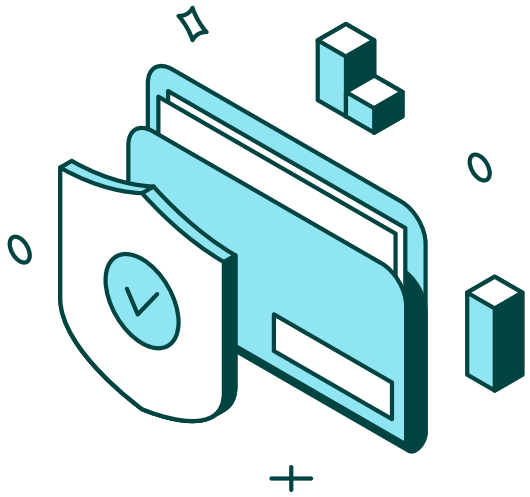
FORTRA

CASE STUDY

Sector:
Education

Canadian University Reduces Data Breach Potential And Strengthens Security Culture Through An Effective Awareness Training Program



A culture of open information sharing is an ideal many academic institutions strive for. This inclination is also why students and employees at universities and other higher education providers are increasingly targeted by hackers and, more than many other industries, fall victim to phishing attacks.

This reality means security awareness training has also become a much more urgent priority for IT teams at universities in recent years. Lots of sensitive information is stored on their systems and accessible through various networks, including proprietary research data, financial information, physical security operation information, and personally identifiable information (PII) for all individuals logging in daily.

Add to that the large number of courses offered exclusively online, and it's clear cyber security awareness needed to be a part of the organization's cultural fabric moving forward. "Students are practically born with technology between their hands, but they don't have the information about security," add the Chief Information Security Officer (CISO) of a major Canadian university who chose Fortra's Terranova Security as their ally in securing their digital ecosystem.

By doubling down on strong cyber security awareness practices, the difference at both the student and staff levels was night and day.

THE CHALLENGE

Developing a Cyber Security Culture in a Non-Mandatory Training Environment

At the time of this writing, the university was home to 40,000 students and nearly 7,000 faculty and staff. Due in part to its commitments to provide students access to the best teaching and the freedom to complete research of the highest quality, many courses are taught and presented in two different languages.

To instill cyber security trust across the campus, from in-person interactions to online course environments, the university set out strategic objectives to govern long-term operational decisions. Many of these goals would be challenging to attain without strengthening the organization's security posture.

For example, university members were frequently receiving phishing emails that bypassed standard barriers, revealing a critical need to educate the entire university community on the growing threat.

The proposed process included:

- ☑ Educating and training faculty and staff
- ☑ Educating and training the student population
- ☑ Ensuring that strong cultural norms were put in place

According to the institution's CISO, what made the challenge even more difficult was that cyber security training was not mandatory on campus. In some cases, people were "reluctant" to participate in simulation exercises, due to fear of repercussions if they failed a phishing email simulation.

As a result, entire campus departments would reject simulation testing deemed "too realistic" for its potential to impact daily communications negatively. However, as the CISO put it, "We have to give people the right to make a mistake."

The solution entailed easing those anxieties and implementing courses, simulations, and other educational initiatives that would inform the university's end users and entice unenthusiastic parties to participate.

THE SOLUTION

Launching Customizable Courses, Campaigns, and Phishing Assessments

The university's CISO, along with the IT team and other stakeholders, implemented a complete Terranova Security solution that included:

- **Multiple end user training courses** geared towards changing unsafe online behaviors
- **Training campaign monitoring** through the Security Awareness Platform
- **Performance measurement** with in-depth reporting and a customizable phishing assessment

Modules from the Terranova Security course library were deployed first and presented to the university campus in a series of campaigns. The university chose 12 modules for their diverse audience based on customization features which is crucial to the training program's success. Security team leaders focused on deploying training courses that aligned best with their existing culture. "Until last year we were focusing on our personnel. Now we are targeting the whole community, including the students," said the CISO.

The goal was to record strong participation in a security training campaign rolled out to staff and faculty first. The training was presented in a safe environment, leveraging module content that all generations could connect with. As a result, participants engaged freely with the training courses without fearing negative consequences.

The university also leverages the Terranova Security Awareness Platform, which allowed program administrators to manage their campaigns and course deployments, with near real-time reporting on course completion metrics. Assessment difficulty levels were also customized to adapt to a wide variety of knowledge bases and aptitudes.

"They call me Mr. Phishing. They see me and say, 'you didn't get me this time!'" *– University CISO*

THE RESULTS

Significantly Improving Security Awareness Training Participation Rates

In a security awareness training program where user participation is not mandatory, boosting voluntary participation numbers is a top priority. After deploying their multifaceted training program, the university saw their **participation rate increases 5% among staff and faculty, a significant push towards their ultimate goal of 15%.**

The university was encouraged by these initial results, expecting it to help the campus reach the desired state of having cyber security ambassadors encouraging peers to remain vigilant. As the university CISO said, "when there's a fire, you don't need everyone to know how to fight it. You need at least one good person to champion telling everyone to get out of the building. The 5% offered hope for the creation of ambassadors."

Following the university's student training campaign, the CISO reported **reaching 17,000 out of the estimated 40,000 students total – a participation rate of more than 42%.**

Having benefitted from the training, learning management and assessment solution provided by Terranova Security, the university CISO said he plans to continue to collaborate with the company's cyber security experts. By working together, both parties can further optimize the training solution based on key metrics and campaign results.

CASE STUDY SUMMARY

Sector: Education

Challenge

Provide university faculty, staff, and students with effective cyber security awareness training in multiple languages to reduce human risk levels and ensure employees avoid falling victim to phishing threats.

Solution

Implement a multilingual Terranova Security awareness training solution and phishing assessment to educate end users participating both on-site and virtually.

Results

With Fortra's Terranova Security as their ally, the organization was able to:

- ☑ Increase global participation by 5% overall
- ☑ Reach 17,000 out of the estimated 40,000 students
- ☑ Make significant progress towards the goal of 15% global participation

READY TO STRENGTHEN YOUR INFORMATION SECURITY?

Book your personalized walkthrough!