MIS
PROUD PARTNER

EMAIL SECURITY ANNUAL REPORT

2024-2025

TABLE OF CONTENTS

Executive Summary

AI takes center stage in email security.

The email security industry is a perpetual battlefield and each year the stakes grow higher. 2024 was no exception, especially in the face of artificial intelligence where the risks for loss have become even more significant.

Phishing threats grew in both volume and sophistication, introducing new attack vectors like QR codes, cross-site scripting, and weaponized file types (e.g., RTF and DOT). Cybercriminals also increasingly exploited trusted services such as DocuSign and PayPal, underscoring the urgent need for adaptive, robust security solutions.

When it comes to Artificial Intelligence (AI), INKY has always been a trailblazer – playing a pivotal role in detecting and mitigating new threats. Now with the release of INKY's Generative AI Detection, we are redefining the future of email security. What does this mean? The future of email security is understanding intent. When cybercriminals disguise their messages with wording that doesn't signal danger, INKY alone can understand the intent.

INKY remains at the forefront of email security, continuously innovating to stay ahead of emerging threats and providing unparalleled protection for our clients. We are committed to maintaining our leadership position and ensuring that our solutions meet the evolving needs of businesses in an increasingly complex digital world.

Cybercrime Worsened Going Into 2024

#1 Phishing Remains the Most Common Attack Vector

BEC **$2.9 Billion** was Lost in Business Email Compromise Schemes

$534 Billion was Lost to Data Breaches

$12.5B

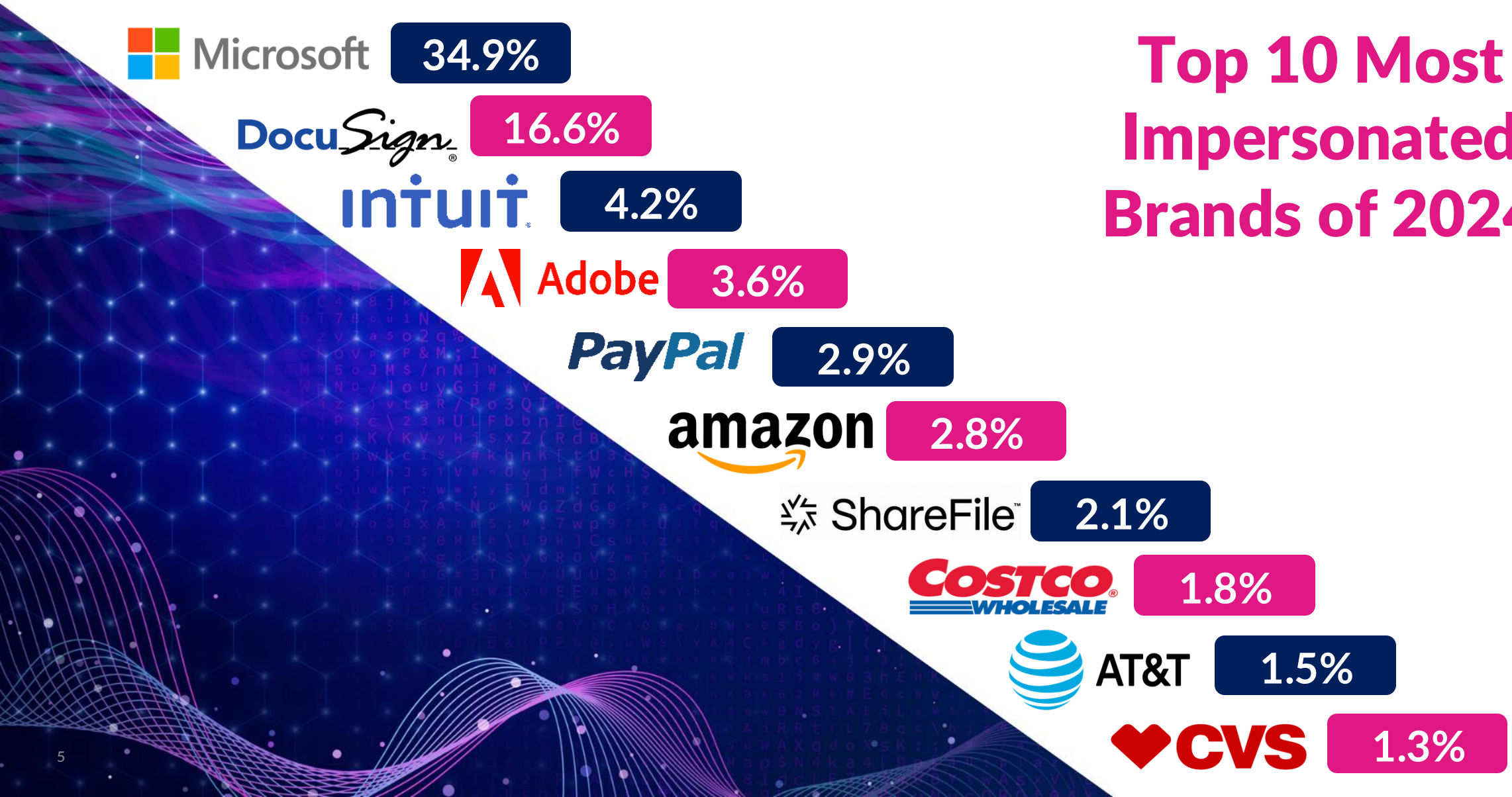
Was Lost to Cybercrime

30%

Of All Reported Cybercrimes Were Phishing Attacks

Source: 2023 FBI Internet Crime Report

Brand Impersonations Were Persistent and Prevalent

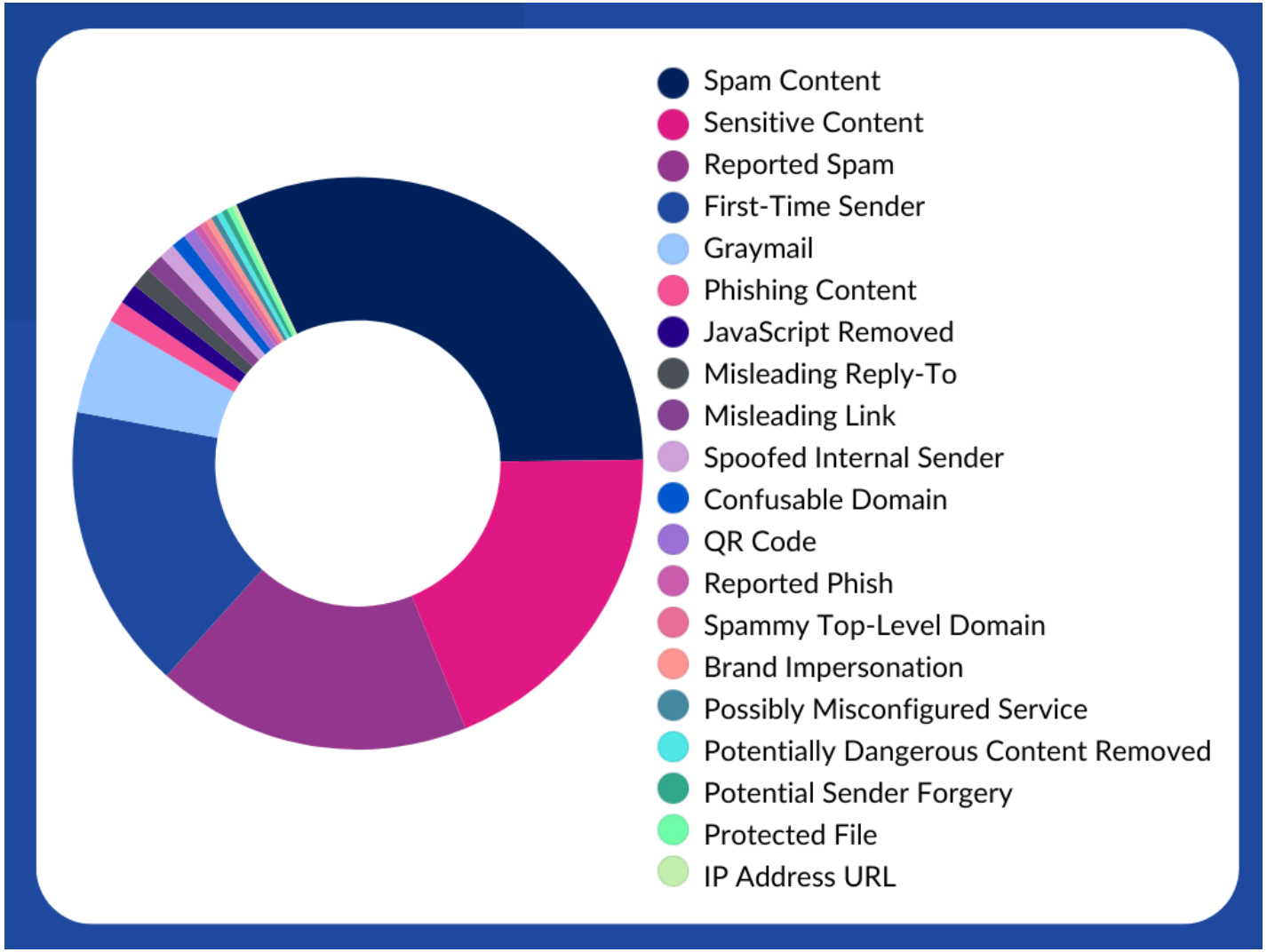


Top 10 Most Impersonated Brands of 2024

New Threat Categories Surfaced

New Threat Categories in 2024

- Newly Registered Domain
- Potential Conversation Hijack
- Potential Fake Conversation
- Possible Spoofed Known Sender
- Released From Quarantine
- External Sharing Link
- Executable File



Sophisticated Phishing Trends Emerged

- QR Code Phish
- Multi-Layered Phish Leveraging Legitimate Tools
- Weaponizing Text Files
- Cross-Site Scripting
- Controversial Telegram Bots

QR Code Phish Continue to Dominate

As predicted last year, QR code phishing has become one of the most rapidly growing forms of phishing. However, in 2024, INKY observed a new evolution of this tactic, where QR codes are constructed using HTML tables and Unicode characters.

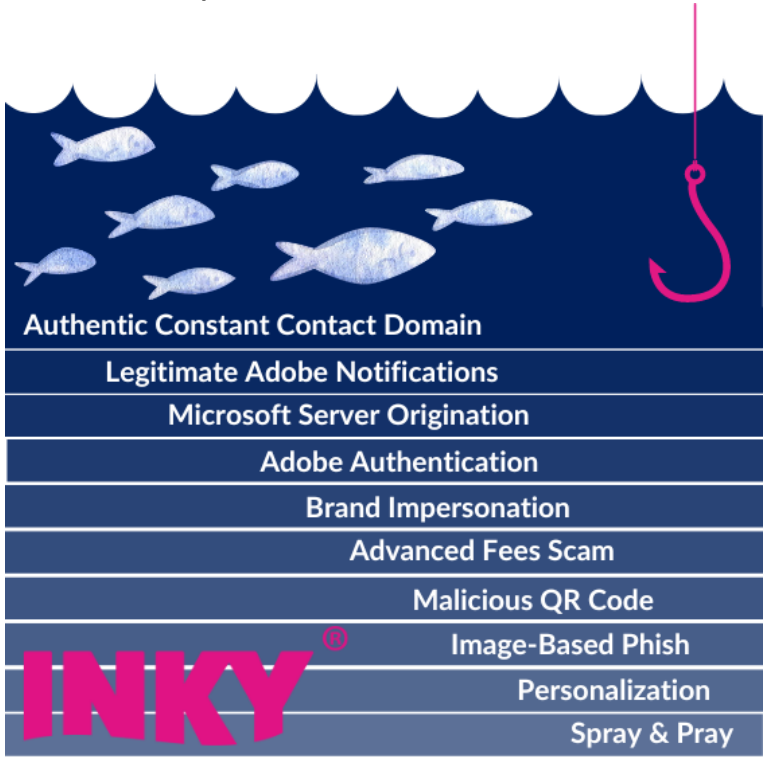
QR codes are simply groups of black squares arranged in a way that allows users to scan them with a camera to navigate to a link. But what if you created a table of squares, filled in with black or white backgrounds, or even used the Unicode character █, to mimic a QR code?

Consider the two images below. The first is the QR code without the table's grid lines—it looks exactly like a typical QR code but is incredibly difficult to detect because it’s not a standard image format. The second example reveals the grid lines, exposing the underlying technique.

INKY analyzed the rendered DOM to see what the user sees. Although the email contains <table> or <pre> tags instead of an image in HTML, our Computer Vision checks recognize that the user is seeing a QR code. INKY then scans the QR code and assesses whether it's dangerous.

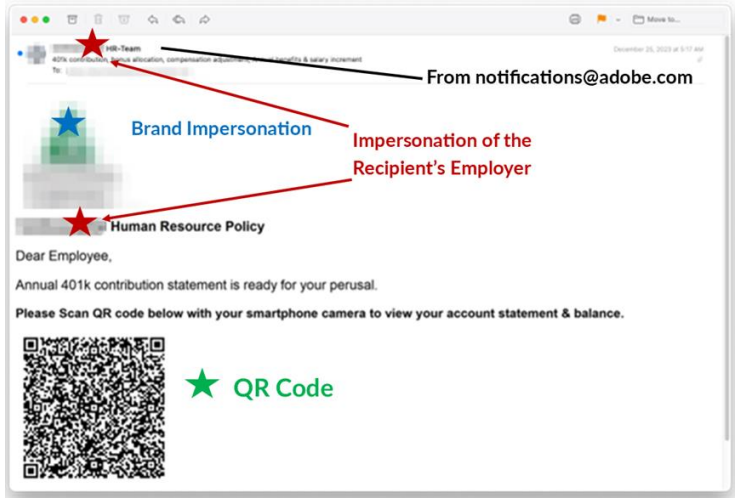
Multi-Layered Phish Leverage Legitimate Tools

Looking for the tell-tale signs of a phishing email is something many of us have come to do automatically. However, things get much trickier when the phishing emails come in the form of legitimate Adobe notifications, have been authenticated (SPF & DMARC) by adobe[.]com, and use actual Constant Contact tools.



Even with these legitimate elements in place, phishers are rising to a whole new level, layering on additional (and we mean lots of additional) phishing tactics to achieve maximum results.

From personalization to QR Code abuse, these phishers were really layering it on. INKY found that the domain of the QR code link belonged to a well-known **authentic Constant Contact domain** used in email marketing. The abused domain redirected users to malicious sites. In the end, the payload is an effective **advanced fees phishing scam**.

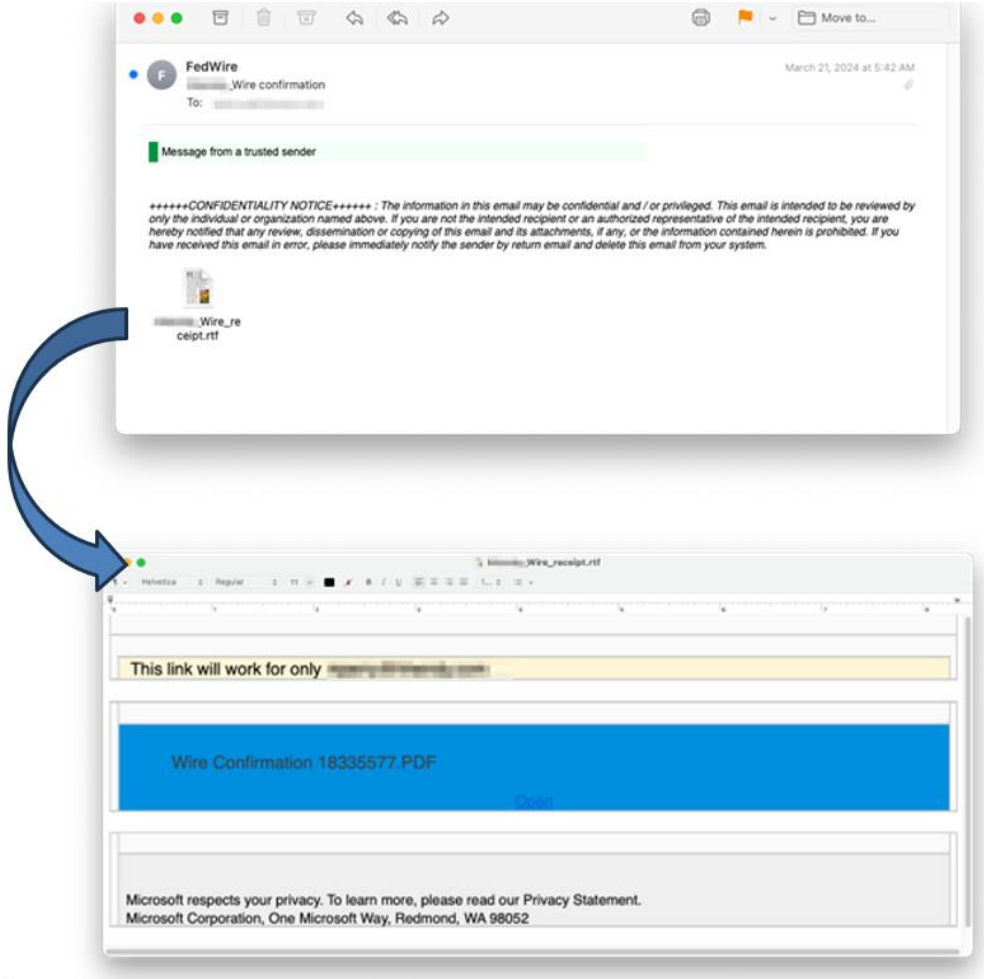


Personalized Text Files Were Weaponized

Computers store many types of data, such as text, images, videos, and spreadsheets. The file type, or format, tells the computer which type of data it contains, and it's usually reflected in the file extension. Of all file formats, a text file is the most common. Rich Text Files fall into that category. RTF files are platform-independent, meaning that they can be opened and edited on any computer regardless of the operating system. In addition to text and graphics, RTF files can also include embedded fonts, tables, and hyperlinks, making it a great choice for the cybercriminals.

INKY caught a variety of these emails, including 1,500 of the one shown here, over the course of just two days. This phishing email includes personalization and brand impersonation to help give it credibility. The recipient's company name is even included in RTF's file name.

Because this phish is impersonating Fedwire, once the RFT link is opened we see what looks to be a link for transferring funds. Note the message at the top even tries to convince the victim that they're reviewing a private transfer just for them. In reality, anyone can use the link, which takes them to a Microsoft credential harvesting site on workers[.]dev.

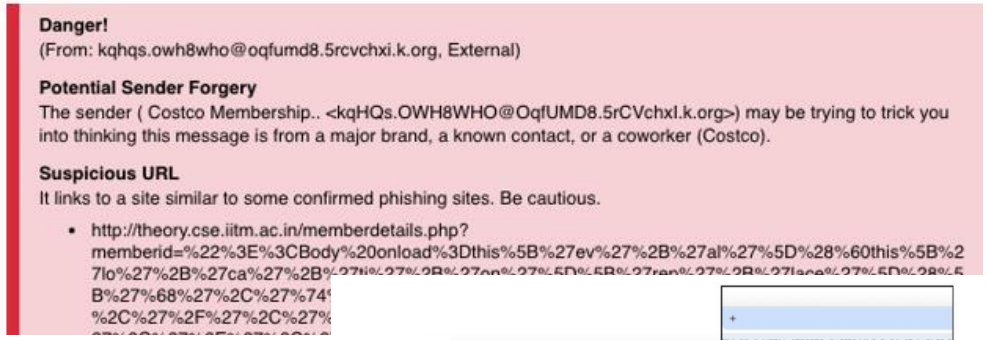


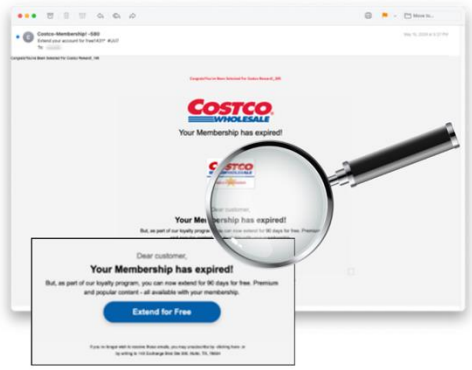
Cross-Site Scripting Made Its Debut

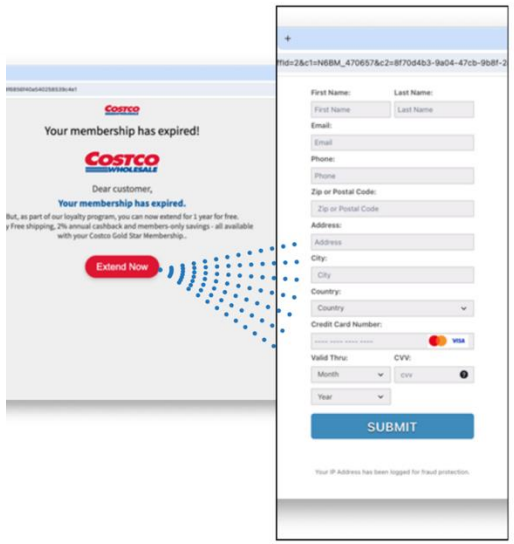
INKY discovered an increase in phishing emails using malicious redirect scripts in URL-encoded links.

A Word About URL Encoding: URL encoding converts characters into a format that can be transmitted over the Internet. This encoding replaces unsafe ASCII characters with a "%" followed by two hexadecimal digits. Spaces are replaced by "+", and special characters like "<", ">", "/", and others are replaced by their respective hexadecimal codes. Then, to the delight of cybercriminals everywhere, web browsers will automatically decode the obfuscated strings back into ASCII.

For now, this technique has only appeared in prize scams that impersonate reputable brands like Costco, YETI, Harbor Freight Tools, and Lowes. Let's take a closer look at a Costco phishing email example.







The message here appears to be a notice of an expired membership. But, read a little more closely and you'll see the email offers **to extend your membership for free!**

However, when clicking on "Extend for Free" the recipient opens a page on a malicious site impersonating Costco. From there, clicking on "Extend Now" brings you to a harvesting form that collects personal and financial information.

Phishers Leveraged Controversial Telegram Bots

Telegram Messenger, known simply as Telegram, is a cloud-based, multi-platform social media and instant messaging (IM) service. INKY discovered an increase in the use of HTML attachments that abuse Telegram bots in phishing attacks. Telegram bots are automated API-driven programs that run inside Telegram, performing tasks like sending messages, retrieving information, or interacting with users. While Telegram is not designed for criminal activities, its focus on privacy and flexibility appeals to those looking for ways to avoid detection or prosecution.

In this phishing scam recipients received an email with an HTML attachment. The attached file name uses the local part of the recipient's email address, in other words, everything before the @ symbol.

Clicking on the HTML attachment isn't "dangerous" (no data is harmed, manipulated, or stolen). However, the HTML attachment builds a local website that's only accessible to the recipient's browser (the file isn't hosted on a public server). The page mimics a legitimate Microsoft login page and uses a form to collect credentials from the user.

The victim is taken to a form (with id="voicemailForm") captures the recipient's email and password when they press the "Sign in" button. Instead of submitting the data to a legitimate Microsoft server, it triggers a JavaScript (jQuery) event that sends the email, password, and the user's IP address to the attacker via a Telegram bot.

The bot's details are stored in the variables chatId and apiToken, which direct the stolen data to the attacker's Telegram account. The script fetches the user's public IP address using the service https://api.ipify.org?format=json and includes this IP address in the message sent to the attacker.

Figure 1: Phishing Email

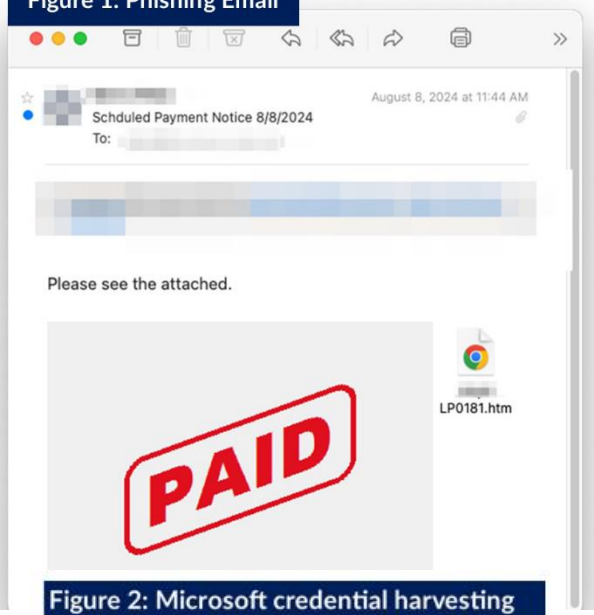
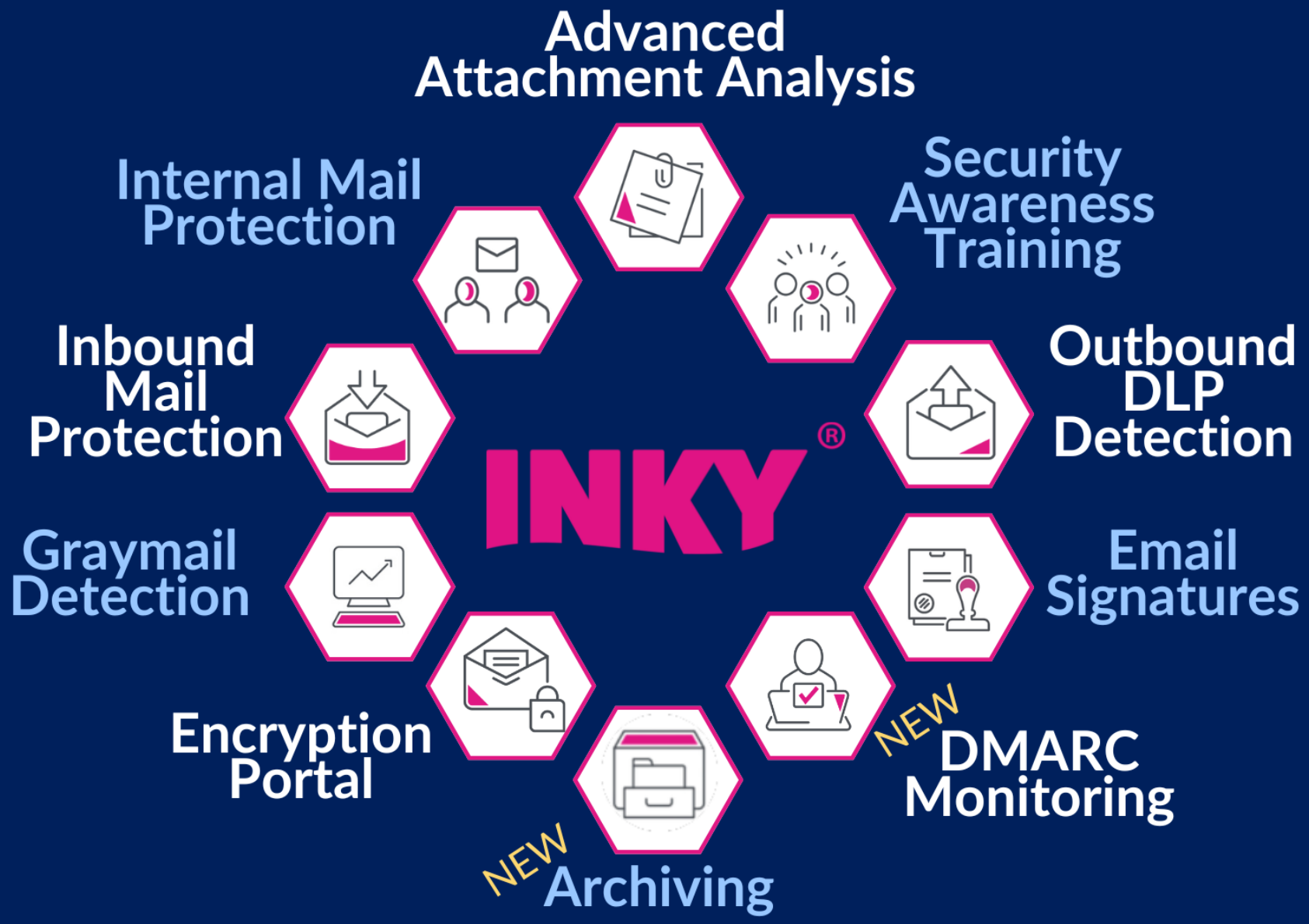


Figure 2: Microsoft credential harvesting page hosted on recipient's local machine

INKY's Portfolio of Products Continued to Grow



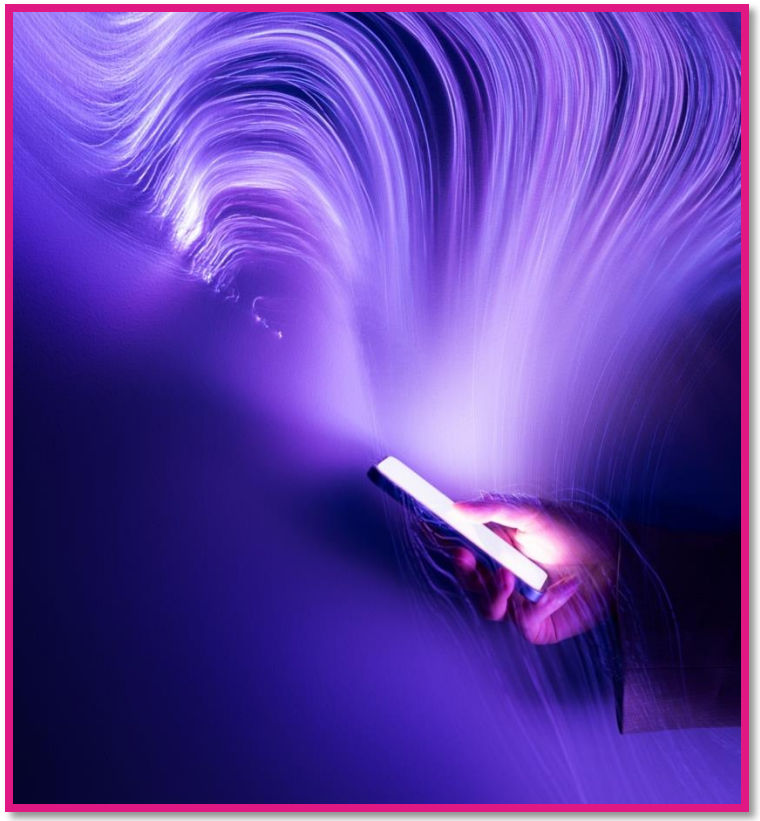
INKY Launches Generative AI Detection

A NEW ERA OF EMAIL SECURITY

INKY's integration of Generative AI has ushered in a new era of email security, providing unparalleled protection against modern threats.

While traditional methods rely on outdated pattern databases, INKY's GenAI detects the true meaning behind the words, ensuring that even the most cleverly disguised scams are caught.

This technology is integrated into INKY's email analysis pipeline, ensuring that all incoming emails are thoroughly analyzed after initial reputational and spam checks. By converting obfuscated content into clean text, the system can more effectively identify the true intent behind each email, making it highly effective at detecting sophisticated phishing threats and zero-day attacks.



Email Security Vendors Are Now Defined By GenAI

- **Traditional methods of threat detection are now falling short.**
- **Tackling tomorrow's email security challenges demands a new level of threat detection—powered exclusively by Generative AI.**
- **Applying Generative AI to email has challenges**
  - **Challenge #1:** Prone to Mistakes
  - **Challenge #2:** High Computational Costs
  - **Challenge #3:** Data Privacy Concerns (Third Party Training)
  - **Challenge #4:** Needs to Adapt to Be A Successful Email Security Tool

INKY Solved the GenAI Challenges

- **Challenge #1:** Prone to Mistakes
  - **INKY's Solution:** Optimized models & rigorous testing for accuracy in email context.
- **Challenge #2:** High Computational Costs
  - **INKY's Solution:** Cost-effective implementation, included in Pro/Advanced bundles.
- **Challenge #3:** Data Privacy Concerns (Third Party Training)
  - **INKY's Solution:** No data sent externally – all models run within INKY infrastructure.
- **Challenge #4:** Needs to Adapt to Be A Successful Email Security Tool
  - **INKY's Solution:** Seamless integration within INKY's analysis pipeline.

Understanding a Message's Intent Becomes Crucial

With the integration of generative AI, INKY can now understand the meaning and intent behind every email, regardless of how cleverly it is worded or disguised. INKY's new intent labels enhance our GenAI-powered detection platform. Examples include:

- **Ultimatum** – Detects when a sender pressures the recipient with an ultimatum.
- **Cold Email** – Identifies senders who haven't reached out in a long time, signaling potential phishing attempts.
- **Support Line** – Flags messages that include a support phone number or email with instructions to contact for assistance.
- **Nudge** – Recognizes subtle prompts designed to elicit a response from the recipient.

“We’re proud to have reached another industry first – this time with GenAI. INKY goes well beyond reading words and can now understand intent. It’s a difficult engineering problem to solve but we've done it so efficiently that we can run it on every single mail.

- *Dave Baggett*
CEO and Founder

INKY®

Learn more about INKY’s GenAI by visiting www.inky.com/product/generative-ai

INKY CONTINUES TO INNOVATE

We Simplified Our Product Offering Structure

STANDARD

Inbound & Internal Email Protection

NextGen AI Detection Capabilities

Advanced Computer Vision

QR Code Defense

Anomaly Detection

Standard Attachment Analysis

URL Time-of-Click Protection

Geo-Blocking

Spam Filtering

End User-Managed Allow & Block List

PRO

Everything in Standard plus:

GenAI Intent Analysis

Zero-Day Malware Protection

Advanced Attachment Analysis

Advanced Graymail Detection

Customer Graymail Delivery Locations

End User-Managed Graymail

DMARC Monitoring

ADVANCED

Everything in Pro Plus:

Outbound DLP Detection

Custom Outbound Rules Engine

Advanced Approval Workflows

Encryption Portal

ADD-ON PRODUCTS

Security Awareness Training

Educate employees with phishing simulation and videos.

Email Signatures

Control email signatures for compliance and branding.

Archiving

Protect, recover, and ensure compliance for business-critical data.

What Does the Future Hold?

Prediction #1

Increasingly Convincing Content Produced Using GenAI

Prediction #2

An Increase in Personalized Phishing Attacks

Prediction #3

AI-Enhanced Phishing Kits Will Become Much More Prevalent

Prediction #4

Numerous False/Positives as Major Email Providers Aggressively Attempt to Block Phishing Attacks

Prediction #5

Mobile Device Integrations Will Become More Crucial as Professionals Return to the Office.

MIS

CONTACT US

770-945-5487

www.mis-solutions.com

info@mis-solutions.com