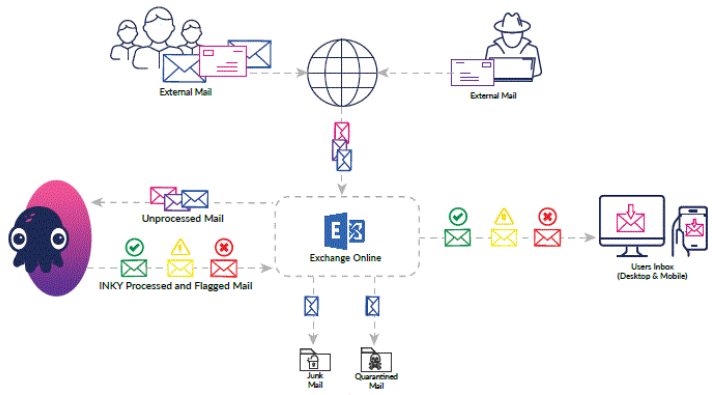
Securing the Inbox for Complete Threat Protection

A guide explaining how to complement existing email security gateway solutions for total threat protection.

In the past several years, phishing attacks have become more frequent and targeted. Legacy email security platforms have attempted to address new attack vectors like impersonations, spear-phishing, and brand forgery, but their technology is falling short. Organizations have observed that phishing attacks are still getting through resulting in employees falling for the bait. This has had a devastating financial impact on corporations worldwide. Below, we will outline how INKY's sophisticated technology can complement these legacy solutions, offering a crucial additional layer of protection from today's sophisticated threats.

How Does INKY complement Proofpoint and Mimecast?

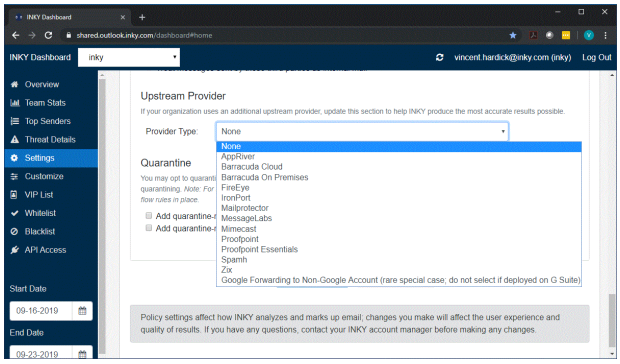


Unlike a traditional MX Security Email Gateway, INKY sits INLINE with the email flow. Our email protection was specifically built to complement the built-in tools of Office 365 and augment the shortcomings of a legacy Proofpoint and Mimecast deployment.

After the email passes through the old traditional MX gateway, Google and Office 365 can no longer interpret two main indicators of phishing because:

The sender IP & SPF Record:

After Mimecast, Proofpoint, or any other traditional MX based gateway is configured, O365 and GMail no longer see the IP address, which identifies the original server that sent the message.



Additionally, since the IP and original sending server domain are no longer available, the domains SPF records are incorrect.

INKY was designed to overcome these shortcomings and be able to read what Office 365 and GMail can't. Even with Proofpoint or Mimecast installed, INKY can customize and retrieve the relevant sender IP and SPF records that Proofpoint and Mimecast obscure.

INKY can integrate with Proofpoint, Mimecast, IronPort, Barracuda, FireEye, Message Labs, Zix, and more.

INKY

Securing the Inbox for Complete Threat Protection

How can INKY catch more Brand Impersonations than a Proofpoint or Mimecast traditional Security Email Gateway?

After the email passes through the INKY Phish Fence (IPF), INKY uses sophisticated techniques such as "*deep learning" and "computer vision"* algorithms to analyze and interpret main indicators of a brand phishing attack.

1. Brand Modeling enables INKY to identify impersonations:

99% of the phishing attacks impersonate the same top 250 – 500 company brands. Microsoft is still number one when it comes to impersonated brands in phishing attacks, followed by Paypal, Netflix, Facebook, Bank of America, Apple, and Dropbox. INKY has built dynamic models for these brands and can identify the smallest inconsistency in the messages sent by their impersonators.

WHOIS Domain Info: INKY scrapes all whois information to identify which domains are:

a) Actually owned by the brand

Many companies have already purchased their so-called "*typo*" domains such as amzon.com or "*confusable*" domains such as yah00.com, to ward off the simple mistaken identity attacks, but there are thousands more out there.

INKY has identified over thirty thousand for amazon alone. We have examined this phenomenon and explained in more detail how INKY protects against in this article: Confusable Text and Homograph Attacks.

No matter how many different permutations or typo domains the hackers create, INKY's data-driven modeling will identify and block these dangerous emails.

b) used by the brand for messaging

INKY dynamically tracks the malicious use of domains and records the legitimate messages and source domains used by the top impersonated brands. Instead of relying on days old threat feed databases/blacklists, INKY can identify and block sender forgeries and confusable domains in real-time for both internal and external mail.

2. Computer Vision sees threats a human eye cannot:

Phishing attacks are getting more sophisticated daily. While the emails are getting harder to detect, INKY uses computer vision to fetter out malicious messages.

INKY

Securing the Inbox for Complete Threat Protection

No amount of training is going to stop phishing attacks from causing havoc or possibly thousands of dollars to your organization. Hackers are using highly developed and elaborate techniques to fool users.

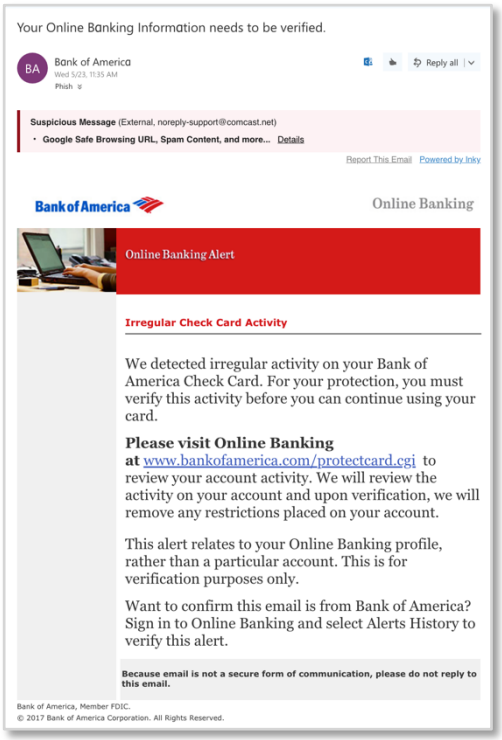
As an email pass through the INKY Phish Fence (IPF) the message is rendered in a headless chrome browser and analyzed as a human security engineer would.

- Starting with the header, source IP reputations are checked
- WHOIS / Valid Sender Domains are analyzed
- DKIM, DMARC, and SPF records are analyzed

This is all pretty standard, but what sets INKY apart is next:

- INKY checks the logos in the body of messages
- Is it the right color, font, shape, size of image (200x200 pixels)
- Is the weight of the image correct (10KB)

Because INKY uses data-driven Machine Learning and Computer Vision models, we can identify and stop these attacks in real-time as compared to a traditional security email gateway reliant upon old school bayesian filtering rules and out of date messaging blacklists/RBL's.

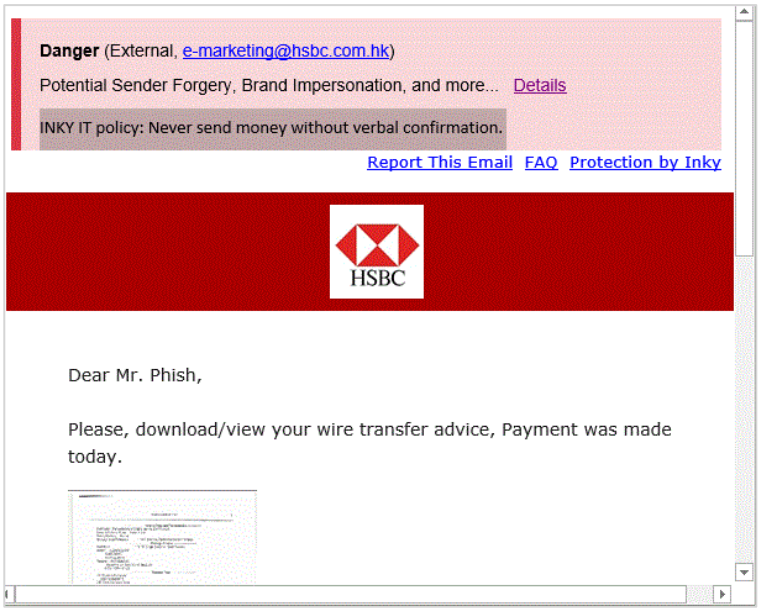


3. Message Intent & Link Rewriting Protection

INKY can go a step further than all traditional SEG's and interpret the intent of the message and display real-time alerts to users in our one of a kind HTML banners.

We call these alerts 'IT policy directives' and they are fully customizable to your organization.

Securing the Inbox for Complete Threat Protection



As INKY starts to move further down into the body of the message, it will analyze the intent of the message.

- **Could this be a financial email?**
- **Could this be a possible bitcoin scam?**
- **Could this be a possible credential harvesting attempt?**

INKY financial policy directive will warn the user, "*Never send money without verbal confirmation.*"

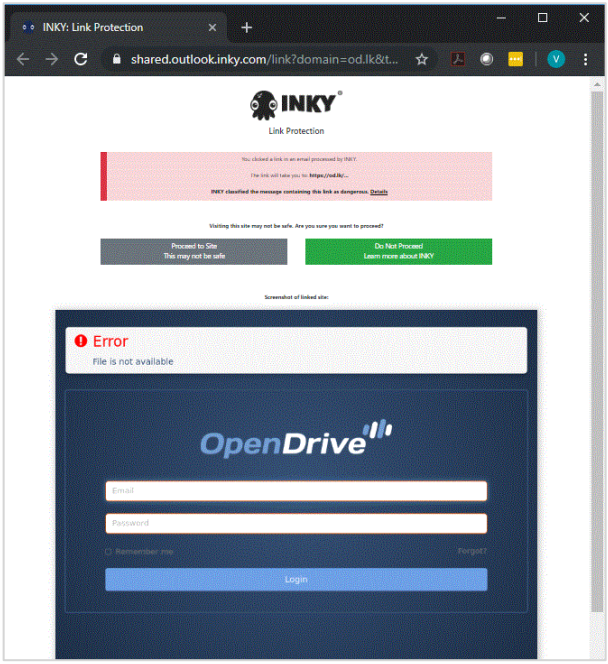
20 different directives exist by default. All are customizable to each organization.

Link Rewriting Protection / Landing Page:

INKY's link protection is NOT your traditional Real time Blackhole List (RBL)/link checker. Real-time targeted zero-day threats NOT reported to the RBL's are caught daily.

As each link is clicked, INKY will analyze it in real-time. NOT afterward like a TRAP or API solution, but right away and every time after.

Confusable domains, misleading links, cross-site xss URL's, and malicious redirects are identified and filtered out. And like the brand impersonation models, INKY's link protection knows where an email link should be taking you. INKY will display the real destination of the URL link in a safe preview screenshot isolating the user from the malicious web page.



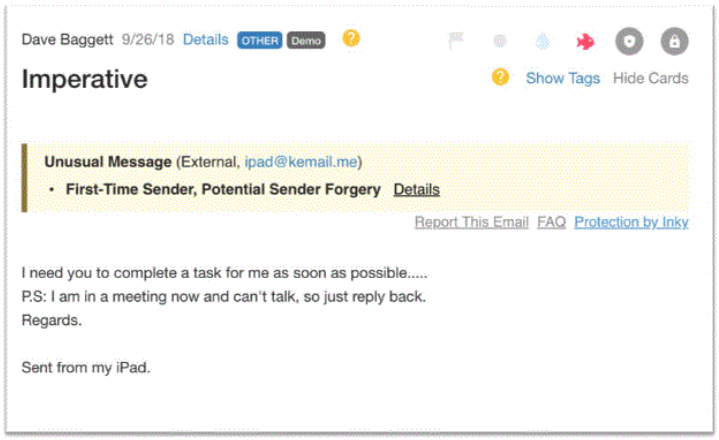
INKY

Securing the Inbox for Complete Threat Protection

How can INKY catch more Spearphishing attacks than its competitors?

Spearphishing, CEO Impersonation, or Whaling Attacks, as they are all called, are difficult to catch because they mostly contain just “text.” Inherently there is nothing wrong with them at first glance.

These messages get through the traditional gateways daily. How does INKY catch these and keep my organization safe?



Dynamic Sender Profiling & Social Graphing:

The more INKY sees mail coming into your organization, the smarter she gets. As your users receive mail from legitimate senders, INKY builds dynamic ‘profiles’ or ‘behavior models’ of the originating sender. As the models grow, INKY uses anomaly detection techniques to filter out and block Impersonation attempts.

How does INKY build its profiles?

INKY observes the incoming mail and builds and index/model of:

1. What email addresses are typically used by the sender
2. What friendly name is normally displayed (Tyler D, vs. Tyler Durden)
3. Where the user sends mail from (home/office/mobile)
4. What devices a user sends mail from (mobile device, traditional PC, or tablet)?
5. What email client is being used? (outlook for the PC, apple mail client for iPad/iPhone, or GMail app)

After approximately 7 – 10 days of normal user mail flow INKY has built enough sender profile/social behavioral graph information to enable our spearphishing and VIP protection.

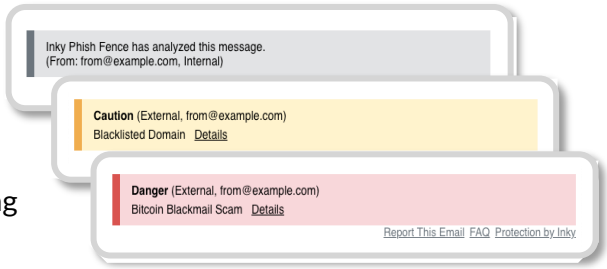
INKY

Securing the Inbox for Complete Threat Protection

Warning Banners: How/Why does INKY add Warning Banners to our email messages?

INKY's unique HTML based warning banners are a key visual feature for users of the software. After INKY analyzes messages, employees receive real-time feedback as to what if anything is fraudulent about the message. Because the banners are HTML based, they will display properly on any email client or platform such as a traditional PC with Outlook, Apple / Android App, or any of the web-based clients. Unlike, for example, Proofpoint, INKY users will see banners without needing an Outlook plugin or a separate mobile app.

Banners are color-coded to empower users, making it simple to determine the potential threat level of delivered messages:



- **Grey Banner**: (safe) INKY did not find anything unusual or suspicious about the message. The banner also displays the email sender's address and notes if the email is internal (within an organization) or external.
- **Yellow Banner**: (caution) 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 an email from a first-time sender. An email that is out of the ordinary like a spear-phishing email would receive a yellow banner.
- **Red Banner**: (danger) A red danger banner indicated INKY thinks the message is suspicious and is likely to be phishing or otherwise dangerous. These messages have the option of being delivered or sent to the quarantine folder.

Security awareness training is helpful, but not very effective at thwarting an attack. With INKY's warning banners, users see these visual cues - preventing phishing threats in real-time instead of training around them.

The "**Report This Email**" link in each INKY banner allows end-users to report spam, phish, and other problematic emails from any endpoint device.

INKY incorporates natural language processing (NLP) algorithms to identify sensitive content like wire or invoice payment requests, password-related emails, etc. and can annotate these with customer-configurable policy guidelines in the banner.

CONCLUSION

Phishing scams continue to evolve and attackers have an ever-growing bag of tricks with which to fool both human recipients and legacy mail protection software. We know attackers will continue to up their game; we're sure to see ever more clever ways for scammers to hide from mail protection. In today's landscape the widely used SEG's are simply not enough defense for a total email security strategy. INKY's feature rich next-gen technology is the final line of defense for companies looking to secure email from these relentless hackers.