Email Protection
Overview

The Ministry of Education has partnered with cybersecurity provider Proofpoint, a global leader in email security, to provide schools with a greater level of protection. N4L will be supporting the Ministry to deliver this new Email Protection to schools and kura.

What are the benefits of this new inbound Email Protection?

- There's **no cost** to the school, as it's fully funded by the Ministry of Education
- **Schools will have better protection** from spam and phishing attacks with an enhanced level of email security
- **It will complement** a school's existing Microsoft or Google email service
- **Peace of mind** that schools will be supported by a highly trusted, industry-leading email solution
- **Improved productivity** as threats and spam are detected before they reach inboxes
- We'll be able to **respond to email-related incidents more quickly** and efficiently in future
- **Proactive blocking** of Business Email Compromise scams, phishing attacks, ransomware and advanced malware before it reaches a school's inbox

Why do schools need Email Protection?

+ As the number of major cyber attacks is steadily increasing, some cloud-based email solutions only offer limited protection, letting through spam, phishing, email fraud and ransomware threats.
+ Security threats in emails are becoming increasingly sophisticated. A couple of common scenarios we see are:
  - Behavioural threats such as bullying or impostors.
  - The subject and content can be very specific and targeted, for example an email could be aimed at principals requesting access to systems, approvals to pay bills, etc.

How does the new Email Protection platform differ from what Google or Microsoft currently offer schools?

Google and Microsoft provide security protection by default but advanced email protection requires additional expertise to implement. Our new service complements Google and Microsoft tools - delivering consistent and recommended email protection settings to secure all school networks. This reduces any inconsistencies in the configuration of these services.

What will this new solution provide schools?

+ **Email firewalling**
+ **Virus protection**
+ **Spam detection**
+ **Malware defence**
+ **Attachment defence**

Please note: The settings will be the same for ALL schools, no customisation is offered.

Emails that don't have a security risk will be delivered to schools with the following cautions:

1. Emails with embedded URLs will be checked to ensure the validity of the site associated with the URL. If the link is safe, the website will open when the email recipient clicks on the link. If the website isn't safe, the site will be blocked and the user will see a message advising them that this is an unsafe site.
2. Emails will be scanned for offensive language and a warning added to the subject line of the email. Any existing rules a school has in place to screen for offensive language will still remain in place.
3. Emails with password protected files will be delivered. A warning will be placed on the email cautioning the recipient to exercise care when opening the email.
4. Any emails with attachments that exceed 50Mb will not be delivered, and both the sender and recipient will be advised of the non-delivery.
5. Emails that have an executable file attached will have the executable file removed, but the rest of the email will still be delivered.

What's required to transition to the new platform?

+ Configuration changes to a school's DNS records that manage email
+ Configuration changes to a school's Microsoft Office 365 or Google Workspace to accommodate the effective relay of email

Which schools are excluded from the offering?

This new service is available to all schools with Office 365 or Google Workspace. If a school has an on-premise email service, they will need to discuss the set up of Proofpoint with N4L.

What's the process for schools to get Email Protection?

1. N4L will send schools an initial communication about the service, which will include the Agreement to Proceed (ATP).
2. Schools complete the ATP, giving permission to N4L to implement the service. They will also be asked to confirm whether their IT provider will be responsible to perform the work.
3. N4L will contact the school's nominated IT provider and provide instructions to implement Email Protection to the school's existing email service.
4. N4L will schedule a date for implementation with the school and the nominated IT provider, and will ensure an N4L engineer is available should there be any challenges.
5. Once the implementation has been completed, N4L will send a communication to the school advising them of the changes that they can expect to see.

We've put together some FAQs which you may find helpful.

If you need any further information, please call our Customer Support team on 0800 LEARNING, Monday to Friday 8am-5pm.