Defend your email from human-activated risk

Encourage protective behaviours

Whether your systems are on-premises or in the cloud, **more than 90% of cyber compromises start with "human-activated risk"**: an email-related action triggered by a real person opening a suspect attachment or clicking on a malicious link.

Organisations therefore need to consider user behaviour as part of a holistic approach to email security, and how it can be informed, guided, and improved.

Northdoor email security solutions are designed with human behaviour in mind. Suspicious emails are delivered with a banner headline to highlight and explain the risk, offering a real-time teachable moment. And central monitoring enables IT and business managers to identify weak spots and vulnerable users, helping to plan suitable preventative action such as dialling up the security measures and offering additional training.

Get in touch today to arrange a demonstration or full proof-of-concept for Northdoor email security solutions.

Comprehensive email defence

No email security system is perfect. In the past, on-premises email servers were loaded with specialist software designed to save us from ourselves—and with some success, too. As companies moved email online, the technology has moved on to include sophisticated cloud-based AI filtering, management, and monitoring.

But technology is just one element in email security. Your overall security posture and the practical impact of your security policies will also impact how you manage human-activity risk. Very strict security tends to increase both IT administration and friction for users, as well as potentially taking away the user's sense that they are responsible for security. At the other extreme, lax security standards will expose the organisation to unacceptable risk, including significant financial and reputational damage.

Northdoor email security solutions take user behaviour into account, and are designed to engage your users as active participants in your cyber defences.

Backed by expert advice, solution design and implementation services, and ongoing support, Northdoor email security solutions:

- Help users resist phishing attacks, attempts to compromise email accounts, and other inbound threats
- Monitor outbound email helps to mitigate misaddressed emails and malicious exfiltration of valuable corporate data
- Protect users and the organisation with highly secure email encryption, at a level depending on the nature of the business and the appetite for risk.

northdoor
Store IT ◦ Protect IT ◦ Use IT

Enrolling users in cyber defence

Over time, our solutions help to educate users and make them an integral element of your cyber defence strategy.

As you would expect, Northdoor email security solutions integrate fully with your existing email infrastructure and minimise the administrative burden on your IT team, while offering comprehensive audit and reporting capabilities to help meet regulatory requirements. The solutions offer both cloud-based and on-premises deployment options.

Northdoor email security solutions take user behaviour into account, and are designed to engage your users as ***active participants*** *in your cyber defences.*

Northdoor value-add services

Northdoor understands both cyber security and the needs of business users to have a friction-free experience with email. We work with leading global vendors of email security technology to design, deploy and support solutions that are tailored to the specific requirements and objectives of each of our clients.

When it comes to deployment, the first step is to complete a full email risk assessment, which will help us work with you to define the appropriate security policy.

From full email lockdown, encryption, and quarantine to simple alerts and notifications of risk, Northdoor can advise on policies that we know work well for other clients.

Get in touch today to arrange a demonstration or full proof-of-concept for Northdoor email security solutions.