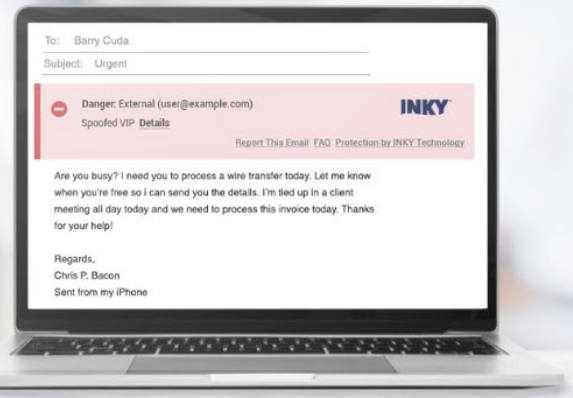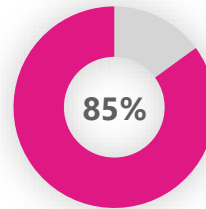# INKY®

## EMAIL ASSISTANT

# Periodic email security training is no match for distracted, busy users.

Awareness training is an important component of any organization's cybersecurity strategy and is often required to meet compliance requirements. However, relying solely on awareness training is not enough, because it is often too generic and cannot keep up with constantly evolving threats.

**85%** Of data breaches are caused by human error.
*Source: Verizon*

Employees using Email Assistant are **48%** better at making safe email security decisions.

## Not all banners are created equal.

When not done right, inserting banners into emails has the potential to disrupt workflow. When banners are over-used or too standardized, they become noise that is quickly disregarded, voiding their effectiveness, creating banner blindness. Banners that utilize standardized text are often ignored in addition to creating an opportunity for attackers to evade them by impersonating standardized banner text. Attackers can also leverage CSS techniques to hide or obscure standard banners.

## Better detection results in richer training content.

The Email Assistant appears to users as a color-coded email banner but is so much more than simply a static warning banner. It acts as a cybersecurity coach, training users in real-time on real email as it arrives. Each time the assistant appears at the top of an email body, the dynamic banner displays a specific combination of findings from its more-than-three-dozen analytical models. We believe dynamic warning banners are such an important part of solving phishing that we include it at no additional fee on INKY Inbound and Internal Mail Protection.

## What makes INKY's banner a *better banner*?

- 55+ threat categories and 75 guidance types
- Customizable company logo assures users of legitimacy
- Admins can configure banners in multiple ways
- A "Details" link provides users with a real-time email security training session in every email
- Warning banner disappears when an email is forwarded outside of the company
- "Report This Email" link allows users to report problematic emails from any device
- Uses NLP to identify sensitive content, such as payment or wire transfer requests, and provide customizable policy tips
- HTML implementation means it works on any mobile device and any email client

**INKY**®
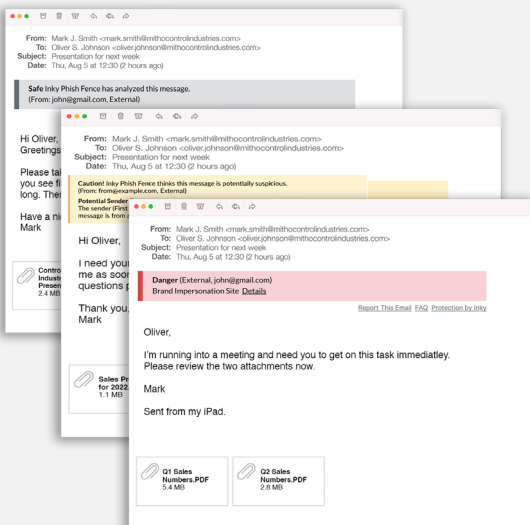
## Report an Email from Anywhere

The "Report This Email" link allows end users to report spam, phish, and other problematic emails from any device. Since email is increasingly consumed on mobile, users are empowered to report potentially fraudulent emails from any device or email client, including iOS.
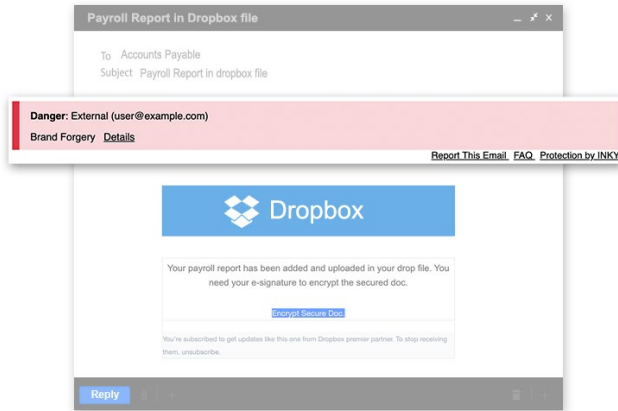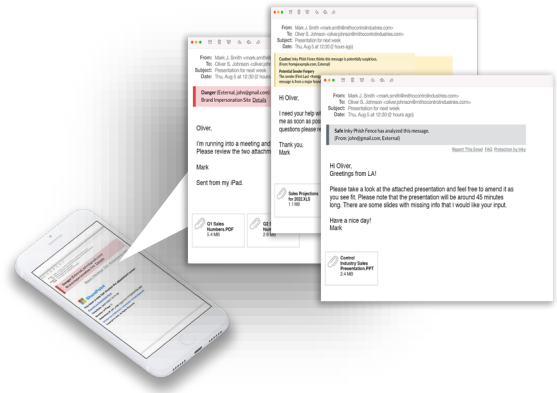
## Real-Time Phishing Awareness Training

The assistant is a more effective learning tool than phishing simulation testing. Clicking the "Details" link explains exactly what is wrong with an email in plain language. This educates users on real-world threats in their inboxes.

## Coach Users to Make Safe Email Decisions

INKY blocks malicious email from impersonators and teaches employees how to handle suspicious emails. With interactive banners that stand out when something's dangerous, the Email Assistant encourages users to think before they act.

---
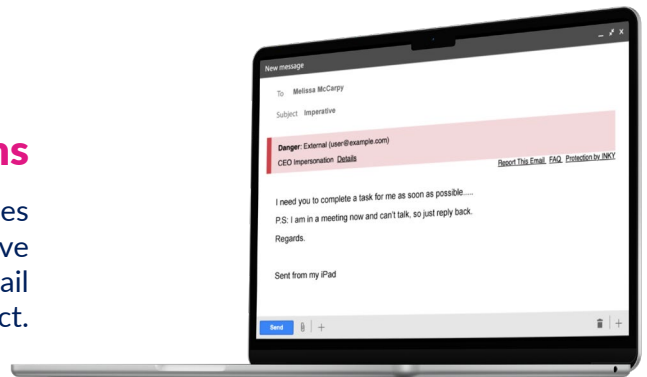
## EMAIL SECURITY PLATFORM

# The behavioral email security platform purpose-built for MSPs.

| INBOUND EMAIL PROTECTION | INTERNAL EMAIL PROTECTION | ADVANCED ATTACHMENT ANALYSIS | OUTBOUND EMAIL PROTECTION | EMAIL ENCRYPTION | GRAYMAIL PROTECTION | SECURITY AWARENESS TRAINING |
|---|---|---|---|---|---|---|
| Block phishing and coach users in real time. | Protect internal email traffic against account takeovers. | Detect deeply hidden malware from inbound attachments. | Prevent data loss with interactive safeguards for outgoing emails. | Guard sensitive data with fast and simple encryption. | Boost productivity by filtering out bulk email. | Educate employees with phishing simulation and videos |

---