MEISAC

MEDIA + ENTERTAINMENT
INFORMATION SHARING ANALYSIS CENTER

PHISHING, SCOURGE OF THE DEEP BLUE INTERNET

What is all this phishing you speak of?

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

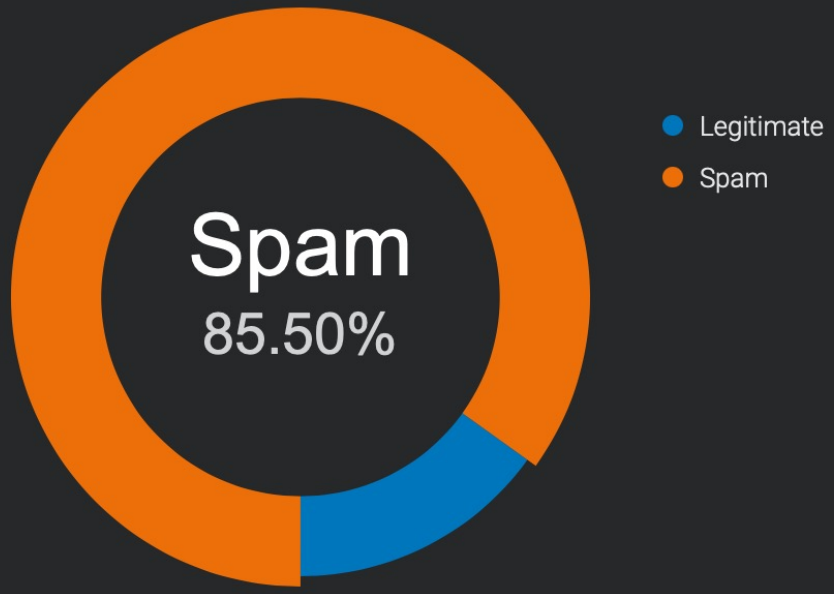
-61.2%

Average Daily Spam Volume

88.21 BILLION

Spam Volume Change from Previous Month

-36%



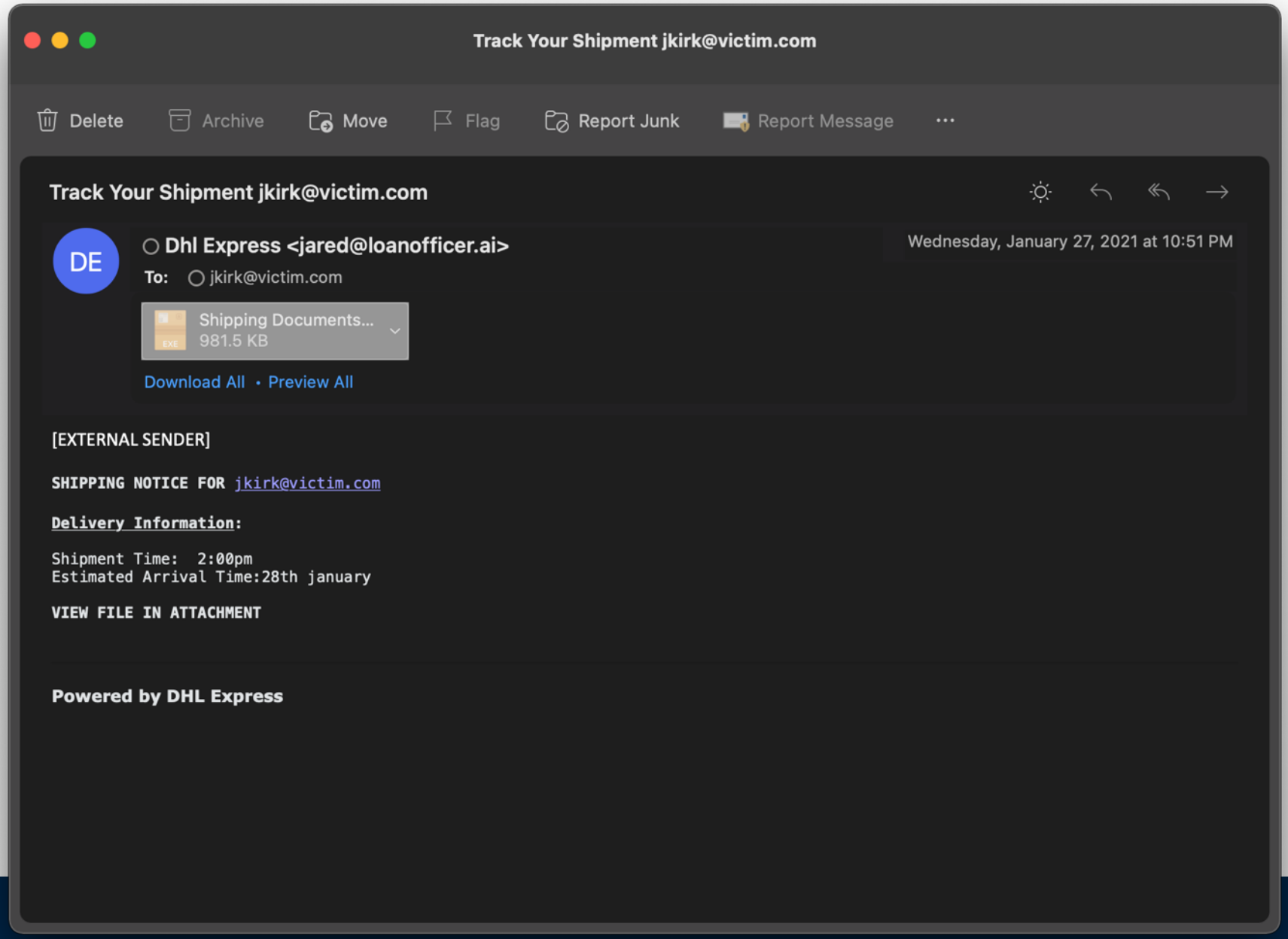
DAILY EMAIL VOLUME

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.



EXAMPLE:

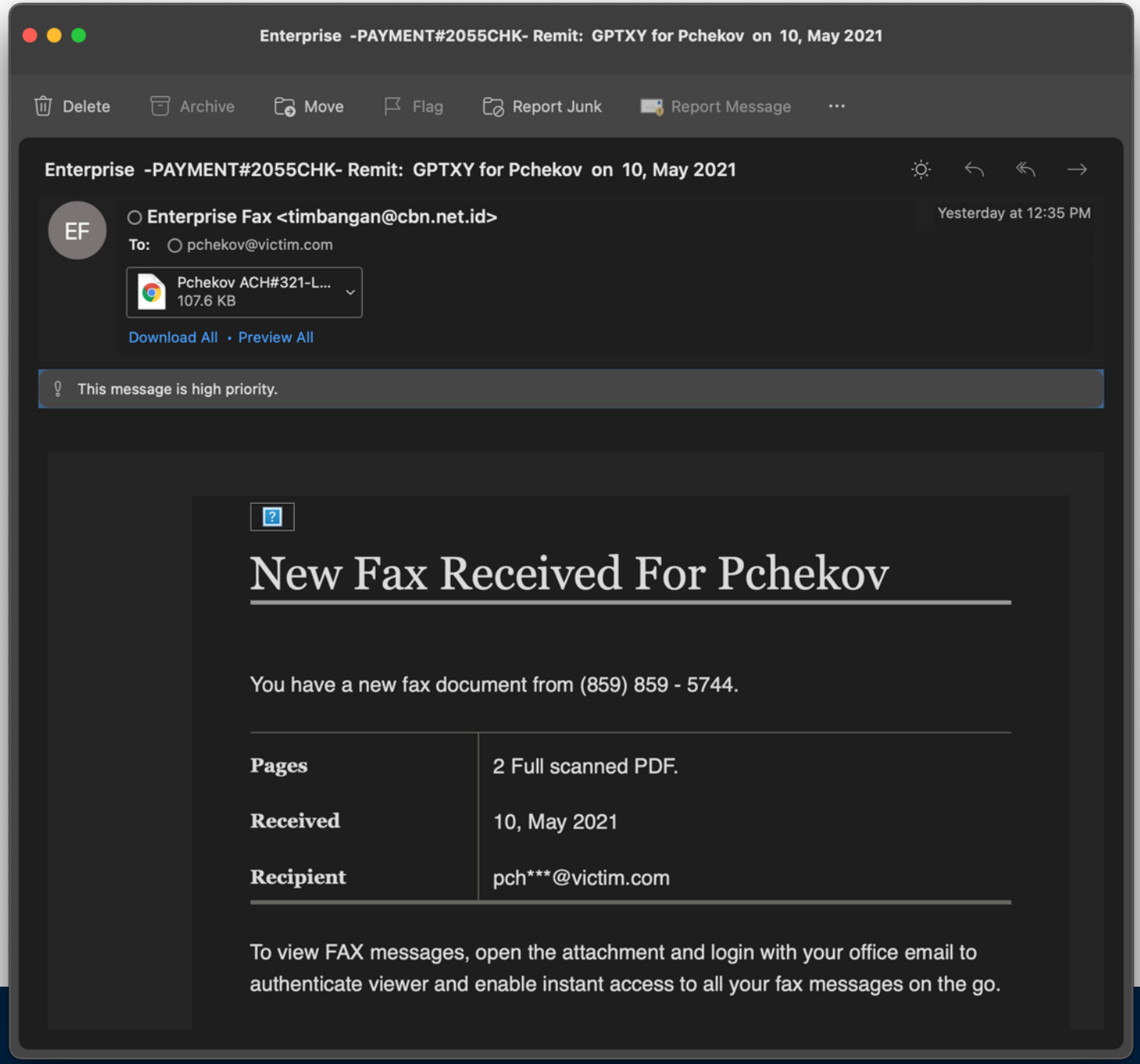
- From?
  Claims to be from your company's fax machine, but actual email is some domain that is completely unrelated.

- 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.

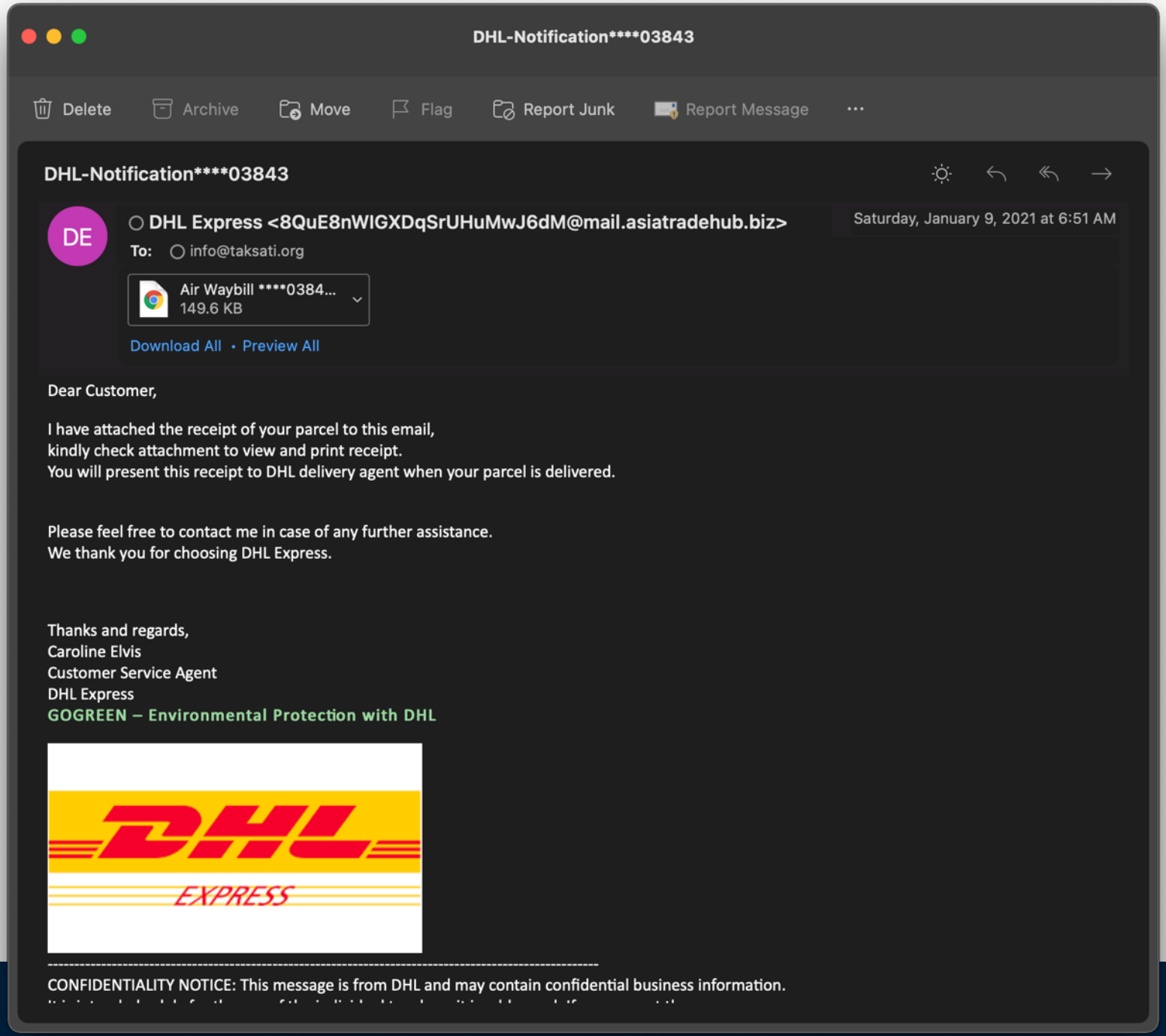
- Format?
  An effort was made to make this look professional, but there are still clues. The included graphics, the name being off, the message says the attachment is a .pdf but it is actually an .htm file.

- 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.



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.



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...

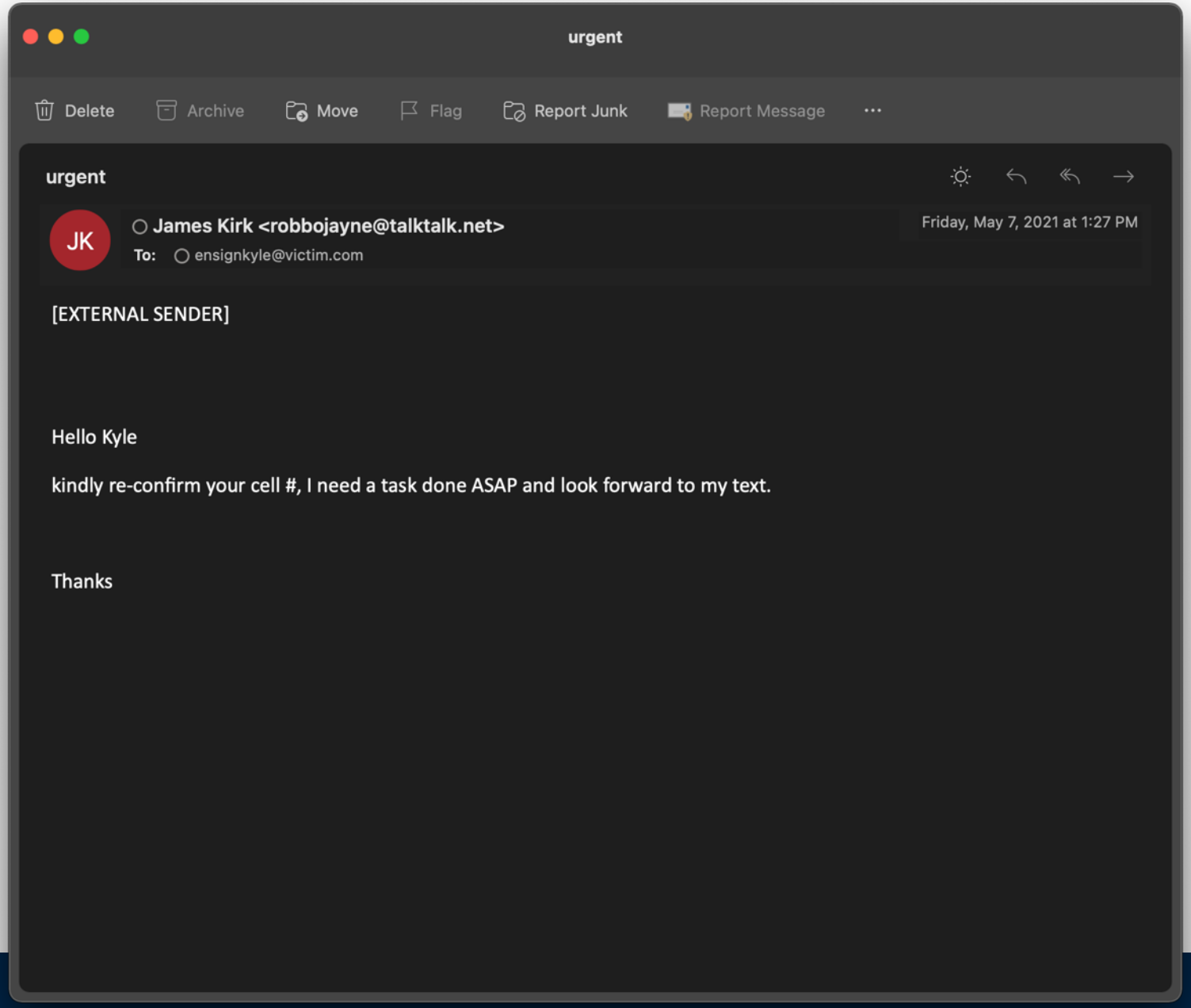
- Context?

  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.



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.

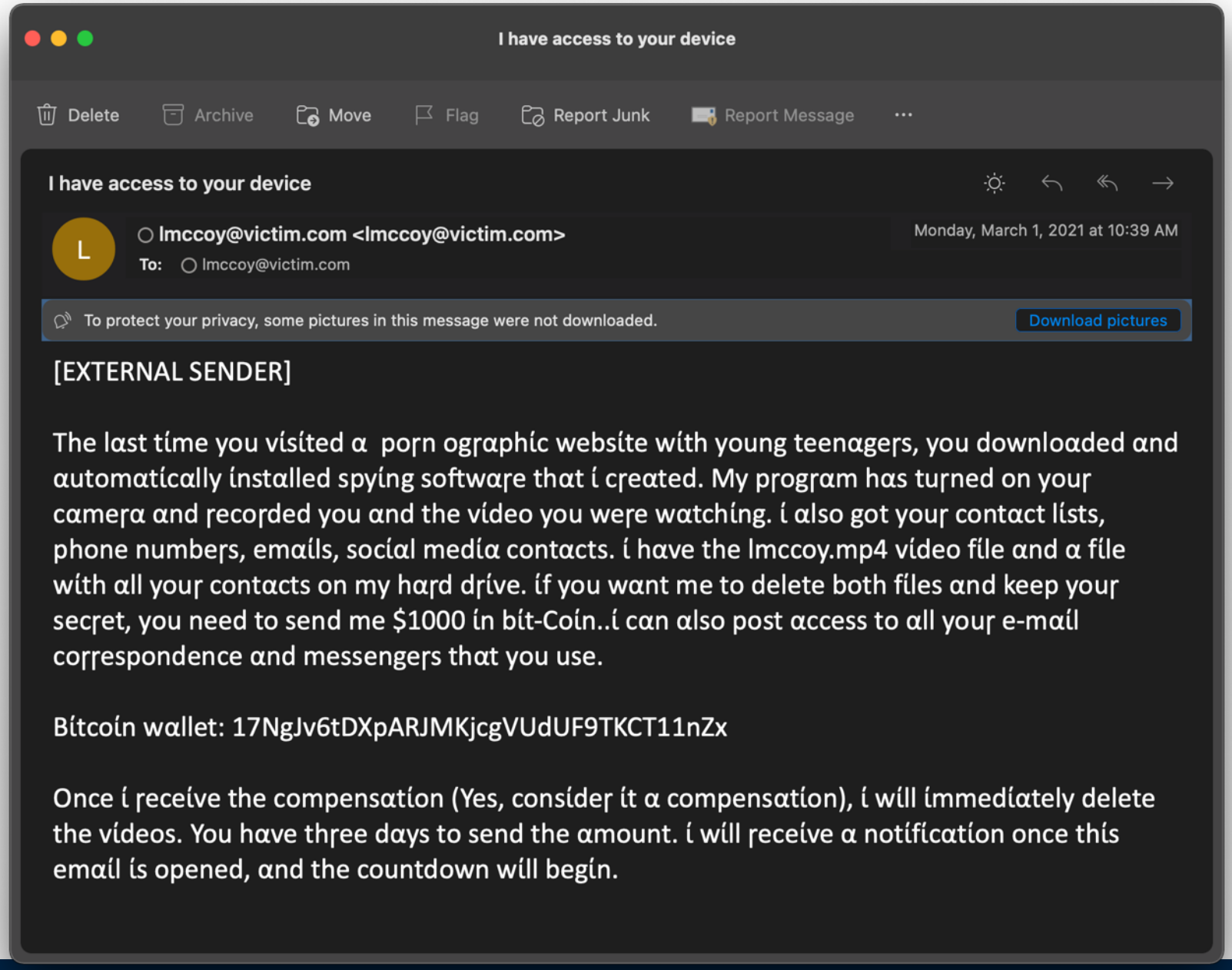
- Context?

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? How the 'a', 'i', 'r', and other letters look odd? They are using letters from another alphabet so that none of the important words will match if we search for them. 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 patterns. They are just hoping to scare someone into sending them money. The sender does NOT have access to your device and there are NO video files.



EXAMPLE:

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

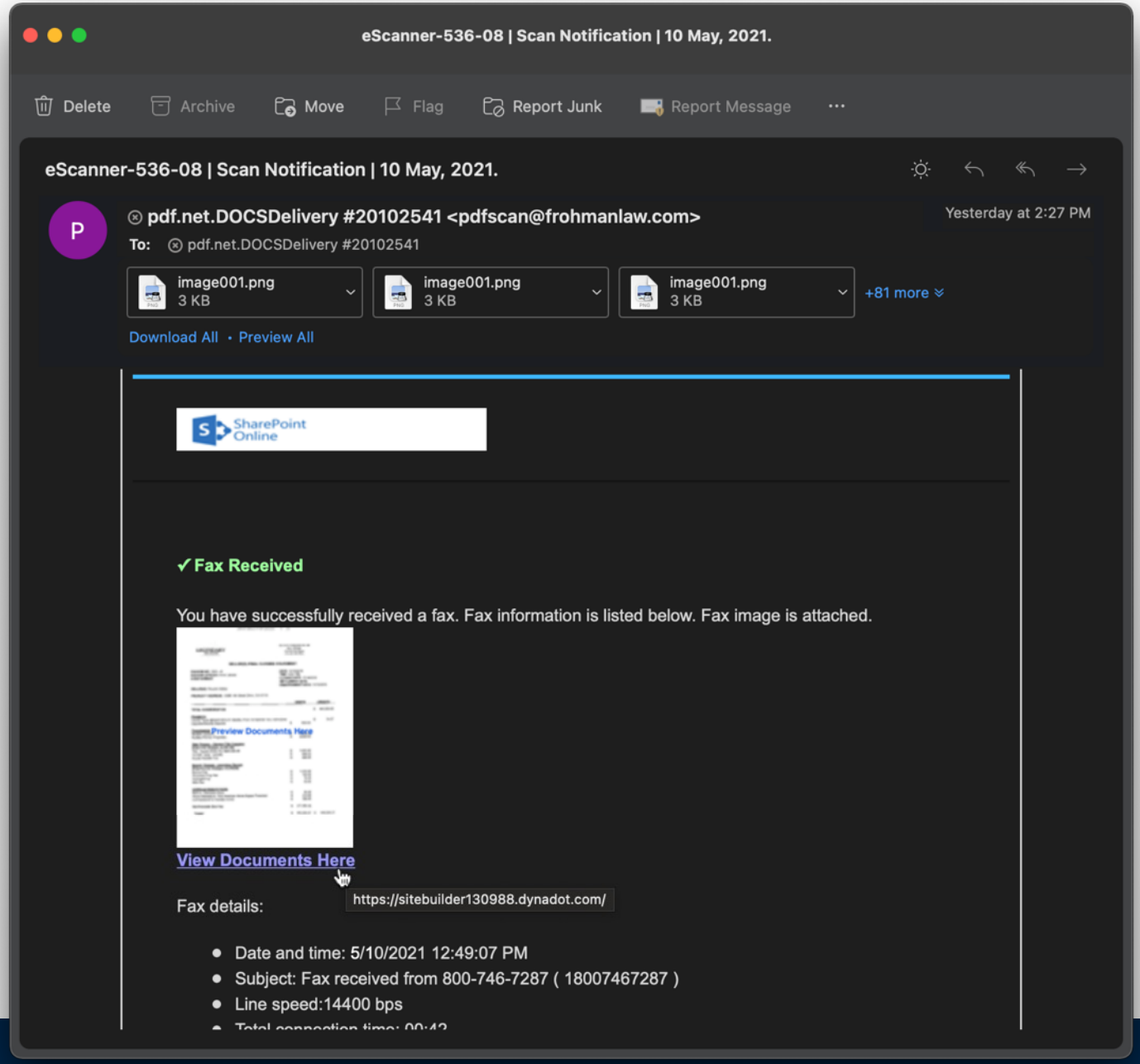
- To?
  Your address isn't even on the to line. That is because you, and a few million other people, were all bcc'ed the same email.

- 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.

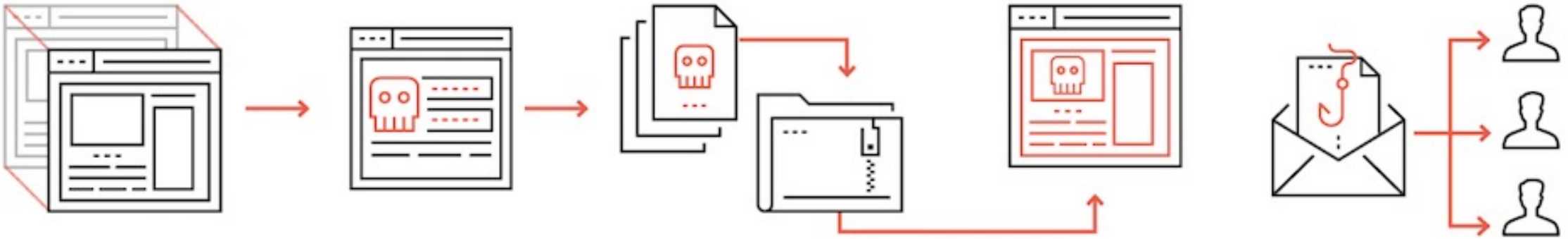
- Links?
  WITHOUT CLICKING, if you hover your mouse of the link a little block of text will appear that tells you the URL the link will open. This message is trying to make you think you are opening a document on your company's SharePoint site, but the domain in that URL is obviously not your company's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



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

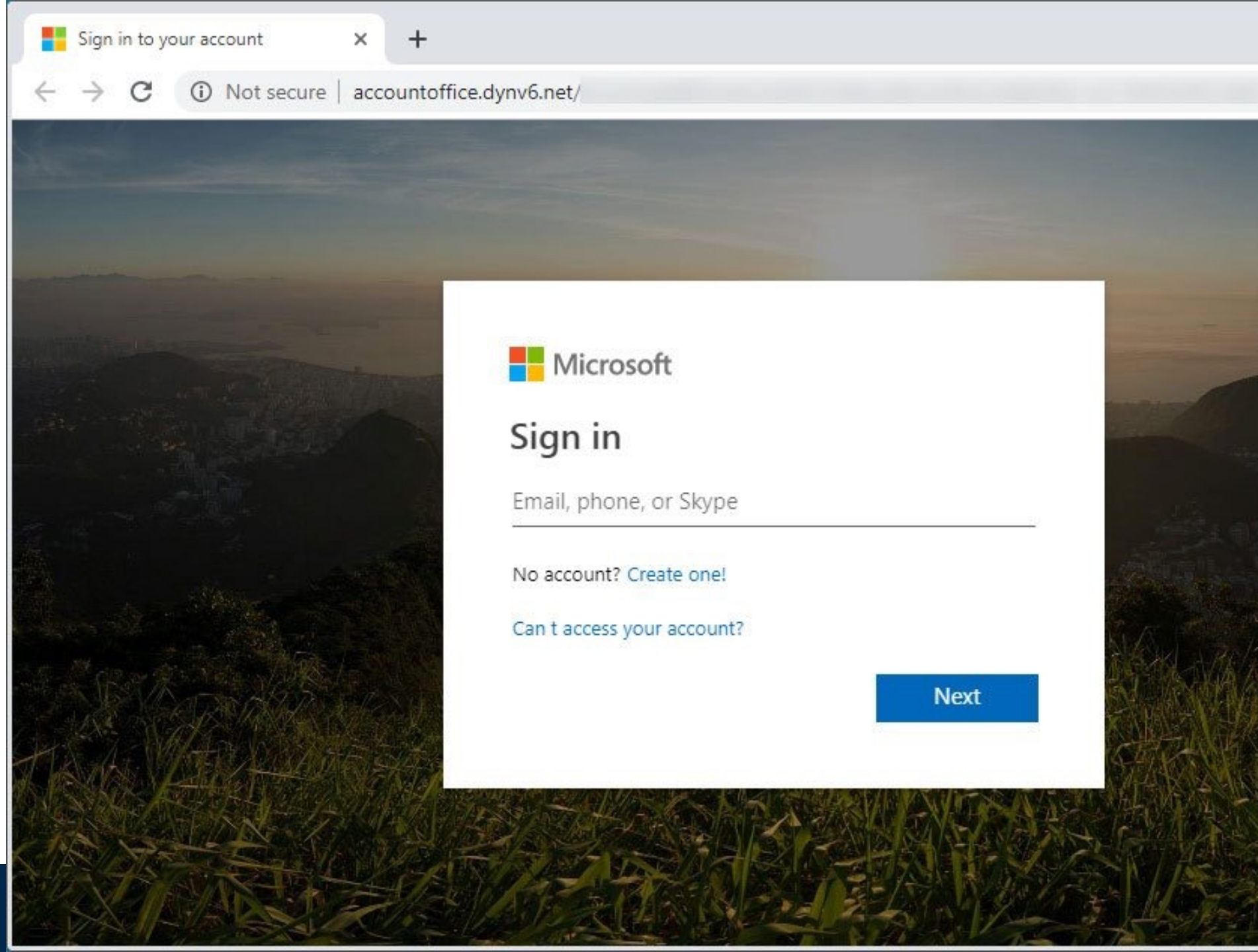
5.
Emails are sent with links pointing to the new spoofed website

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

EXAMPLE:

- URL?
  That domain is not either Microsoft or your company's domain, so this login prompt is a fake.
- Padlock?
  It says the site is "not secure". The real login page would have a padlock, indicating it is encrypted.
- Format?
  This is a good copy of a default Office 365 login page. This is why most organizations will not leave their login page default.
- Graphics?
  Most organizations will brand their Office 365, the Microsoft logo will be replaced by their company logo. If your page is normally branded and suddenly it isn't, back away!

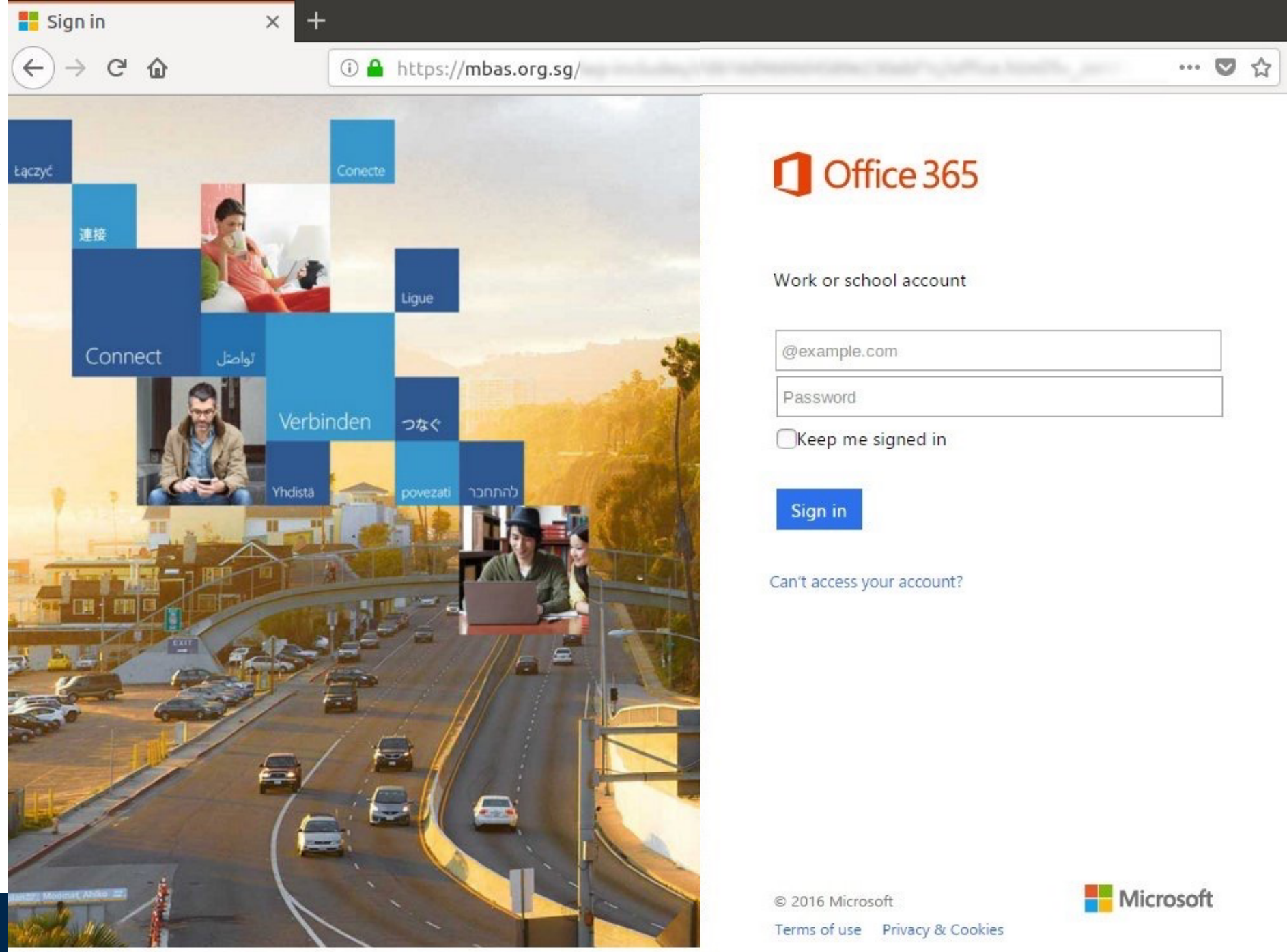
  Sometimes, the attacker will copy your company's branded page in a more targeted attack. The URL is always the best tell.



EXAMPLE:

- URL?
  That domain is not either Microsoft or your company's domain, so this login prompt is a fake.
- Padlock?
  Sometimes the attacker will spend the money to get that padlock. Just because the page is encrypted doesn't mean it isn't fake.
- Format?
  This is a good copy of a default Office 365 login page. This is why most organizations will not leave their login page default.
- Graphics?
  Most organizations will brand their Office 365, the Microsoft logo will be replaced by their company logo. If your page is normally branded and suddenly it isn't, back away!

  Sometimes, the attacker will copy your company's branded page in a more targeted attack. The URL is always the best tell.



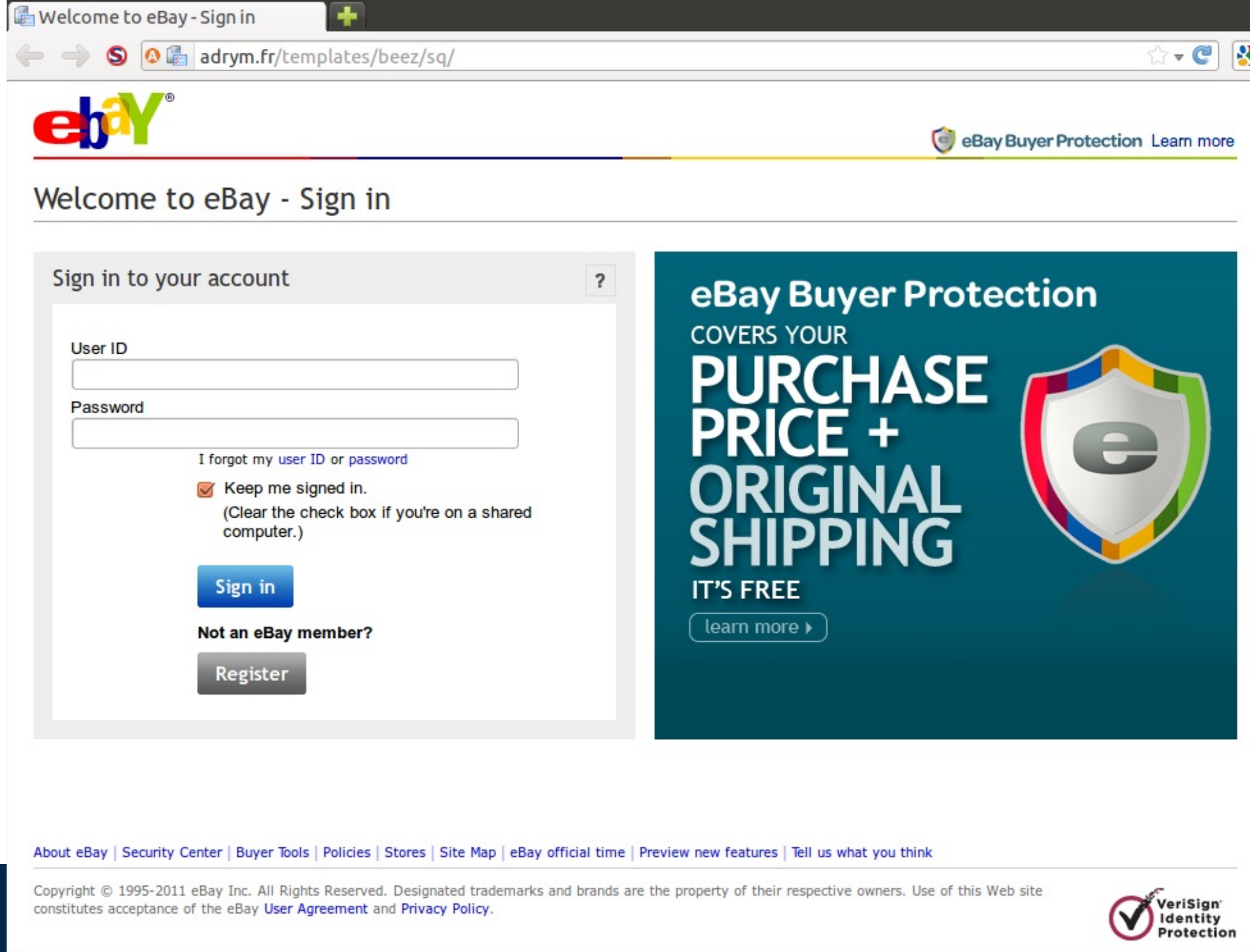
EXAMPLE:

- URL?
  That domain is not not eBay, so this login prompt is a fake.

- Padlock?
  This site is encrypted.

- Format?
  This is a good copy of the eBay login page. It can be hard to tell at a quick glance when the site is a forgery. Always check the address bar. Sometimes you'll have to actually click into address bar to see the full address, depending on which browser you are using.

  If the link in the email that brought you here provides even the slightest hint of doubt, type the address into the address bar instead of clicking the link. If you really did get a shipping notification, fax, receipt, invoice, or whatever the email claims, when you log into the site there will be a notice in there. When the real site doesn't agree with the email, the email is probably phishing.



What do you do?

- Slow down!
- Always consider the context
- Don’t click links or open attachments if there is ANY doubt
- Report the phishing emails
  - Use your email client’s ”Report Message” button
  - Start a new message, drag the offending message in, send it as an attachment
    - Sending as an attachment instead of hitting forward allows the security team to see all the headers, including the hidden fields that tells us where the email actually came from.
  - This report helps your security team tune the filters
- Employ a good Secure Email Gateway that filters out the evil
  - ↑ aka a Spam Filter ↑

Chris Taylor

https://meisac.org

info@meisac.org