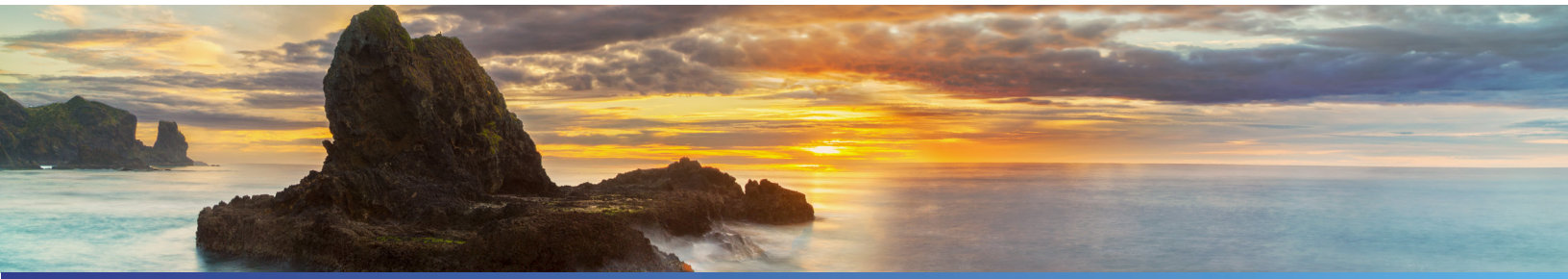

Harpooning the whalers for Les Mills International

Secure email management solutions from SMX, including inbound email filtering and the custom rules engine, stopped spam, phishing and whaling attacks almost instantly for international fitness industry giant Les Mills International, with the custom rules engine providing an essential extra layer of defence against further cyberattacks.

Spear phishing and whaling attacks, where social engineering and email spoofing techniques are used to steal money or confidential information from businesses, are increasingly common and pose a significant email cybersecurity threat for New Zealand companies. No business, big or small, is safe. Just ask Les Mills International.

Les Mills is a family owned and operated business. Founded in Auckland in 1968 by four-time Olympian Les Mills Snr, today the company employs a core staff of 400 globally (including 150 in New Zealand). Les Mills workouts are licensed by more than 17,500 club and gym partners in 100 countries.

With most of its business overseas, Les Mills has adopted a 'cloud-first' approach, says Les Mills International General Manager of Technology, Steve James. Nearly every technology application the business runs is in the cloud.

"Les Mills is a very fast moving company. Our cloud-first strategy means we can quickly and easily stand up a fully mobile, serviced office with an internet connection anywhere in the world."

When Microsoft released its cloud-based Office 365 service, Steve says Les Mills was probably one of the first organisations in New Zealand to move its email from Microsoft Exchange to the new service.

"We moved to Office 365 and thought spam would be dealt with as part of the service, and to a degree it was. But then, phishing and whaling emails started creeping in. They were very targeted and well disguised – there were only very small clues that things weren't quite right," Steve says.

The company was using email to manage its revenue flow, opening it up as a target for cybercriminals to subvert its internal processes.

> "Since the SMX custom rules engine has been in place, we've had no issues. We've gone from receiving a high volume of targeted whaling and phishing email to virtually nothing. SMX said they could solve our issues, and they have. This is one of the best cases of 'it's as easy as flicking a switch' as I've experienced. My pain is just gone."

Steve James
General Manager of Technology
LES MILLS INTERNATIONAL

By late 2015, Les Mills' senior executives were under heavy phishing and whaling attack. A sophisticated whaling attack on the CFO was the final straw.

Picture the scene: Les Mills International's CFO received an email, supposedly from the CEO, instructing him to transfer USD$192,000 to an international bank account. The spoof email looked completely legitimate, down to the sender's email address displayed in the CFO's mail client looking 100 percent correct. The incoming email contained no malware or links to malicious sites that would trigger the multiple security filters already in place.

The CFO only became suspicious when a final email response from the CEO prior to the funds transfer was written too formally for 'guys who've known and worked with each other for years and are quite casual in their emails.' The CFO checked in with the CEO and the scam was fortunately derailed.

Steve and his team tried to configure the Office 365 rules to stop the spam and whaling emails, but it simply wasn't enough. He tried talking to Microsoft as well to see what else could be done but couldn't find a solution.

The emails kept coming and the chief executives kept forwarding them to Steve and his team. It was causing them no end of pain.

"We considered other options, including going back to a physical filtering device but quickly ditched that idea – it seemed so far removed from our cloud-first strategy that we didn't want to go back there," Steve says.

"We also engaged a security consultant and asked if we were doing something wrong to be targeted in this way. The simple answer was, 'no'."

Finding a better way

In early 2016 Steve turned to Thom Hooker, Co-Founder and CTO of SMX, for advice.

"I've known Thom for a very long time, so I'm familiar with SMX and I knew how the product worked. But I just assumed that SMX wouldn't be compatible with Office 365. I called Thom for advice anyway," Steve says.

"I told him what was happening and Thom said, 'our product can fix that'."

Les Mills runs a tight ship and Steve says he initially met some resistance: "I did get a bit of pushback from the CEO and CFO around SMX being yet 'another thing you're asking me to buy' but Thom said, 'why not just give it a try – no obligation.' So we did."

SMX was still developing a whaling module for its custom rules engine, so Steve signed Les Mills up to initially trial the SMX inbound email filtering service, on the understanding the company would add the custom rules engine when the whaling module was ready. The trial commenced in March 2016 and integration with Les Mills' Office 365 service was no problem.

SMX is essentially a premium email filtering add-on that complements and enhances Microsoft Office 365. SMX's robust, technically sound process makes a Microsoft Office 365 + SMX solution fast and easy to implement.

Les Mills' Office 365 service was configured to only receive email from SMX's IP ranges, guaranteeing that all inbound email – Les Mills typically receives between 10,000 to 12,000 emails a day – would be delivered, filtered and cleaned by SMX, to users' inboxes globally.

Steve says the results were immediate: "We trialed it and it just worked."

"It was a case of 'just turn it on.' We didn't notice any user impact – but we noticed immediately that things calmed right down."

Although the really targeted whaling emails didn't stop entirely at that stage, SMX was able to review suspicious emails that did slip through and adjust the rules to stop them.

When the custom rules engine whaling module launched, Les Mills was one of the first customers to use it.

The whaling module relies on email header inspection. This feature of the custom rules engine allows customers to restrict the number of addresses senior executives can send email from. Les Mills created a list with the details of all staff

who might have their identities spoofed, as well as all staff who might receive whaling emails (e.g. senior executives, board members, finance team). The custom rules engine whaling module looks for emails that are spoofing nominated executive names and if the Reply-To or From headers aren't from allowed addresses it side-lines or rejects the email.

Les Mills is also using the 'block executables' custom rules engine template, which helps protect against CryptoLocker-type attacks. This rule stops common executable attachments from passing through the SMX filters. Any required exclusions can be added as exceptions to the rule.

Les Mills' email users are alerted to any potential cyberattack emails by a message appended to the email by SMX.

"Since the custom rules engine filters have been in place, we've had no issues," Steve says. "We've gone from receiving a high volume of targeted whaling and phishing emails to virtually nothing. Thom said SMX could solve our issues, and they have.

"This is one of the best cases of 'it's as easy as flicking a switch' as I've experienced. My pain is just gone."

Reporting hits the mark

SMX's reporting capabilities were a factor in Les Mills' decision to proceed with a trial. Steve says being able to provide evidence of the effectiveness of the solution to the executive team was valuable.

"Microsoft provides reports but not with the level of detail SMX does. Reporting from SMX is very good," he says.

Initially, Les Mills wanted SMX to provide reports and advice on email security trends every one to two months, but these days reporting is more ad hoc. "It is important that we can go back and see how effective the SMX solution has been, if someone asks for proof. But because it's a problem that's gone away, we don't report as much anymore."

Signing up for the long haul

For Steve, continuing with SMX was a no-brainer following the successful trial. "It was very easy for me to say to the executive team, 'let's sign up,'" he says.

"We hadn't budgeted for SMX but the ROI is worth it. The ROI is huge. If our CFO had been caught out in that whaling attack, the amount of money we could've lost is significant."

For less than the cost of two flat whites per user per month, Les Mills now has a robust cloud-based email filtering solution, effortlessly integrated with its Office 365 service, along with the extra, essential layer of protection against cyberattacks and malware offered by the custom rules engine. SMX is now part of the application suite Les Mills provides across all its offices.

If the executive team ever questions the need for SMX, Steve points them to the total absence of spam and cyberattacks as justification the investment was worth it. And they have to agree, he says.

> "We rely on people who are experts in their area – and when it comes to email security SMX just knows what to do."
>
> **Peter Darlington**

Trusted partnership

For Steve, a key benefit of Les Mills' partnership with SMX is being able to forget about email security because he knows SMX has it under control.

"SMX provides great email consultancy," Steve says. "Our IT team is pretty advanced – but SMX are the email experts. I like that they are genuinely passionate about it. They live and breathe what they do – just like we do with fitness.

"I have a lot on my plate and I have to choose what to prioritise. For a while the whaling issue was all-consuming – but because SMX has dealt with the email so well, I genuinely don't feel I need to worry about it anymore."