SOLUTION BRIEF

INKY™

How INKY Fits With Secure Email Gateways

Like a traditional MX Secure Email Gateway (SEG), INKY sits **in line** with the email flow. But unlike a SEG, INKY installs in minutes and need not be the MX handler. In fact, INKY can run either stand-alone or alongside your existing SEG.

We built INKY to complement the built-in tools of Office 365 and Google Workspace and augment the shortcomings of legacy Proofpoint and Mimecast deployments. In this guide, we'll explain how to complement existing SEG solutions for total threat protection.

Request a demo.

How INKY Fits With Secure Email Gateways

As they assess today's myriad email security offerings corporate leaders often ask us how INKY fits with existing Secure Email Gateway (SEG) solutions like Proofpoint and Mimecast.

INKY and the SEGs can work together: the SEGs filter out spam and obviously malicious emails, while INKY provides guidance to end users with dynamic color-coded educational banners and quarantines the more sophisticated and targeted phishing, account takeover, and ransomware emails. In this way, INKY can function purely additively – augmenting the SEGs' capabilities – without requiring any changes to the SEG itself.

Sitting in line between the SEG and the recipient's inbox, INKY's cloud service analyzes each email as it arrives, using dozens of AI models, in an average of two seconds, prior to delivery. Since INKY runs after the SEG and before the inbox, customers know exactly what the upstream SEG allows through. Based on policy, INKY either blocks a bad email or adds a banner. The banner indicates a threat level via color coding and displays the reasons INKY found the mail suspicious. Since INKY catches what the SEGs miss, the additional value is obvious.

In this brief, we outline INKY's novel dynamic banner capability, which is like just-in-time awareness training for recipients.

Also included are real-world examples of sophisticated phishing emails – with personally identifiable information redacted, of course – that demonstrate tactics attackers use to get past the SEGs, but which INKY detects.

INKY™

Dynamic Banners that Educate Recipients

One of INKY's most distinguishing features is its banner system. While much of INKY's work detecting phish takes place "under the hood," the banners are what recipients see. These distinctive yet unobtrusive signposts tell the reader where each email sits on the safe-dangerous spectrum. The color (gray - safe, yellow - suspicious, red - dangerous) gives a general impression. The brief text phrases explain why INKY marked the email that way. The links in the banner allow the recipient to inquire further or report the mail to INKY staff for further analysis.

Each text phrase in INKY's dynamic banners is actually the output of one of INKY's dozens of threat assessment models, all of which go to work simultaneously on each email as it makes its way from the SEG to the recipient.

Thus, INKY both protects recipients and educates them as well as takes their input. The banners are dynamic in that each one contains the results of the analysis on that particular email. Every one is different.

Using clever CSS, hackers have learned how to suppress the simple static banners inserted by the SEGs. They've also figured out how to insert their own fake green "safe" banners (in emails that are anything but safe). INKY has instituted countermeasures that prevent our banners from being hidden and detect the presence of fake banners.

If nothing else, banner suppression and fake banner insertion argue in favor of working with an experienced company like INKY that counters these measures automatically. So, don't roll your own banners!

INKY™

Proofpoint

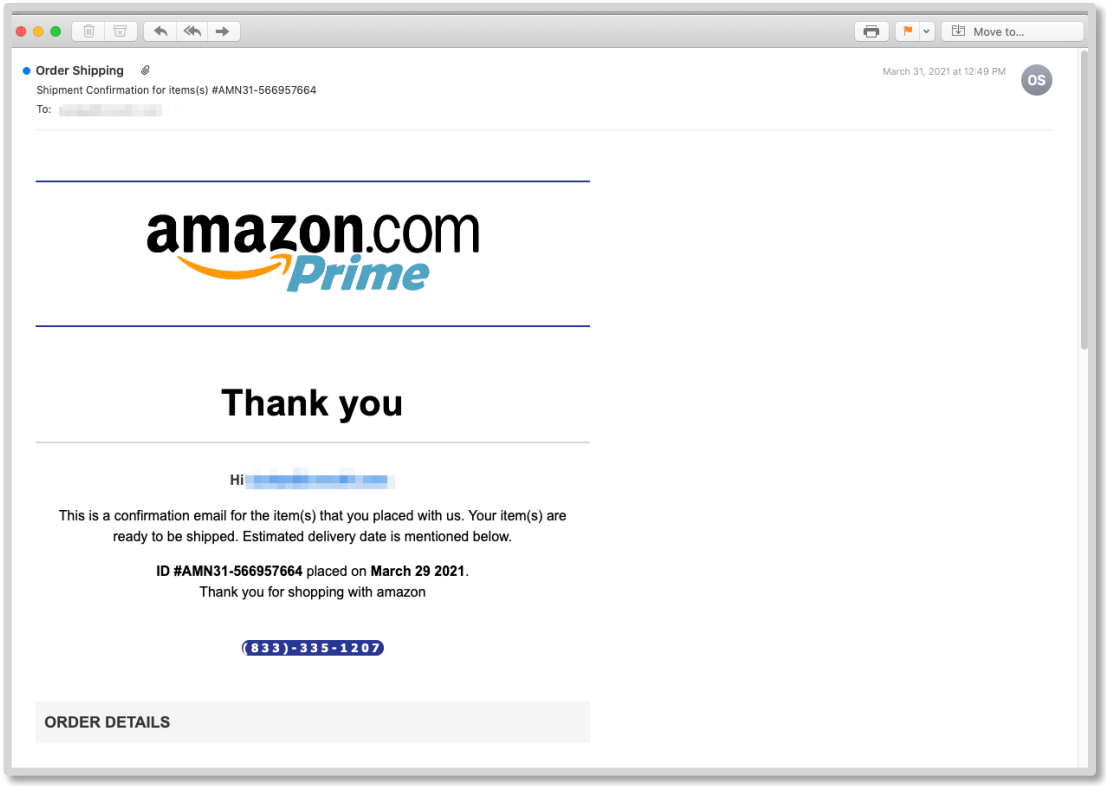
The following three examples include phish that Proofpoint let through — but INKY caught.

PROOFPOINT | BRAND FORGERY

Downstream from Proofpoint, INKY flagged an email impersonating Amazon.

The message appeared to be an order confirmation and featured realistic-looking Amazon branding elements. The content seems to indicate that the recipient ordered several expensive electronic items from the online retailer.

Although the order confirmation was fake, it contained no malicious links or attachments. From which direction did the danger come? The attack vector was the phone number. When the recipient called to object that they hadn't ordered the equipment, bad actors pretending to be Amazon tried to steal the recipient's Amazon login credentials and credit card information.



PROOFPOINT | BRAND FORGERY (Cont.)

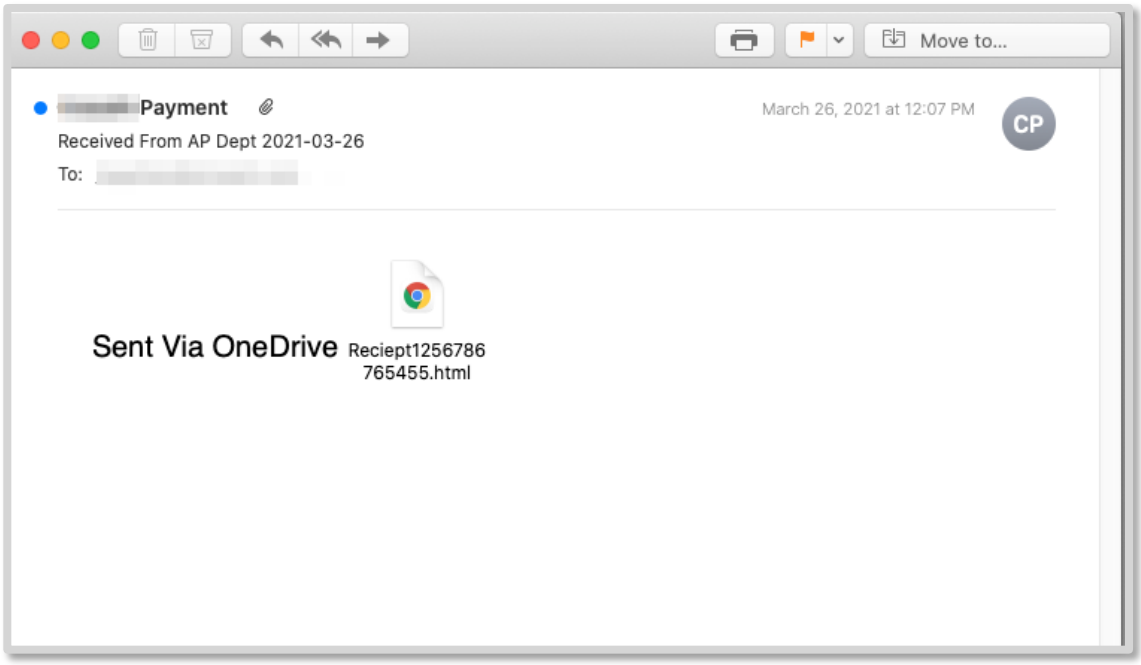
This type of attack is fairly new. Phishers have become aware that many anti-malware programs search for booby trapped attachments and poisoned links. Therefore, they try to fly below the radar with a relatively innocuous message.

INKY flagged the message anyway. On mobile, only the friendly name "Order Shipping" would show. On desktop, a careful reader could have seen that the sending domain was “amaznshippinghub22.co,” which still might have looked to the human reader like an Amazon domain but was different enough to avoid detection by Proofpoint’s regular-expression analysis. With computer vision, INKY was able to detect the Amazon branding elements in the body. It then checked to see whether amaznshippinghub22.co was under Amazon’s control. It wasn’t. So, INKY tagged the message as a phishing attack.

PROOFPOINT | ACCOUNT TAKEOVER

Dangerous emails sent from legitimate accounts in real domains are hard to detect. In this case, the mail came from a university email server. The phisher cleverly inserted the recipient's domain name into the sender line (obscured here). The message asserted that the email was sent "Via OneDrive," perhaps to instill confidence in the source.

The email claimed to contain a receipt from accounts payable. The "receipt" attachment was an HTML file that would take the victim to a malicious site with the URL https://thenmbc.net/pul/test/amluZ3JhaGFtQGNyYXZhdGguY29t. The site — thenmbc.net — has since been deactivated.



Proofpoint missed this one, but INKY tagged it with a number of warnings.

Danger! This message looks malicious.
(From: [redacted], External)

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).

Potentially Dangerous Content Removed
A large amount of potentially dangerous content was removed from this message. Be cautious.

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.

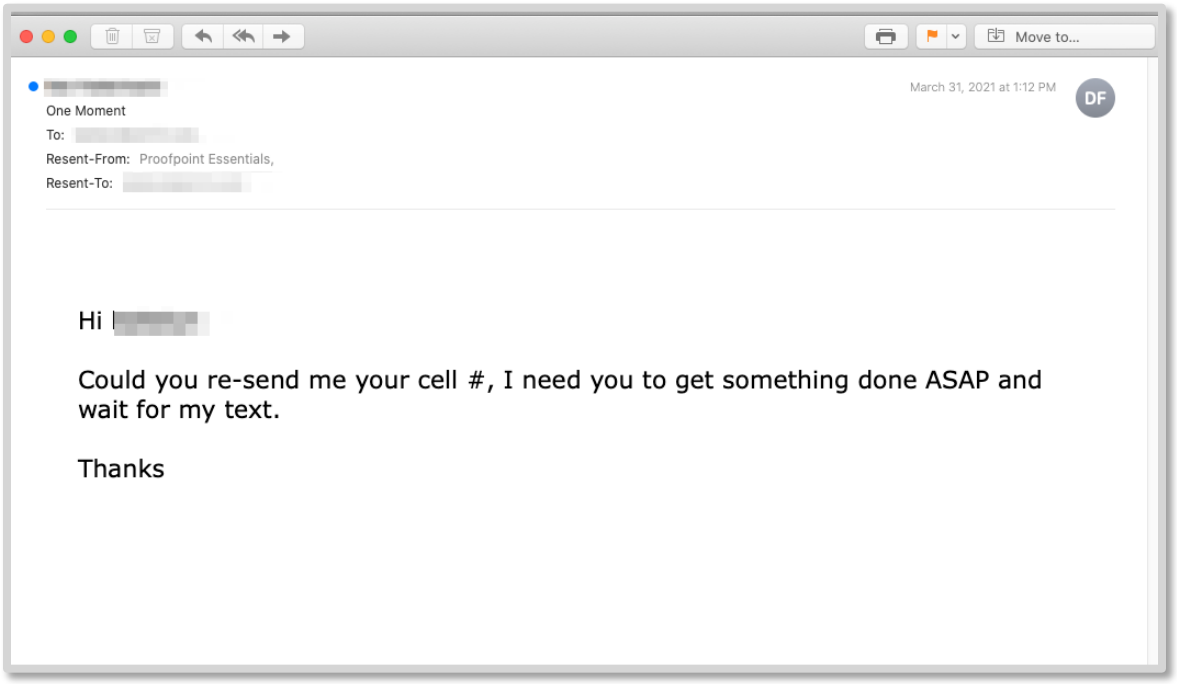
First-Time Sender
This is the first message you've received from this sender. Be careful when replying or interacting with any attachments or links.

INKY™

PROOFPOINT | CFO IMPERSONATION

This impersonation email is the first stage of a gift card scam. The phisher had the CFO's name right, and on a mobile platform, that's all the recipient would see. In fact, the sending domain was in Vietnam.

The text was innocuous, and there were no malicious links or attachments, allowing the message to slip through Proofpoint's defenses. If the victim had replied, they would have been instructed to buy gift cards and send the code to the bad actor.



Two INKY modules flagged this one. One issued a general warning; the other pointed specifically to the VIP spoof. During install, INKY customers can set up a simple list of VIPs with their email addresses; so, INKY can check a message that purports to come from a company VIP against where it really came from.

Danger! This message looks malicious.
(From: jessie.songhong.vn@mail.com, External)

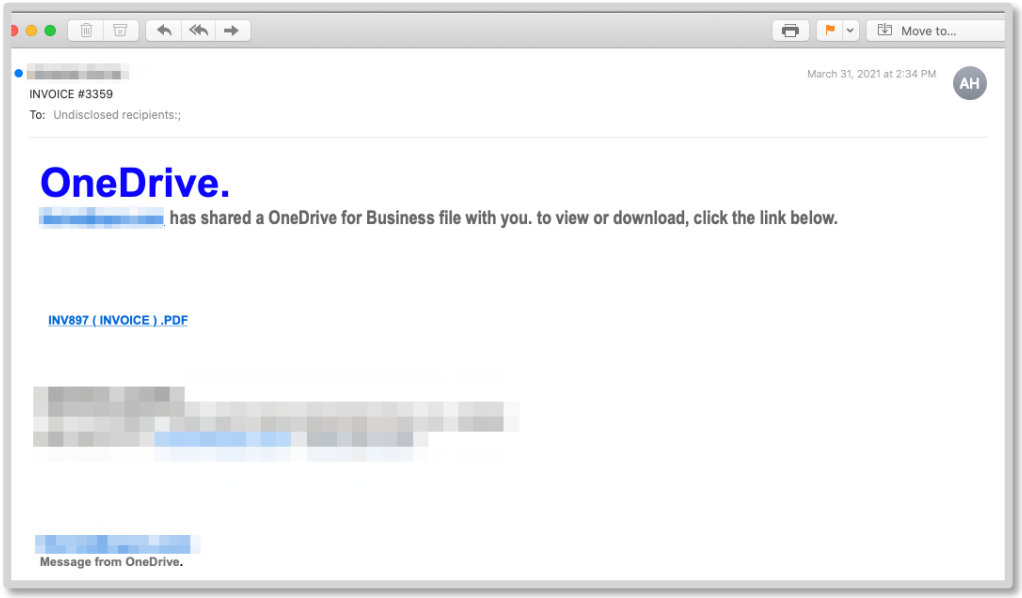
Spoofed VIP
The sender (Dan Federmann <jessie.songhong.vn@mail.com>) may be trying to trick you into thinking this message is from an executive or VIP related to your organization (Dan Federmann).

Mimecast

The following three examples include phish that Mimecast let through — but INKY caught.

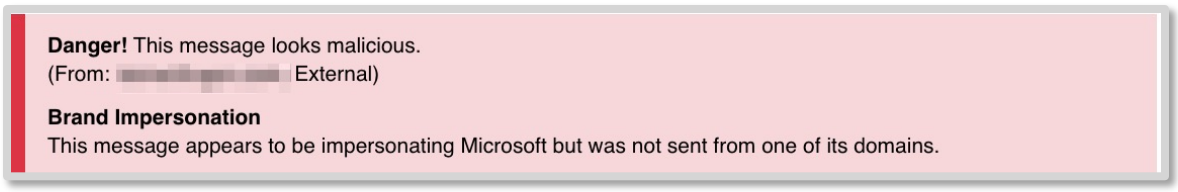
MIMECAST | BRAND FORGERY

A message purported to come from "OneDrive." The logo was the right color, but, for whatever reason, the phisher thought to put a period at the end of the logo text.



In this case, Mimecast did rewrite the link, but failed to detect anything malicious because the actual hosting site was Google Docs, which is considered benign. Unfortunately, that particular sender's account had been taken over by a phisher. Mimecast might have done real-time scanning of the site, checking for similar domains or sites on threat intelligence feeds, and may even have checked for automatic downloads or run the file in a sandbox to determine if it was safe, but none of these measures found anything wrong.

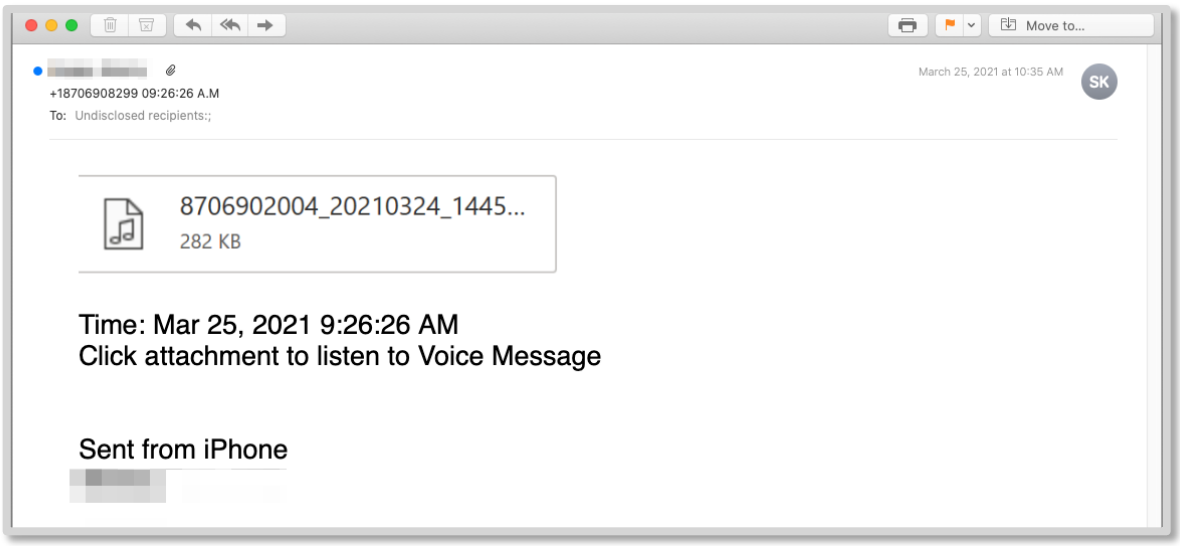
INKY classified this phishing attempt as a Microsoft impersonation because the branding in the message mimicked a Microsoft product. The bad actor uploaded to Google Docs malware or a malicious link, which Google has since removed. Another interesting thing that INKY turned up: the hijacked sender was one of the recipient's regular contacts. We know that because the First-Time Sender banner was missing.



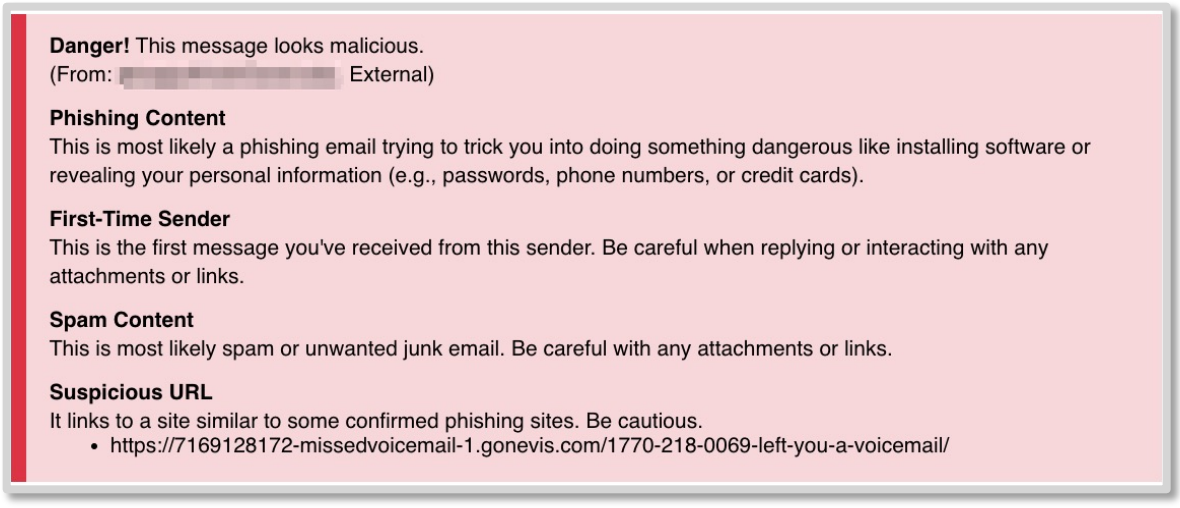
INKY™

MIMECAST | ACCOUNT TAKEOVER

A hijacked account that passed rudimentary checks for legitimacy was able to send a phish that looked like a voicemail. In fact, the supposed attached voicemail file was a fake. There was no attachment there. It was instead an embedded image that looked like an attachment but was instead a link that led to a malicious site that either injected malware or harvested credentials.



Although Mimecast had no problem with this email, it triggered five of INKY's anti-phishing modules.

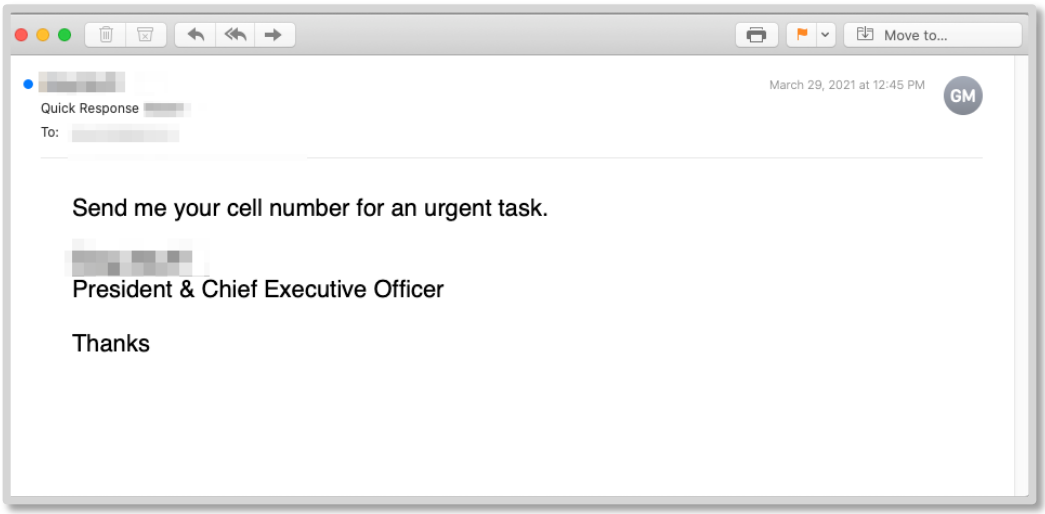


INKY™

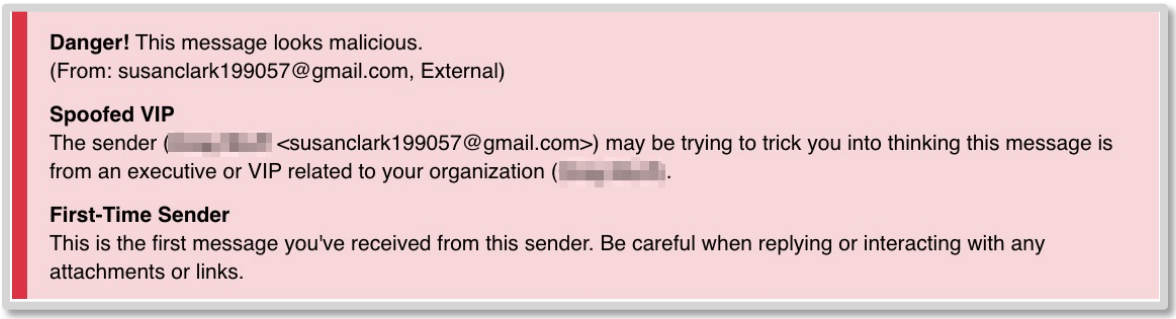
MIMECAST | CEO IMPERSONATION

Phishers can easily harvest rich contact information from social sites like LinkedIn. In this case, the black hat was able to get enough details to send to an employee a terse, one-line message that appeared to come from the CEO of the company.

The mail contained no malicious links or attachments. The scam was to get the employee to send their cell number, to which the phisher could text a request, likely to buy some gift cards and send the numbers via text. On a mobile phone, only the CEO's name would show.



INKY caught this one three ways. First, the Spoofed VIP module found, from the company's VIP list, the discrepancy between the real CEO's email address and the actual sender. The sender's address — susanclark199057@gmail.com — was a perfectly legitimate one from gmail. It just wasn't the CEO's. Also, the message tripped the First-Time Sender and general Danger! modules.



INKY™

Comparison Chart

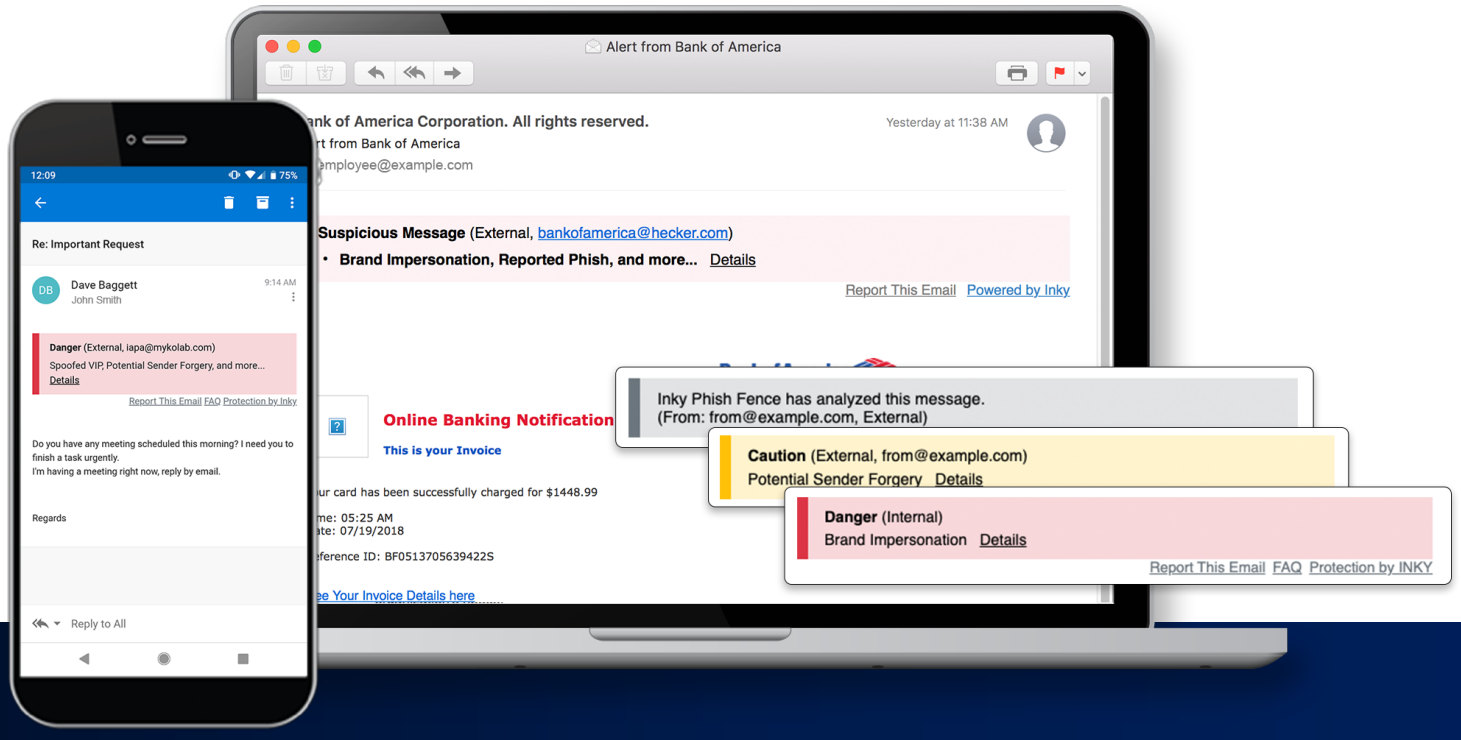
The chart below highlights how INKY compares with Proofpoint and Mimecast across various capabilities.

	PROOFPOINT	MIMECAST	INKY
Threat Protection	- Malware protection - Basic phishing protection - Basic Impersonation prevention - Attachment sandboxing - URL rewriting - Remediation	- Malware protection - Basic phishing protection - Attachment sandboxing - URL rewriting - Comparison to known threats	- Malware protection - Advanced phishing protection - Sender profiling - Confusable domain protection - Brand forgery detection with computer vision - URL rewriting - Deep link analysis - HTML sanitization / JS removal - Fake green banner detection - Banner-hiding CSS detection
Spam Filtering	- Inbound spam protection	- Inbound spam protection	- Inbound spam protection
Reporting	- Real-time mail flow reports - Inbound and outbound reports - PDF reports - Per-user reports - SIEM feed	- Real-time mail flow reports - Inbound and outbound reports - PDF reports - Per-user reports - SIEM feed	- Real-time status page for admins - Visualization dashboard gives admins the ability to search every part of an indexed message - Dashboard customization with filters - SIEM feed
End User Features	- Per user allow and block listing - Email quarantine - Quarantine digest - Static EXTERNAL banner	- Block and permit senders - Email quarantine - Bulk email delivery controls - Quarantine digest - Per user sender- and domain-level blocking - Static EXTERNAL banner	- Dynamic guidance banners - Report this Email link - Banners stripped from replies - Per user sender- and domain-level blocking
Data Loss Protection	- Outbound filtering and encryption - Desktop-centric workflow - Must use vendor DLP	- Outbound filtering and encryption - Must use vendor DLP	- Outbound filtering and encryption - Mobile-centric workflow with banners and actions in the inbox - Autocomplete/CC error detection - Can deploy with 3rd party DLP

INKY™

Why you should add INKY to your email security mix

- INKY catches phish that Secure Email Gateways like Proofpoint and Mimecast miss.
- Based on first-principles analysis (looking only at what's in the email itself), INKY catches phish that no one has ever seen before.
- INKY's computer vision allows it to see an email the way a person does. Its thorough analysis of the underlying header information lets it compare where the mail really came from with where it appears (to a person) to come from. When those two views don't line up, INKY flags the mail.
- INKY finds phish even if they are sent from legitimate (but perhaps hijacked) accounts.
- INKY's dynamic banners both educate users about dangerous emails AND let them report emails to INKY staff.
- When a user reports spam from an authenticated account (in the subscriber pool), they can block that sender — or even the entire domain — with a single click.



inky.com