



**INKY**<sup>®</sup>

EMAIL SECURITY ANNUAL REPORT **2022 - 2023**

# Insights, Predictions, and Growing Trends



## ➤ Executive Summary

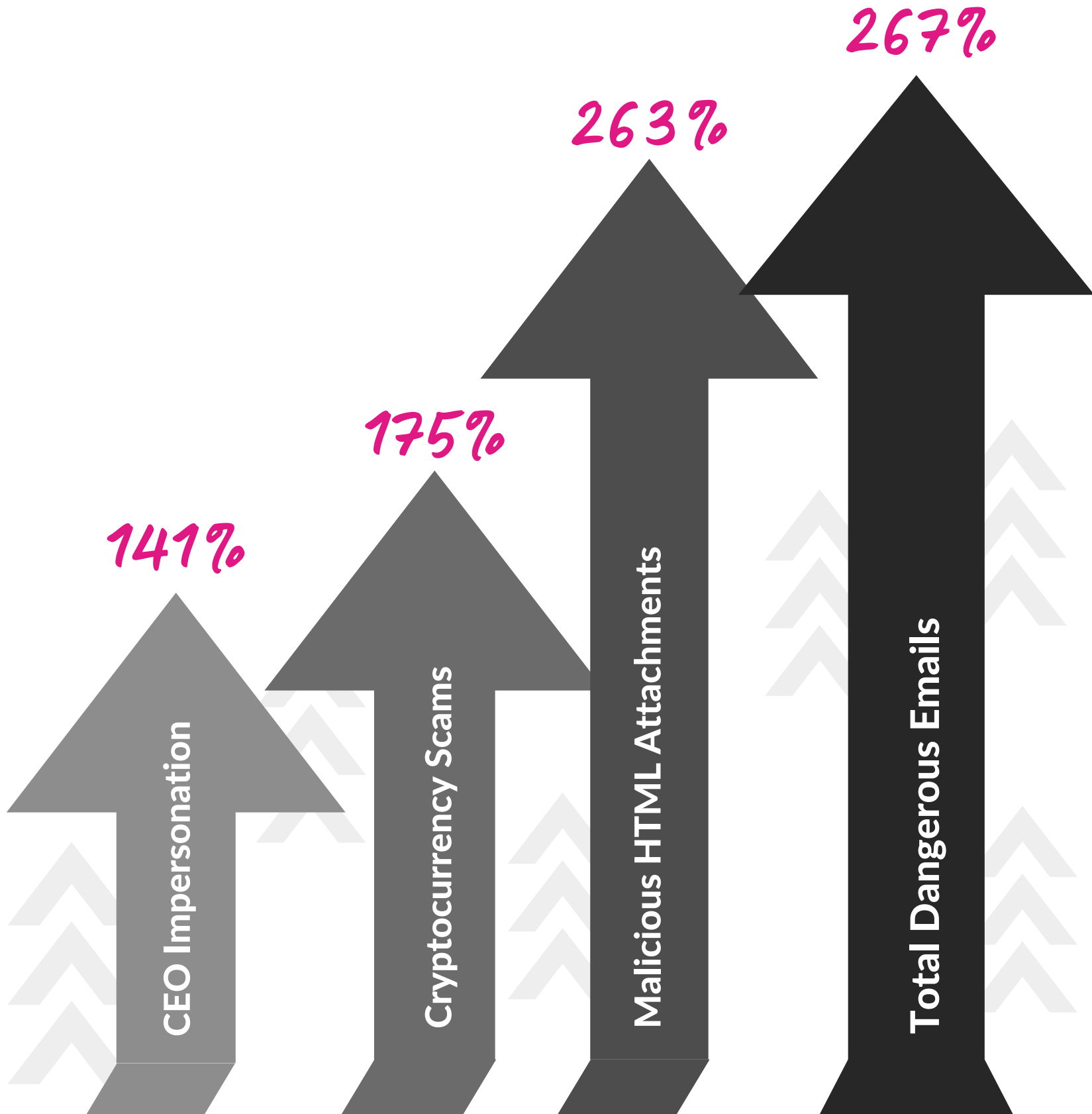
Phishing attacks have grown exponentially over the last decade with a five-year increase of **1,178.8%**, according to the FBI. That means the number of reported phishing attacks in 2021 was nearly 13 times higher than they were just five years prior.

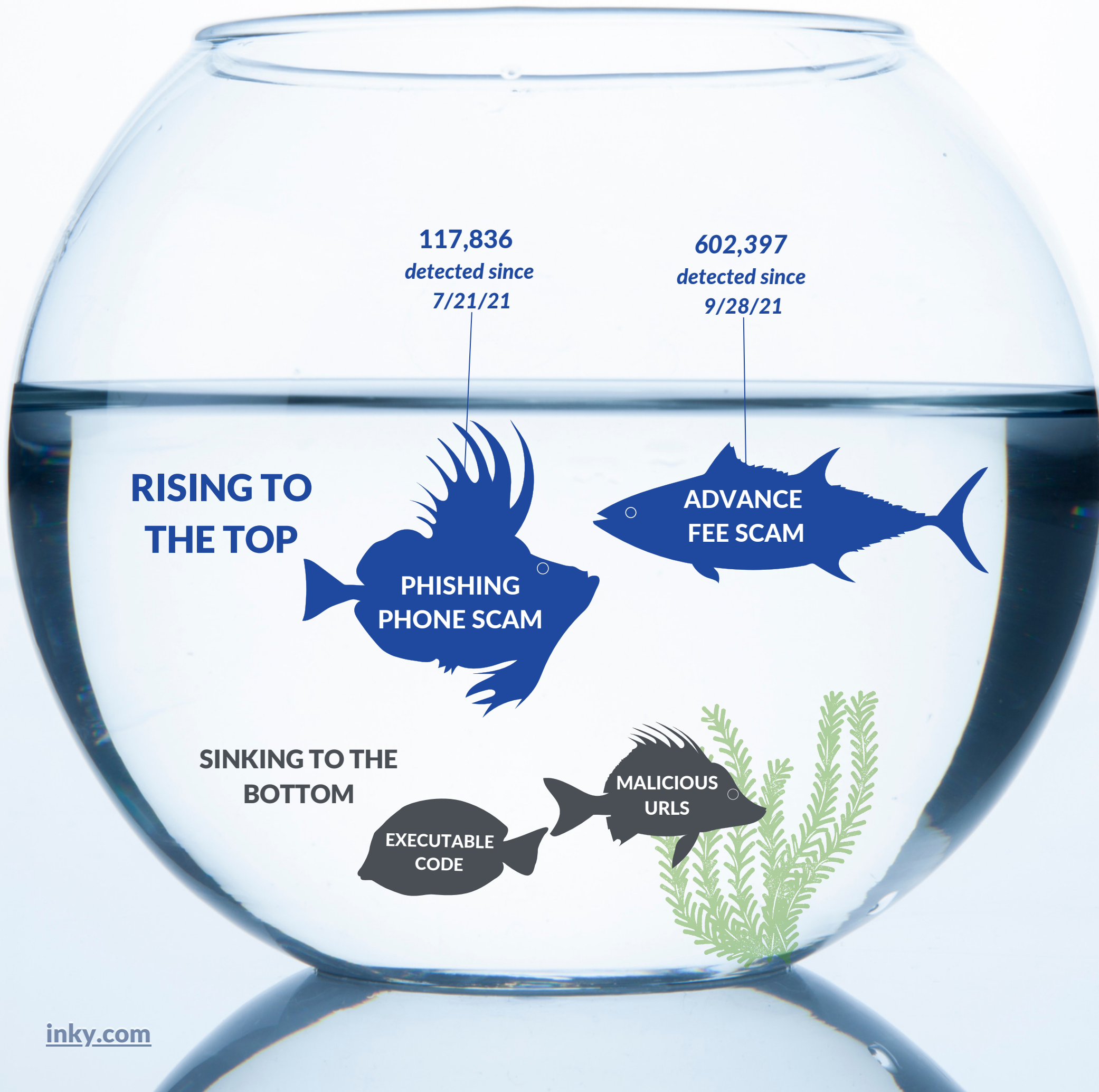
At INKY, we've been witnessing an equally egregious level of activity from bad actors. In fact, over a recent 12-month stretch, INKY observed alarmingly large increases in the areas of total dangerous emails, emails with malicious HTML attachments, cryptocurrency scams, and CEO impersonation attempts.





**INKY detected an alarmingly large increase in dangerous email over the past 12 months.**





## New Phish in the Pool

It's no secret that cybercriminals are constantly upping their game – looking for new and inventive ways to be effective and profitable. To do so, they must fool their two main audiences. The first audience consists of email filters and scanners, Secure Email Gateways (SEGs), and other security platforms. The second audience phishers must fool are email users. Regularly, INKY discovers, investigates, and stops phishing scams that are clever enough to hook both audiences.

INKY's nets were jam-packed in 2022. Many of the phish we caught were quite common, however we also saw several new phish entering the pool. These new phish include everything from emails with no text to the exploitation of cloud-based forms.



## ➤ Top Phishing Trends in 2022

### 1. Simple use of malicious URLs or executable code in the body of the email have waned.

Phishing can only be traced back to the late 1990s, but its evolution has been continuous. In the early 2000s it was obvious that these types of scammers existed. Looking back, the progression has included automated campaigns, new engaging subject lines, and simple sender impersonation. Every time users caught on, a new phishing strategy entered the scene. Seeing fewer malicious URLs and executable code in the body of emails – as we have this year – has been a clear warning from phishers of the complexities to come.

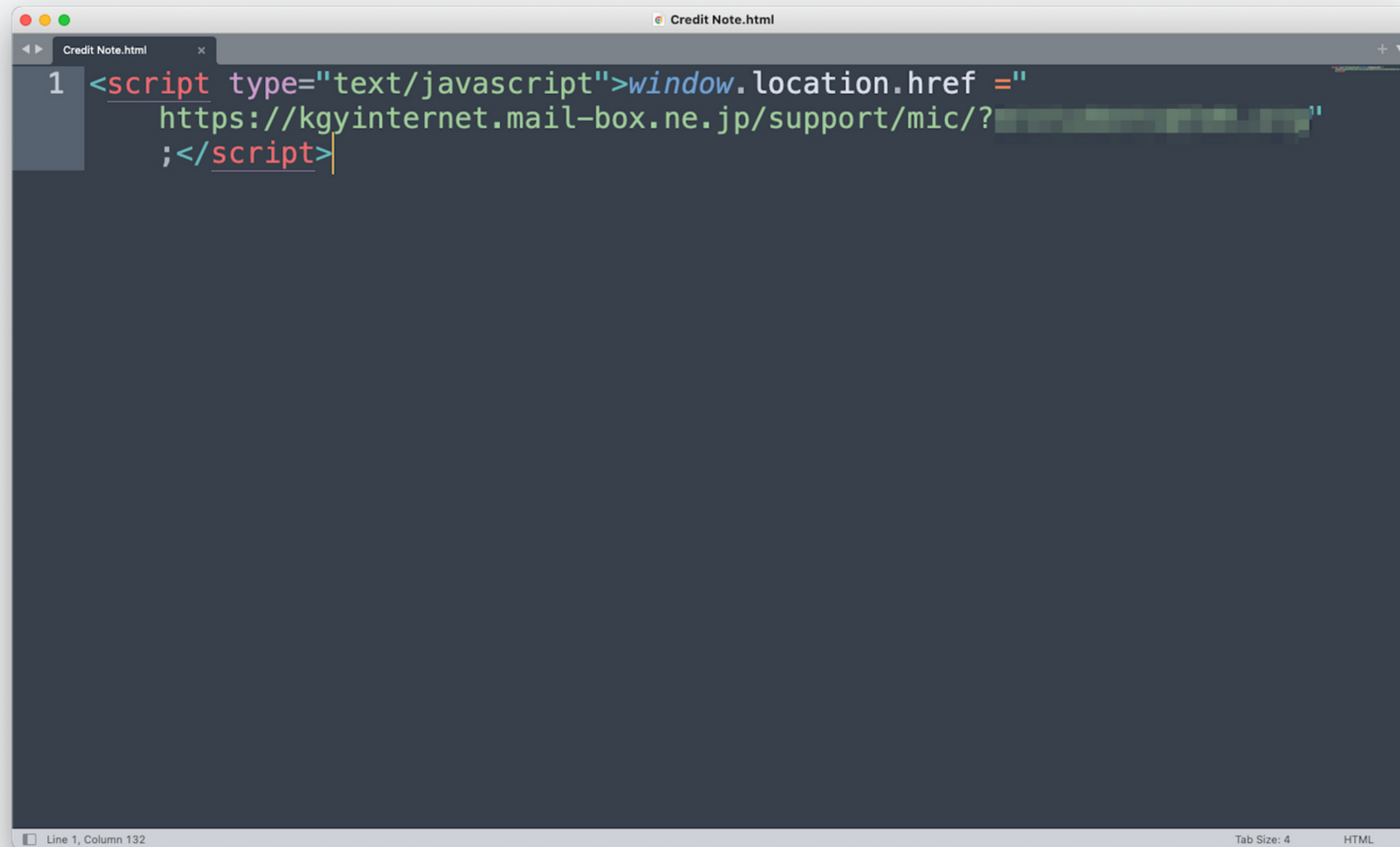


## 2. Sharp rise in the use of HTML and PDF attachments that SEGs do not block.

The attacker has a simple script tag in JavaScript in the HTML attachment that redirects the victim's browser to a malicious site. The attacker puts his JavaScript in the attachment because most email clients won't run JavaScript in the body of the email. By putting the JavaScript in the attachment, the attacker is hoping the user clicks on it, which will then open in a full browser, which of course will happily run the JavaScript.

Let's take a closer look on the next page.

```
1 <script type="text/javascript">window.location.href =  
  https://kgyinternet.mail-box.ne.jp/support/mic/?  
;</script>
```



```
1 <script type="text/javascript">window.location.href =  
  https://kgyinternet.mail-box.ne.jp/support/mic/?  
  ;</script>
```

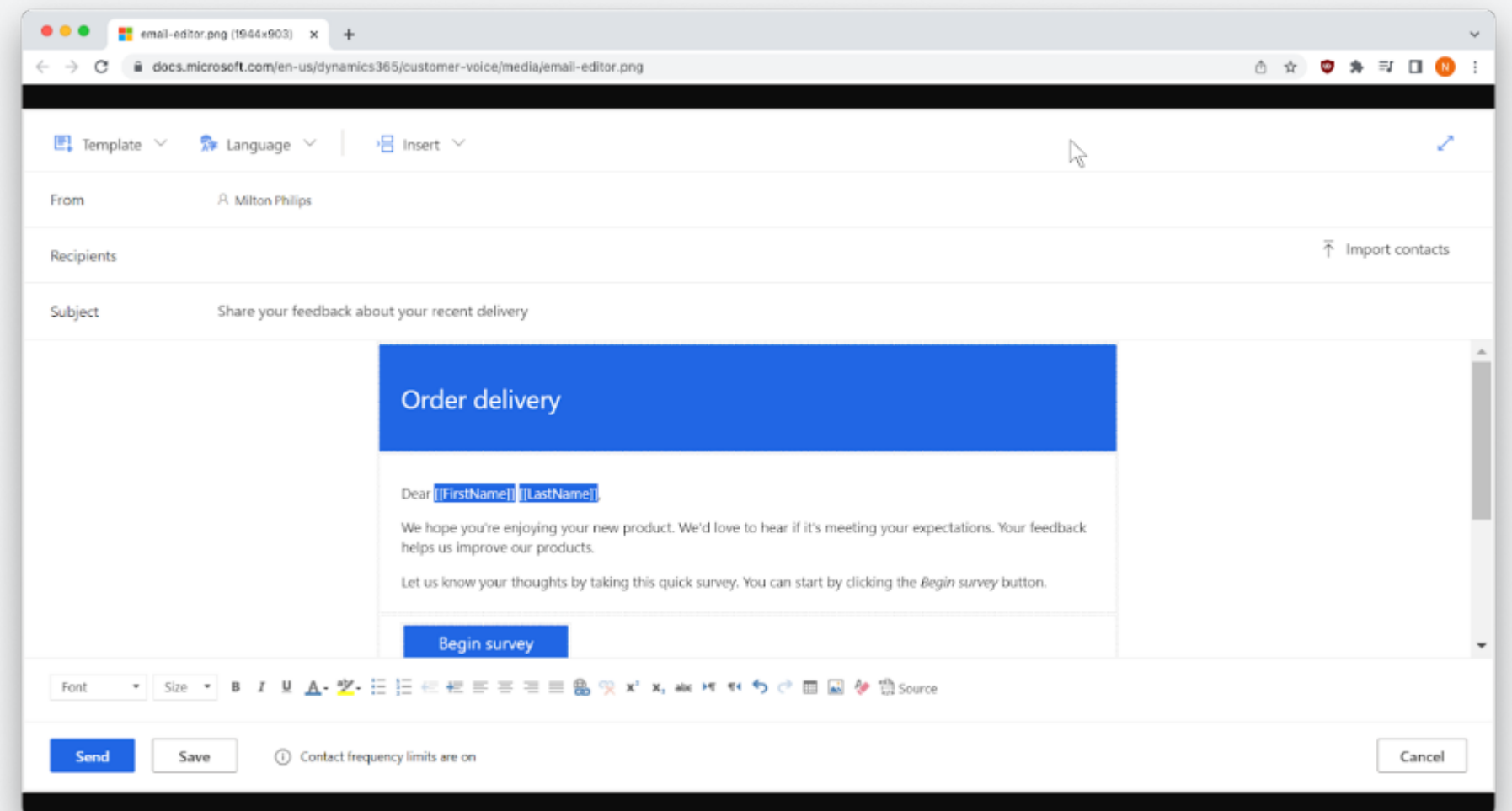
The screenshot shows a code editor window titled 'Credit Note.html'. The code is a JavaScript payload designed to redirect the browser to a phishing site. The payload is: `<script type="text/javascript">window.location.href = "https://kgyinternet.mail-box.ne.jp/support/mic/?";</script>`. The code is highlighted in a dark-themed editor. The status bar at the bottom indicates 'Line 1, Column 132', 'Tab Size: 4', and 'HTML'.

## Why this tactic works:

This phishing scheme is successful because legacy email protection systems don't generally scan HTML attachments as they do the body of the email itself – and even if they do, they do not remove JavaScript. In most systems, the attacker is able to sidestep the email protection system by moving his malicious payload to an attachment. With INKY, however, this phish was caught. INKY both strips JavaScript from HTML attachments (and email bodies) and analyzes HTML attachments to look for malicious content.

### 3. Cybercriminals are using indirect and multi-step methods to lure in the end user, making the experience feel more real.

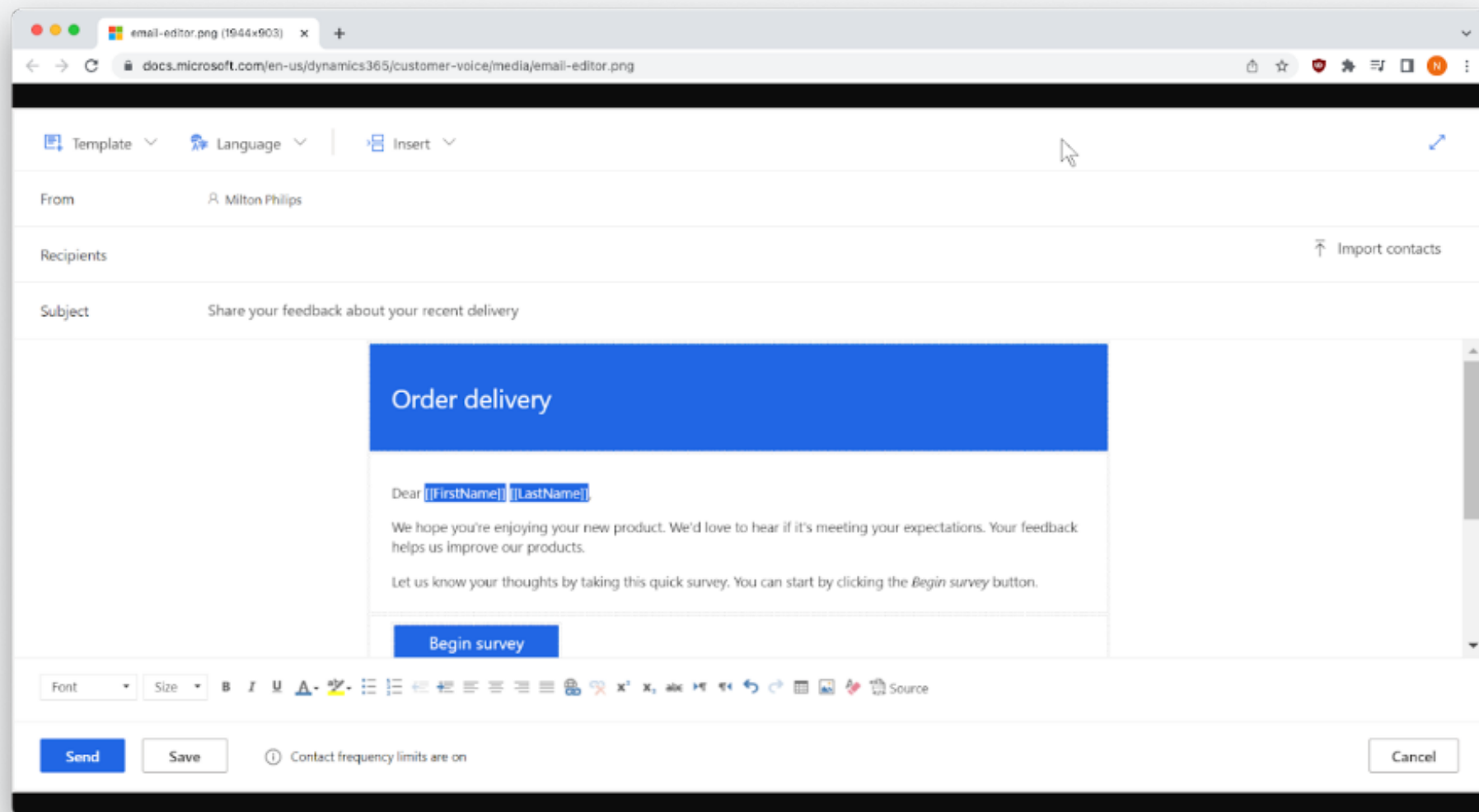
We each have our own level of awareness when it comes to recognizing a potential phishing email. For most people, that level of awareness is based on certain tell-tale signs of phishing they were trained to look for, such as suspicious links, unknown senders, or an unfamiliar greeting. In this particular phishing tactic, hackers throw victims off the scent by adding steps to the phishing email to make it seem more realistic. While this multi-step tactic could include any number of things, INKY has seen the use of different surveys pop up quite often. In one example, the phishers sent an email that appears to be a known vendor who would like to get some feedback on a recent product they have delivered. They're simply asking for you to fill out a quick survey.





## Why this tactic works:

The phishers used Microsoft Dynamics 365 Customer Voice, which is a customer feedback tool that allows users to create custom surveys. INKY picked up more than 2,000 of these malicious emails over the course of three months. Here are a few reasons why this phish is successful:



### *It arrived.*

Fooling email security platforms can be tricky for phishers, but using an established survey tool makes it easier for the phishing email to disguise itself and get past a variety of security checkpoints.

### *It looks legitimate.*

Because phishers are using an actual survey tool, the domain name is docs.microsoft.com and the email address is surveys@email.formspro.microsoft.com. Plus, if the phishers got things right, your name could have been populated in the opening.

### *It's well written.*

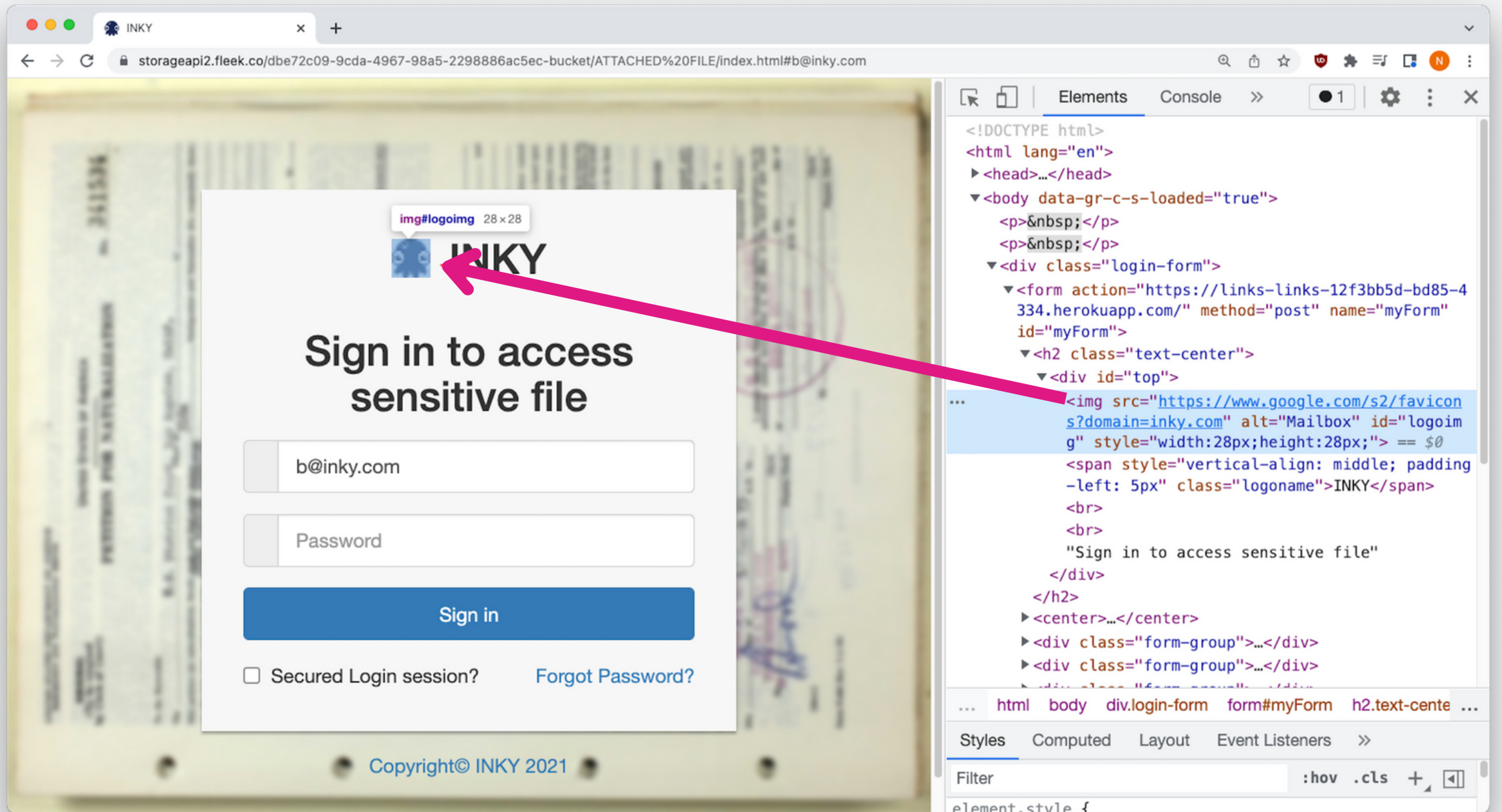
This email also lacks the typical grammar and spelling errors we expect in phishing emails. This might be attributed to the fact that Microsoft Dynamics has a built-in email composer used to send customized email invitations to survey recipients.

### *It doesn't feel phishy.*

Up until now, phishing emails didn't usually include multiple steps such as going to a survey site to provide feedback. Because that doesn't feel like phishing, it's easy to fall for the scheme.

## 4. INKY has identified a new trend we call Personalized Phish.

We're sure to see more of this clever phish in the coming months, especially considering how lucrative it can be when the user takes the bait. In short, a fake sender lifts someone's title from social media, usually LinkedIn, and creates a personalized phishing site with the end user's domain.



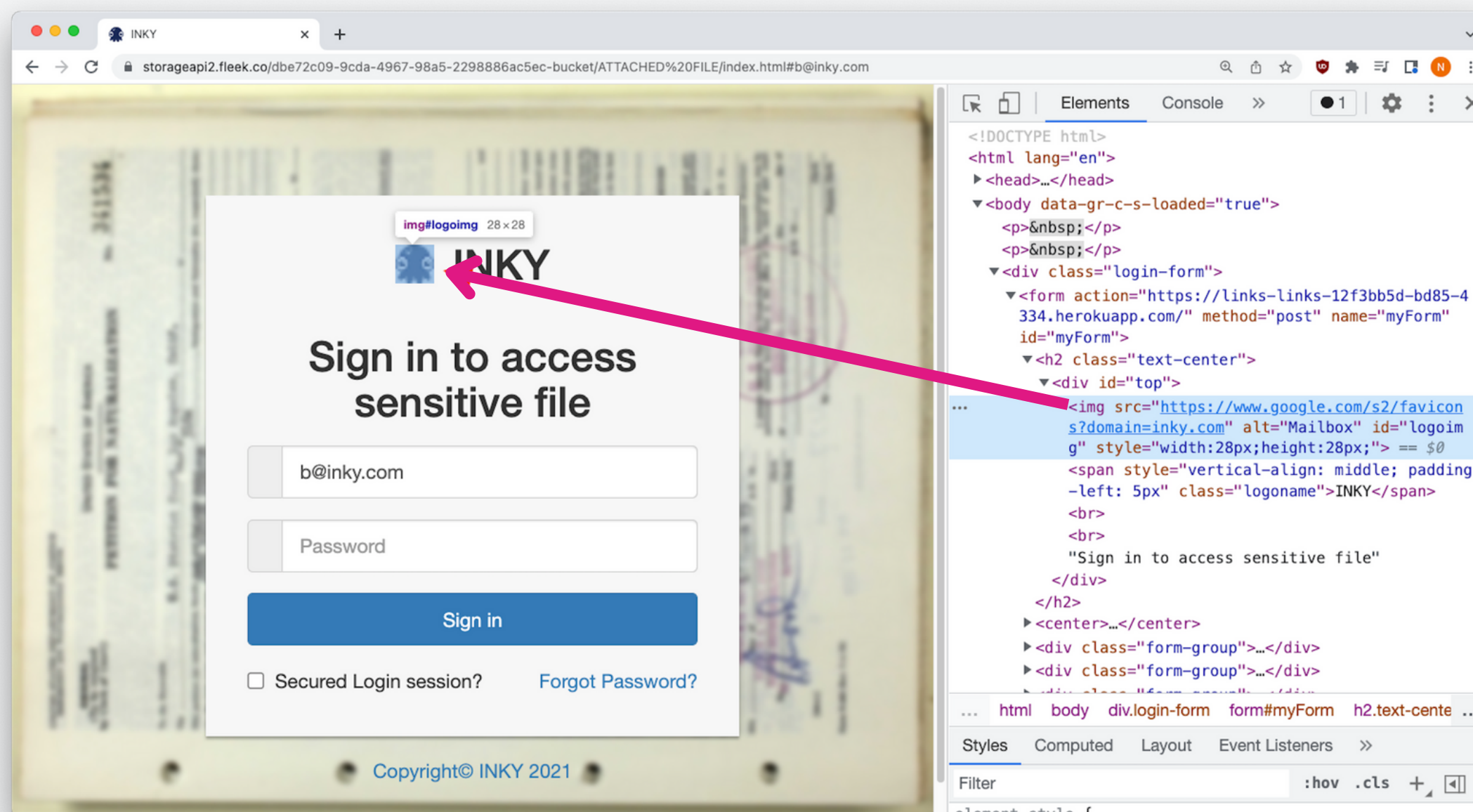


## Let's take a closer look at this example:

The attacker has a generic template and then customizes it for each recipient's individual and company identity.

Via Google search, the site automatically retrieves the favicon image of the recipient's domain to create a personalized phishing site in real time.

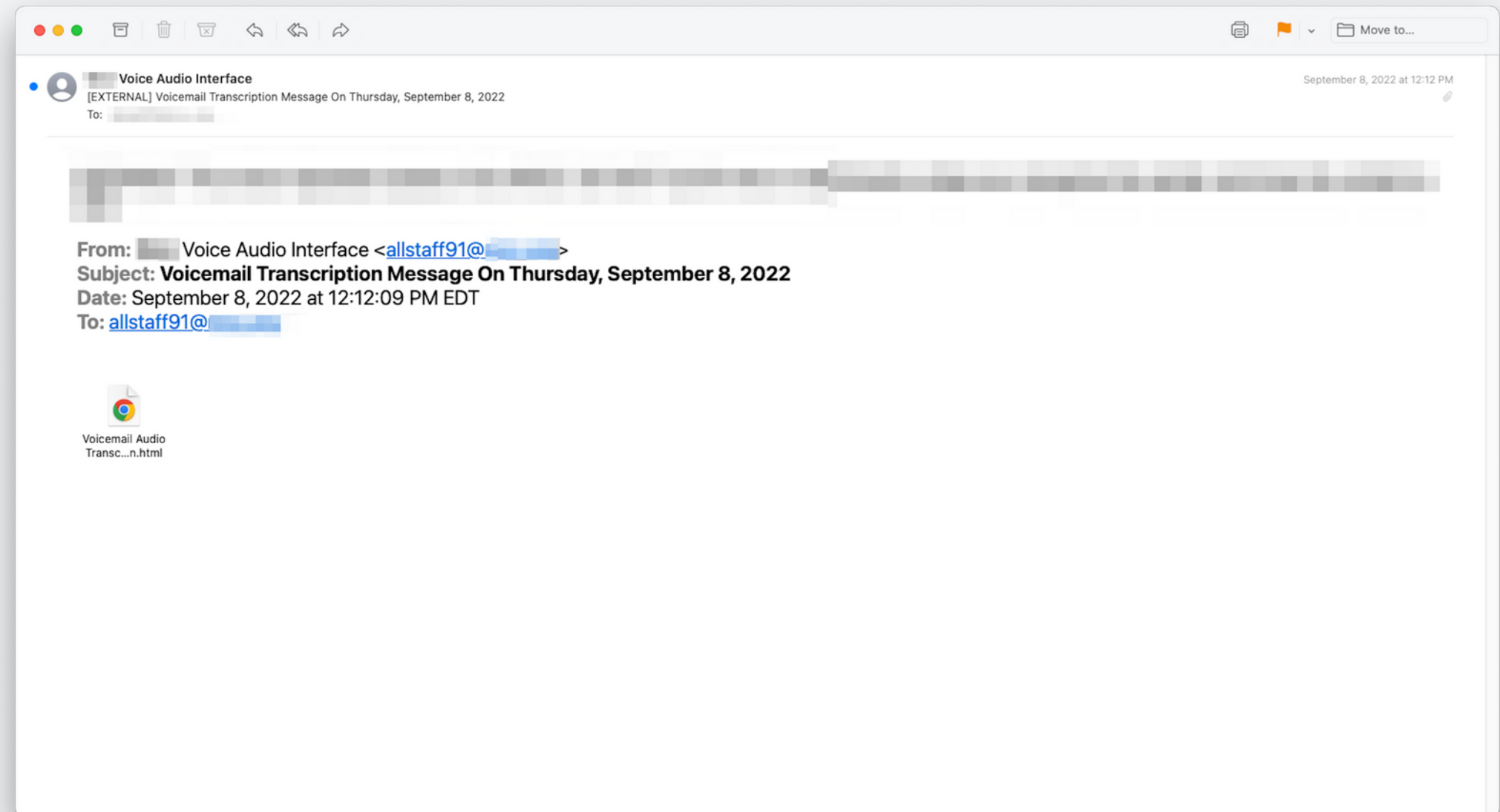
The HTML used for this technique is interesting. It turns out you can get the favicon for any domain via a correctly crafted URL. This isn't even a Google search; it's a generic redirect that Google has set up for themselves that gives you the favicon for the domain name specified in the URL query parameter (where it says domain=inky.com above). It's essentially a magic impersonation redirect hosted by Google – always available to the attacker at no cost and able to handle an unlimited number of requests.



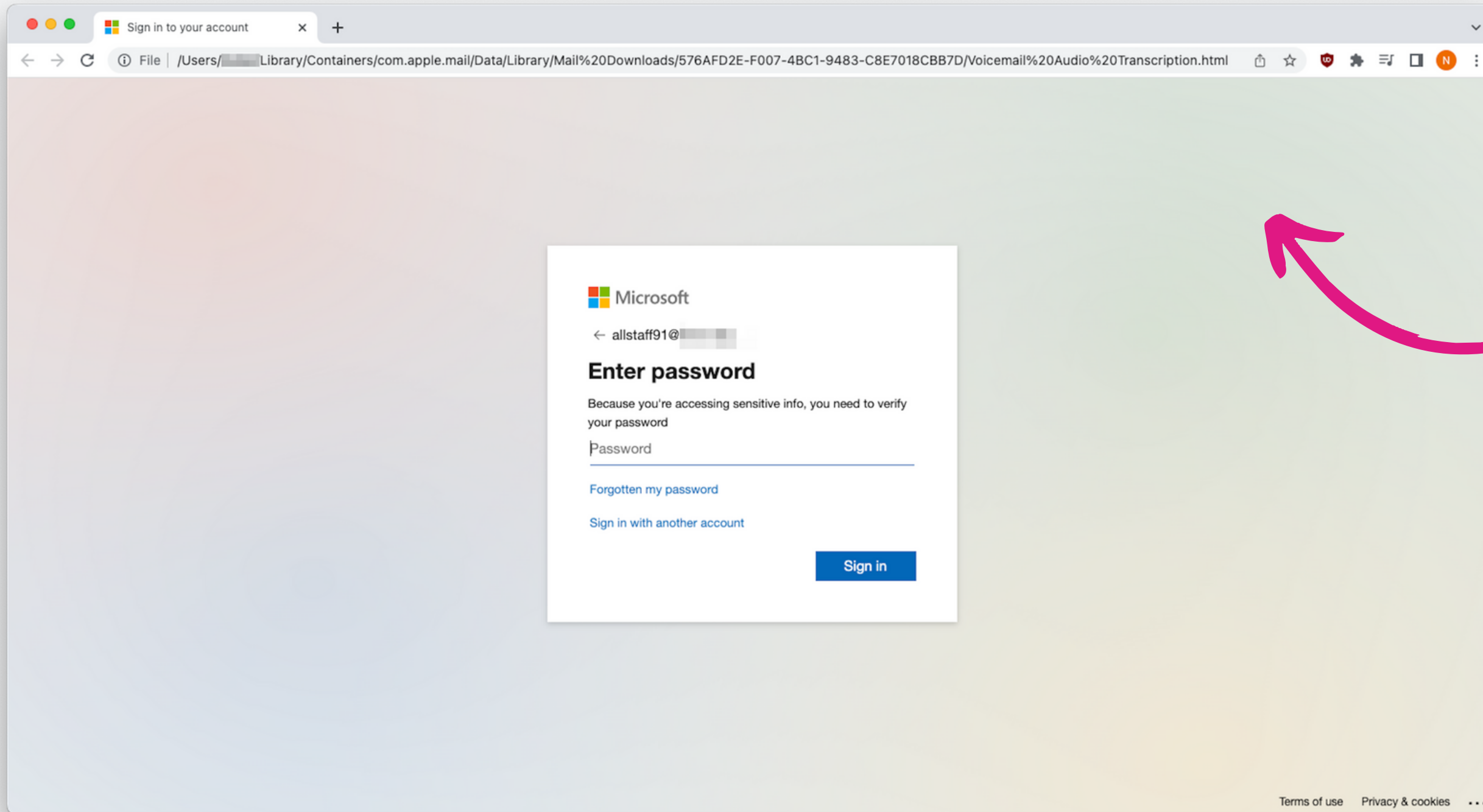
## 5 • Fake Voicemail Alerts – another common type of Personalized Phish.

Faking voicemail email alerts is popular because with so many different voicemail and transcription services available on the market, it's harder to distinguish real from fake. In fact, even the legitimate notifications tend to look pretty phishy.

As before, the malicious payload is pushed into an attachment so most email protection systems will largely ignore it. One new thing we see here is INKY labeling this “spoofed internal sender”. That means INKY knows the named individual is an employee or other internal sender, and that this email is pretending to be that person.







And as before, upon opening the attachment the user is taken to a fake login page. However, in this attack the page is not hosted anywhere. Instead, it's running on the user's local machine. By looking at the address bar we can see it's pointing to a local file on the user's machine.

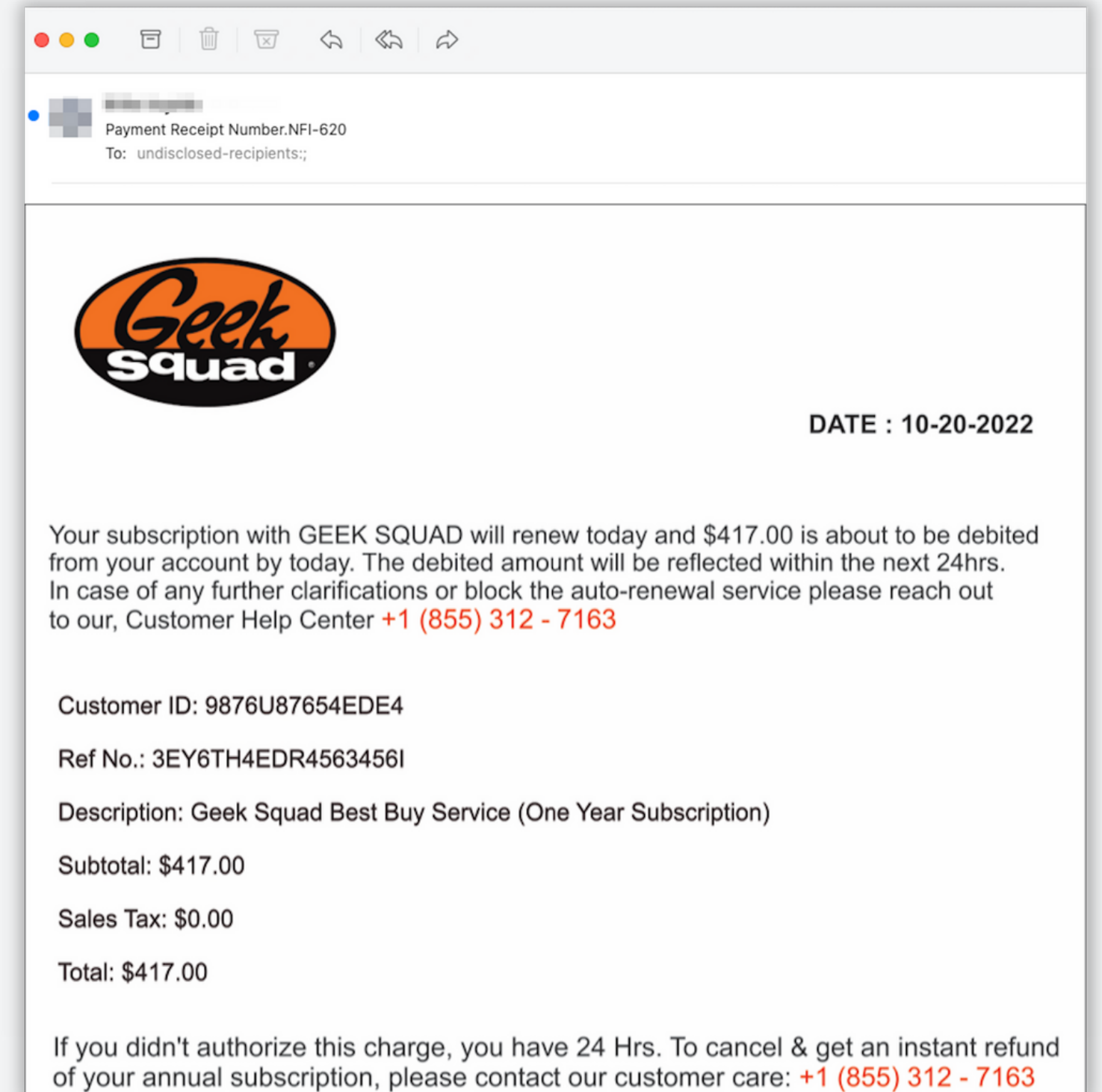




## 6 • No-text emails that slip through the SEG.

It's not often that you find a team of phish fighters standing around talking about body image, but in this situation, it was certainly warranted.

To the recipient, these phishing emails might appear to be standard, but in reality, the entire body of the email is an image. That's right – in a simple, yet clever attempt to get through Secure Email Gateways (SEGs), black hats are attaching a screenshot of their phishing message to an empty email. Most email clients will display the image file directly to the recipient rather than delivering a blank email with an image attached. As a result, what's delivered looks like a regular email. In most cases, the recipient is made aware of an expensive phony charge or fake issue. They are instructed to call a phone number if they want to dispute the purchase or resolve the problem. Then, once recipients call the phone number, an operative will try to extract valuable information from them.



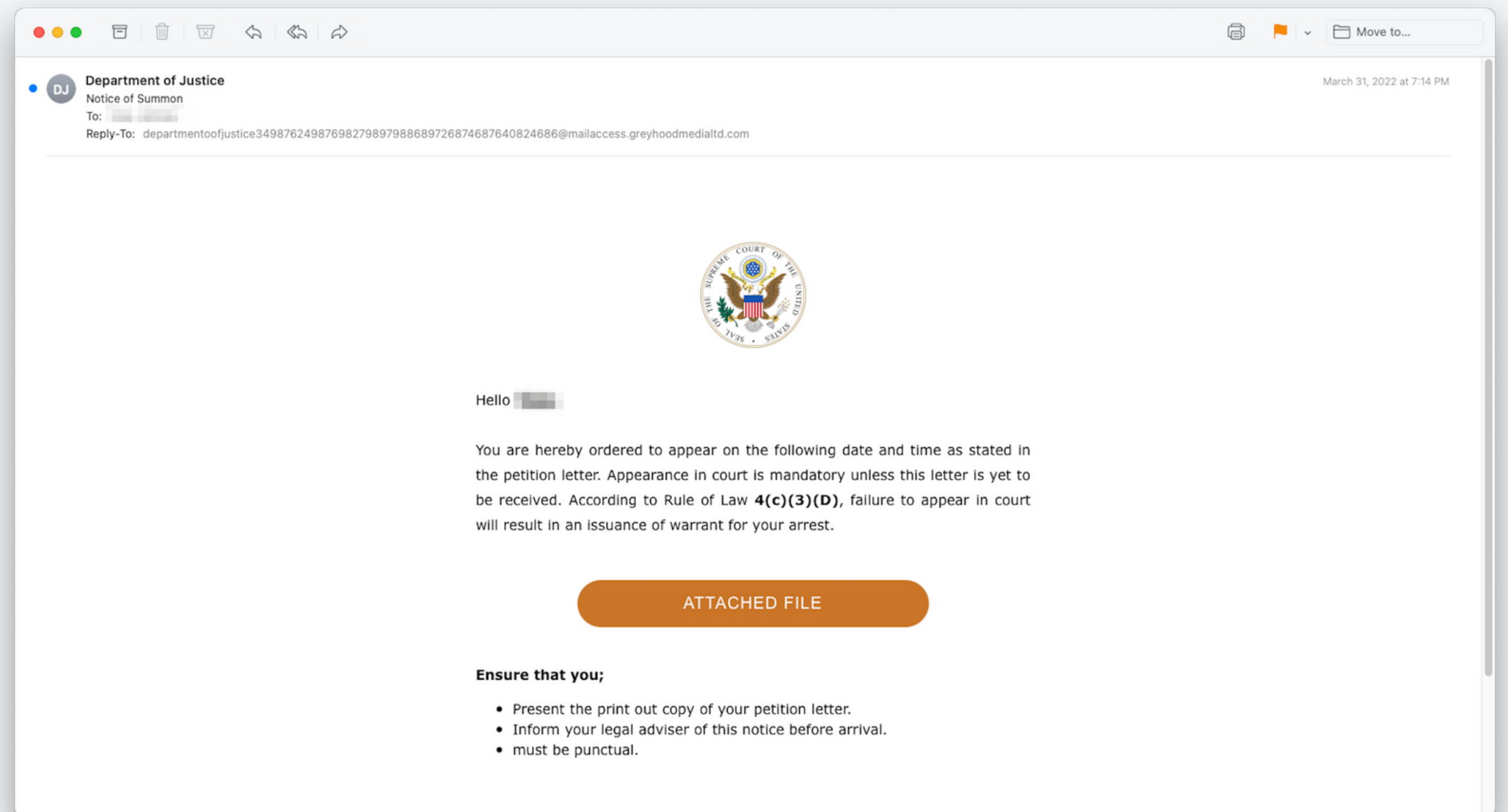




## 7. Phishers are now taking over cloud infrastructure to send emails, which again adds additional steps to look more legitimate.

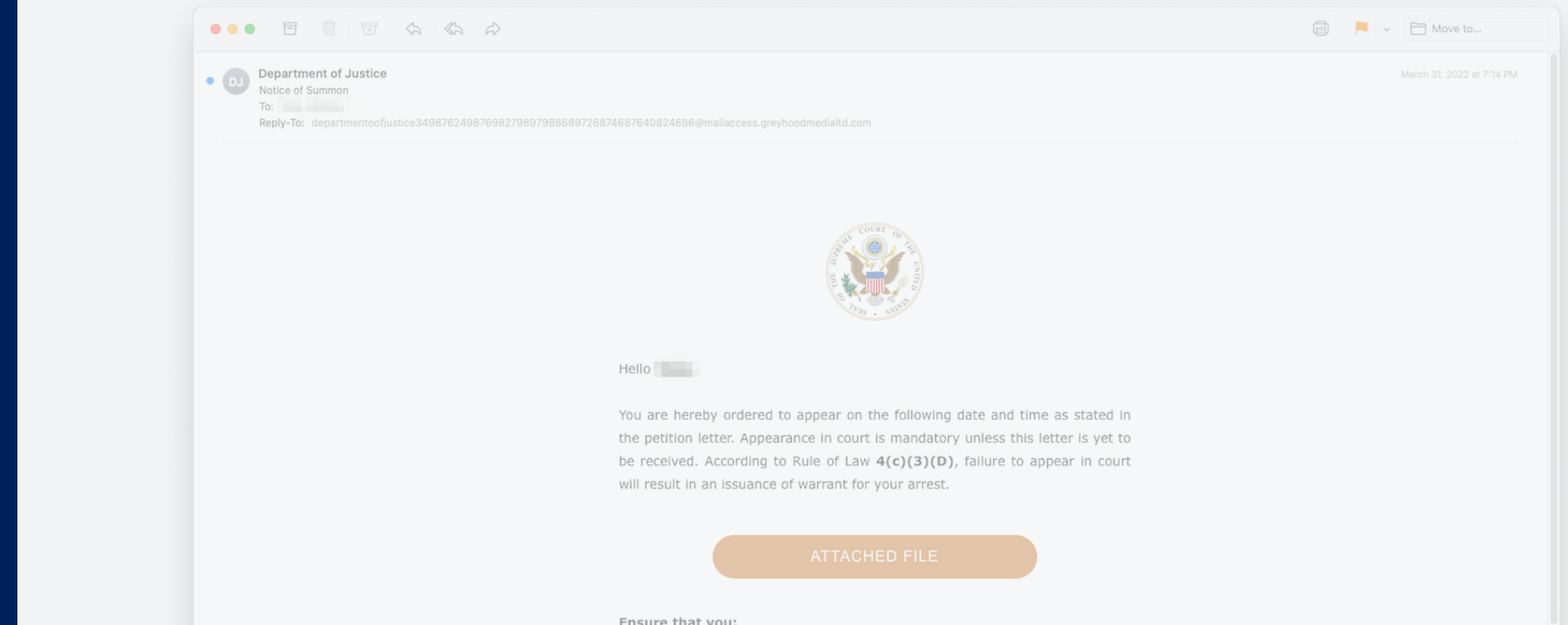
Attackers can then send email on behalf of someone in their system, hiding behind another layer of authentication.

SendGrid is a customer communication platform for transactional and marketing emails. In this example, phishers hijacked a legitimate SendGrid mailing list to send phishing emails that impersonated the Supreme Court of the United States. The message was a fake Notice of Summons, threatening arrest if the recipient didn't appear in court. Victims were asked to click on a big orange "ATTACHED FILE" button to view or print their petition letter.



## Why this tactic works:

- Phishers like to prey on strong emotions because when people are highly emotional, they tend to make mistakes. Sending an email from the high court telling someone they are to appear in court or be arrested...well, that's enough to make most people jumpy and anxious.
- Using SendGrid allows phishers to send email on behalf of someone in their system, hiding behind another layer of authentication.
- Because phishers used an actual SendGrid distribution list and sent the phish from an authentic SendGrid IP address (149.72.57.95), it passed email authentication and was delivered.
- If the recipient were to have hovered over the link behind the orange "ATTACHED FILE" button, they would have seen a legitimate and safe SendGrid link. What they would not expect was that upon clicking, that link would redirect them to a malicious credential harvesting site.



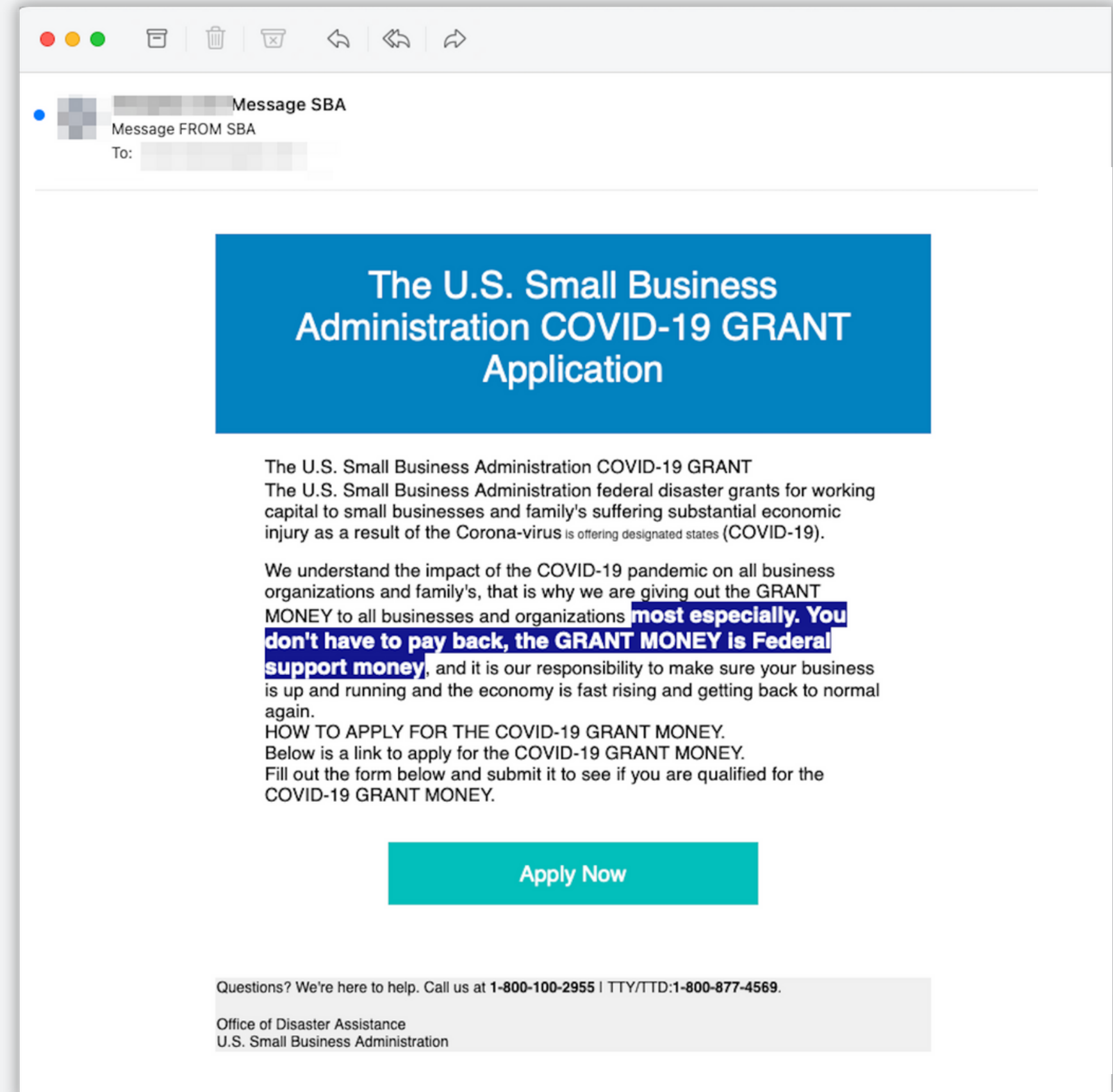
```
Ensure that you:
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5081.23 via Frontend
Transport: Thu, 31 Mar 2022 23:14:17 +0000
Authentication-Results: spf=pass (sender IP is 149.72.57.95)
smtp.mailfrom=sendgrid.net; dkim=pass (signature was verified)
header.d=sendgrid.net; dmarc=none action=none
header.from=mailaccess.greghoodmedialtd.com; compauth=fail reason=001
Received-SPF: Pass (protection.outlook.com: domain of sendgrid.net designates
149.72.57.95 as permitted sender) receiver=protection.outlook.com;
client-ip=149.72.57.95; helo=wrqvprf.outbound-mail.sendgrid.net;
Received: from wrqvprf.outbound-mail.sendgrid.net (149.72.57.95) by
SN1NAM02FT0057.mail.protection.outlook.com (10.97.4.123) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.5123.19 via Frontend Transport; Thu, 31 Mar 2022 23:14:16 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=sendgrid.net;
h=content-type:from:mime-version:subject:reply-to:to:list-unsubscribe;
s=smtppapi; bh=FsqceR2UYfdr+SLWVjdYTt6bpq8JtRS0eCbuDR7Gel0=;
b=c+Ewca0o8bfD5qqaWD1v3ntmional0dHVU90TWWIq/sSyDX9NaQwTCfr3J/U5Qd+DZ
qCg7x5ML4LYmx3oNkCL2cKj18fDd6JqjteGIrwKuanrFAt1E0nAqxIc0z4zLrrkwh0XBZm
bbuHYfjAT+icFo9RL7TWwCbMAYkTb8w0s=
Received: by filterdrecv-75ff7b5ffb-z69hd with SMTP id filterdrecv-75ff7b5ffb-z69hd-1-624635C7-44
2022-03-31 23:14:15.958782024 +0000 UTC m=+18233665.163325476
Received: from MjYxMTQyOTE (unknown)
by geopod-ismtpd-1-2 (SG) with HTTP
id z4jLlLpRQmb0crfABQjaQ
Thu, 31 Mar 2022 23:14:15.590 +0000 (UTC)
Content-Type: multipart/alternative; boundary=27f4c694045fe466a88aa064d53f6df92b27b85d2a99beb63c47bf7b2bc6
Date: Thu, 31 Mar 2022 23:14:16 +0000 (UTC)
From: Department of Justice
<departmentoofjustice34987624987698279897988689726874687640824686@mailaccess.greghoodmedialtd.com>
Mime-Version: 1.0
Message-ID: <z4jLlLpRQmb0crfABQjaQ@geopod-ismtpd-1-2>
Subject: Notice of Summon
Reply-To: departmentoofjustice34987624987698279897988689726874687640824686@mailaccess.greghoodmedialtd.com
X-SG-EID:
=?us-ascii?Q?U1qZqr=2FIBld53rMFB7pJ=2F73MSH1hNDGIx0F0inZcLozWIpQ0ivTw9fNXjV730k?=>
```

← SPF & DKIM pass for sendgrid.net

← Sendgrid custom header

## 8 • The utilization of legitimate cloud services like Google forms.

Struggling small business owners who likely received government funds to help them manage through the pandemic were sent a notice that appeared to be a grant application for additional funding. The email was disguised to look as though it came from the U.S. Small Business Administration (SBA) and it encouraged recipients to see if they were qualified for this special grant by filling out an application form. Phishers took to the cloud, using a legitimate survey option on Google Forms. They included wording that appears to have been taken from a previous SBA communication to help make things look legitimate. In the end, however, this was a mix of brand impersonation and the exploitation of legitimate cloud services (Google Forms) to harvest credentials.





## Why this tactic works:

There are a few reasons why this phishing threat is successful. To begin, it preys on vulnerable business owners who were financially impaired by the pandemic. However, its greatest strengths are its familiar feel and multiple steps.

Many of the email's recipients are familiar with the SBA from prior financial assistance. Even though we're dealing with brand impersonation in this case, that familiar feel is one reason posing as the SBA works. These cybercriminals also set this scam up to have more than one step so that it would feel more authentic. Finally, to help seal the deal, phishers chose to use a legitimate Google Forms survey to harvest credentials – another familiar element.

The image shows a screenshot of a phishing form titled "Federal Government Small Business Grant Form". The form is hosted on a Google Forms page, as indicated by the URL in the browser's address bar: docs.google.com/forms/d/e/1FAIpQLScZ4Uf8D1VWHxgkzsbBhJCGU9NpGc6AGXpY5O2FWp6Tv5Q/viewform. The form content includes the following sections:

- Title:** Federal Government Small Business Grant Form
- Organization:** U.S Small Business Administration, Coronavirus (COVID-19): Small Business Loan & Grant
- Introduction:** Created in 1953, the U.S. Small Business Administration (SBA) continues to help small business owners and entrepreneurs pursue the American dream. The SBA is the only cabinet-level federal agency fully dedicated to small business and provides counseling, capital, and contracting expertise as the nation's only go-to resource and voice for small businesses.
- Context:** Our nation's small businesses are facing an unprecedented economic disruption due to the Coronavirus (COVID-19) outbreak. On Friday, March 27, 2020, the President signed into law the CARES Act, which contains \$376 billion in relief for American workers and small businesses.
- User:** (not shared) Switch account
- Required:** A red asterisk indicates that the following fields are required.
- Gender:** Radio buttons for Male, Female, and Other: \_\_\_\_\_
- EIN/SSN for Sole Proprietorship:** Text input field with "Your answer" placeholder.
- SSN:** Text input field with "Your answer" placeholder.
- Organization Type:** Text input field with "Your answer" placeholder.
- Is the Applicant a Non-Profit Organization?:** Radio buttons for Yes.
- Drivers License / State ID Expiration date:** Text input field with "Your answer" placeholder.
- Drivers License / State ID issue date:** Text input field with "Your answer" placeholder.
- how do you want to receive your fund:** A dropdown menu with "Choose" selected.
- Account & routing for bank deposit:** Text input field with "Your answer" placeholder.
- Buttons:** "Submit" (purple) and "Clear form" (light blue).
- Footer:** "Never submit passwords through Google Forms." and "This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy".



# ➤ Expanded Technologies

The INKY suite of offerings is regularly expanding to stay ahead of the ever-growing slew of threats. In 2022, three new technologies were released.

## OUTBOUND EMAIL PROTECTION



INKY's **Outbound Email Protection** reinvents the interaction between email users and the policy enforcement system with a mobile-first design that requires no specific email client plug-in. This provides a vastly improved mobile experience as well as more choices about how a given policy violation should be handled, all in an endpoint and client-agnostic way.

## EMAIL ENCRYPTION

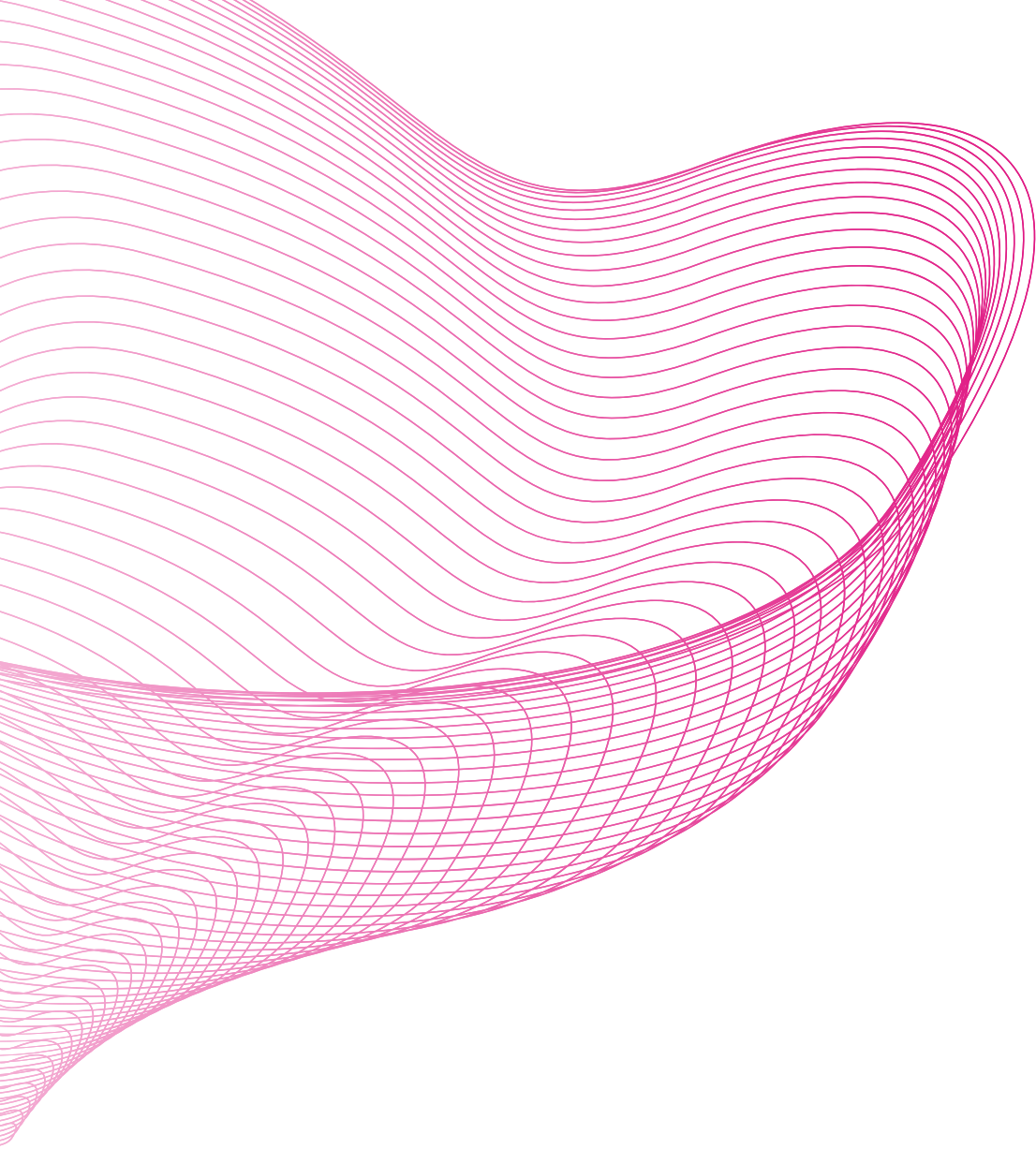


INKY's **Email Encryption** technology allows users to easily encrypt a message and store it in a secure web portal. This ensures the recipient is authenticated before they can read the email. Administrators can create customizable rules that require senders to encrypt outgoing emails with sensitive content. Simple to use and no plug-ins to maintain.

## ADVANCED ATTACHMENT ANALYSIS



**Advanced Attachment Analysis** delivers patented, deep evaluation of inbound email attachments in less than a second. It detects malware embedded deep within files, and because of the unique approach to file inspection, it can even detect zero-day threats. Speed, accuracy, privacy, volume, and the overall user experience are what set this new technology apart from its competition.



## ➤ Moments Worth Mentioning

INKY's accomplishments over the last 12 months went beyond the many phish we stopped. Here are a few of our most notable highlights.

[inky.com](https://www.inky.com)

### 2022 CRN Tech Innovator Awards Finalist

INKY Technology was named as a Finalist for the 2022 CRN Tech Innovator Awards which celebrates innovative IT vendors. Selected from among hundreds of vendor products, INKY is being recognized for its Advanced Attachment Analysis, which delivers patented, cutting-edge, deep evaluation of inbound email attachments in less than a second.

### Winner in the 2021 SINET 16 Innovator Awards

SINET is dedicated to introducing leading innovators into the Cybersecurity industry and accelerating innovation. From a pool of 190 applications from 18 countries, INKY was one of 16 emerging companies SINET awarded for delivering the most innovative and compelling technologies in their fields to address Cybersecurity threats and vulnerabilities.

### “Best of” Email Security for Google Workspace

Expert Insights' Best-Of Cybersecurity Awards recognize the world's best cybersecurity companies and products based on research by Expert Insights' independent technical analysts and editorial team, customer feedback, and industry recognition.

## Our Partner Program Received a 5-Star Rating

CRN®, a brand of The Channel Company, recognized INKY with a prestigious 5-star rating in its 2022 Partner Program Guide. CRN's annual Partner Program Guide provides a definitive list of the most notable partner programs from industry-leading technology vendors that provide innovative products and flexible services through the IT channel. The 5-star rating is achieved only by select vendors that deliver the best of the best, going above and beyond in their partner programs to help push growth and positive change.

## Partnered with GoDaddy

In a strategic partnership between INKY and GoDaddy, INKY's innovative anti-phishing and email assistant offering will be made available to customers of GoDaddy's Advanced Email Security (AES) solution for Microsoft 365, replacing GoDaddy's prior advanced secure email gateway solution.

## INKY surpassed 2,300 customers

now using its advanced email phishing and security solutions.

[inky.com](https://inky.com)

## Recognized as one of the World's Most Innovative Companies

INKY was named to Fast Company's prestigious annual list of the World's Most Innovative Companies for 2022, ranking top 10 in the Security category.





***As for the INKY banners, you really can't get anything on the market that looks as nice. You're not ever going to find banners like these that list all the reasons why things are being flagged.***



MICHAEL TRILLO  
Director of End User Engineering  
AGIO



# ➤ Beyond the Banner

In the past you have heard it referred to as the INKY Banner. However, compared to other products in the market, the term 'banner' doesn't do it justice. It's so much more than a set of warning messages. On top of intelligently eliminating security threats by blocking malicious emails, it assists employees, in real time, to handle suspicious emails. In 2022, the INKY Banner has been affectionately referred to as INKY's Email Assistant.

INKY's Email Assistant provides users with immediate insight into specific issues within the email they've just opened. Whether it is differentiating between trustworthy colleagues and questionable senders, detecting a fake logo embedded in your email, or taking a deeper look behind an email address to warn of potential fraud, the INKY Email Assistant delivers the level of insight that keeps companies safe and improves their employees' email security decision making.

## Beyond the Banner

Enterprise Security Group, better known as ESG, is an IT analyst, research, validation, and strategy firm that provides market intelligence and insight to the global IT community. In their ESG Showcase entitled, “Quashing the Phishing Epidemic,” senior analyst Dave Gruber spoke to an often-overlooked aspect of phishing attacks that, when implemented properly, can deliver a sharp reduction in successful phishing attacks. It involves education – the right way.

According to Gruber, “New, innovative email security solutions that directly involve the end-user are showing real promise in combating email-borne threats.” In particular, ESG’s report shared, “the insertion of a highly optimized, real-time email assistant can result in up to a 95% reduction of successful phishing attacks.” Those are the kind of results every company can have, with INKY.

As threats grow, so does INKY. In 2022 we added several new threat categories. Three of our favorites include:

### **Phishing Phone Scam**

This threat doesn't utilize attachments or links. INKY caught more than 91,500 of these "Phone Scam" emails once we created this new category.

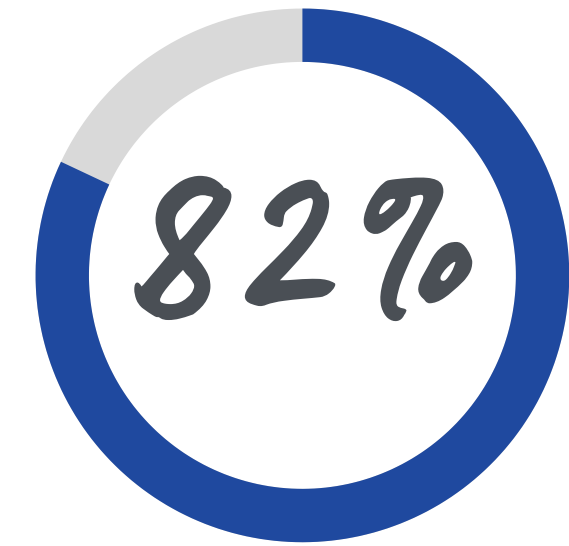
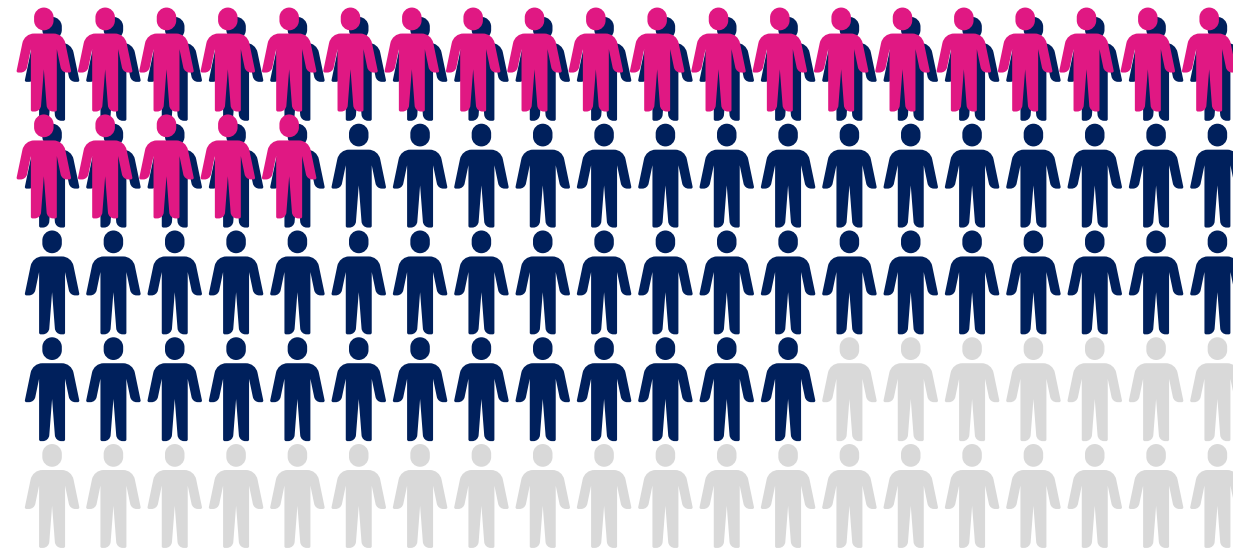
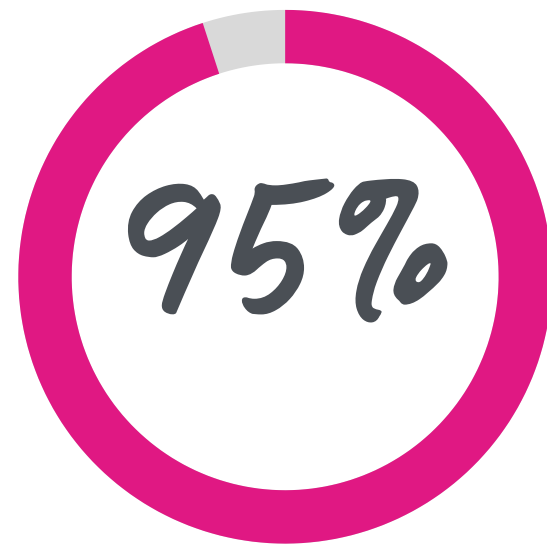
### **Protected File**

This one warns users of bad actors compressing malware in password protected zip files.

### **Potential Exploit**

Once we set this one in motion, INKY detected more than 16,000 "Potential Exploit" emails, many linked to the Log4Shell vulnerability.

## ➤ Beyond the Banner



More than **95%** of all cybersecurity incidents involve human error.

*In an experiment with simulated phishing tests,*  
**73%** of participants clicked on a simulated phishing email,  
*with 25% of test participants taking at least one dangerous action – such as providing credentials.*

**82%** of data breaches involve a human element.

Source: <https://www.verizon.com/business/resources/reports/dbir/>

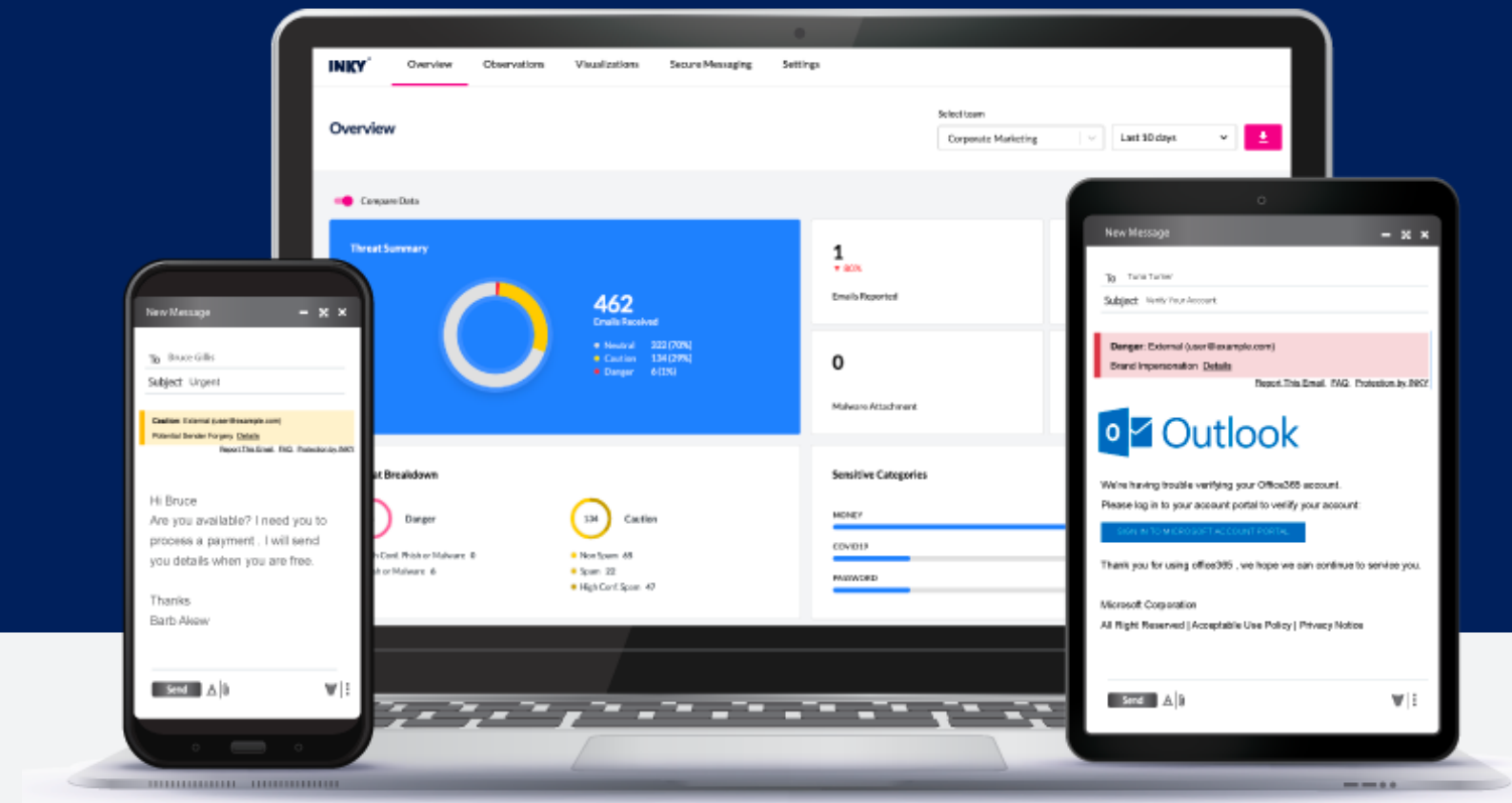
# ➤ A Call for Behavioral Change

The experts at INKY agree that one of the most important elements that will be driving future change is a focus on changing user behavior. It's a sentiment shared by many in the industry and was signaled out as an issue in the 2022 Data Breach Investigations Report.

“In 2021 we reported that the human element impacted 85% of breaches, which decreased slightly to 82% this year,” the report said. “...you’re going to need to change the behavior of humans, and that is quite an undertaking.”

But what if the same email security platform that is preventing phishing and malware attacks from compromising your company could also deliver continuous user behavior modification? Well, it's possible. In 2022, INKY set its sights on changing user behavior. Leveraging more than 60 different interactive banners, the INKY Email Assistant coaches employees to make safe choices with their email, on any device or email client.

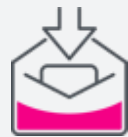




## EMAIL SECURITY PLATFORM

# INKY's behavioral email security platform catches everything.

Like a security coach, it signals suspicious behaviors with interactive banners that guide users to take safe action on any device or email client. IT teams don't face the burden of filtering every email themselves or maintaining multiple systems. Through powerful technology and intuitive user engagement, INKY keeps bad actors out for good.



### INBOUND EMAIL PROTECTION

Block phishing and coach users in real time.

[learn more](#)



### INTERNAL EMAIL PROTECTION

Protect internal email traffic against account takeovers.

[learn more](#)



### OUTBOUND EMAIL PROTECTION

Prevent data loss with interactive safeguards for outgoing emails.

[learn more](#)



### ADVANCED ATTACHMENT ANALYSIS

Detect deeply hidden malware from inbound attachments.

[learn more](#)



### EMAIL ENCRYPTION

Guard sensitive data with fast and simple encryption.

[learn more](#)

[inky.com](https://www.inky.com)

EMAIL SECURITY PLATFORM

# Key Capabilities

Phishing is still the number one cause of data breaches for companies and the hooks are getting sharper. Most people don't realize how far the problem has advanced. Today's criminals employ a variety of incredibly sophisticated techniques that elude even the most skeptical and well-trained eyes. This is where INKY excels. Through innovative computer vision, AI, and machine learning INKY catches everything.



## THE BANNER

Color-coded banners on every email offer threat assistance to your employees in real-time.

[learn more](#)



## MOBILE PROTECTION

Email protection that works across any device and any email client.

[learn more](#)



## THE DASHBOARD

Admins have complete control over customization and how your end-users will interact with INKY's banners.

[learn more](#)



## COMPUTER VISION

Self-adapting AI algorithms and a deep understanding of how email works is what makes INKY effective at keeping up with zero-day attacks.

[learn more](#)



## SOCIAL GRAPHING

INKY gets to know users and detects anyone impersonating someone from within the organization or external.

[learn more](#)



## REPORTING

Identify, analyze, and remediate from one pane of glass, making it easy to identify trends and share reports with the executive team.

[learn more](#)

[inky.com](https://inky.com)



# INKY<sup>®</sup>

## Secure Email. Change User Behavior.

INKY is an award-winning, behavioral email security platform that blocks phishing threats, prevents data leaks, and coaches users to make smart decisions. Like a cybersecurity coach, INKY signals suspicious behaviors with interactive email banners that guide users to take safe action on any device or email client. IT teams don't face the burden of filtering every email themselves or maintaining multiple systems. Through powerful technology and intuitive user engagement, INKY keeps phishers out for good. Learn why so many companies trust the security of their email to INKY.

[Request a demo](#)

