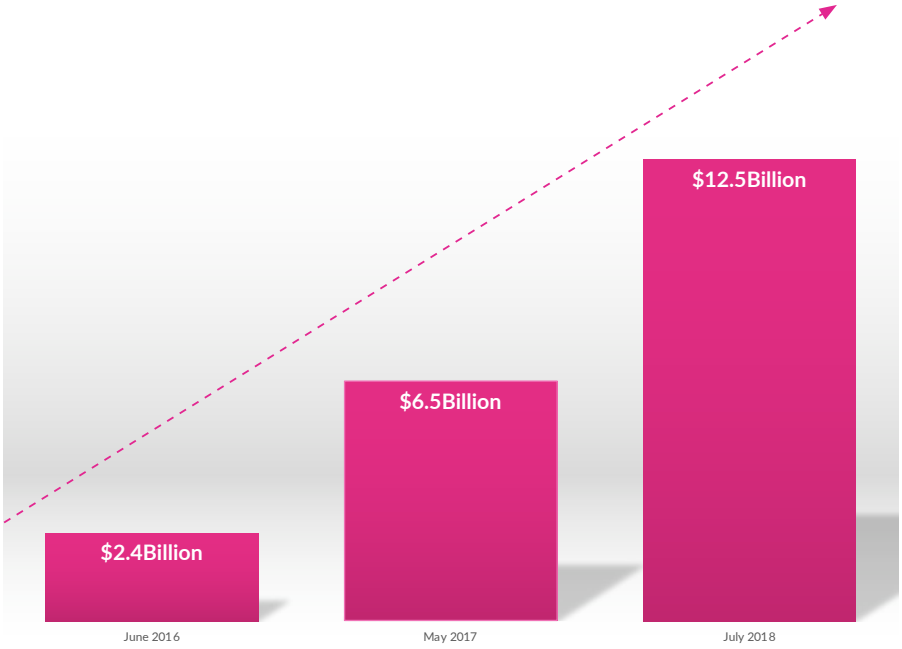
INKY™

Special Phishing Report

Introduction

Phishing remains the #1 cyber threat — and it's getting worse. As attacks evolve and losses mount into the billions of dollars annually, organizations seeking a solution are inundated daily with sales pitches from both established incumbent vendors and new upstarts promising phishing cure-alls. Unfortunately, most of these purported solutions do little in practice to reduce the flood of inbound phishing emails.

This report quantifies just how many phishing emails still breach the leading email protection systems, and examines why identifying and blocking these attacks still poses such a challenge.



Background

At INKY, our customer mix affords us a unique perspective; some customers integrate INKY as their sole mail protection system, while others deploy INKY downstream from an incumbent Secure Email Gateway (SEG) as the last line of a layered defense. In either case, INKY can perform some or all of the functions of a SEG: spam, malware, phishing, URL protection, and so on. Uniquely, though, our hybrid customer base gives us visibility into *both* the broad range of email attacks *and* precise data on what INKY flags that still passes through legacy SEGs. Stated plainly: we know exactly what INKY blocks that legacy SEGs miss. Throughout 1Q19, with our customers' permission, we captured statistics measuring this phenomenon, and provide the relevant data in this report. While we won't name the SEGs here, they are all well-established "Gartner SEG Magic Quadrant" vendors.

Analysis Period: 12/1/18 - 4/9/19 (130 days)

Unlike traditional SEGs, INKY uses a ternary rather than binary classification scheme. This gives end users more insight and understanding, and provides admins flexibility as to which emails to quarantine and which to simply flag with a warning banner. Here are brief descriptions of our three classifications.

Safe

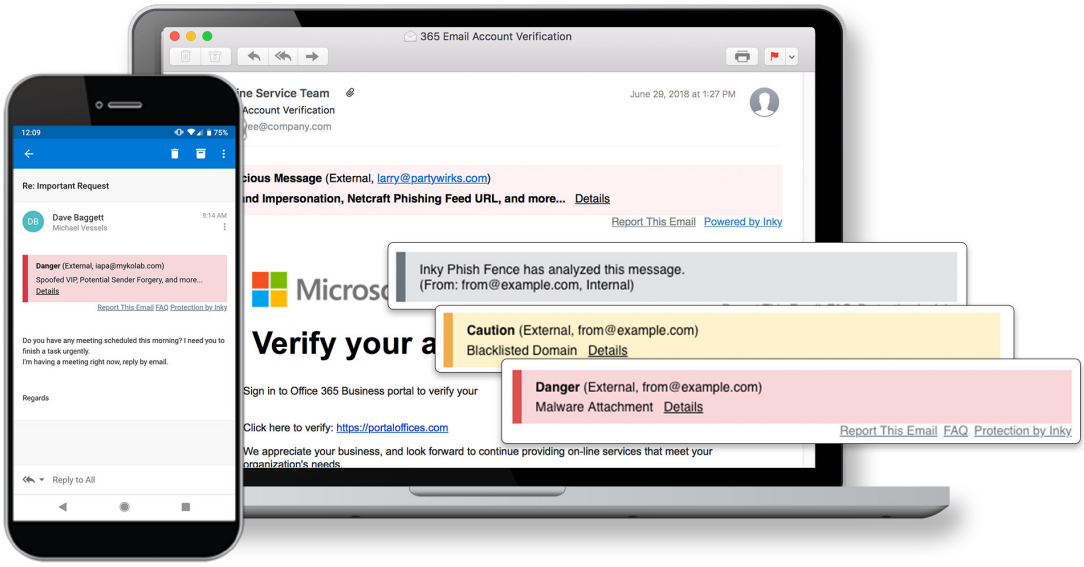
Neutral emails that INKY would normally add a gray banner to; these emails are predicted to be legitimate messages and are considered safe for the end user to act on.

Caution

Emails requiring caution or specific guidance. These may meet specific negative criteria, may simply appear unlike typical mail for the purported sender, or may be legitimate emails containing sensitive content — such as a wire request — requiring a company policy reminder. INKY adds a yellow banner to the top of these emails.

Danger

Emails for which INKY has high confidence of malicious intent, generally via INKY's computer vision, artificial intelligence, and machine learning engines. We manually verified these to ensure they weren't false positives. Customers configure whether these emails are delivered with a red banner or are moved to quarantine; INKY supports either behavior.



Customer One / SEG One

VIPs/C-Level:

The first thing we looked at was the C-Suite and "VIPs." With VIP impersonation so valuable, attackers try hard to compromise VIP email accounts. Customer One has seven VIP email accounts. Here are the stats for these mailboxes:

Level	# VIPs	# of Messages
Safe	7	18,750
Caution	7	2,599
Danger	7	166

Customer One's seven VIPs received 18,750 emails for which INKY and the upstream SEG One concurred that the content was safe and legitimate.

However, INKY flagged an alarming 2,599 emails with yellow caution banners. These numbers suggest that many of the emails had at least some cause for concern — or involved some sensitive content meriting special guidance. *Without INKY inline, these emails would have been delivered with no warning or annotation.*

Even worse, 166 malicious emails made it into the VIPs' inboxes. This means that under SEG One alone, VIPs would have been required to self-identify 166 phishing

attacks over four months — an annualized rate over 500. And all this while the vendor behind SEG One continues to not only tout but *charge extra for* their claimed phishing protection.

We next examined all users — not just the VIPs. The good news here is that INKY agreed with SEG One that the vast majority of emails (>87%) were safe and unremarkable. The bad news is that 1,454 users received 128,954 emails that INKY considered to be worthy of the yellow caution banner — a little over 1%. In each case, INKY provided either guidance on sensitive content or specifically warned about something atypical or suspicious. And keep in mind that INKY works *at the individual user level*, so these yellow caution banners aren't simple catch-all warnings; they are tailored to each recipient's personal mail traffic profile.

But obviously the most troubling stat is that 416 users received a total of 2,210 verified-malicious emails that SEG One happily delivered without any warning whatsoever. Think about that: without INKY and only SEG One in place, this customer would have received over 2,000 malicious emails in a four month period!

Level	# Users	# of Messages
Safe	1,610	893,069
Caution	1,454	128,954
Danger	416	2,210

Customer Two / SEG Two

VIPs/C-Level:

As before, our first goal for Customer Two / SEG Two was to understand the impact of attacks specifically targeting company executives. Again, we tallied INKY's classification of all emails to these seven recipients that SEG Two allowed through:

Level	# VIPs	# of Messages
Safe	7	26,481
Caution	7	6,016
Danger	7	519

INKY agreed with SEG Two that 26,481 emails looked unremarkable. However, in over 6,016 cases, INKY attached a yellow caution banner to an email, and provided the recipient executive with additional guidance on the content of the message, its sender, etc. Further, these executives received a remarkable 519 verified-malicious emails in just 130 days. Without INKY as the protection of last resort, these malicious mails would have been delivered to these executives with no warnings of any kind. Thanks for nothing, SEG Two!

Next, we looked at stats for all users at Company 2. Over six and a half million times INKY and SEG Two reached the same conclusion that the emails were legitimate. However, over 1,500 users received 346,347 messages that INKY flagged as unusual, sensitive, or suspicious — and consequently added a yellow caution banner to.

Again, INKY doesn't quarantine or remove these yellow emails; instead it delivers them along with additional information the user can use to decide how to treat the email. So users get real-time information and guidance right in their inboxes.

Level	# Users	# of Messages
Safe	1,544	6,602,125
Caution	1,537	346,347
Danger	1,152	12,627

Now look at the Danger category: that SEG Two allowed through 12,627 verified-malicious emails to 1,152 users. Without INKY, these would have ended up in users' inboxes. With INKY they are either moved to quarantine or given red danger banners.

Customer Three / SEG Three

VIPs/C-Level:

For Customer Three / SEG Three, we again isolates the C-suite and VIPs from the broader pool of email users. Let's examine the stats for these 11 VIP email accounts:

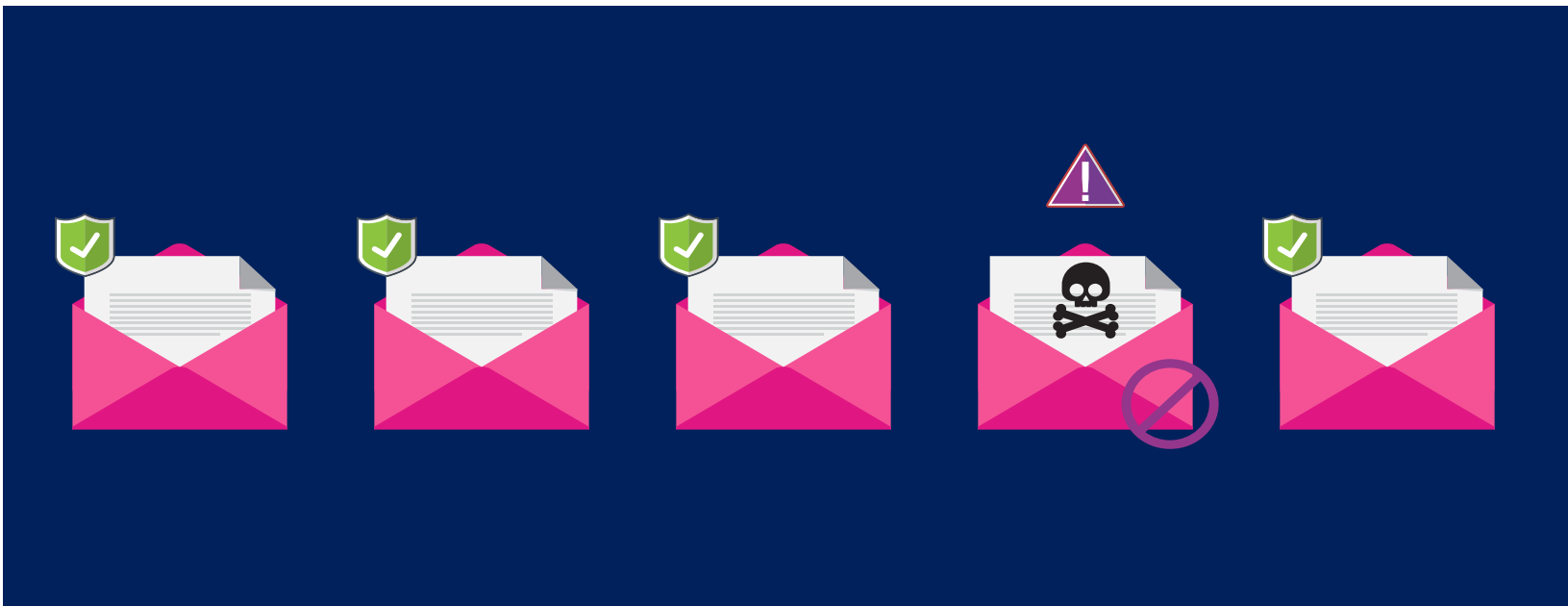
Level	# VIPs/C-Level	# of Messages
Safe	11	25,823
Caution	11	1,993
Danger	11	198

INKY concurred with the legacy platform 25,823 times, with both platforms agreeing that these messages were legitimate. Looking at the yellow caution banner emails, though, we can see that INKY flagged almost 2,000 emails as requiring additional caution and further review; without INKY recipients would receive none of these prompts. Worse, without INKY, 198 phishing emails would have been delivered to these VIPs entirely unmarked.

Finally, here are the numbers for all of the users at Customer Three:

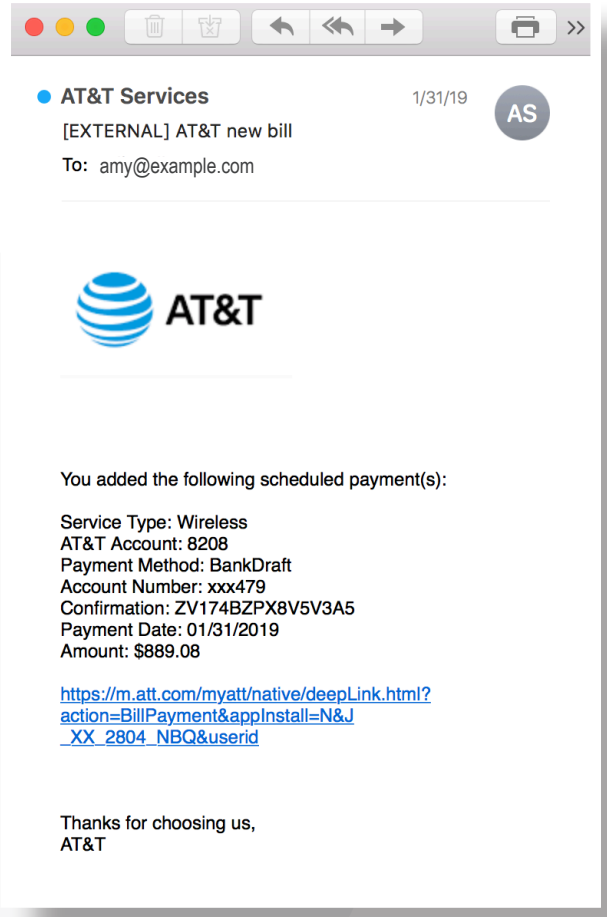
Level	# Users	# of Messages
Safe	2,386	407,168
Caution	1,874	29,989
Danger	441	1,603

Thankfully, INKY and SEG Three agreed on 407,168 messages; however, the trend of Caution and Danger emails getting through the SEG is again clear: 29,989 emails required a level of caution, while a stunning 1,603 verified-malicious emails made it through SEG Three.



As they say, a picture is worth a thousand words. So here we've included a rogues' gallery of some of the zero-day phish INKY caught among the 16,000 phishing emails detailed above:

What the phish looked like:



AT&T Services 1/31/19

[EXTERNAL] AT&T new bill

To: amy@example.com

AT&T

You added the following scheduled payment(s):

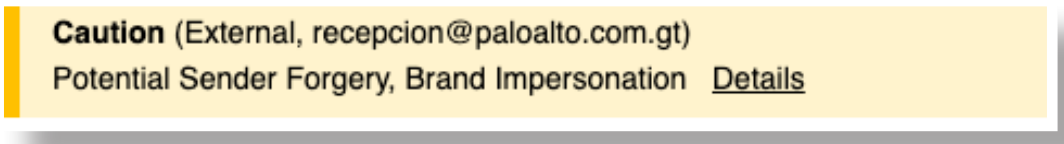
Service Type: Wireless
AT&T Account: 8208
Payment Method: BankDraft
Account Number: xxx479
Confirmation: ZV174BZPX8V5V3A5
Payment Date: 01/31/2019
Amount: $889.08

https://m.att.com/myatt/native/deepLink.html?action=BillPayment&appInstall=N&J_XX_2804_NBQ&userid

Thanks for choosing us,
AT&T

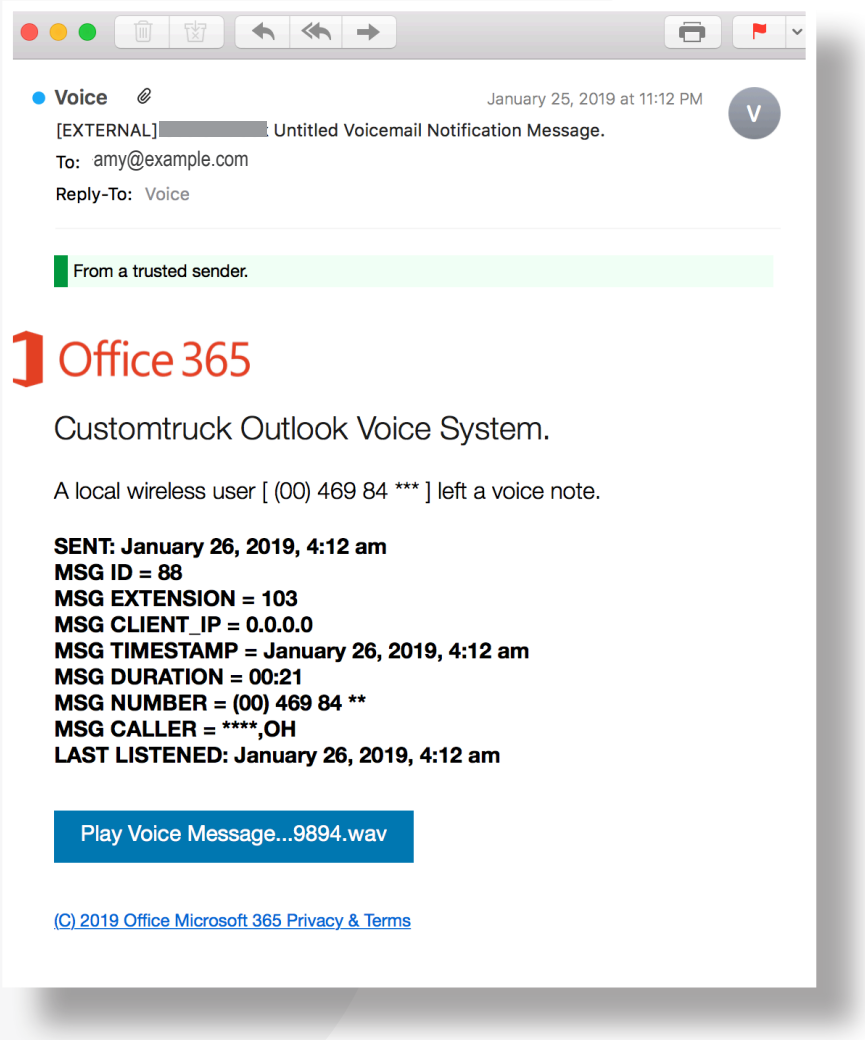
In this case, INKY was able to identify that this email was a likely sender forgery and brand impersonation.

What the user saw:



Caution (External, recepcion@paloalto.com.gt)
Potential Sender Forgery, Brand Impersonation Details

What the phish looked like:



Voice January 25, 2019 at 11:12 PM

[EXTERNAL] Untitled Voicemail Notification Message.

To: amy@example.com

Reply-To: Voice

From a trusted sender.

Office 365

Customtruck Outlook Voice System.

A local wireless user [(00) 469 84 ***] left a voice note.

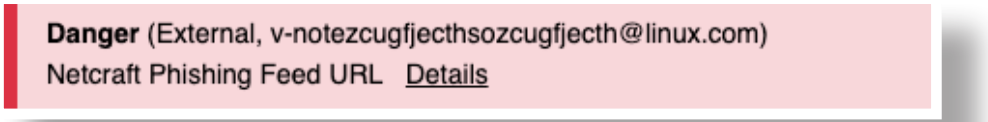
SENT: January 26, 2019, 4:12 am
MSG ID = 88
MSG EXTENSION = 103
MSG CLIENT_IP = 0.0.0.0
MSG TIMESTAMP = January 26, 2019, 4:12 am
MSG DURATION = 00:21
MSG NUMBER = (00) 469 84 **
MSG CALLER = **,OH**
LAST LISTENED: January 26, 2019, 4:12 am

Play Voice Message...9894.wav

(C) 2019 Office Microsoft 365 Privacy & Terms

In this O365 example, INKY recognized the link as a route to a known phishing site and warned the recipient. Notice, too, the fake green banner added by the attacker.

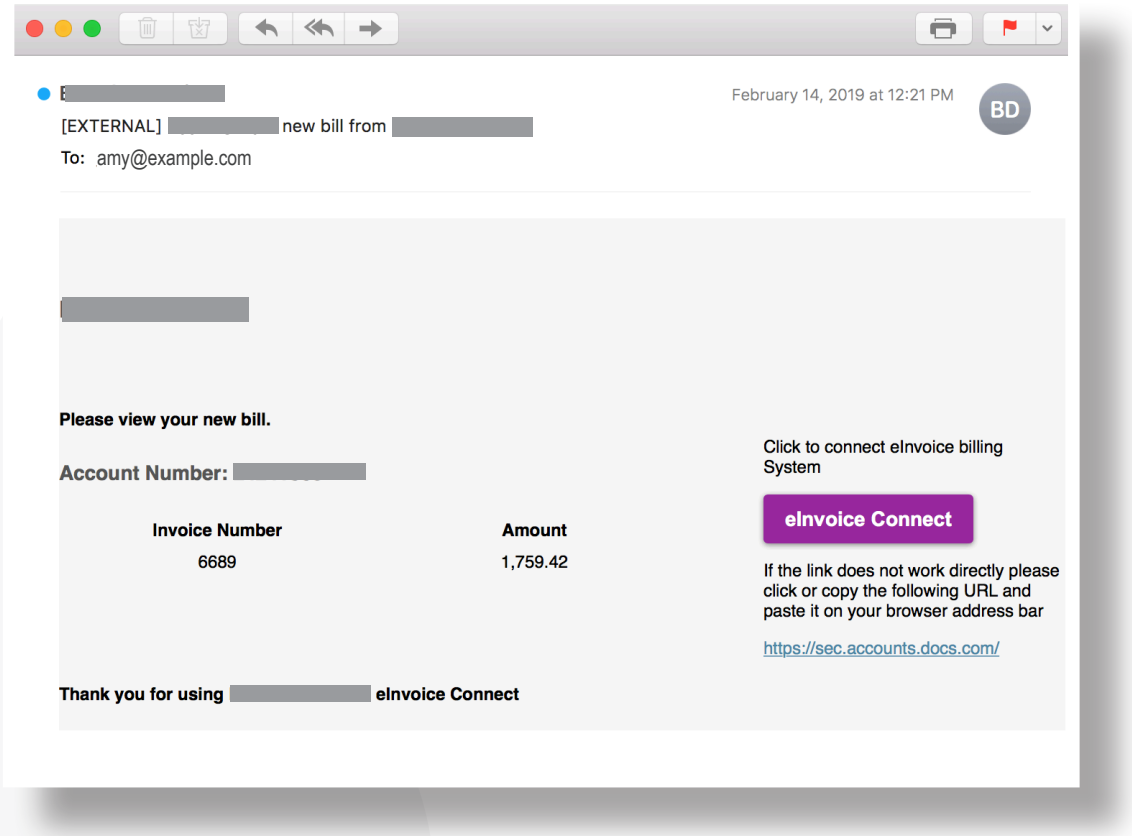
What the user saw:



Danger (External, v-notezcugfjecthsozcugfjecth@linux.com)
Netcraft Phishing Feed URL Details

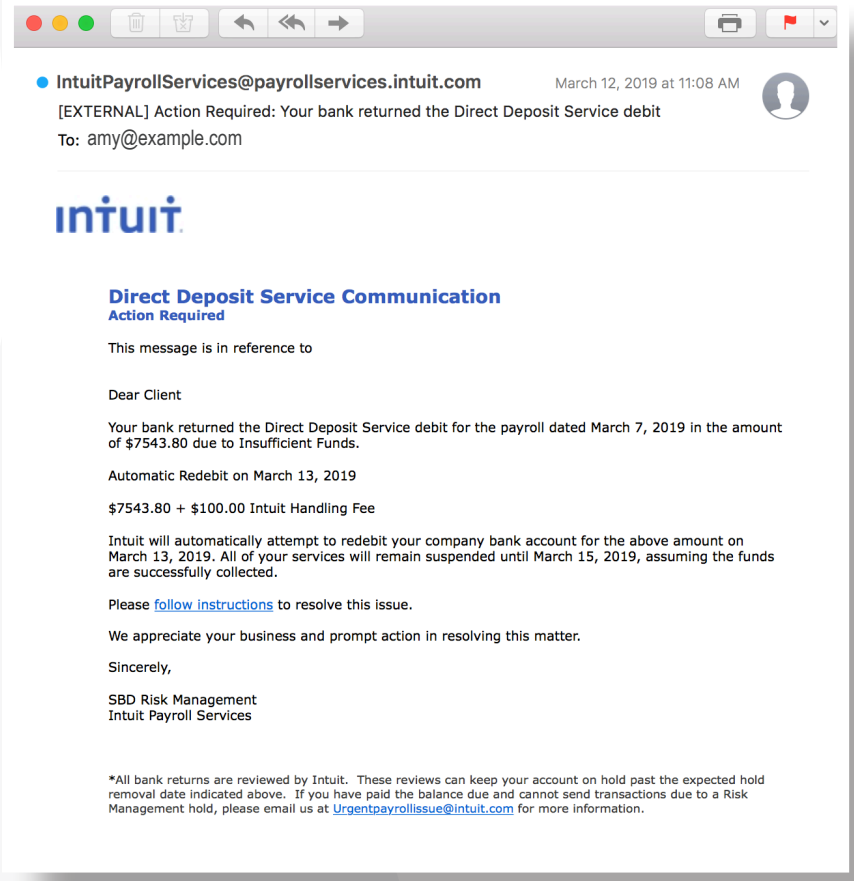
For this invoice payment request, INKY was able to discern that the content of the email was both sensitive *and* fraudulent.

What the phish looked like:



What the user saw:

What the phish looked like:



IntuitPayrollServices@payrollservices.intuit.com March 12, 2019 at 11:08 AM

[EXTERNAL] Action Required: Your bank returned the Direct Deposit Service debit

To: amy@example.com

INTUIT

Direct Deposit Service Communication
Action Required

This message is in reference to

Dear Client

Your bank returned the Direct Deposit Service debit for the payroll dated March 7, 2019 in the amount of $7543.80 due to Insufficient Funds.

Automatic Redebit on March 13, 2019

$7543.80 + $100.00 Intuit Handling Fee

Intuit will automatically attempt to redebit your company bank account for the above amount on March 13, 2019. All of your services will remain suspended until March 15, 2019, assuming the funds are successfully collected.

Please follow instructions to resolve this issue.

We appreciate your business and prompt action in resolving this matter.

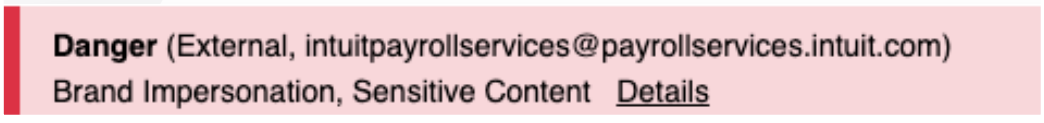
Sincerely,

SBD Risk Management
Intuit Payroll Services

*All bank returns are reviewed by Intuit. These reviews can keep your account on hold past the expected hold removal date indicated above. If you have paid the balance due and cannot send transactions due to a Risk Management hold, please email us at Urgentpayrollissue@intuit.com for more information.

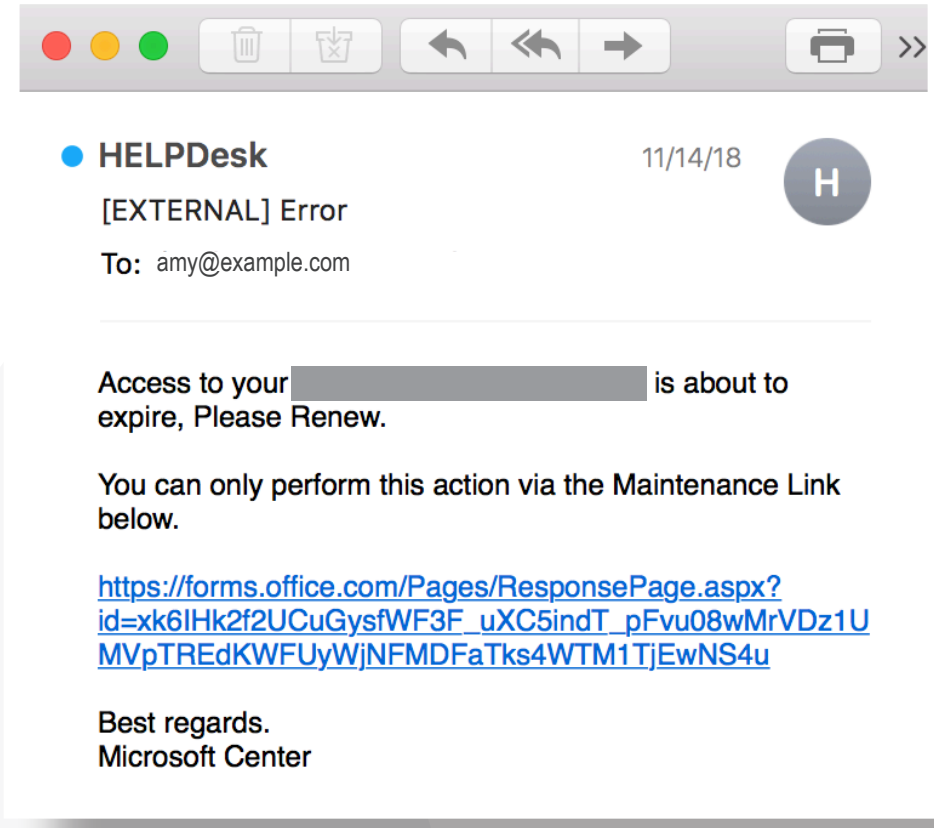
INKY saw right through this attacker's rather convincing attempt to impersonate Intuit.

What the user saw:



Danger (External, intuitpayrollservices@payrollservices.intuit.com)
Brand Impersonation, Sensitive Content Details

What the phish looked like:



HELPDesk 11/14/18

[EXTERNAL] Error

To: amy@example.com

Access to your [redacted] is about to expire, Please Renew.

You can only perform this action via the Maintenance Link below.

https://forms.office.com/Pages/ResponsePage.aspx?id=xk6lHk2f2UCuGysfWF3F_uXC5indT_pFvu08wMrVDz1UMVpTREdKWFUyWjNFMDFaTks4WTM1TjEwNS4u

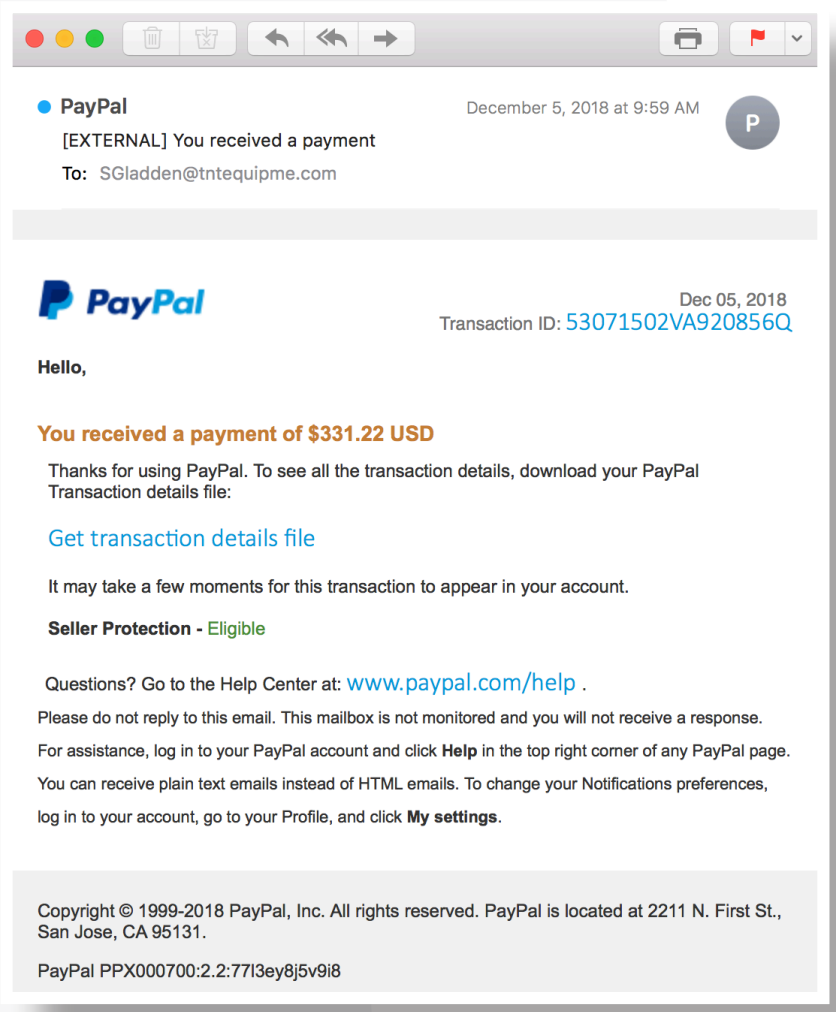
Best regards.
Microsoft Center

The links in this email look legitimate enough that the legacy phishing applications failed to spot them, but INKY recognized them as a clever attempt at Brand Impersonation.

What the user saw:

Danger (External, ogoj195@hughes.net)
Brand Impersonation Details

What the phish looked like:



PayPal
December 5, 2018 at 9:59 AM
[EXTERNAL] You received a payment
To: SGladden@tntequipme.com

PayPal
Dec 05, 2018
Transaction ID: 53071502VA920856Q

Hello,

You received a payment of $331.22 USD

Thanks for using PayPal. To see all the transaction details, download your PayPal Transaction details file:

Get transaction details file

It may take a few moments for this transaction to appear in your account.

Seller Protection - Eligible

Questions? Go to the Help Center at: www.paypal.com/help .

Please do not reply to this email. This mailbox is not monitored and you will not receive a response.

For assistance, log in to your PayPal account and click **Help** in the top right corner of any PayPal page.

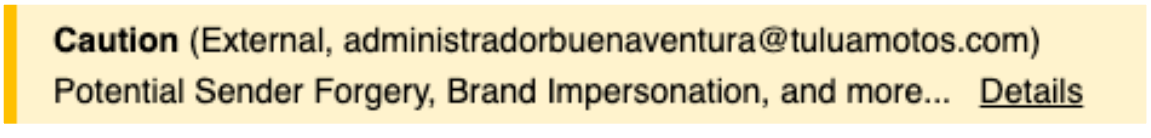
You can receive plain text emails instead of HTML emails. To change your Notifications preferences, log in to your account, go to your Profile, and click **My settings**.

PayPal PPX000700:2.2:77l3ey8j5v9i8

We'd bet good money that this PayPal forgery is good enough to fool even diligent users of phishing awareness training.

INKY can tell this mail looks like it's from PayPal — just like the intended victim — but suspects the sending domain is not legitimate for PayPal.

What the user saw:



Caution (External, administradorbuenaventura@tuluamotos.com)
Potential Sender Forgery, Brand Impersonation, and more... Details

What the data means:

Just a single phishing attack can cost an organization hundreds of thousands, if not millions, of dollars — and untold IP theft and reputation damage. Yet the three widely-used SEGs we examined here allowed over 16,000 malicious emails through in a four-month period. Fortunately, INKY wasn't fooled by any of them, because INKY uses new technologies in novel ways to "see" emails much like the human recipients do. So ask yourself:

Can you afford hundreds or even thousands of phishing attacks every year?

Do you still trust your current SEG solution to protect your VIPs and users?

Are you ready to stop phishing attacks once and for all?

Schedule a demo today.

What Makes INKY Best

INKY provides the most comprehensive malware and email phishing protection available. To see INKY's anti-phishing solution in action, request a demo. Let us show you what a difference it can make.

INKY® Phish Fence uses a proprietary blend of Machine Learning and Artificial Intelligence that blocks even the most sophisticated phishing attacks that get past other systems.

Alerts are added to the email itself, which means they look the same on desktop or mobile. This is a significant difference from other systems, which display warnings in headers or with add-ins that may not render properly, or at all, in mobile applications.

INKY® Phish Fence sits on top of any email system, including Microsoft Office 365 and Google Suite.

INKY® Phish Fence scans every sent and delivered email automatically and flags malicious emails.

A comprehensive dashboard allows admins to see both the bigger pictures and to drill down to specific attacks, individuals, and individual messages. A robust search allows for detailed reporting at the granular level.

It can be set up and ready to go in just a few hours.

Unlike any other anti-phishing systems, **INKY® Phish Fence** uses proprietary technology and algorithms to "see" each email as the recipient would. Unlike a person, however, it can detect an email forgery and/or malicious or suspicious content. Once detected, it can redirect the email to a quarantine area or deliver it with disabled links and warnings.

We're passionate about email.

Ready to talk about an issue you're facing in email security at your organization?

www.inky.com