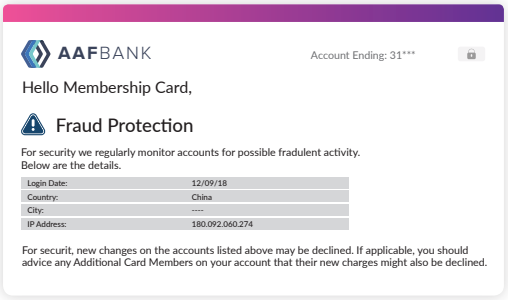
What Makes INKY Different?

INKY Phish Fence is a mail protection gateway that uses sophisticated AI, machine learning and computer vision algorithms to block deep sea phishing attacks that get through every other system. INKY stops phish before it reaches your users!

INKY has three levels of classification.

INKY's clean/unusual/malicious model means that malicious emails can be quarantined while merely suspicious or unusual mails can be delivered with a user-friendly warning banner than explains what is wrong.

INKY thinks this message may be fradulent.



INKY automatically detects zero-day brand forgeries.

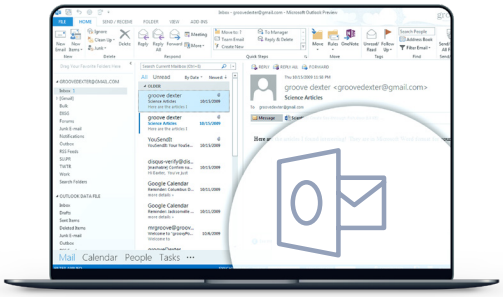
INKY uses computer vision algorithms to recognize brand-indicative imagery, HTML, text, colors, etc. INKY can even spot logo-like text (logotypes) where there is only text and no image.

INKY catches zero day spear phishing attacks.

Social graph-based sender profiling and sender anomaly detection algorithms make INKY spot these "Business Email Compromise" (BEC) attacks. These emails often lack URLs or attachments, so they elude detection by most mail protection systems.

John Ridder

Employee



Easy to deploy and fully scalable.

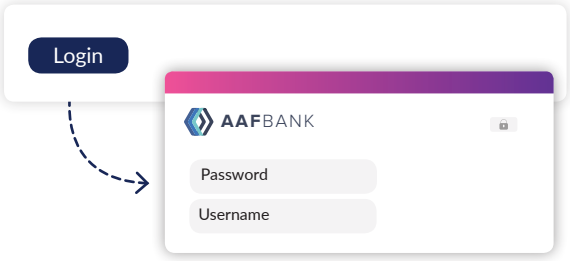
Some newer anti-phishing solutions rely on EWS or REST API access to the Exchange tenant. This method scales poorly, adds latency to mail delivery, creates security concerns (since the service requires admin access to the Exchange tenant), and doesn't integrate with Exchange Mail Flow Rules for quarantining malicious emails. In contrast, INKY deploys inline, integrated with Exchange, as part of the normal mail flow. This means INKY supports quick deployment, staged roll-out to users by groups, and the ability to quarantine, folder, or drop malicious email using standard Exchange controls.

Real Time Threat Detection

INKY supports policy-based URL rewriting to prevent users from clicking through malicious links. The malicious link check occurs both at message delivery time and in real-time when the user clicks through, meaning click-throughs are protected with up to-the-minute threat information.

Deep Link Inspection

As well as looking up URLs in known threat feeds, INKY performs deep link inspection. This means INKY simulates a click through to the linked site and examines the destination page for evidence of phishing and other security risks.

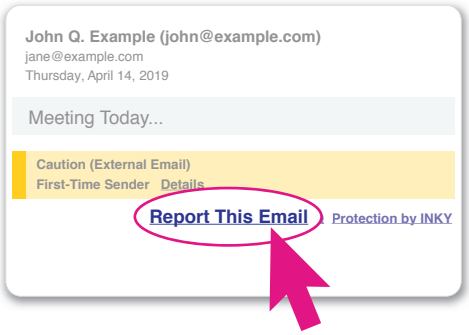


No Installation Required

INKY is cloud-based solution and can be completely installed in 1 - 2 hours with no client software installation needed.

Report Phishing Attempts

INKY adds a “Report this Email” link to every email, allowing end users to report spam, phish, and other problematic emails from any endpoint device, with no special software (i.e, from any mail client).



HTML Sanitization

INKY parses and sanitizes all HTML email to remove cross-site scripting (XSS) attacks. By default, INKY upgrades plain text emails to HTML emails, to support link rewriting in plain text emails.

Advanced Reporting

The admin reporting dashboard shows which threats have been identified and blocked. Admins can run time-bounded queries to view what threats have been encountered and blocked, and can drill down into individual messages.