Supercharge your cybersecurity with Email Protection

Email is the most common way people are targeted for online attacks, with phishing and other email-based cyber threats on the rise. It's important that you do what you can to protect your kaiako and ākonga from these threats, and that's why N4L is supporting the Ministry of Education to deliver a fully funded email protection solution to all eligible schools and kura.

How does Email Protection boost my existing email security?

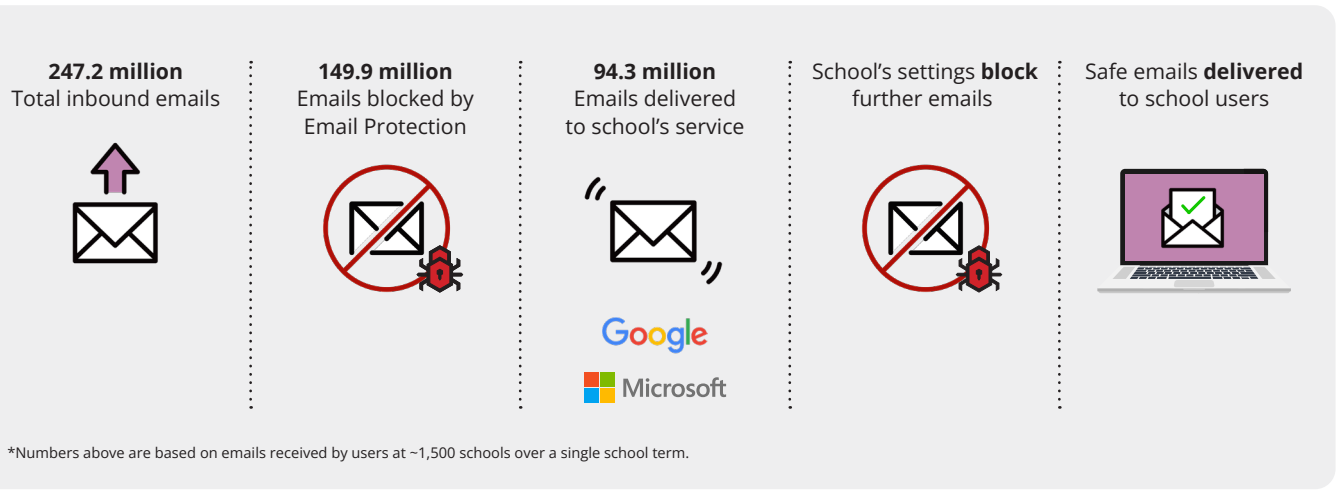
- **Builds on your Microsoft or Google email service** by adding an additional layer of security, which provides advanced threat detection and blocks malicious emails before they enter inboxes.
- **Proactively blocks** business email compromise scams, phishing attacks, ransomware and advanced malware.
- Should an email-related incident arise, you'll get a **faster, more efficient response** from our team.

Have visibility of blocked emails via MyN4L

The Email Protection tool within MyN4L (our self-service platform) lets you see your blocked emails in quarantine and safely release any legitimate ones - ensuring important emails are never missed.

The platform is provided by Proofpoint, a global leader in email security, so you can have peace of mind knowing that your school has advanced protection from malicious emails - and that you're safeguarding confidential and sensitive information to help protect the privacy of kaiako and ākonga.

How Email Protection works



*Numbers above are based on emails received by users at ~1,500 schools over a single school term.

1. When emails are sent to school addresses, our Email Protection platform intercepts these to scan for security risks and filter out malicious emails.
2. The remaining emails are passed on to the school's Google or Microsoft email service, which filter out further emails based on their respective settings.
3. Safe emails are delivered to school users' inboxes.

It's quick and easy to set up

This service is available to all state and state-integrated schools and kura with Office 365 or Google Workspace. Schools and their IT providers can set it up, **but we're able to help with this if a school needs it**. Once your eligibility is confirmed, we'll send the principal an Agreement to Proceed (ATP) form, from which:

1. The principal completes the ATP, giving N4L permission to implement the service.
2. We contact your school and nominated IT provider (if you have one) with instructions on implementing Email Protection.
3. Your school or IT provider make configuration changes to your DNS records that manage email.
4. We schedule a date for implementation with your school and nominated IT provider, and will ensure an N4L engineer is available should there be any challenges.
5. Your school or IT provider make configuration changes to your Microsoft 365 or Google Workspace.

There will be no impact to your school's internet or email systems while Email Protection is put in place, and **we'll be there to guide you all the way should you have any issues with any of the steps above**. If you don't have an IT provider and need support to implement the service, please let us know.

Email Protection in action - a real example

In August 2023, a large phishing campaign sent emails to multiple schools. The pattern of the campaign meant we could analyse its distribution for both Email Protection schools and those not using the service.

For those using Email Protection, we were able to:

- Ensure no further clicks of the phishing URL were possible.
- Block further emails containing the phishing URL.
- Notify schools which users clicked the URL, meaning they could reach out to these users and review their login history for suspicious logins, indicating a successful phish.

Our support extended beyond the school gate, with these measures applied regardless of whether a user was on the school network or another.

Our response for schools not using Email Protection was far more limited:

- We blocked the phishing host on school firewalls, but the link could still be clicked on another network, e.g. a mobile phone using data.
- We were unable to block further emails with the phishing URL. We notified schools, who had to put their own measures in place.
- We could see that the phishing URL had been clicked at a school, but couldn't identify the specific users. that had done so.

You can find more information on Email Protection in our FAQs on Support Hub. If you have any questions or would like to speak to someone, please contact us on support@n4l.co.nz or **0800 LEARNING**.