MEISAC

MEDIA + ENTERTAINMENT
INFORMATION SHARING ANALYSIS CENTER

PHISHING,
SCOURGE OF THE DEEP BLUE INTERNET

WHAT IS ALL THIS PHISHING YOU SPEAK OF?

SPAM

PHISHIN

Whale Phishing

SMISHING:

SMS
es

Spea

te
ey

Business Email Compromise (BEC)

use of phishing or compromised account to commit fraud, usually targets c-suite

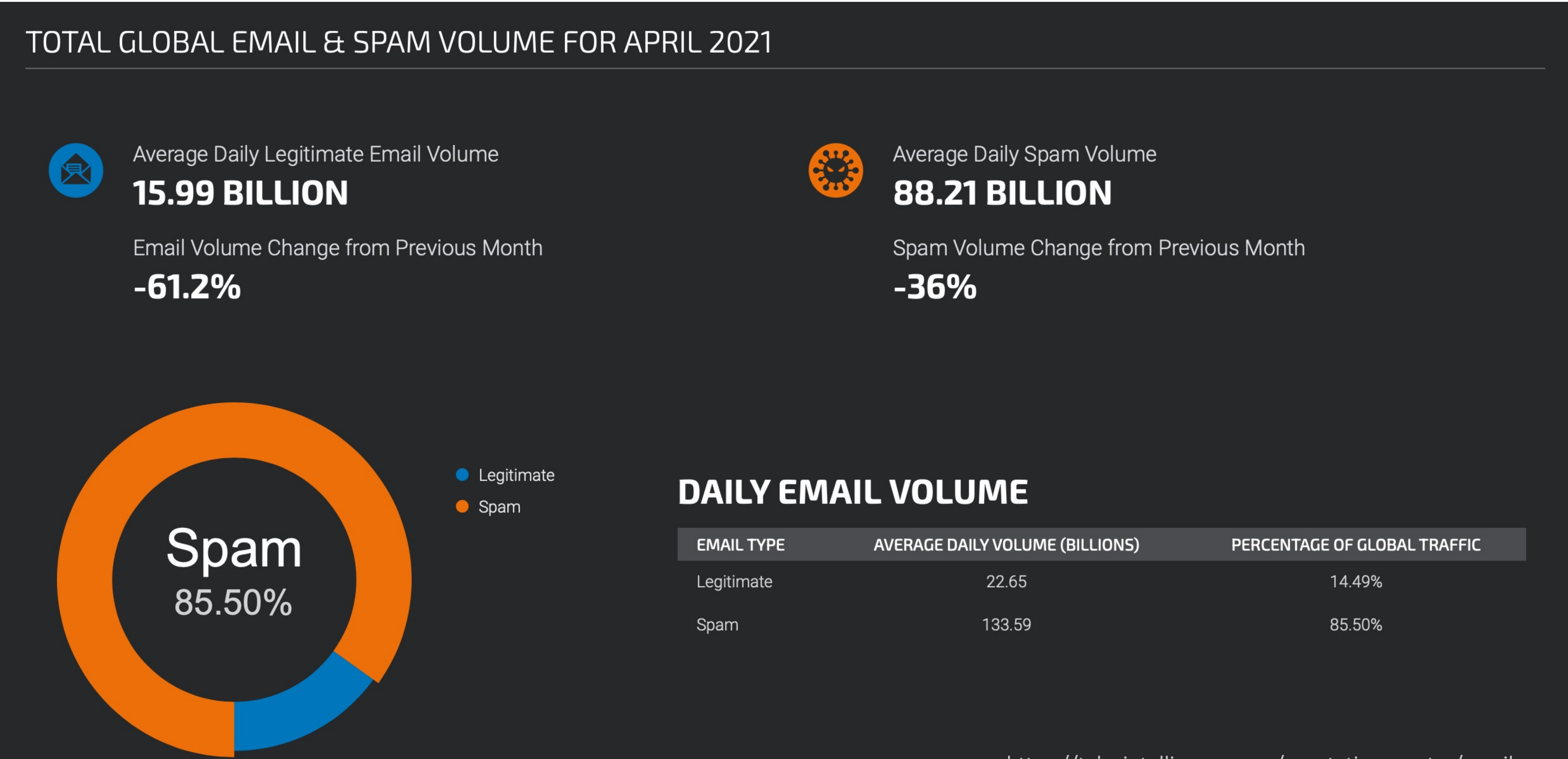
So many PHISH in the sea

- 94% of malware is delivered by email
    - Verizon 2019 Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

- 65% of cybercrime gangs use phishing as their primary way in
    - Symantec 2019 Internet Security Threat Report - https://www.symantec.com/security-center/threat-report

- 70% of newly registered domains are malicious
    - Palo Alto Unit42 research - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

We get A LOT of spam



TOTAL GLOBAL EMAIL & SPAM VOLUME FOR APRIL 2021

Average Daily Legitimate Email Volume

15.99 BILLION

Email Volume Change from Previous Month

-61.2%

Average Daily Spam Volume

88.21 BILLION

Spam Volume Change from Previous Month

-36%

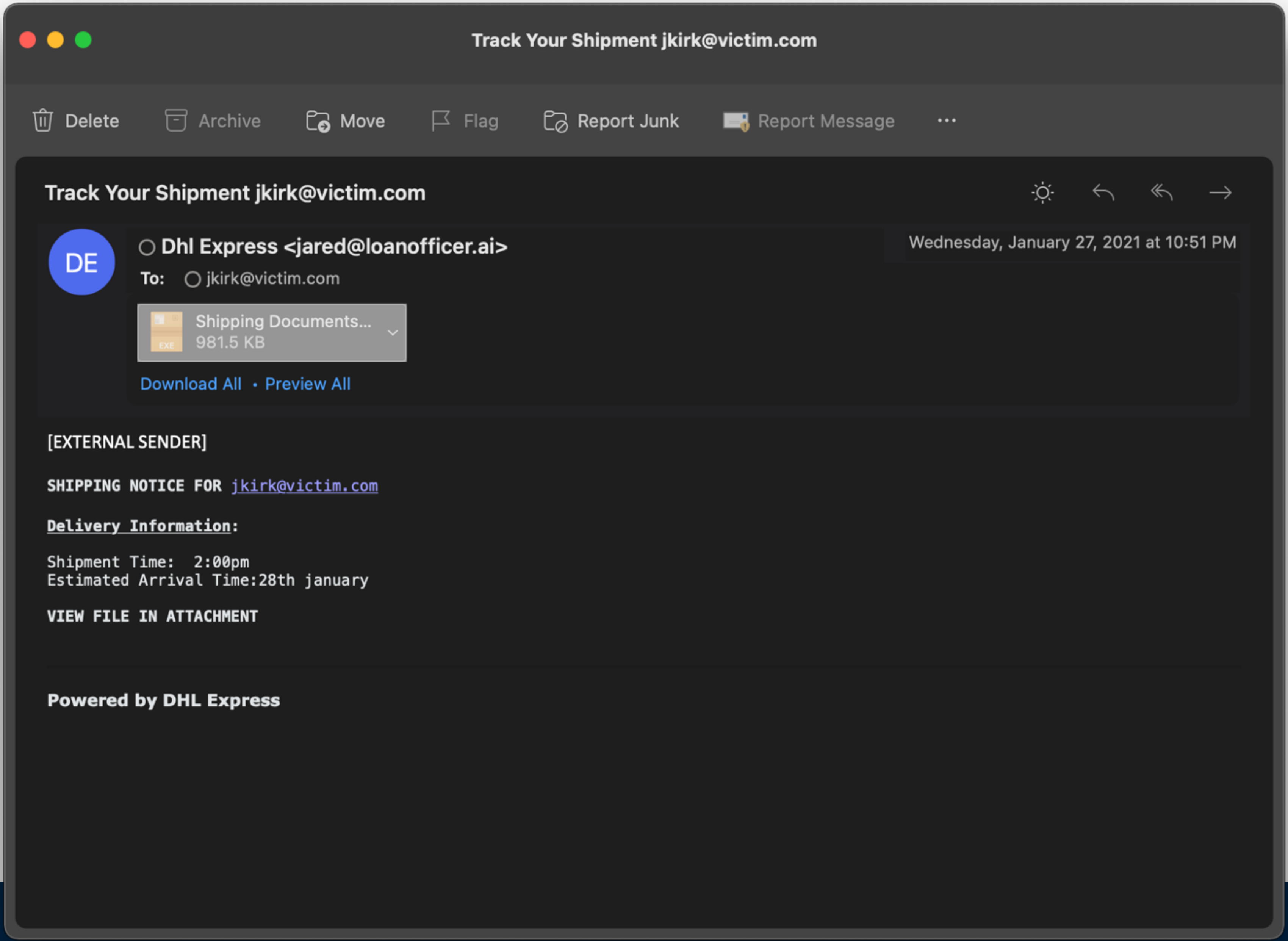
DAILY EMAIL VOLUME

EMAIL TYPE	AVERAGE DAILY VOLUME (BILLIONS)	PERCENTAGE OF GLOBAL TRAFFIC
Legitimate	22.65	14.49%
Spam	133.59	85.50%

https://talosintelligence.com/reputation_center/email_rep

EXAMPLE:

- From?
  Claims to be from DHL, but actual email is some domain that is completely unrelated.
- To?
  Is this the address you expect to get a shipping notification sent to?
- Context?
  Are you expecting a shipment?
- Format?
  This looks nothing like a real DHL email. This check doesn’t always work, though, since some attackers will copy real emails so theirs looks very convincing.
- Attachment?
  The attachment is an executable with a ”.EXE” extension. No real shipping notification will executable files, so this undoubtedly malicious.



Track Your Shipment jkirk@victim.com

○ Dhl Express <jared@loanofficer.ai>
Wednesday, January 27, 2021 at 10:51 PM
To: ○ jkirk@victim.com

Shipping Documents...
981.5 KB

Download All • Preview All

[EXTERNAL SENDER]

SHIPPING NOTICE FOR jkirk@victim.com

Delivery Information:

```
Shipment Time:  2:00pm
Estimated Arrival Time:28th january
```

VIEW FILE IN ATTACHMENT

Powered by DHL Express

EXAMPLE:

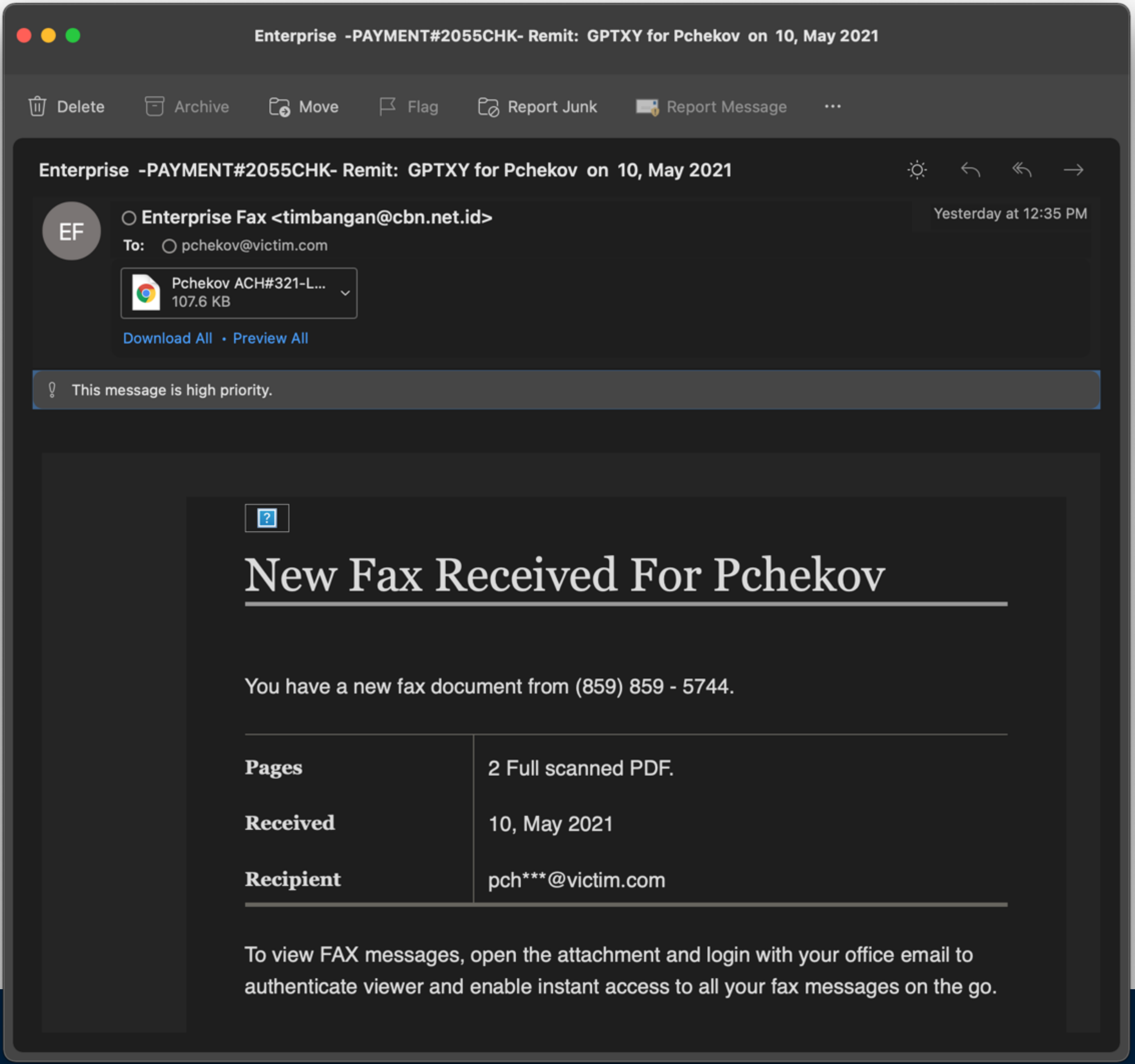
- From?
  Claims to be from your company's fax machine, but actual email is some domain that is completely unrelated.

- To?
  Is this the address you expect to get a fax notification sent to?

- Context?
  Who sends faxes in the 21st century? Voicemail another common theme. Unless it is a service that you completely know, trust, and expect to receive notifications from, don't open any attachments from faxes, voicemails, invoices, etc.

- Format?
  An effort was made to make this look professional, but there are still clues. The included graphics, the name being off, the message says the attachment is a .pdf but it is actually an .htm file.

- Attachment?
  The attachment is a web page that will open in your browser. Code in the page will then cause your browser to go open another page that is a fake login, giving you the impression you need to log into your Office 365 account to read the fax. This is all an elaborate scheme to steal your password.



Enterprise -PAYMENT#2055CHK- Remit: GPTXY for Pchekov on 10, May 2021
Delete
Archive
Move
Flag
Report Junk
Report Message
···

Enterprise -PAYMENT#2055CHK- Remit: GPTXY for Pchekov on 10, May 2021

○ Enterprise Fax <timbangan@cbn.net.id>

To: ○ pchekov@victim.com

Yesterday at 12:35 PM

Pchekov ACH#321-L...
107.6 KB

Download All · Preview All

This message is high priority.

New Fax Received For Pchekov

You have a new fax document from (859) 859 - 5744.

Pages	2 Full scanned PDF.
Received	10, May 2021
Recipient	pch***@victim.com

To view FAX messages, open the attachment and login with your office email to authenticate viewer and enable instant access to all your fax messages on the go.

Example:

- From?

  Claims to be from DHL, but actual email is some domain that is completely unrelated.

- To?

  Is this the address you expect to get a shipping notification sent to?

- Context?

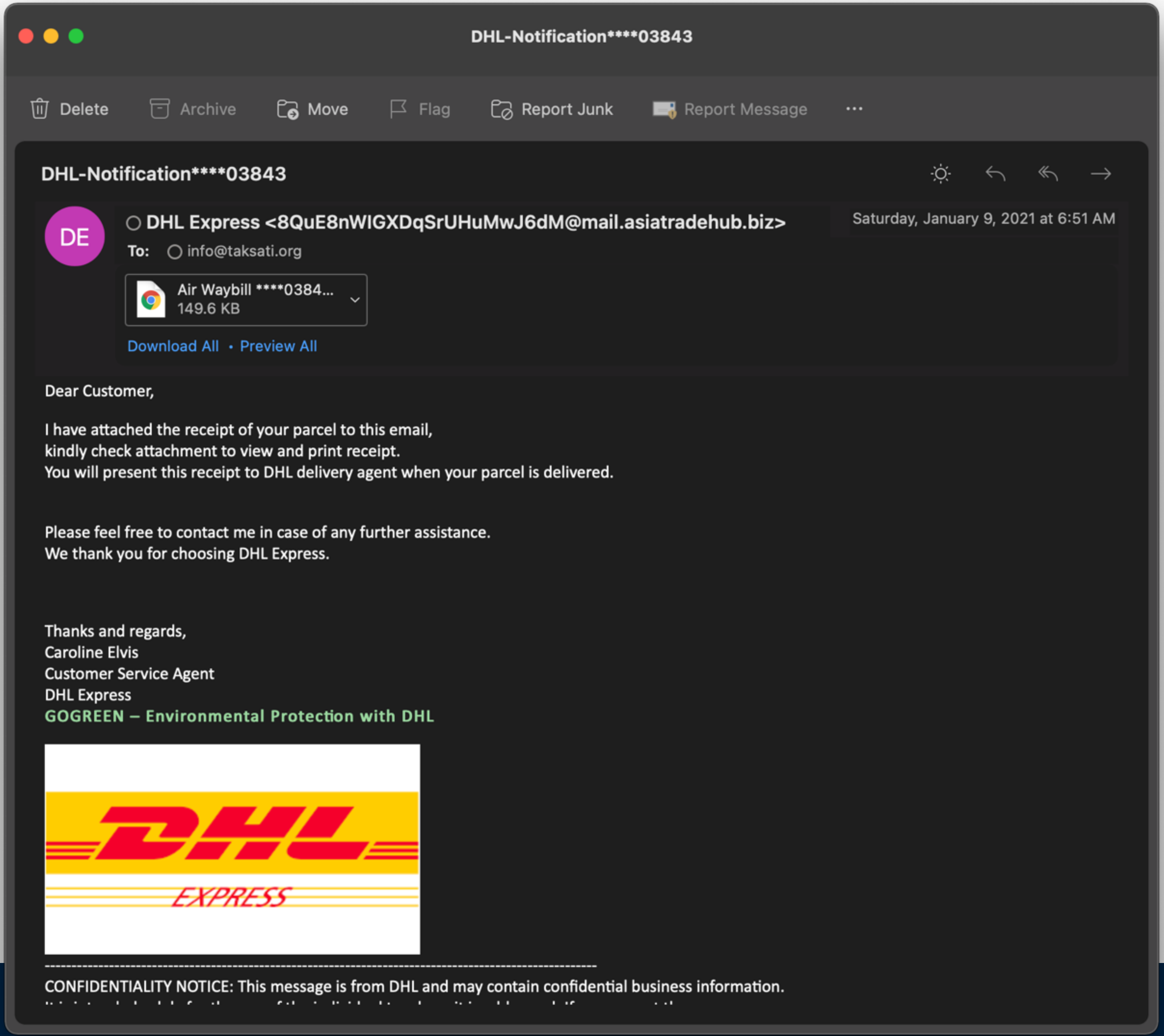
  Invoices and receipts are common themes in phishing. The goal is to trick you into opening that attachment.

- Format?

  An effort was made to make this look professional, but there are still clues. Generic greeting, grammar and structure problems in the body of the message, signature block feels off. Nice try, ”Caroline”.

- Attachment?

  The attachment is a web page that will open in your browser. Code in the page will then cause your browser to go open another page that is a fake login, giving you the impression you need to log into your Office 365 account to read the fax. This is all an elaborate scheme to steal your password.



DHL-Notification****03843

○ DHL Express <8QuE8nWIGXDqSrUHuMwJ6dM@mail.asiatradehub.biz>

Saturday, January 9, 2021 at 6:51 AM

To: ○ info@taksati.org

Air Waybill ****0384...
149.6 KB

Dear Customer,

I have attached the receipt of your parcel to this email,
kindly check attachment to view and print receipt.
You will present this receipt to DHL delivery agent when your parcel is delivered.

Please feel free to contact me in case of any further assistance.
We thank you for choosing DHL Express.

Thanks and regards,
Caroline Elvis
Customer Service Agent
DHL Express
GOGREEN – Environmental Protection with DHL

DHL EXPRESS

CONFIDENTIALITY NOTICE: This message is from DHL and may contain confidential business information.

Example

- From?

  Claims to be from your company's CEO, but actual email is some domain that is completely unrelated, even has a different name in the left side of the @.

- To?

  This email passes this check, but...

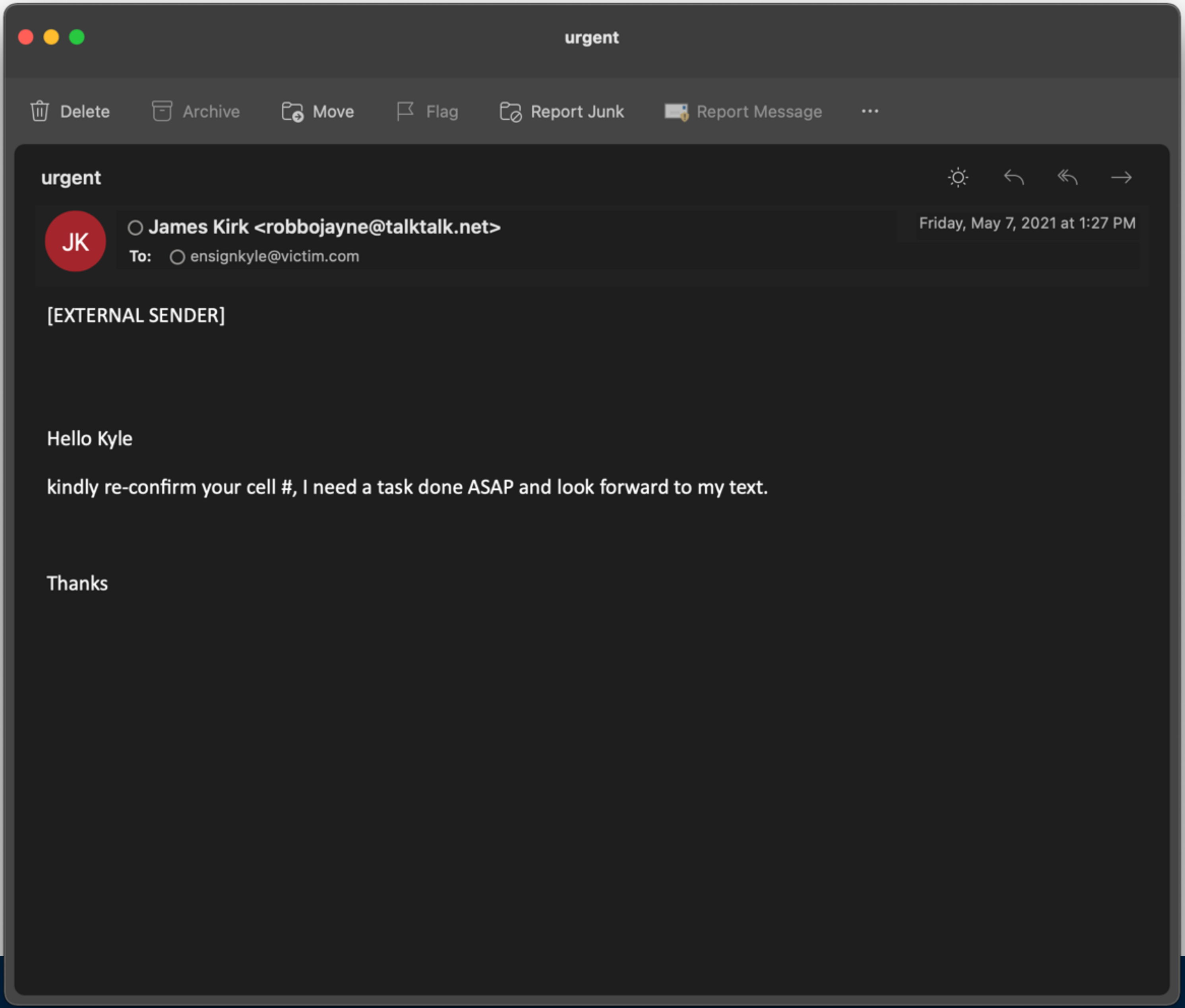
- Context?

  Why is the CEO emailing me? Why are they asking me to do them an "urgent" "task"?

- Format?

  The format, tone, grammar, and general feel of this email should raise multiple red flags. Is this how your CEO normally writes?

If you reply, the next message will tell you they need gift cards. Sometimes they will provide some elaborate story about giving out those gift cards to employees as a bonus, birthday gift, or whatever. Don't spoil the surprise. They'll want you to secretly email or text them the numbers from those cards, which they quickly cash out. This is all just an elaborate ploy to steal money from you.



urgent

○ James Kirk <robbojayne@talktalk.net>

To: ○ ensignkyle@victim.com

Friday, May 7, 2021 at 1:27 PM

[EXTERNAL SENDER]

Hello Kyle

kindly re-confirm your cell #, I need a task done ASAP and look forward to my text.

Thanks

Example:

- From?

The attacker faked the from address. You can't see it in this view, but there are additional hidden fields we will use to identify the sender.

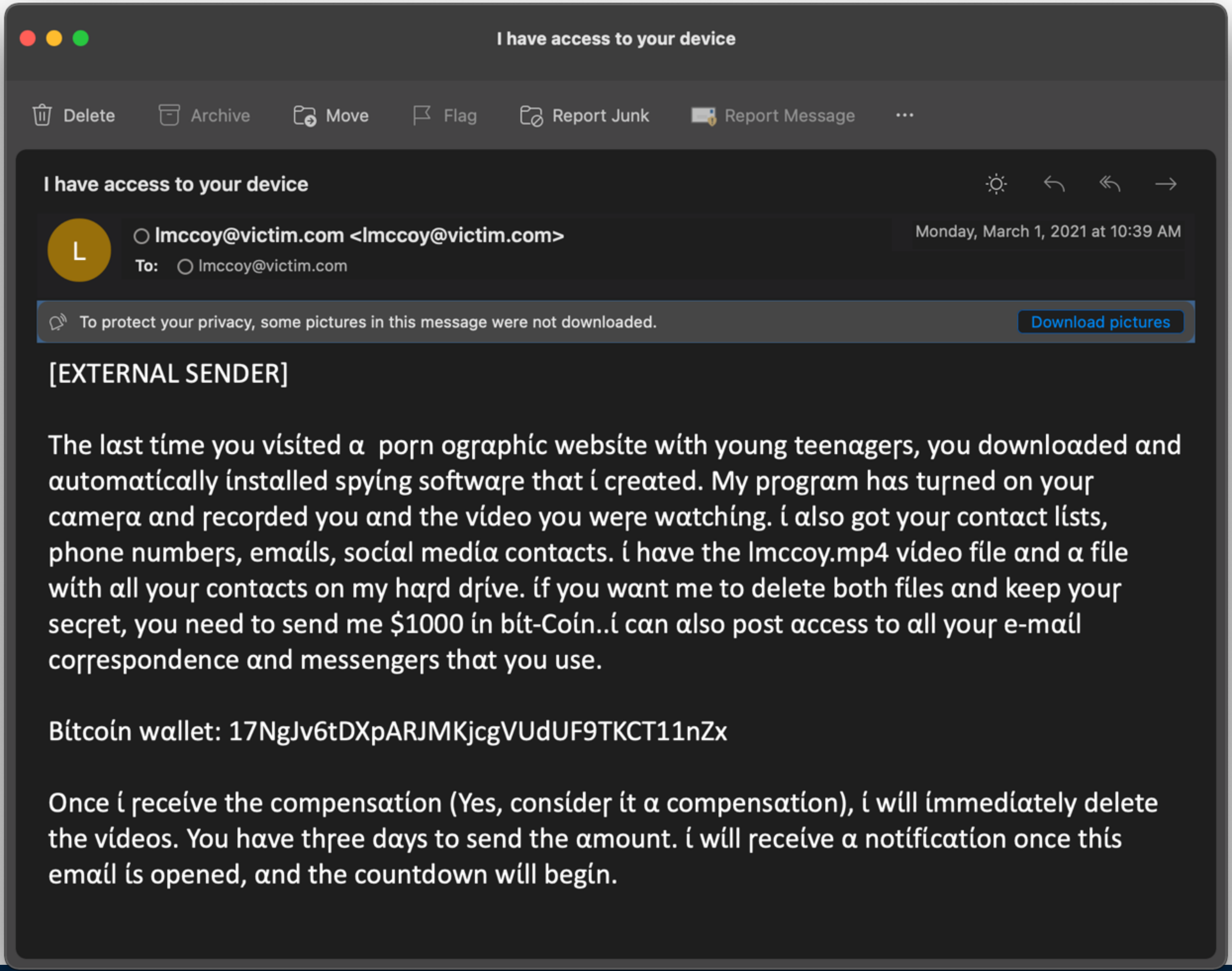
- Context?

This messages drops all the pretend themes and just boldly attempts to extort money out of you. Did you actually do what they are accusing you of? Do they provide any proof?

- Format?

Notice how the letters are oddly formed? The 'a', 'i', 'r', and other letters look odd? They are using letters from another alphabet so that none of these words are actually English words. This is an attempt to sneak past your spam filter.

This is a weak attempt at extortion. They provide no proof of their claims, and their claims don't match the users' actual work patters. They are just hoping to scare someone into sending them money.



I have access to your device

I have access to your device

L ○ lmccoy@victim.com <lmccoy@victim.com>

To: ○ lmccoy@victim.com

Monday, March 1, 2021 at 10:39 AM

To protect your privacy, some pictures in this message were not downloaded.

[EXTERNAL SENDER]

The last time you visited a porn ographic website with young teenagers, you downloaded and automatically installed spying software that i created. My program has turned on your camera and recorded you and the video you were watching. i also got your contact lists, phone numbers, emails, social media contacts. i have the lmccoy.mp4 video file and a file with all your contacts on my hard drive. if you want me to delete both files and keep your secret, you need to send me $1000 in bit-Coin..i can also post access to all your e-mail correspondence and messengers that you use.

Bitcoin wallet: 17NgJv6tDXpARJMKjcgVUdUF9TKCT11nZx

Once i receive the compensation (Yes, consider it a compensation), i will immediately delete the videos. You have three days to send the amount. i will receive a notification once this email is opened, and the countdown will begin.

Example:

- From?
  Claims to be from your company's fax, but actual email is some domain that is completely unrelated.

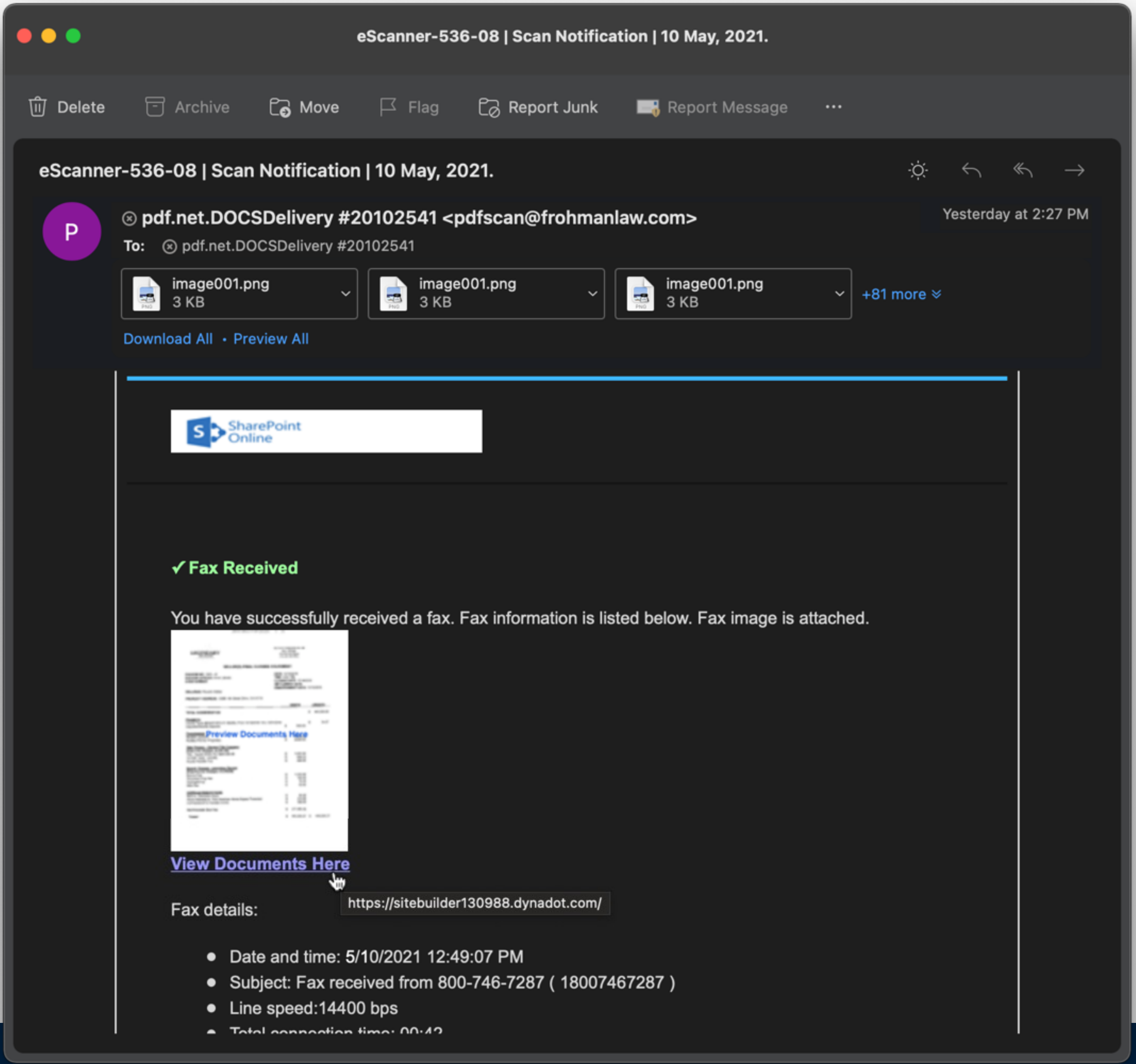
- To?
  Your address isn't even on the to line. That is because you, and a few million other people, were all bcc'ed the same email.

- Context?
  Who sends faxes in the 21st century? The SharePoint logo is low quality and doesn't match the context of the message. That's just setting the stage for the next step where they ask you to log into a fake SharePoint page to view the "fax".

- Format?
  The grammar and structure of the message is off.

- Links?
  WITHOUT CLICKING, if you hover your mouse of the link a little block of text will appear that tells you the URL the link will open. This message is trying to make you think you are opening a document on your company's SharePoint site, but the domain in that URL is obviously not your company's SharePoint site.

  If the URL is ANYTHING other than a site you absolutely know and trust, don't click it. Even if the URL is a site you know and trust, with the other red flags above you still shouldn't click the link.



eScanner-536-08 | Scan Notification | 10 May, 2021.

pdf.net.DOCSDelivery #20102541 <pdfscan@frohmanlaw.com>

To: pdf.net.DOCSDelivery #20102541

Yesterday at 2:27 PM

✓Fax Received

You have successfully received a fax. Fax information is listed below. Fax image is attached.

View Documents Here

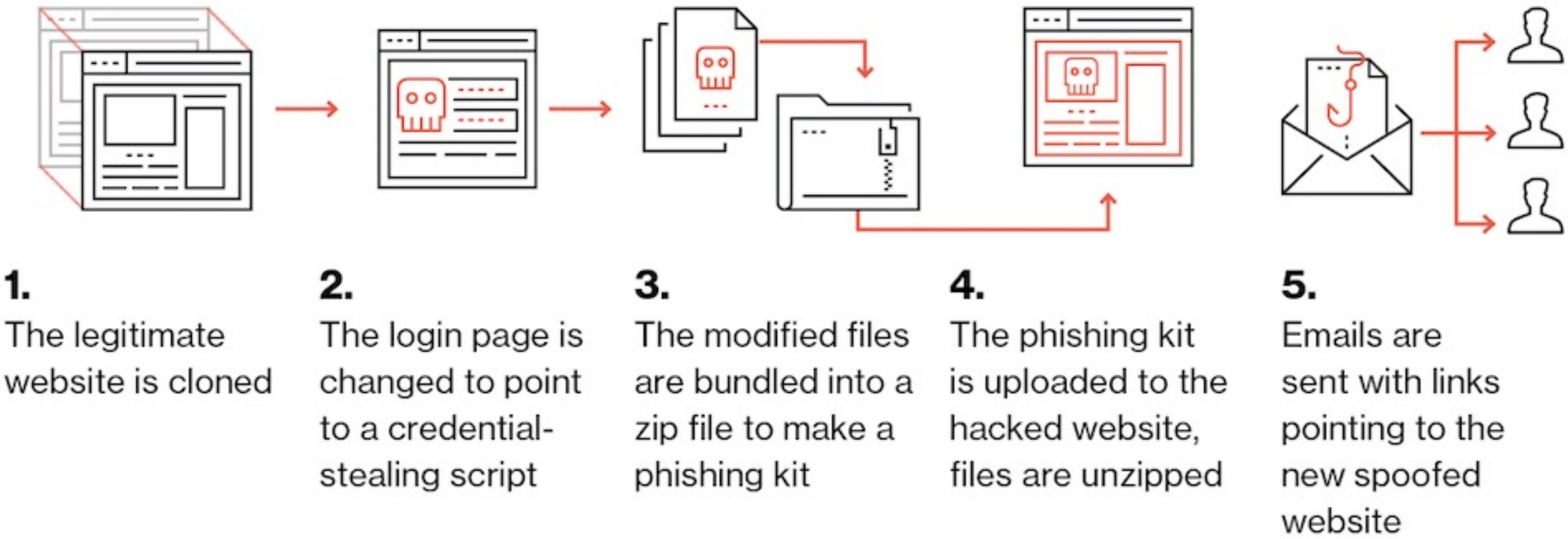
https://sitebuilder130988.dynadot.com/

Fax details:

- Date and time: 5/10/2021 12:49:07 PM
- Subject: Fax received from 800-746-7287 (18007467287)
- Line speed:14400 bps
- Total connection time: 00:42

Phishing Kits

- Collection of code and tools used to run a phishing campaign



1. The legitimate website is cloned

2. The login page is changed to point to a credential-stealing script

3. The modified files are bundled into a zip file to make a phishing kit

4. The phishing kit is uploaded to the hacked website, files are unzipped

5. Emails are sent with links pointing to the new spoofed website

https://duo.com/blog/phish-in-a-barrel-hunting-and-analyzing-phishing-kits-at-scale