FORTH TECH
IT SERVICES FOR BUSINESS

INKY Email Assistant

What's Changing with Your Email?

INKY is now protecting your inbox from phishing attacks, malware, and suspicious emails. You'll see coloured banners at the top of your emails that instantly tell you if something's safe or risky. This works on any device and email client you use.

Understanding the Banners

Gray banners mean INKY analysed the email and found nothing suspicious. The banner shows the sender's real email address and confirms if it's from someone inside or outside your organisation.

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. You’re unlikely to see a red banner as typically these emails go straight into quarantine. Read on for guidance on how to deal with red-banner-emails.

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, Phish,** and **Graymail** 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 or mark bulk mail as graymail.

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.

To learn how to quickly block spam, watch this guided demo:
https://inky.storylane.io/share/hbngmb7dtbk0

Your reports make INKY smarter for everyone. The system learns from your feedback and uses it to improve threat detection across your organisation. 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.

Managing Graymail (Bulk Email)

INKY can identify graymail, newsletters, promotions, and bulk emails that aren't dangerous but clutter your inbox. When you see a graymail banner, click **"Details"** then **"User Dashboard"** to access your settings.

You can automatically route all graymail to a dedicated folder to keep your inbox clean. Just check the box in your dashboard and INKY will create the folder and handle the sorting. If something gets mis-categorised, use the Report link to fix it.

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.

Even if an email had a gray banner originally, INKY's real-time protection can catch newly identified threats when you click.

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.

Quick Reference

- **Blue = Known External**
  INKY found nothing wrong and confirmed authentication for a known sender
- **Gray = Neutral**
  INKY found nothing wrong
- **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 the Forth Tech team on 0333 9000 100 or by email: support@forthtech.co.uk

Created by Forth Tech | 15 January 2026