ValiMail

VTS Quells Phishing Attacks and Improves Deliverability Rates with Email Authentication

The Business

Headquartered in New York City, VTS offers an asset management platform for commercial real estate that helps owners manage and lease their properties. VTS is one of the hottest SaaS companies in New York, serving hundreds of customers who collectively manage 6 billion square feet on the platform.

The Challenge

Unfortunately, VTS became the target of spear phishing attacks directed at company executives, attempting to trick them into clicking on malicious links or download Trojan horse files. Fraudsters would impersonate the CEO in an attempt to get the CFO to wire money into an account controlled by the attackers. These phishing attempts tended to spike immediately after the company announced a new round of funding.

VTS had managed to avoid any security-compromising events despite these phish, and had educated staff on how to identify phishing scams, but it remained a risk: just one mistaken click could compromise the whole company. “Trying to train people to be aware of phish and not to click on them is a hard thing to do,” says Robert Lowry, Director of Security for VTS.

Separately, the VTS account managers and marketing team noticed that a large number of its emails were winding up in some customers’ spam folders — a serious deliverability problem. VTS uses email

In Brief

CHALLENGE: Stop spear-phishing attempts aimed at VTS executives and improve email deliverability to customers.

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

RESULTS: Spear phishing emails are completely blocked from executive inboxes, email deliverability to customers is improving, and the IT and security teams have greater visibility into “shadow email” services used by employees.

with customers as an integral, critical part of its product platform, sending notifications and daily dashboard updates. Each customer has its own unique VTS email alias that the company uses for all communications. “We use email as the oil of our operation,” says Lowry.

> *“We use email as the oil of our operation.”*
>
> Robert Lowry,
> Director of Security for VTS

The Solution

Email authentication had long been on IT’s security to-do list, but they didn’t know how to tackle it effectively. “It can be overwhelming if you never worked with DKIM, SPF, and DMARC,” Lowry says. “Besides, making DNS changes is tricky for companies like ours without a ‘sandbox’ to test changes in. There is always the worry that a mistake could take the company’s entire website (and our business) offline for hours. With DMARC automation by ValiMail, those concerns are now gone.”

VTS implemented DMARC via ValiMail as a proof of concept in November 2016, and immediately began collecting data on which email services were using the VTS.com domain name in their emails. The reports quickly uncovered about 10 legitimate senders: SaaS providers that VTS was actually using, such as Gmail, Salesforce.com, Mailchimp, Hubspot, and Greenhouse. A few less-known senders were tricky to configure for authentication. ValiMail worked with those SaaS providers to ensure that email from their systems would properly authenticate.

Within 90 days, the company had deployed DMARC fully and moved to “reject” mode, which directs all email servers on the Internet receiving non- authenticated emails with the VTS.com sender address to drop those messages.

“We wanted to wait on moving to reject mode until we were confident that we weren’t accidentally blocking an infrequent email sender that was actually a critical service,” Lowry said. “We now have that confidence.”

Results

Spear phishing attempts directed at VTS executives have stopped entirely. These attacks are now completely blocked by ValiMail, because attackers can no longer use VTS.com addresses in the From fields of their phishing messages—such messages get deleted before they are even delivered.

Over the past few months, ValiMail has authenticated more than 2.5 million emails for VTS and has blocked almost 150,000 suspicious messages, which it began doing when VTS moved to a “reject” policy.

> *“We wanted to wait on moving to reject mode until we were confident that we weren’t accidentally blocking a critical service. We now have that confidence.”*
>
> Robert Lowry,
> Director of Security for VTS

Deliverability problems for VTS customer and marketing emails have almost entirely disappeared. And the VTS IT team has greater visibility into which SaaS providers employees are using now, with a monthly report that lists all senders, whether they are approved or not, and how many messages they sent (or attempted to send) on behalf of VTS. Three or four of the legitimate services discovered by the ValiMail Authentication platform were services that the security team hadn’t been aware of beforehand.

“For me, it’s a relief to know that it’s taken care of,” Lowry says. “I’m certainly still going to monitor it, but it’s good to know that this problem is in the past and that ValiMail is monitoring it on my behalf.”