CASE STUDY

Aviation

Aviation Company Stops Phishing Attacks From Taking Flight

COFENSE

Cofense Case Study

AVIATION COMPANY STOPS PHISHING ATTACKS FROM TAKING FLIGHT

Background

A leading Australian aviation company wasn't going to wait for disaster to strike before strengthening its phishing defense.

"We were lucky enough to have forward-thinking management," said the General Manager of Technology and Innovation. "We hadn't suffered losses from phishing, but our board of directors grasped the threat, so they instructed us to launch an anti-phishing program."

Executive Summary

- Leading Australian aviation company with high public profile
- Board of directors mandated an anti-phishing program
- User susceptibility has dropped in simulation training
- Better still, employees are reporting real phishes to security teams

He added, "Because we're in aviation, we have a lot of visibility. If a phish led to a security incident, our name would be in the headlines. We need to protect not only our data but our reputation."

Solutions and Results

The company implemented Cofense PhishMe™ to help users spot phishing and Cofense Reporter™ to enable one-click reporting. With Cofense PhishMe, program administrators are able to simulate phishes and educate users on how to recognize them.

> *"We identify employees that may be vulnerable, give them the training they need, and report this up to the board of directors."*
>
> **— General Manager of Technology and Innovation**

When the company announced the program, it clearly explained the goals and methods. The announcement also educated users about phishing, including a sample simulation. This transparency paid off. From the first round of simulation training to the next, user susceptibility dropped by 10%. And users who clicked an embedded link dropped by 9%.

"The results to date are encouraging," said the General Manager. "We know that our metrics are affected by the complexity of simulations, the emotional levers they pull, and the user groups we target. As we continue to move forward, we'll be basing our simulations on attacks we've actually seen."

Next Steps

He plans to further customize simulations by team and location, using Cofense PhishMe's adaptable templates. "We understand that the people and organizations behind these attacks are smart," he said. "They mimic trusted people and brands and refine their deployment methods to evade automated safeguards. You can never become complacent."

> *"Our security teams are stopping attacks that employees report."*
>
> **— General Manager of Technology and Innovation**

Now that Cofense Reporter is deployed across all teams, the company is better able to promote and track email reporting. "To measure success, we first look at the number of users not opening and/or reporting potential threats," said the General Manager.

"Next, and possibly more important, we examine the number who report after they may have inadvertently opened an email. Basically, we identify employees that may be vulnerable, give them the training they need, and report this up to the board of directors."

Underscoring the point he added, "Initially, some people at our company thought the program was unnecessary. They believed our automated systems and firewalls gave us enough protection. This was dispelled when security professionals fell prey to Cofense simulations."

Even better, "Our security teams are stopping attacks reported by employees."

For more information about Cofense's award-winning phishing defense solutions, please email info@cofense.com.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175