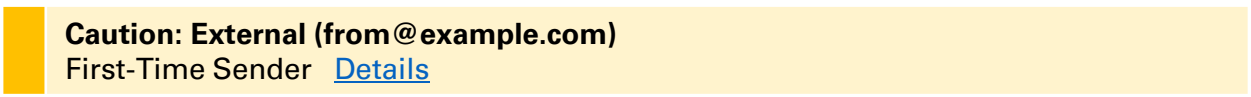
Banner Guide

INKY analyzes an email in less than two seconds and inserts a banner called the Email Assistant near the top. This color-coded banner details exactly what, if anything, is fraudulent or suspicious about the email message. Below the banner are three links that empower users to learn more or take actions. The experience looks and works the same whether users are on their desktop, tablet, or mobile device.

Banner Levels

GRAY BANNER
A gray banner indicates that INKY did not find anything unusual or suspicious about the message. The banners also display the email sender's address and mark the email as external.

YELLOW BANNER
A yellow caution banner indicates that 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 email from a First-Time Sender. Email that seems out of the ordinary like a spear phishing email would also receive a yellow banner.



RED BANNER
A red danger banner indicates that INKY thinks the message is suspicious and likely to be phishing or otherwise dangerous. This includes brand impersonations, blacklisted phishing URLs, or attempts to spoof mail to look like it came from an internal company account. Dangerous messages can also be quarantined.

Banner Guide

Banner Threat Types

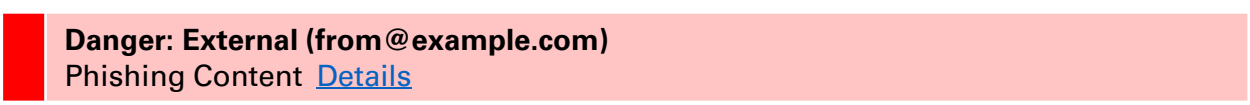
INKY banners include various threat types such as Brand Impersonations, Spoofed VIPs, and Spam. These are a sample of the most common types, and new ones are added occasionally as new threats appear in the wild.

BRAND IMPERSONATION
Messages sent from major brands almost always have certain technical properties indicating they are legitimate. This message lacks one or more of these properties but appears to be from a major brand. Attackers send brand forgery emails to entice you to click through and log in to a fake site, which gives them your login credentials. In rare cases, this warning can be triggered by a legitimate mail from one company that incorporates another seemingly unrelated company's branding element. Use the feedback link if you're sure this message is legitimate, to help train the system to allow mail like this one in the future.

SPOOFED INTERNAL SENDER
This appears to be a spoofed internal email. The message claims to be from example@email.com but the sender was not authenticated to your organization's mail server.

SPOOFED VIP
The sender (Internal VIP) may be trying to trick you into thinking this message is from an executive or VIP related to your organization.

PHISHING CONTENT
This is most likely a phishing email trying to trick you into doing something dangerous like installing software or revealing your personal information (e.g., passwords, phone numbers, or credit cards).



Banner Guide

BITCOIN BLACKMAIL SCAM
This message is a scam attempting to extort money from you via bitcoin. Do not pay the ransom. These scams often include a valid password obtained via a data breach. Be sure to update any accounts that may still use that password. Learn more about Bitcoin blackmail scams from the FTC.
(https://www.consumer.ftc.gov/blog/2018/08/how-avoid-bitcoin-blackmail-scam)

Danger: External (from@example.com)
Bitcoin Blackmail Scam Details

Report This Email FAQ Protection by INKY

GOOGLE SAFE BROWSING URL
This message links to one or more potentially unsafe web resources. Advisory provided by Google (https://developers.google.com/safe-browsing/v4/advisory)

Danger: External (from@example.com)
Google Safe Browsing URL Details

Report This Email FAQ Protection by INKY

MALWARE ATTACHMENT
At least one attachment appears to be malware, such as a virus or other malicious code that could harm your computer if opened.

Danger: External (from@example.com)
Malware Attachment Details

Report This Email FAQ Protection by INKY

SPAM CONTENT
This is most likely spam or unwanted junk email. Be careful with any attachments or links.

Caution: External (from@example.com)
Spam Content Details

Report This Email FAQ Protection by INKY

FIRST-TIME SENDER
This is the first message you've received from this sender. Be careful when replying or interacting with any attachments or links.

Caution: External (from@example.com)
First-Time Sender Details

Report This Email FAQ Protection by INKY

Banner Guide

SENSITIVE CONTENT
The message appears to discuss sensitive information (e.g., passwords, account information, etc). If possible, instead of clicking a link, go directly to the sender's web site to carry out the requested action, or confirm the request outside of email before replying.

Caution: External (from@example.com)
Sensitive Content Details

Report This Email FAQ Protection by INKY

MISLEADING LINK
It contains a misleading link that appears to go to example.com but will actually go to domain.com.

Caution: External (from@example.com)
Misleading Link Details

Report This Email FAQ Protection by INKY

FREE WEB HOSTING URL
The web site uses a free web hosting service provider. Such providers are often home to phishing scams. Be cautious.

Caution: External (from@example.com)
Free Web Hosting URL Details

Report This Email FAQ Protection by INKY

POTENTIALLY DANGEROUS CONTENT REMOVED
A large amount of potentially dangerous content was removed from this message. Be cautious.

Caution: External (from@example.com)
Potentially Dangerous Content Removed Details

Report This Email FAQ Protection by INKY

CONFUSABLE DOMAIN
It contains a domain name that may be confused with a more legitimate website. The domain may look familiar but uses unusual letters in order to deceive you. Learn more about so-called homograph attacks (https://en.wikipedia.org/wiki/IDN_homograph_attack).

Caution: External (from@example.com)
Confusable Domain Details

Report This Email FAQ Protection by INKY

For further assistance please contact support.