mimecast®

The Human Firewall is on fire – Anatomy of an email-based attack.

Cyber Security Today

Defense Arms Race

Threats are constantly evolving!

Data Recovery

Can we recover to the last safe state!

Skills Deficiencies

It’s difficult to attract and retain talent!

Business Disruptions

How do we maintain availability during a disruption!

Email Attacks

~30%

of phishing attacks were opened[1]

100S

Median time to first click[1]

91%

of attacks start with a phish[2]

66%

of malware was installed via malicious email attachments[3]

$5B

BEC is $5B global scam[4]

1 Verizon Data Breach Report 2016 | 2 Wired 2015 | 3 Verizon Data Breach Report 2017 | 4 FBI, Public Service Announcement, May 4, 2017

Why do attackers rely on email?

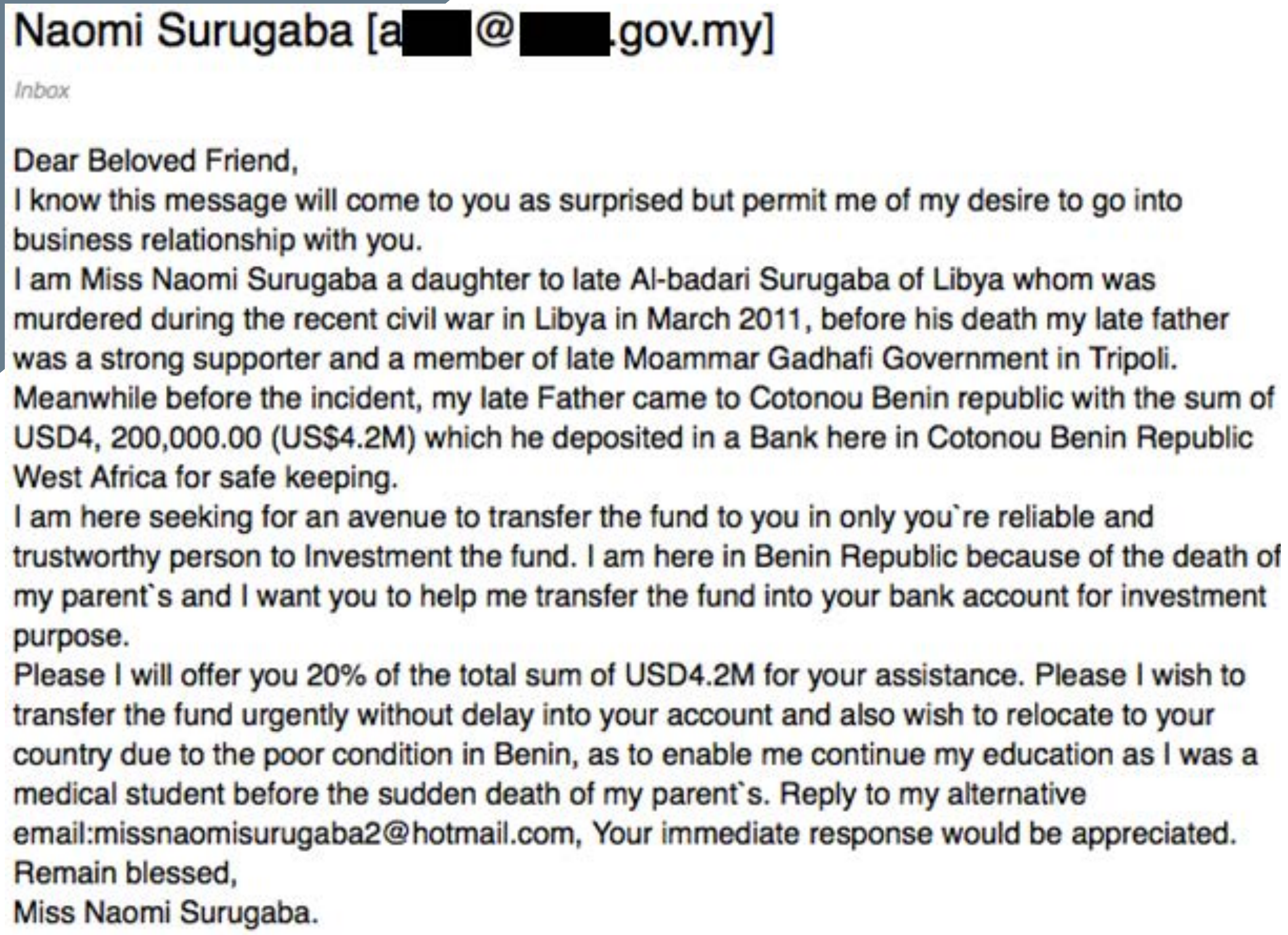
Cheap, ubiquitous, global, flexible, anonymous, trusted by users, integral to so many business processes

225B
Emails sent everyday

#1
Office 365 Cloud Service by User Count

6.3B
Email Mailboxes in 2017, growing to 7.7B by 2021

Original Phishing Scams - What do you notice about them?



Naomi Surugaba [a[redacted]@[redacted].gov.my]

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

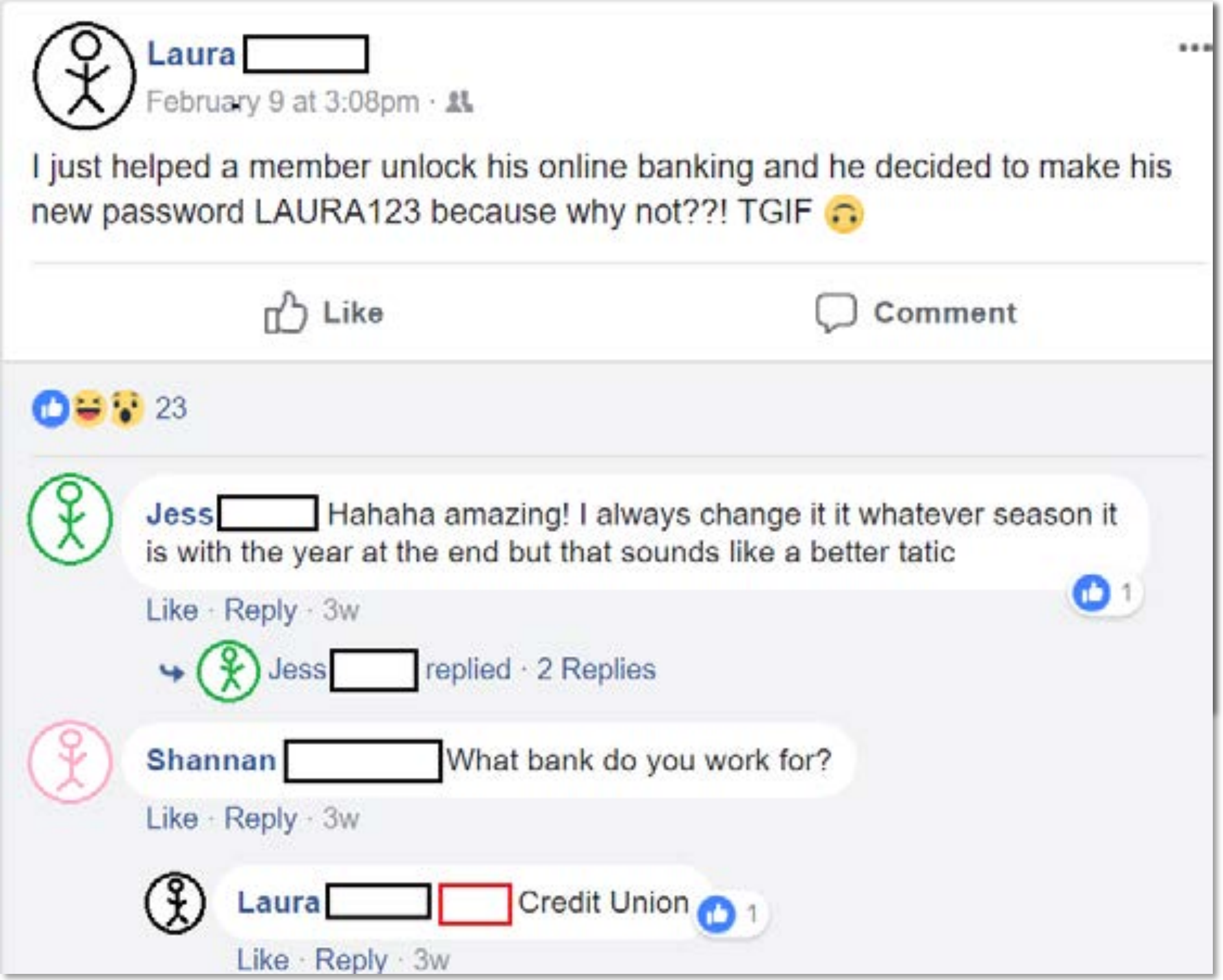
Your company is at **risk** if you…

- Have certain letters in your domain name
- Accept resumes on your website
- Highlight your Management or Leadership Team on your website
- Have a in™ profile
- Think your life is deemed *interesting* enough to be on f

It Only Takes One.

mimecast®

Introducing: Your Users



Laura [redacted]

February 9 at 3:08pm ·

I just helped a member unlock his online banking and he decided to make his new password LAURA123 because why not??! TGIF

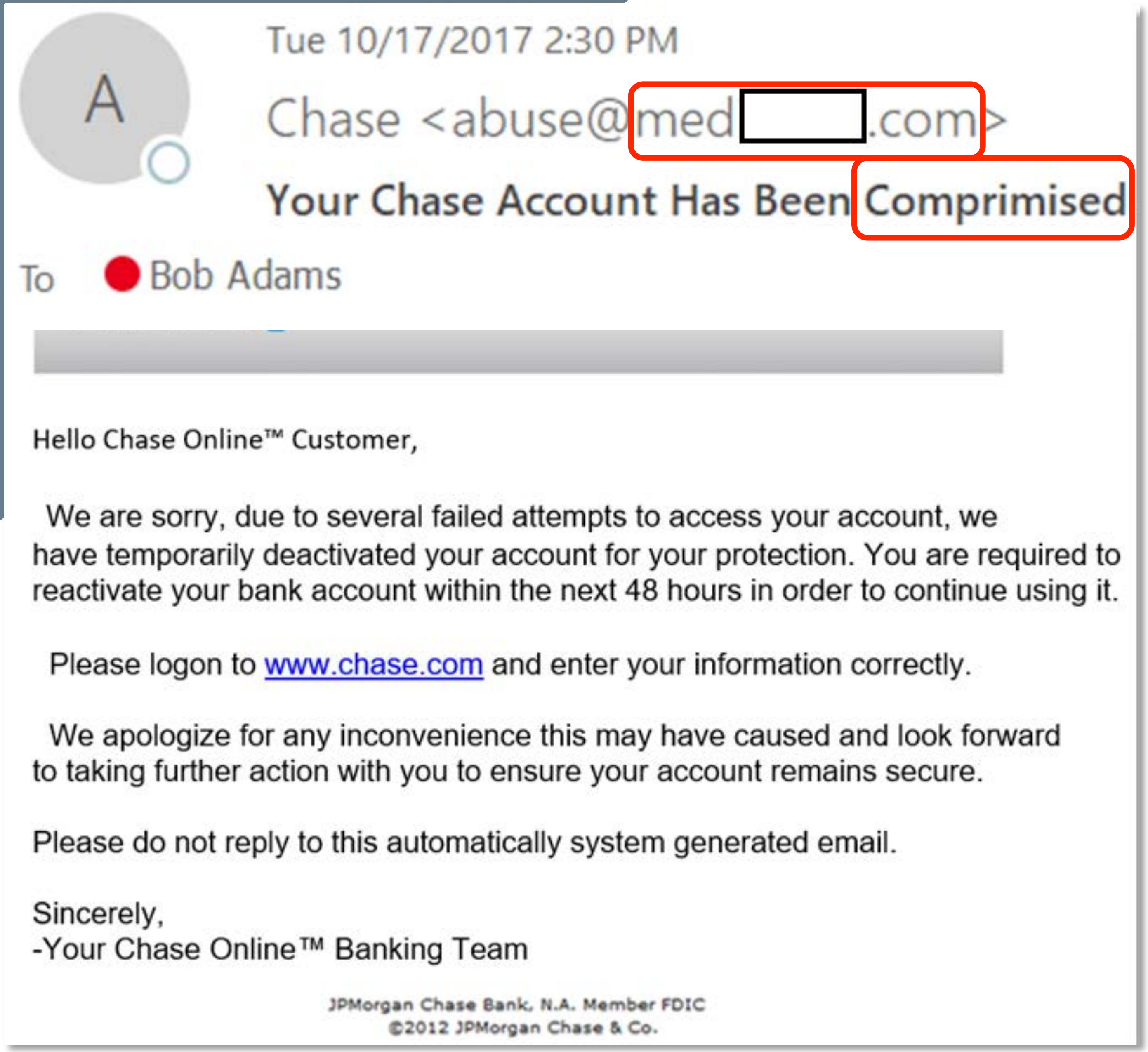
Jess [redacted] Hahaha amazing! I always change it it whatever season it is with the year at the end but that sounds like a better tatic

Jess [redacted] replied · 2 Replies

Shannan [redacted] What bank do you work for?

Laura [redacted] [redacted] Credit Union

Would You Click?



Tue 10/17/2017 2:30 PM

Chase <abuse@med[redacted].com>

Your Chase Account Has Been Comprimised

To Bob Adams

Hello Chase Online™ Customer,

We are sorry, due to several failed attempts to access your account, we have temporarily deactivated your account for your protection. You are required to reactivate your bank account within the next 48 hours in order to continue using it.

Please logon to www.chase.com and enter your information correctly.

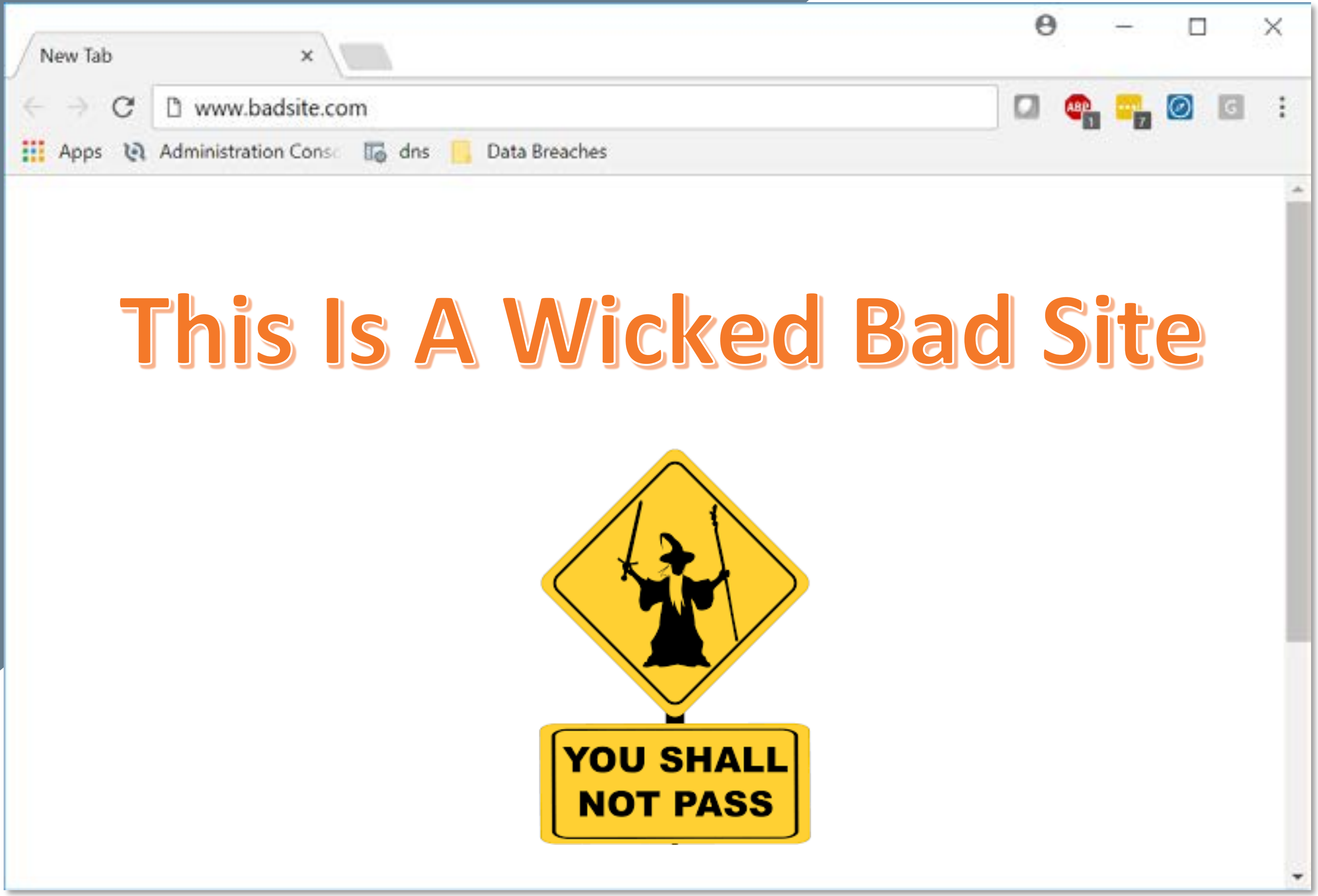
We apologize for any inconvenience this may have caused and look forward to taking further action with you to ensure your account remains secure.

Please do not reply to this automatically system generated email.

Sincerely,
-Your Chase Online™ Banking Team

JPMorgan Chase Bank, N.A. Member FDIC
©2012 JPMorgan Chase & Co.

mimecast®



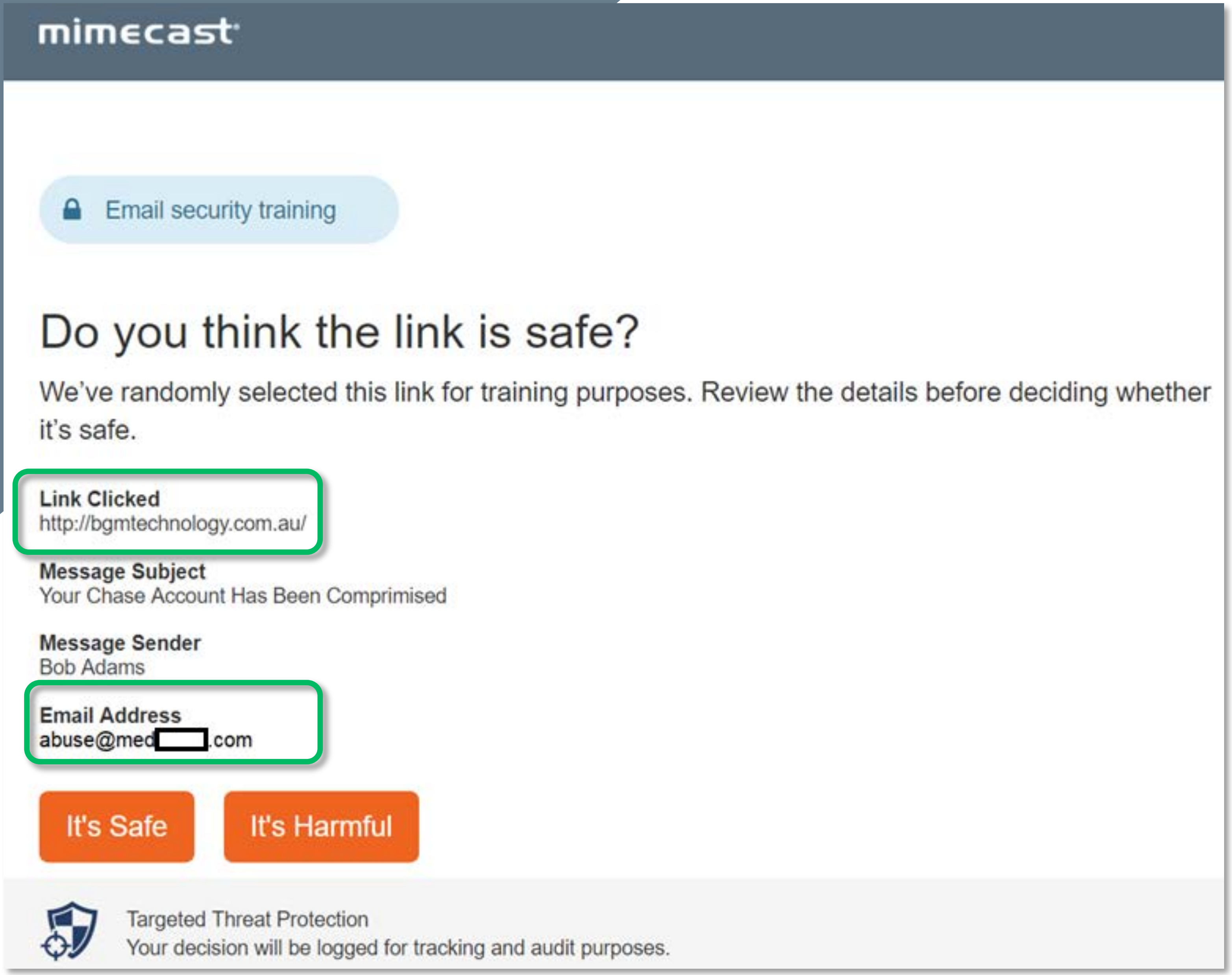
This Is A Wicked Bad Site

mimecast®

WSYUD?

What Should Your User Do?

URL Protect



Do you think the link is safe?

We've randomly selected this link for training purposes. Review the details before deciding whether it's safe.

Link Clicked
http://bgmtechnology.com.au/

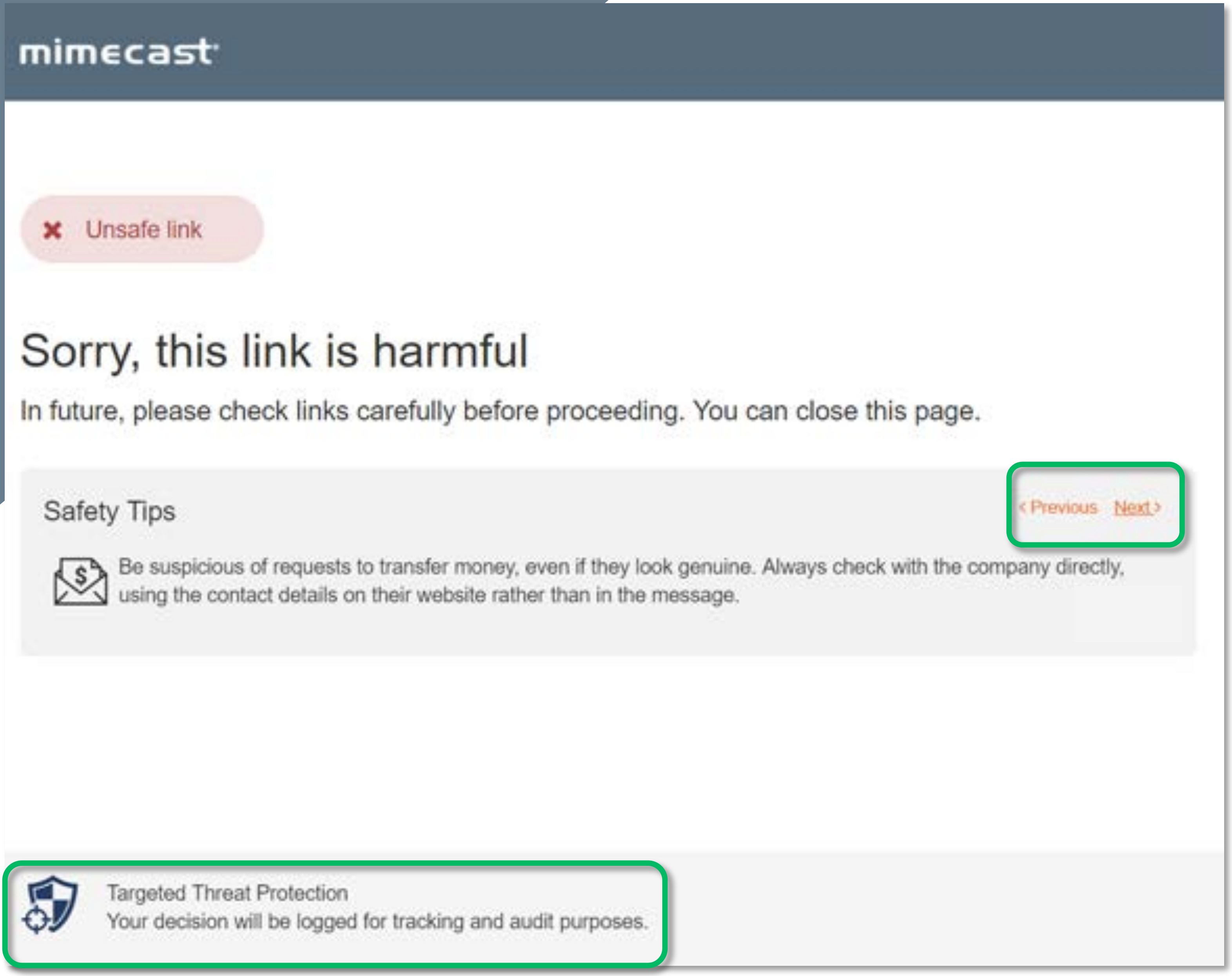
Message Subject
Your Chase Account Has Been Comprimised

Message Sender
Bob Adams

Email Address
abuse@med[redacted].com

Targeted Threat Protection
Your decision will be logged for tracking and audit purposes.

URL Protect



mimecast

✖ Unsafe link

Sorry, this link is harmful

In future, please check links carefully before proceeding. You can close this page.

Safety Tips

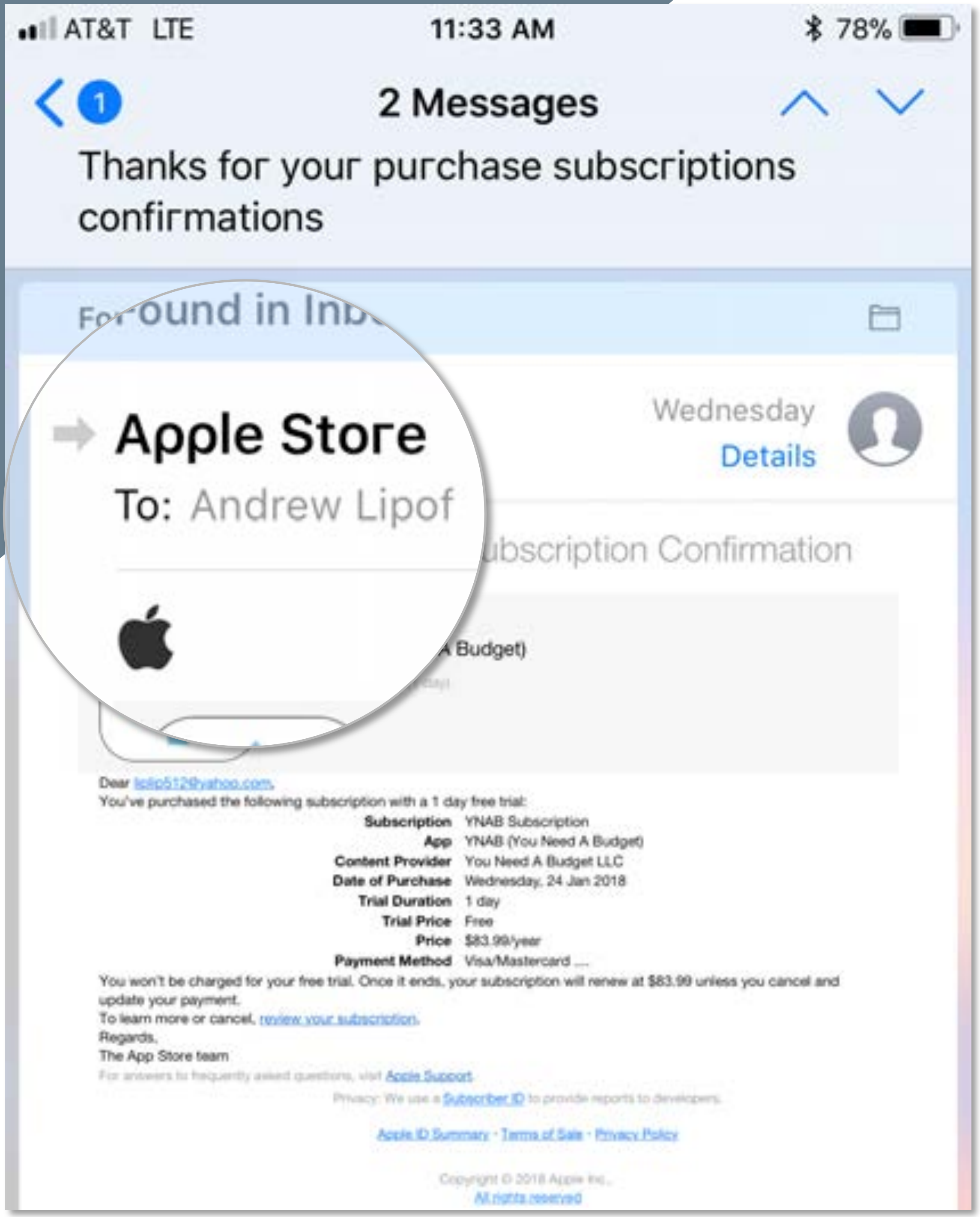
< Previous Next >

Be suspicious of requests to transfer money, even if they look genuine. Always check with the company directly, using the contact details on their website rather than in the message.

Targeted Threat Protection
Your decision will be logged for tracking and audit purposes.

mimecast

Real or fake?



AT&T LTE 11:33 AM 78%

1 2 Messages

Thanks for your purchase subscriptions confirmations

Found in Inb

Apple Store

To: Andrew Lipof

Wednesday

Details

ubscription Confirmation

A Budget)

Dear lelip512@yahoo.com,

You've purchased the following subscription with a 1 day free trial:

Subscription	YNAB Subscription
App	YNAB (You Need A Budget)
Content Provider	You Need A Budget LLC
Date of Purchase	Wednesday, 24 Jan 2018
Trial Duration	1 day
Trial Price	Free
Price	$83.99/year
Payment Method	Visa/Mastercard ....

You won't be charged for your free trial. Once it ends, your subscription will renew at $83.99 unless you cancel and update your payment.

To learn more or cancel, review your subscription.

Regards,

The App Store team

For answers to frequently asked questions, visit Apple Support.

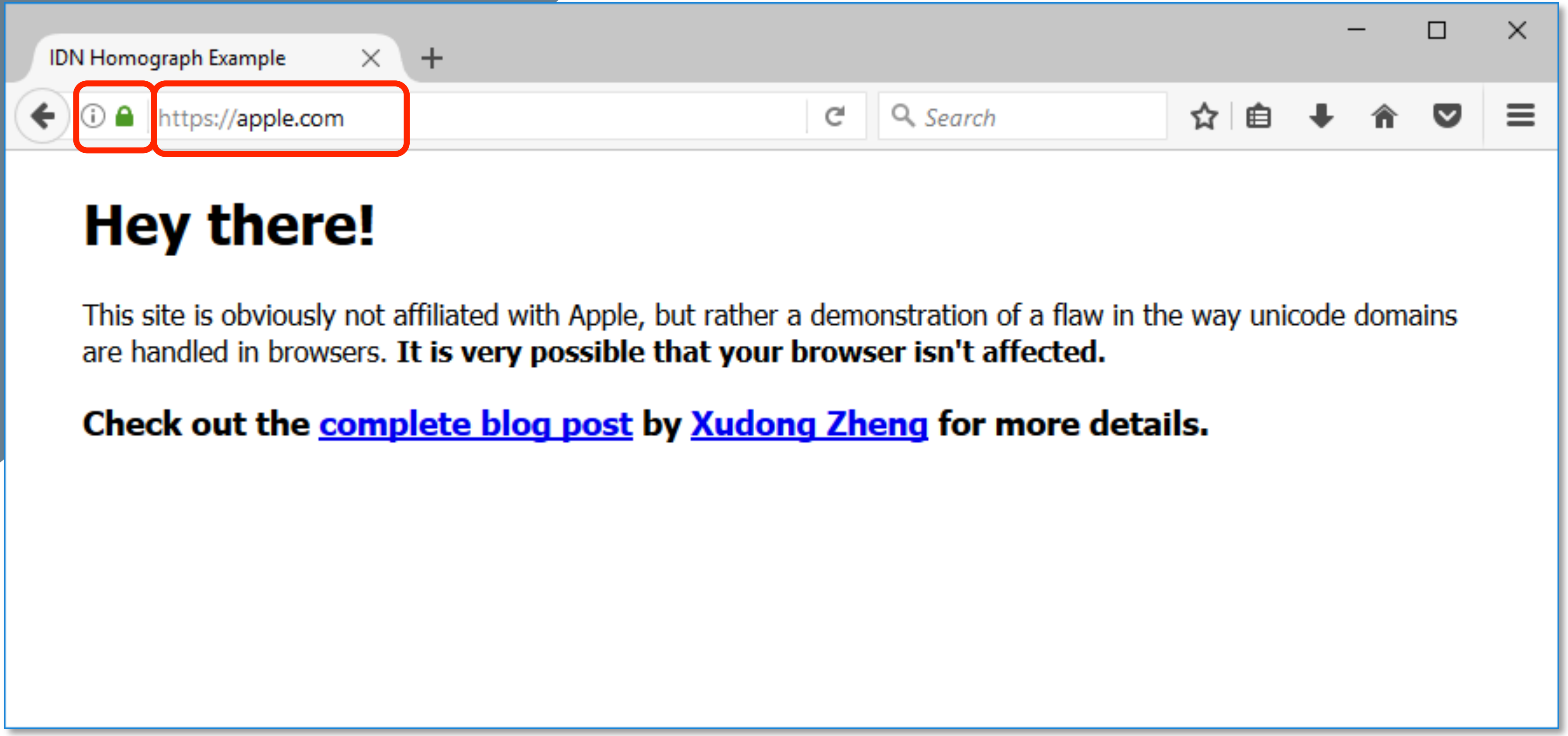
Privacy: We use a Subscriber ID to provide reports to developers.

Apple ID Summary · Terms of Sale · Privacy Policy

Copyright © 2018 Apple Inc.,
All rights reserved

mimecast®

Is this really Apple.com?



Hey there!

This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.**

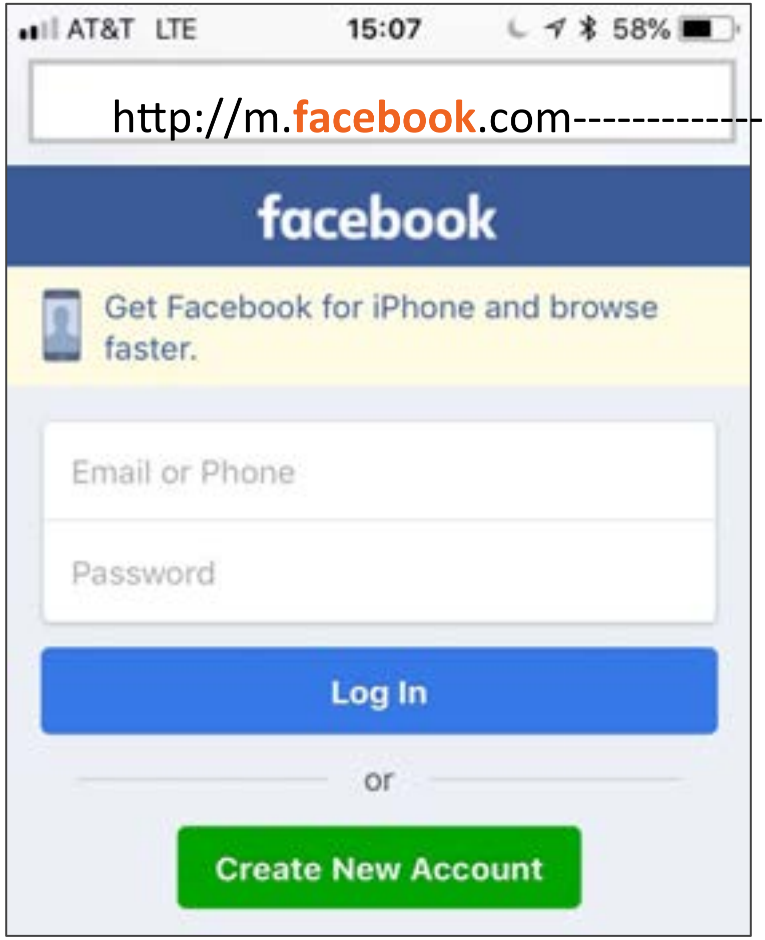
Check out the complete blog post by Xudong Zheng for more details.

That "Apple.com" URL is really this….

xn--80ak6aa92e.com

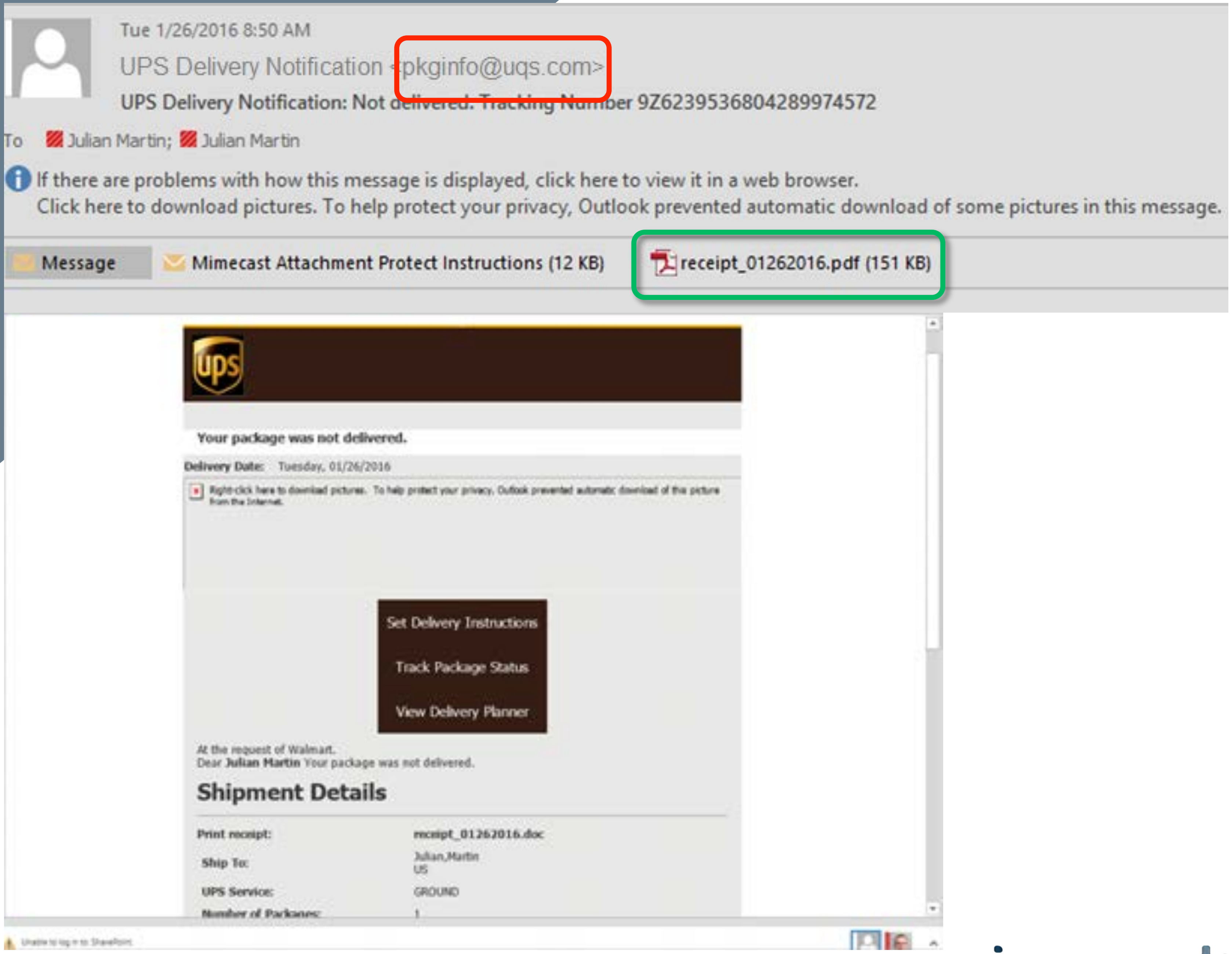
Watch Out Mobile Browsers!

Phishing with Elongated URLs – What site are you really on?



http://m.facebook.com---securelogin.liraon.com/sign_in.htm

Would You Open This Attachment?



Tue 1/26/2016 8:50 AM

UPS Delivery Notification <pkginfo@uqs.com>

UPS Delivery Notification: Not delivered: Tracking Number 9Z6239536804289974572

To Julian Martin; Julian Martin

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Message | Mimecast Attachment Protect Instructions (12 KB) | receipt_01262016.pdf (151 KB)

Your package was not delivered.

Delivery Date: Tuesday, 01/26/2016

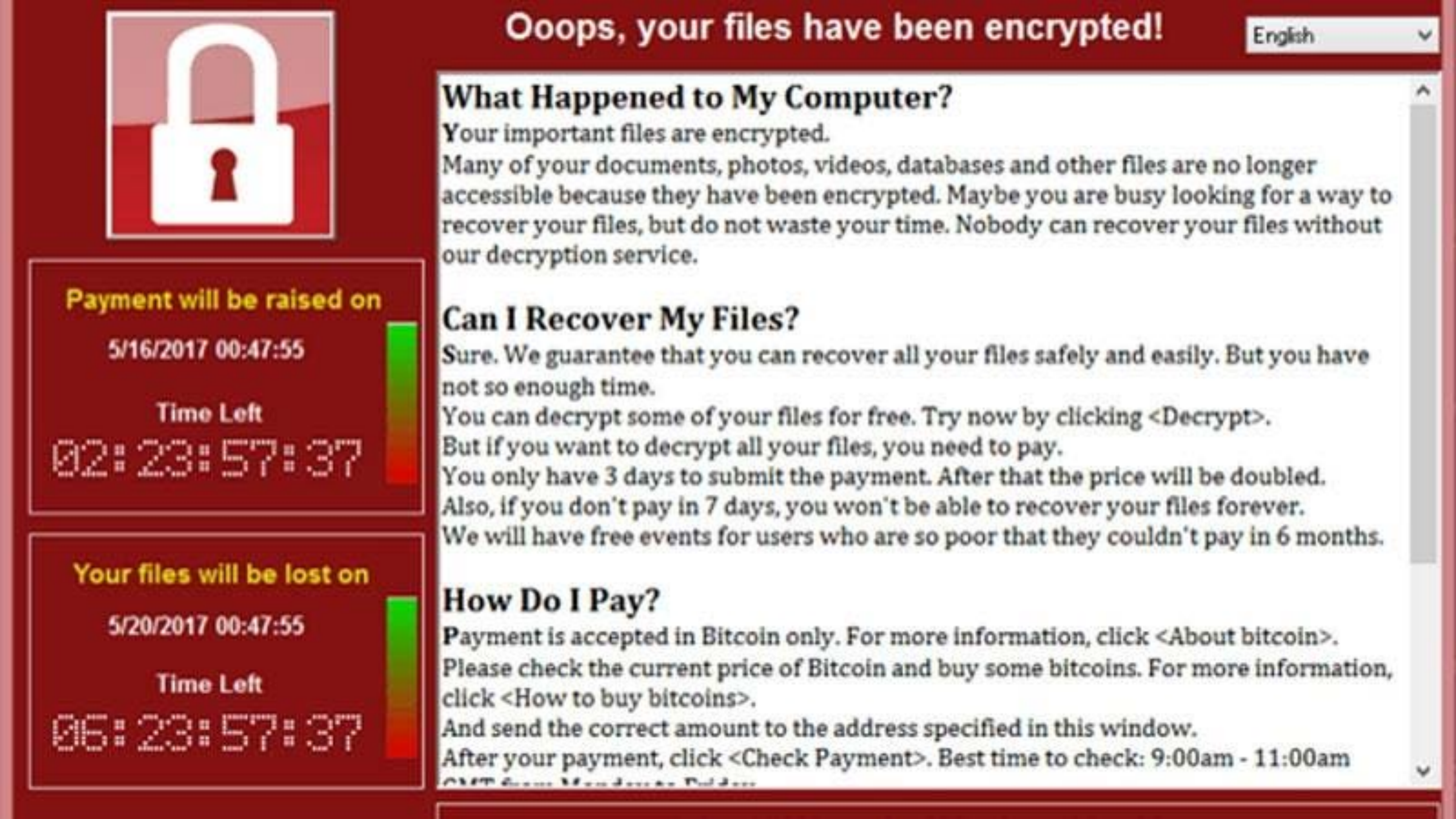
Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

At the request of Walmart.
Dear **Julian Martin** Your package was not delivered.

Shipment Details

Print receipt:	**receipt_01262016.doc**
Ship To:	Julian,Martin US
UPS Service:	GROUND
Number of Packages:	1

Unable to log in to SharePoint.



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

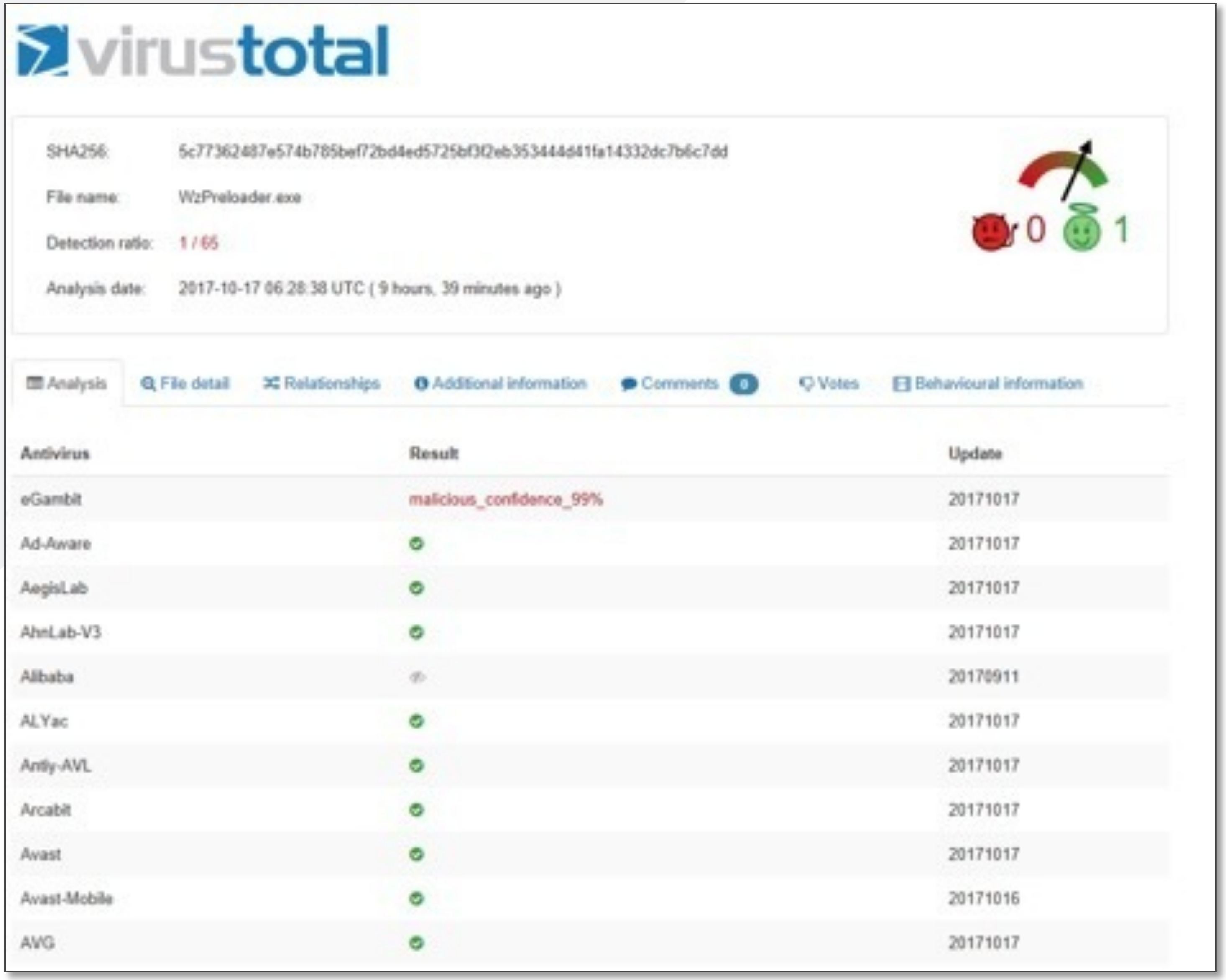
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday.

No One Way to Catch Malware



SHA256: 5c77362487e574b785bef72bd4ed5725bf3f2eb353444d41fa14332dc7b6c7dd

File name: WzPreloader.exe

Detection ratio: 1 / 65

Analysis date: 2017-10-17 06:28:38 UTC (9 hours, 39 minutes ago)

Antivirus	Result	Update
eGambit	malicious_confidence_99%	20171017
Ad-Aware	✓	20171017
AegisLab	✓	20171017
AhnLab-V3	✓	20171017
Alibaba	⊘	20170911
ALYac	✓	20171017
Antiy-AVL	✓	20171017
Arcabit	✓	20171017
Avast	✓	20171017
Avast-Mobile	✓	20171016
AVG	✓	20171017

We all know the risks

Trust your users not to click?

Imagine being able to stop *EVERY* malicious file

Static File Analysis

Expedites scanning and scan time for users

~1-2 seconds attachment scan

Analyze inbound attachments with **multiple AV engines** + **static file analysis** + **behavioral sandboxing** + **Safe file conversion**

Enhanced Threat Remediation

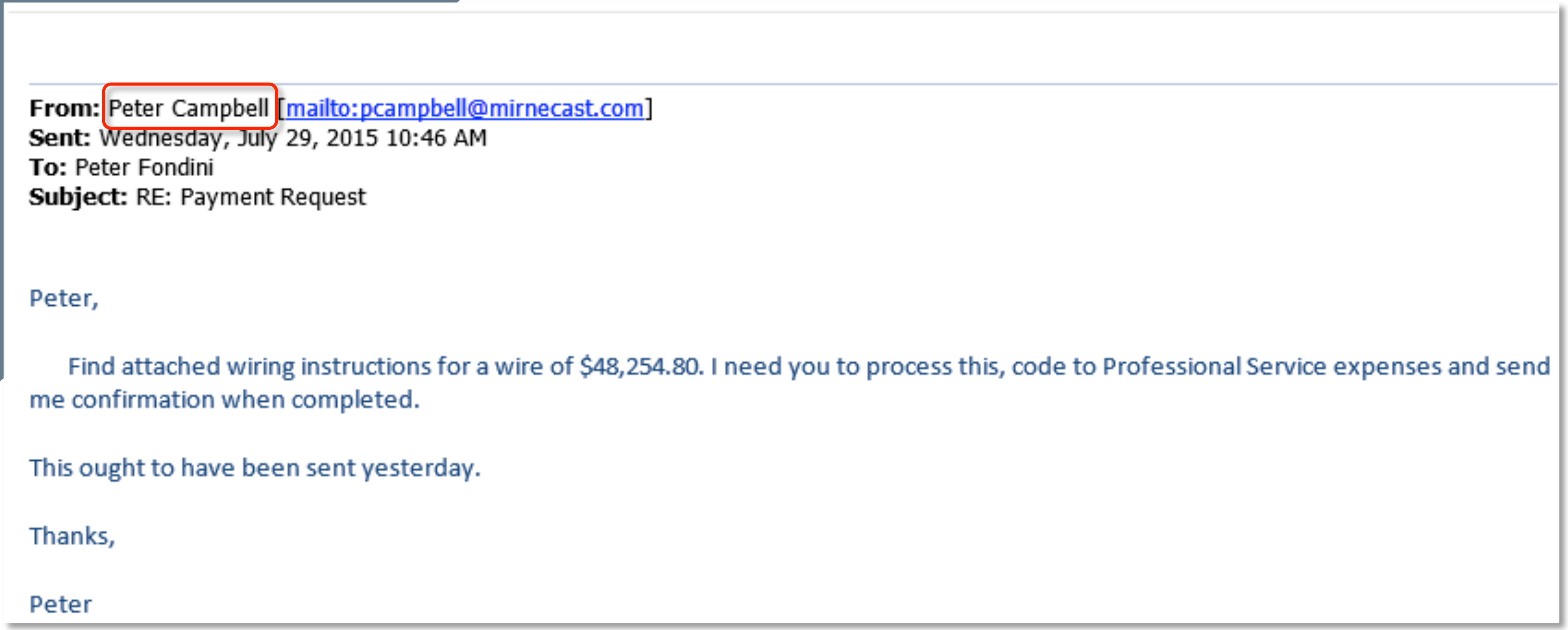
- Leverage global threat intelligence
- Incident / Response Dashboard
- Constantly monitor and re-check status of all file attachment fingerprints globally
- If security score of a delivered file changes:
  - Quickly alert and update administrators
  - Automatically or manually remediate attachment based malware
  - Log incident actions

Who Says Attacks Need to Involve Malware?

- Business Email Compromise
- Whaling
- Wire transfer or W-2 Fraud

mimecast®

Who would send the money?



From: Peter Campbell [mailto:pcampbell@mirnecast.com]
Sent: Wednesday, July 29, 2015 10:46 AM
To: Peter Fondini
Subject: RE: Payment Request

Peter,

Find attached wiring instructions for a wire of $48,254.80. I need you to process this, code to Professional Service expenses and send me confirmation when completed.

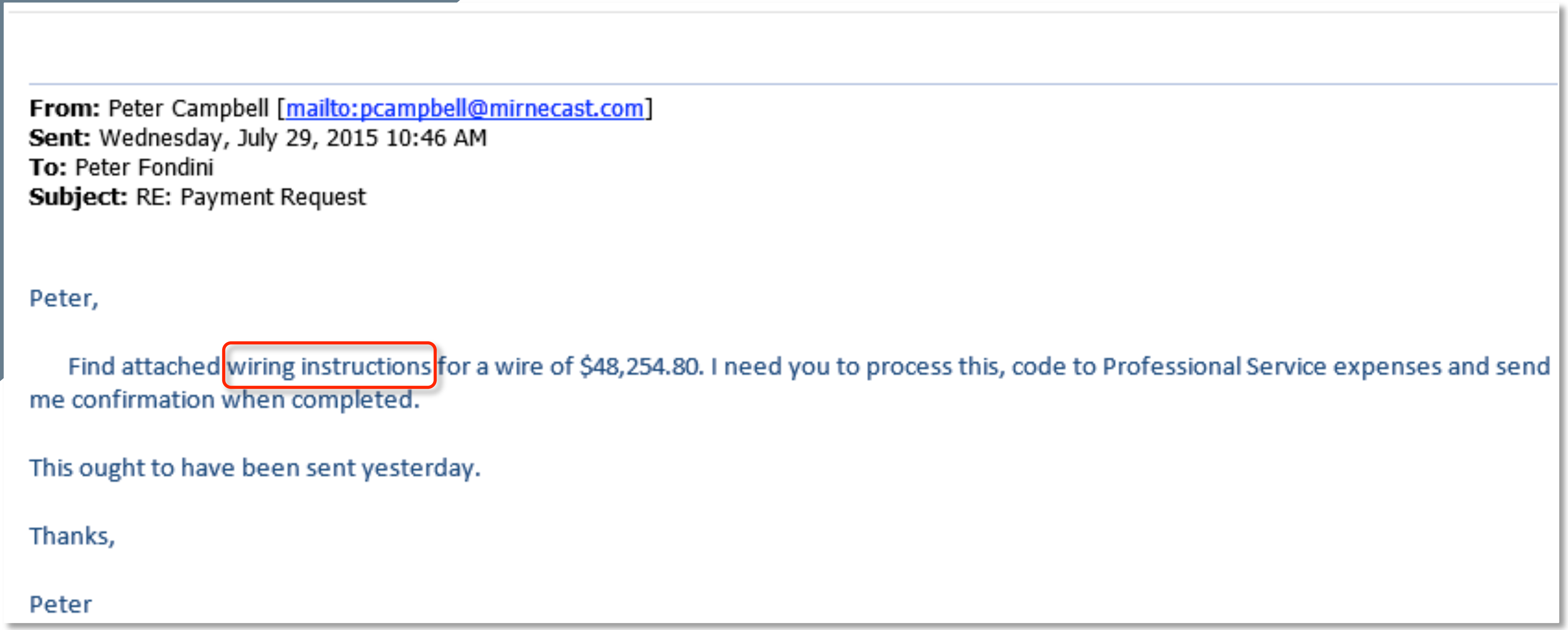
This ought to have been sent yesterday.

Thanks,

Peter

mimecast®

Impersonation Protect



From: Peter Campbell [mailto:pcampbell@mirnecast.com]
Sent: Wednesday, July 29, 2015 10:46 AM
To: Peter Fondini
Subject: RE: Payment Request

Peter,

Find attached wiring instructions for a wire of $48,254.80. I need you to process this, code to Professional Service expenses and send me confirmation when completed.

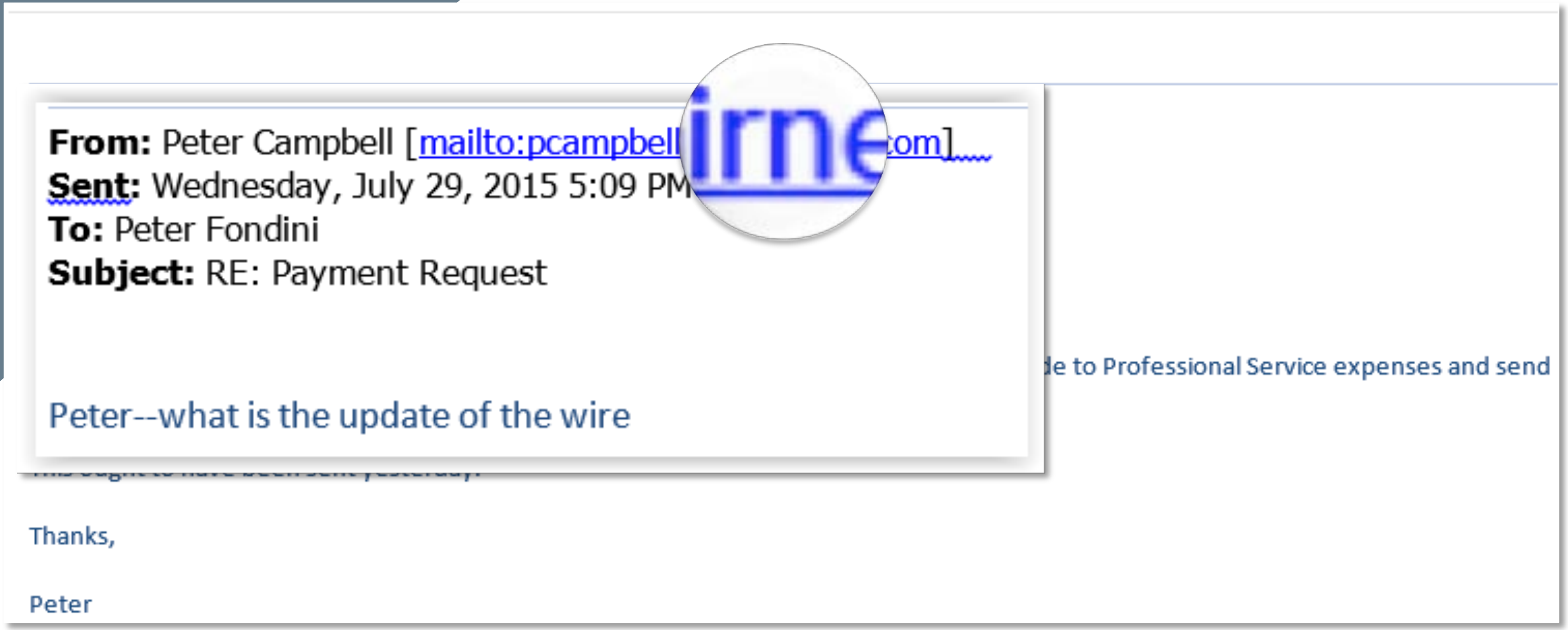
This ought to have been sent yesterday.

Thanks,

Peter

mimecast®

Impersonation Protect



From: Peter Campbell [mailto:pcampbell irne com]

Sent: Wednesday, July 29, 2015 5:09 PM

To: Peter Fondini

Subject: RE: Payment Request

Peter--what is the update of the wire

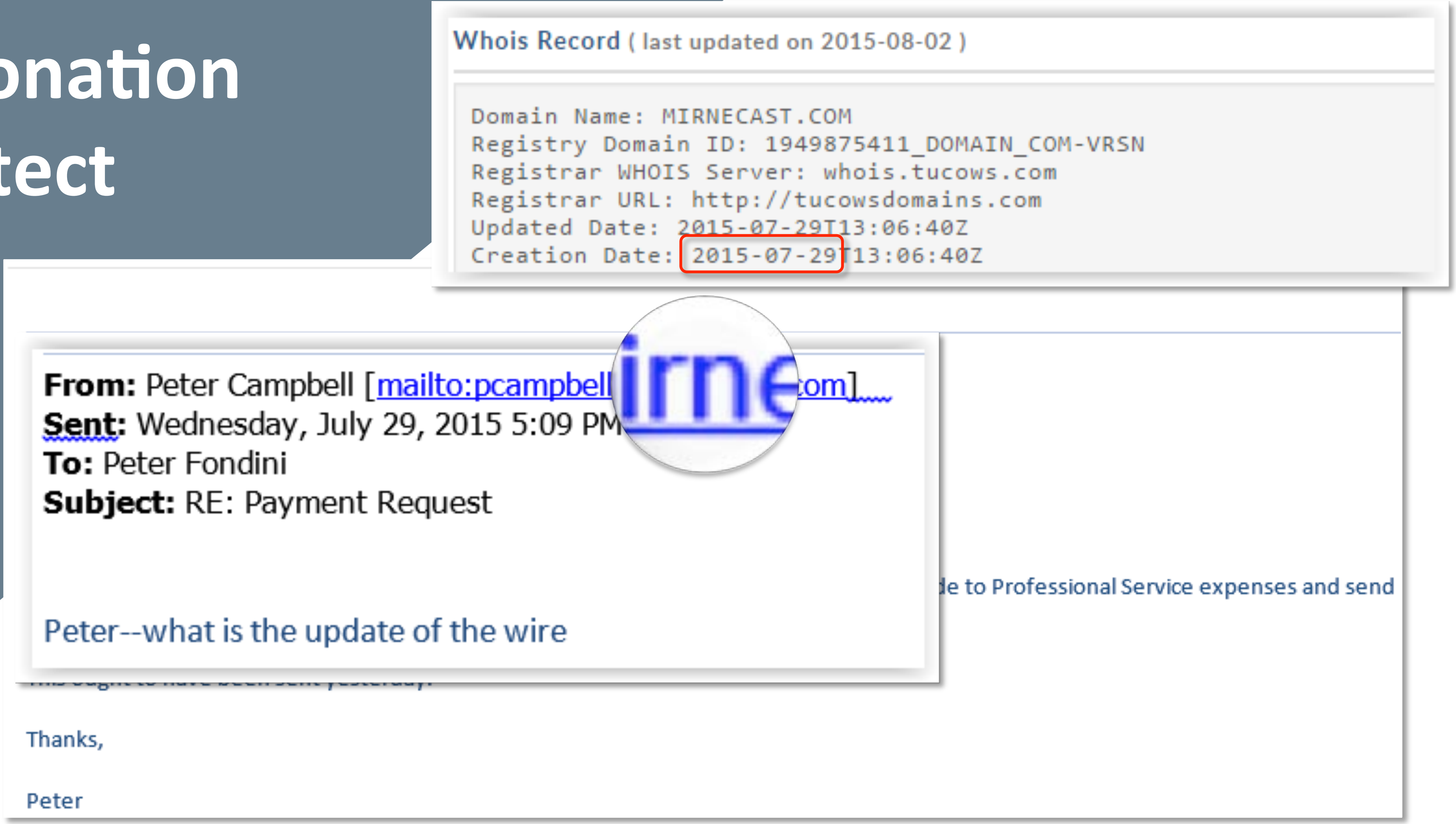
de to Professional Service expenses and send

This ought to have been sent yesterday.

Thanks,

Peter

Impersonation Protect



Whois Record (last updated on 2015-08-02)

```
Domain Name: MIRNECAST.COM
Registry Domain ID: 1949875411_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-07-29T13:06:40Z
Creation Date: 2015-07-29T13:06:40Z
```

From: Peter Campbell [mailto:pcampbell@mirnecast.com]
Sent: Wednesday, July 29, 2015 5:09 PM
To: Peter Fondini
Subject: RE: Payment Request

Peter--what is the update of the wire

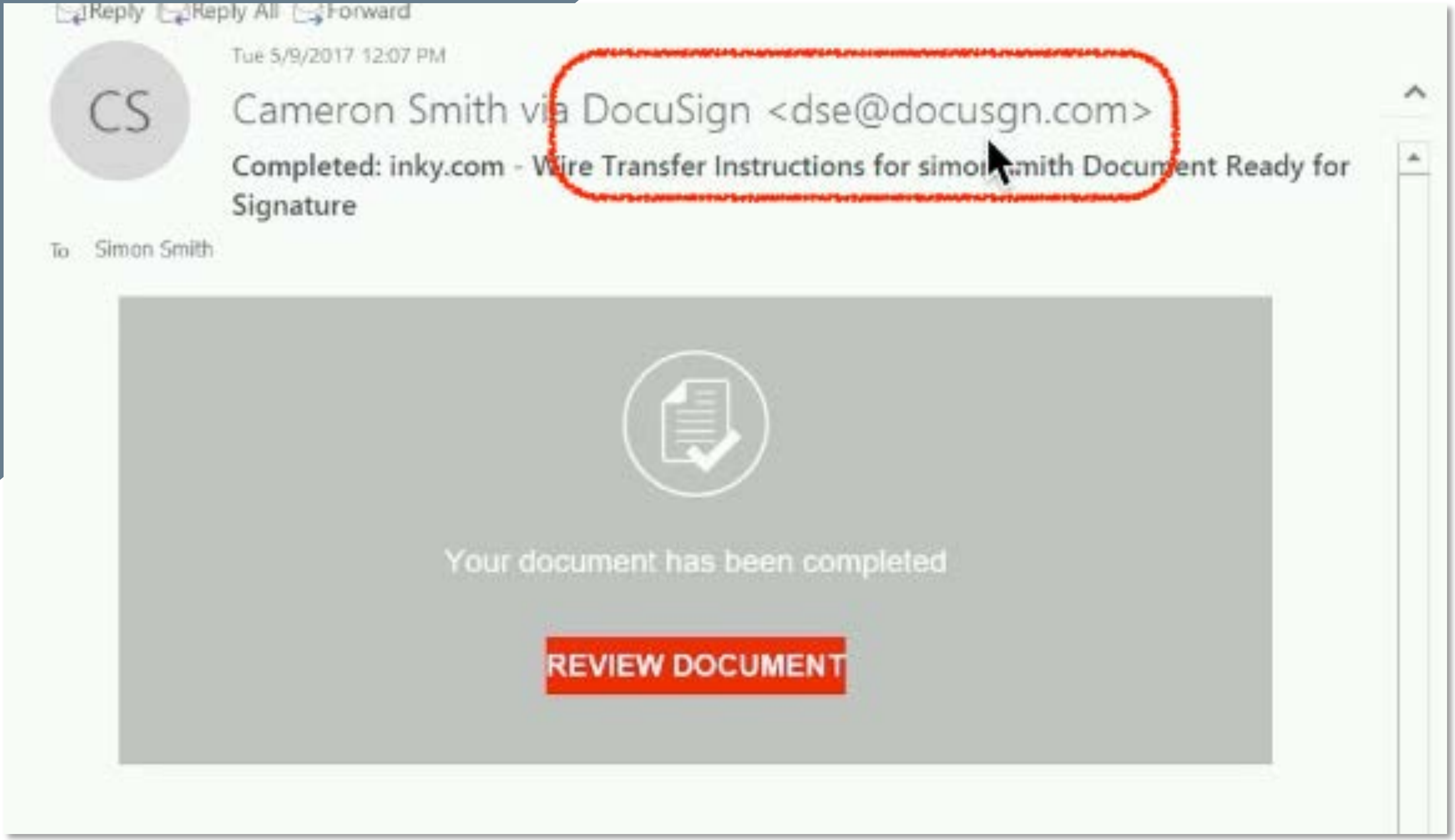
de to Professional Service expenses and send

This ought to have been sent yesterday.

Thanks,

Peter

Supply Chain Impersonation



Tue 5/9/2017 12:07 PM

Cameron Smith via DocuSign <dse@docusgn.com>

Completed: inky.com - Wire Transfer Instructions for simon smith Document Ready for Signature

To Simon Smith

Your document has been completed

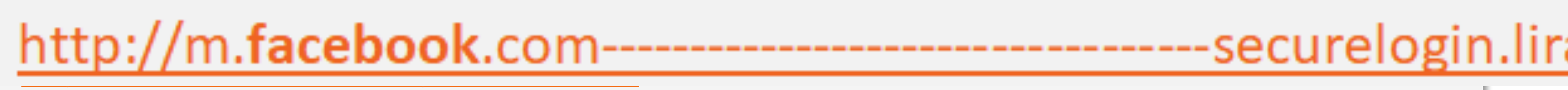
mimecast®

One of these things is not like the others!!!

“Similar” Domains Being Registered Every Day – Why?

- **Serer - faƈebook.com - xn--faebook-ozb.com [facebook.com]**
- **Old English - ɑƿƿle.com - xn--le-m1aa24e.com [apple.com]**
- **Math Symbol - hotmail¬.com - xn--hotmail-jka.com [hotmail.com]**
- **German - microsöftonline.com - xn--microsftonline-0pb.com [microsoftonline.com]**
- **Chinese - amazon.购物 - amazon.xn--g2xx48c [amazon.com]**
- **Cyrillic - applḙ.com - xn--appl-t64a.com [apple.com]**
- **Polish - ażure.com - xn--aure-bbb.com [azure.com]**
- **Fula/African - dropɓox.com - -dropox-sxc.com [dropbox.com]**
- **Fula/African - eɓay.com - xn--eay-osb.com [ebay.com]**
- **Polish - ebąy.com - xn--eby-jpa.com [ebay.com]**
- **Danish - facebøøk.com - xn--facebk-fyaa.com [facebook.com]**

Similarity matching capabilities

Real Domain	Similarity Match
mimecast.com	**mimecast**.co.za
apple.com	**xn--80ak6aa92e.com**
amazon.co.uk	www.**amazonn**.co.uk
facebook.com	http://m.**facebook**.com--------------------------------securelogin.liraon.com/sign_in.htm
paypal.com	 http://m.**facebook**.com----------------------------securelogin.lira
CustomDomain.com	**CustomDornain.com**

- Detect similarity both simple and complex
  - Character switching, Homoglyph/Homograph, long domain strings and more

Are Users part of the solution or part of the problem?

Internal Email Protect

☠Compromised Accounts

➢Attacker uses stolen user credentials to spread attack internally and/or externally

☠Careless Users

➢“Oops, I sent it to the wrong person…again.”

☠Malicious Insiders

➢Purposely distributing malware or malicious URLs

Threat Protection

Recoverability

Adaptability

Durability

Cyber Resilience for email

mimecast®