End-User Rollout Guide

What's Changing with Your Email

Based on direct feedback from our customers, we are transitioning from Graphus to INKY to better align with how users prefer to interact with and manage their email. This change is focused on reducing noise, improving usability, and integrating more naturally with Microsoft 365.

Key changes driven by customer feedback:

- Reduced banner fatigue
  We will no longer display banners on known internal or trusted external emails. Please note, this does *not* mean INKY will stop showing ALL banners, even if the sender is internal/known and there is a threat, sensitive material, etc in the emais. Instead, we will rely on Microsoft's native external/internal tagging in Outlook, which clearly identifies message origin without adding visual clutter.
- No Graymail feature
  INKY's graymail functionality will not be enabled. Customers indicated this overlaps with Microsoft's Focused vs. Other inbox experience, and they prefer Microsoft's built-in controls to decide how their inbox is organized.
- Quarantine and notifications
  Quarantined or suspicious emails will continue to be delivered to the Junk Email folder, allowing users to review and take action as needed. However, there will no longer be a separate "Key Defense Insights" email notification.

Overall, this change simplifies the email experience while maintaining strong security protections, using Microsoft-native features where they already work well and reducing unnecessary duplication and noise.

Please continue to read below for more in-depth information.

INKY Rollout Guided Demo

View the guided demo below or share out this link with end users!

https://inky.storylane.io/share/lqswoqpjgb4x

Understanding the Banners

Yellow banners flag something unusual that deserves extra attention. This might be a first-time sender, a request for sensitive information, or something that seems out of character. Proceed with caution—double-check before clicking links or opening attachments.
Red banners indicate serious danger. INKY detected likely phishing, brand impersonation (like fake Microsoft alerts), spoofed internal senders, or known malicious links. Your IT team may have configured these to go straight to quarantine, so they never reach your inbox.

What To Do with Flagged Emails

When you see a yellow or red banner, look carefully at who sent it and whether the request makes sense. If you're unsure about a legitimate-looking email that got flagged, verify through another channel—call the sender or check with IT before taking action.
For red-flagged emails, the safest move is to delete them immediately. If you absolutely must access the content, be aware that clicking links will take you to an INKY warning page that shows a screenshot of the destination and asks you to confirm you want to proceed.

Help INKY Learn

Every INKY banner includes quick action links that let you report emails with a single click. You'll see options like **Safe**, **Spam**, and **Phish** directly in the banner—just click the one that matches your assessment.
INKY shows different options depending on what it detected. On dangerous emails, you might see options to confirm it's phishing, downgrade it to spam, or mark it safe if it's a false alarm. On clean emails, you can flag unexpected threats.
When you click a quick action, you'll get a simple confirmation screen where you can proceed with one click, cancel, or choose **More Options** for advanced settings like blocking the sender permanently or adding detailed notes.
Your reports make INKY smarter for everyone. The system learns from your feedback and uses it to improve threat detection across your organization. It takes just seconds and helps catch the next attack before it reaches someone else's inbox.
If you need the traditional reporting form with all the options, click **More...** in the banner to access the full reporting page.

Guided demo: https://inky.storylane.io/share/hbngmb7dtbk0

If You Click Something Suspicious

INKY rewrites links in flagged emails to check them in real-time. If you click a dangerous link, you'll see a blocker page with a screenshot of the destination site, an explanation of why it's risky, and options to proceed or go back. When in doubt, don't proceed—contact IT instead.
INKY's real-time protection can catch newly identified threats when you click.

Important Behavior of INKY Banners

INKY does NOT add banners to reply or forward messages. Banners only appear on the original incoming email.
INKY does NOT block your preview pane. You can still preview emails normally.
INKY does NOT use its own quarantine. It relies on **Microsoft 365’s built-in quarantine**, which means messages are easier for you and IT to review, release, or block using familiar tools.

Email Handling Changes

Highly confident phishing and malware emails may be placed in Microsoft Quarantine.
You may receive daily Microsoft quarantine summaries depending on configuration.
You may see fewer phishing or malicious emails in your inbox.
Please report false positives to IT so we can adjust safelist settings.

What You Need to Do

Read INKY banners before clicking links or opening attachments.
Report any suspicious or incorrect warnings to IT.
If a message is in quarantine and you need it, request release only if you are confident it is legitimate.
Please forward this off to your employees for their awareness of these changes.

Quick Reference

- **Yellow = Caution** – Something unusual, verify before acting
- **Red = Danger** – Likely phishing or malware, delete it
- **Report emails** using Quick Actions
- **Access dashboard** through Details → User Dashboard (uses your Microsoft/Google login)
- **Questions?** Contact tickets@angelcom.com

Desktop and Mobile

INKY banners work identically across Outlook for Windows, Outlook for Mac, Outlook Web App, Apple Mail, Gmail, and mobile apps. You'll see the same protection whether you're at your desk or checking email on your phone.

Created 2025-11-13 17:18:10 UTC by Brandon Spencer
Updated 2026-01-30 16:44:35 UTC by Brandon Spencer