

The Banner

There are four million lines of code that enable INKY's unique banner to work, but our users will never have to encounter any of them. What they will experience, however, is a seamless system that catches even the most elusive of threats, while protecting, training, and empowering users across the enterprise. INKY instantly analyzes an email and displays a banner at the top of the email. These banners detail exactly what, if anything, is fraudulent or suspicious about the email message. Warning banners are color coded to empower the employee.

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.

External (example@email.com)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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.

Caution (External, example@email.com)

First-Time Sender [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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.

Danger (External, example@email.com)

Brand Impersonation [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

INKY Banner Types

INKY banners come in different forms, each banner could have one or more of the threat types with the color corresponding to most severe among them. They also can include custom policy statements showing end users helpful security reminders.

Danger (External, example@email.com)

Potential Sender Forgery, Brand Impersonation, and more... [Details](#)

INKY IT policy: Never send money without verbal confirmation.

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

INKY 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 — a valid digital signature, for example. This message lacks one or more of these properties but appears to be from a major brand. Attackers send brand forgery emails like these to entice you to clicking through and logging 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.

Danger (External, example@email.com)

Brand Impersonation [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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

Danger (External, example@email.com)

Spoofed Internal Sender [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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.

Danger (External, example@email.com)

Spoofed VIP [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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, example@email.com)

Bitcoin Blackmail Scam [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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).

Danger (External, example@email.com)

Phishing Content [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, example@email.com)

Google Safe Browsing URL [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

PHISHTANK URL

The URL is a confirmed phishing site. Learn more at PhishTank. (<https://phishtank.com>)

Danger (External, example@email.com)

PhishTank URL [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

NETCRAFT PHISHING FEED URL

It links to a confirmed phishing site on the Netcraft Phishing Site Feed. (<https://www.netcraft.com/anti-phishing/phishing-site-feed/>)

Danger (External, example@email.com)

Netcraft Phishing Feed URL [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

REPORTED PHISH

It is similar to emails that have been reported as phishing.

Danger (External, example@email.com)

Reported Phish [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, example@email.com)

Malware Attachment [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

MALWARE CONTENT

This message contains malware that may harm your computer.

Danger (External, example@email.com)

Malware Content [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, example@email.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, example@email.com)

First-Time Sender [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

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, example@email.com)

Sensitive Content [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

IP ADDRESS URL

The URL includes an IP address.

Caution (External, example@email.com)

IP Address URL [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

SPAMMY TOP-LEVEL DOMAIN

It contains a URL or email address ending in a frequently abused top-level domain.

Caution (External, example@email.com)

Spammy Top-Level Domain [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

INVALID SENDER

The message does not have a valid email address in the From: field.

Caution (External, example@email.com)

Invalid Sender [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

REPORTED SPAM

It is similar to emails that have been reported as spam.

Caution (External, example@email.com)

Reported Spam [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, example@email.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, example@email.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, example@email.com)

Potentially Dangerous Content Removed [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

JAVASCRIPT REMOVED

JavaScript code was removed from this message or its attachments. This code could be used to track your activity or perform malicious actions.

Caution (External, example@email.com)

JavaScript 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, example@email.com)

Confusable Domain [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

SUSPICIOUS URL

It links to a site similar to some confirmed phishing sites. Be cautious.

Caution (External, example@email.com)

Suspicious URL [Details](#)

[Report This Email](#) [FAQ](#) [Protection by INKY](#)

For support inquiries and questions, please send an email to support@inky.com.