Internal Mail Protection

INKY Internal Mail Protection is an add-on service to the industry leading INKY Phish Fence and protects your organizations internal email traffic. Utilizing the core functionalities of INKY Phish Fence, Internal Mail Protection provides robust detection and remediation capabilities for email security threats originating within the organization.

Features

Internal Sender Profiling and Social Graphing

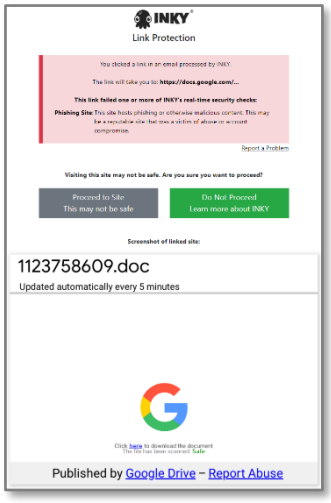
As your users send mail internally, INKY builds dynamic 'profiles' or 'behavior models' of the originating sender. As the models grow, INKY uses anomaly detection techniques to filter out and block impersonation attempts originating from outside your organization.

INKY observes the incoming email and builds an index/model of:

1. Email addresses typically used by the sender
2. The display name for each user (i.e., Tyler D. vs. Tyler Durden)
3. Location the user primarily sends mail from (home/office/mobile)
4. Device users typically send mail from (mobile device, Mac/PC, or tablet)
5. The email client used by each sender (i.e., Outlook for the PC, Apple Mail client for iPad/iPhone, or Gmail app)

Active Link Protection

INKY's link protection is NOT your traditional Real-time Blackhole List (RBL)/link checker. Real-time targeted zero-day threats NOT reported to the RBL's are caught daily.



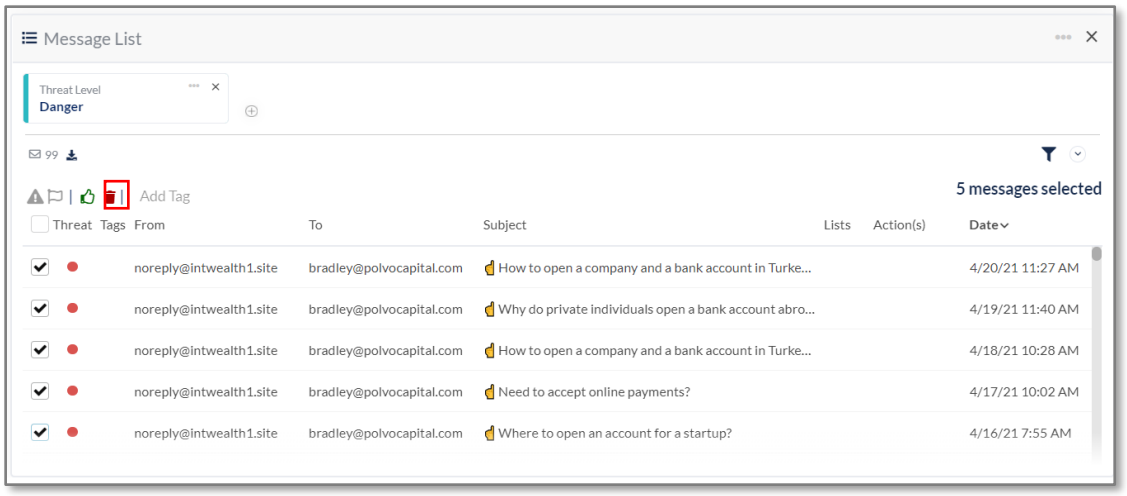
Each time a link is clicked, INKY analyzes it in real-time. NOT afterward like a TRAP or API solution.

Confusable domains, misleading links, cross-site XSS URL's, and malicious redirects are identified and filtered out. Much like the brand impersonation models, INKY's link protection knows where an email link should be taking you. INKY's detail screen will display the actual destination of the URL link in a safe preview screenshot isolating the user from the malicious web page.

Internal Mail Remediation

Remediation Access within INKY allows administrators to remove messages from their end-user's Office 365 and Google mailboxes for emails originating outside their organization. With Internal Mail Protection by INKY, admins now have the capability to not only remove external emails but internal emails as well. This process is done from the same INKY Dashboard your admins currently utilize and ensures they have the tools needed to protect against lateral movement within your internal email infrastructure.

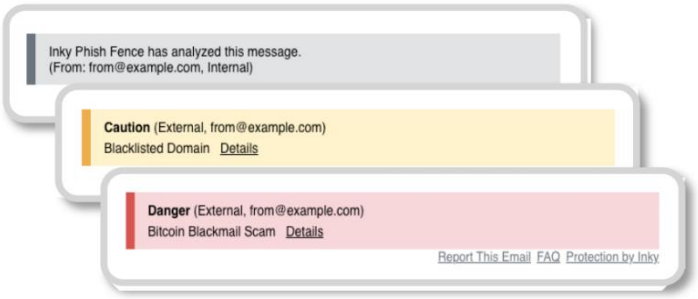
Internal Mail Protection



User-Friendly Warning Banners

INKY's unique HTML based warning banners are a key visual feature for your users. After INKY analyzes messages, employees receive real-time feedback as to what, if anything, is fraudulent about the message. Because the banners are HTML based, they will display properly on any email client or platform such as a traditional PC with Outlook, Apple / Android App, or any of the web-based clients and on any mobile device.

Banners are color-coded to empower users, making it simple to determine the potential threat level of delivered messages:



- **Grey Banner:** (safe) INKY did not find anything unusual or suspicious about the message. The banner also displays the email sender's address and notes if the email is internal (within an organization) or external.
- **Yellow Banner:** (caution) INKY found something unusual about the email message. It is not necessarily dangerous but has something a user should be aware of. For example, INKY displays a yellow banner for an email from a first-time sender. An email that is out of the ordinary like a spear-phishing email would receive a yellow banner.
- **Red Banner:** (danger) A red danger banner indicated INKY thinks the message is suspicious and is likely to be phishing or otherwise dangerous. These messages have the option of being delivered or sent to the quarantine folder.

The **"Report This Email"** link in each INKY banner allows end-users to report spam, phish, and other problematic emails from any endpoint device.