KeyStone solutions, llc

HOW-TO GUIDE
For all email users

INKY Email Protection — What You Need to Know

Keeping you up. Keeping you safe. Keeping you compliant.

KeyStone is rolling out **INKY**, a new email spam filtering and threat protection service. INKY analyzes your incoming and outgoing email for phishing attempts, malware, domain spoofing, and social engineering. Banners and reporting work straight from your inbox; quarantined messages are viewed in Microsoft's quarantine portal (details below).

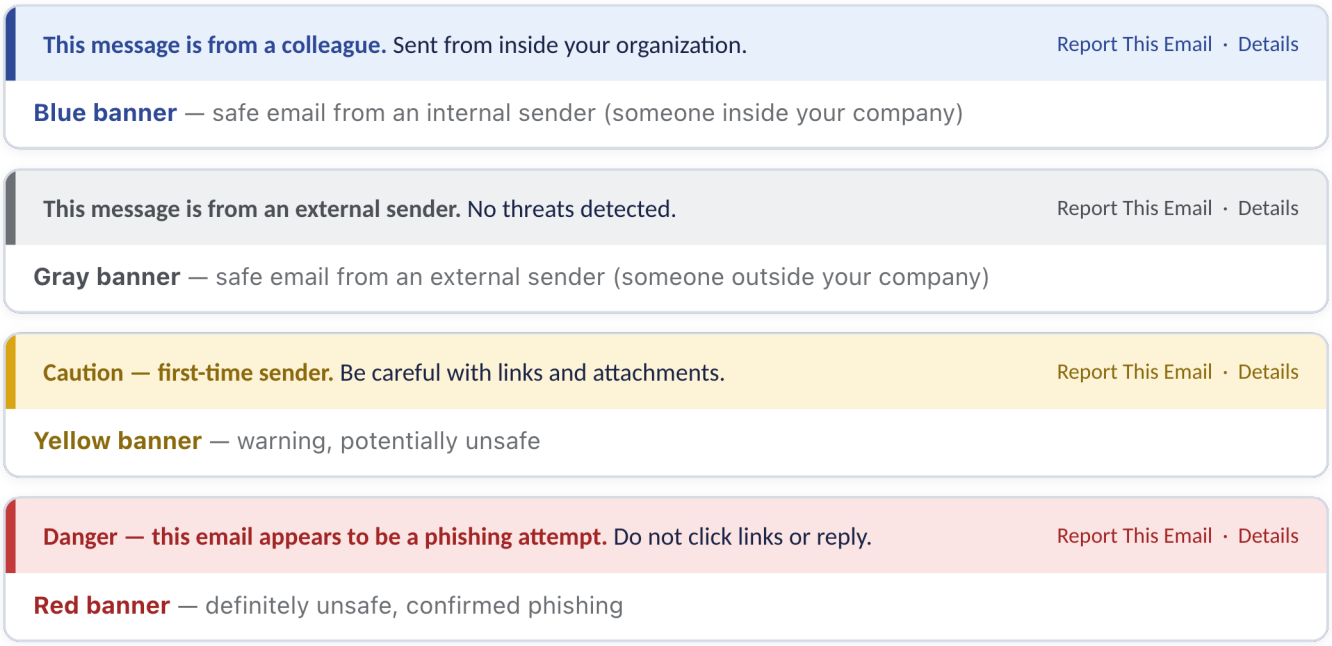
How does INKY work?

INKY monitors three directions of mail: **inbound** mail from external senders, **internal** mail between users in your organization, and **outbound** mail — so you never unknowingly forward a threat.

Threats are moved to your junk folder automatically. If something lands there that isn't junk, you can move it back to your inbox.

What will this look like?

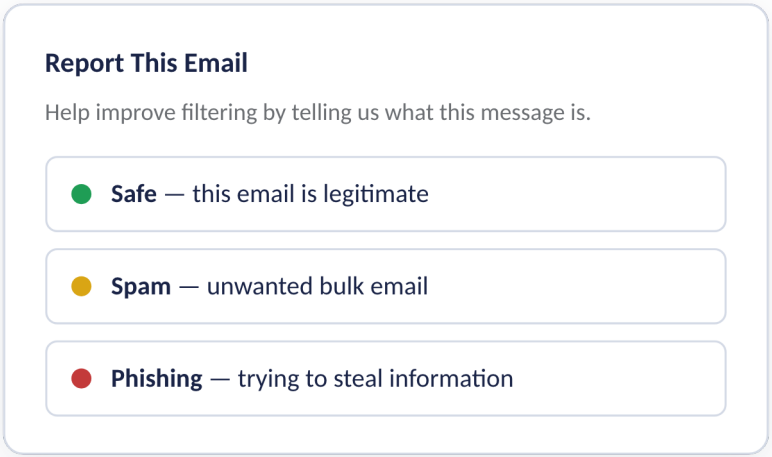
You'll start seeing a banner at the top of your emails. It tells you why an email was flagged (first-time sender, suspicious link, etc.) and gives you options on the right to report the email as **Safe**, **Spam**, or **Phishing**. The banner's color tells you where the email came from and how risky it is:



Banner mockups shown for illustration — colors and wording match what you'll see in your inbox.

Reporting an email

When you report an email, a pop-up asks you to confirm how you want to classify it:



Need more information about why an email was flagged? Click **Details** in the banner — a browser tab opens with a full analysis of the message.

Emails from others *within* your organization also get a banner — always in **blue**, so you can easily tell internal mail apart from external senders.

Where does flagged email go?

Based on INKY's analysis, Microsoft 365 routes each message to one of three places:

Safe / Caution	Delivered to your **inbox** with a banner.
Spam	Moved to your **junk folder**. Not junk? Move it back to your inbox yourself — no ticket needed.
Phishing / Malware	Held in **admin quarantine** before reaching you. To request a release, submit a support ticket with KeyStone — we review and approve or deny.

Checking your quarantine

Microsoft sends you quarantine digest notifications, or you can view quarantined messages anytime at **security.microsoft.com/quarantine**. For each message you'll see the subject, sender, date, the quarantine reason, a safe preview option, and a Release or Request Release button. Every released message is re-analyzed by INKY and delivered with the appropriate banner.

What's the difference between Spam, Phish, and Graymail?

Spam

Bulk emails you don't want to keep receiving. Mark these as spam and they'll automatically go to your junk folder in the future.

Phishing

Any email trying to get you to give out information or click a suspicious link. Report these as phishing and they'll be moved to the deleted folder.

Frequently Asked Questions

1. How long does it take for my changes to show up after I report a message?

INKY reports it can take up to an hour for changes to take effect.

2. If an email went to junk and I report it as not spam, does it move back automatically?

No — report it as not spam, then manually move it back to your inbox. Future messages from that sender should arrive in your inbox as normal.

3. I'm missing an email I've been waiting on. Is there a portal I need to check?

Some emails are quarantined before they ever reach your inbox — usually because they contain explicit phishing links. Check security.microsoft.com/quarantine, or submit a ticket with KeyStone so we can investigate or release it.

4. I clicked a link in a phishing email by mistake. How do I fix it?

Report it to KeyStone ASAP. The quicker you let us know, the quicker we can make sure your information isn't compromised.

Questions? We're here 24/7/365.

Submit a ticket or call our 100% US-based help desk.

Chat, email, or Call https://keystone.solutions/support