

Cofense Case Study

*Generali Turns the
Tide in the Fight
Against Phishing*





Background

With some 61 million customers, Generali is Italy's largest insurance company and one of the world's most recognizable financial services brands. As part of a comprehensive overhaul of its security programs, Generali decided to focus on phishing awareness.

"The number of attacks targeting us was increasing," said Francesco Nonni, Head of IT Operations & Security Risk at Generali. "We were seeing phishing attacks of all types and employees weren't sure how to respond."

Solutions and Results

Generali chose to use **Cofense PhishMe** and **Cofense Reporter** to teach employees to recognize and report evolving phishing threats. Why Cofense? "You offer so many different templates for phishing simulations based on real threats," Nonni said. "Also, the solutions are easy to implement."

"With Cofense PhishMe and Cofense Reporter, we can easily gather statistics on phishing resiliency and susceptibility," he added. "By sharing results across the company, we created a shared understanding of our readiness and where to improve."

"Employees are now helping security teams stop real phish."

— Francesco Nonni, Head of IT Operations & Security Risk, Generali Group

Are employees getting the message—are they reporting phish? "Absolutely yes," he said, "both in simulations and in real life. Our simulation results are trending in the right direction—reporting is increasing and susceptibility is dropping. We use the Cofense benchmarks for our industry specifically and across verticals, so we can compare our level of awareness and exposure. We know where we stand and are able to put it in context."

Even better, "Employees are now helping security teams stop real phish," he said. "Now it's easy to report an email that might be part of a real attack. One click of Cofense Reporter is all it takes. When that happens, our security operations teams are able to respond faster."

Executive Summary

- Top global insurance company with over 70K employees in nearly 50 countries
- Began to bolster phishing defense as part of broader security upgrades
- Implemented Cofense PhishMe™ and Cofense Reporter™
- Phishing awareness and reporting are both improving as the company educates employees across countries, languages, and cultures
- Best of all, "Employees are now helping security teams stop real phish"

Implementation & Peer-to-Peer Advice

Once Generali's phishing defense program was up and running, Nonni launched their first simulation. While the solutions worked seamlessly, the results showed that the company had its work cut out. "A lot of people clicked," he said, "and reporting levels were low. That wasn't surprising, since it was our first campaign." There was a silver lining, though. Armed with data, Nonni was able to further underscore the risks of phishing and generate more support from corporate leadership.

"We've started to model our simulations after attacks that we receive."

— Francesco Nonni, Head of IT Operations & Security Risk, Generali Group

He recently launched a simulation campaign in 11 countries across Europe and Asia. "The campaign is still ongoing, but the results are encouraging," he said, "We're learning that click rates often vary from country to country. We prepared content on a more global level and asked local offices to translate to their language and manage the rollout to their teams. Depending on the country and the culture, the local communications department might try different tactics to promote the awareness program and keep employees engaged."

Nonni makes certain to share progress with his counterparts throughout the company. "We have a security council representing our various regions and disciplines," he said. "By showing proof that awareness and reporting work, we can establish them as best practices."

As a global financial services leader, Generali continues to see high volumes of phishing emails—real attacks that trained employees are reporting more consistently. "We see a lot of spear phishing attacks targeted to our managers, along with crypto-lockers, credential phish, and business email compromise. We've started to model our simulations after attacks that we receive, for example, phishing emails with malicious attachments."

Nonni mixes basic phishing scenarios with more complex emails. "As the program develops, we're targeting some of our simulations by location, department, and function," he said, preparing Generali for the most likely threats. "As the global program manager, I personally hear from employees throughout the organization. Increasingly, they understand the importance of staying vigilant and reporting what they see."

"We've truly begun to build a stronger culture of security," he added. "A big part of that is employees who embrace their roles as defenders of the organization."

Nonni plans to run more large-scale campaigns in multiple countries, with greater customization reflecting cultures, operations, and more.

His advice to anyone launching their own phishing defense program: "Don't be discouraged by initial results. It's important to know where you stand and identify where to improve, in particular critical departments," whose employees have greater access to sensitive data or can authorize financial transactions.

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

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization-wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.



W: cofense.com/contact T: 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175