the rest of its domains, then used ValiMail to implement DMARC, and ultimately moved to enforcement within a 90 day period.

> *"Our clients can be assured that when they receive an email from City National, it actually came from us. That has enormous benefits for the client and the trust they have in our communication."*

The ValiMail platform automates email authentication to ensure that senders of City National email are legitimate, whether those emails originate with the bank's own servers or one of its trusted cloud providers. It protects the bank's domains from being used by spear phishing attackers and authenticates third parties SaaS apps that send email on its behalf.

"ValiMail made the technical implementation really turnkey," says Mattson. "It was very simple and seamless." In addition to the technical implementation, City National Bank also used ValiMail to bring its internal teams, like HR, legal, and marketing on board with the authentication project, by detailing how email authentication impacted their work. For example, the marketing team benefits because implementing DMARC will enable City National Bank to increase the deliverability of marketing emails.

Results

City National Bank is already seeing an array of benefits from working with ValiMail. It has blocked 700,000 suspicious emails and authenticated 2 million emails since entering the enforcement phase. "The security benefits were immediate and obvious," says Mattson. "Our brand can't be used to conduct phishing campaigns. That type of brand damage really is taken off the table for phishing attacks against us and our clients."

> *"We had struggled for years, focusing on training users what to look for, what to click, what not to click, when not to download files, and that struggle really had limited results over time."*

Secondly, City National Bank has gained confidence in its relationships with third parties. Through greater visibility into who is doing business on its behalf, the bank has gained greater control over its ecosystem of email senders.

Finally, the company has gained greater confidence that its marketing campaigns are getting through—that its messages are getting heard and its marketing dollars are not being wasted. "This is a case where we're actually empowering the business. We're empowering marketing campaigns. We're empowering our brand's strength, and that's something that a CISO should take advantage of," says Mattson.