

Staying Safe Online



Pam Holland, TechMoxie

Staying Safe Online



Knowledge is Power

What are fraudsters looking for?

- Credit card numbers
- Personal information
- Money (or Bitcoin!)
- Mischief

Staying Safe Online



Key to staying safe:

Think before you click

Cybercrime is big business

Payment Card Number With CVV2	United States	United Kingdom	Canada	Australia	European Union
Random	\$5–\$8	\$20–\$25	\$20–\$25	\$21–\$25	\$25–\$30
With Bank ID Number	\$15	\$25	\$25	\$25	\$30
With Date of Birth	\$15	\$30	\$30	\$30	\$35
With Fullzinfo	\$30	\$35	\$40	\$40	\$45

Estimated per card prices, in US\$, for stolen payment card data (Visa, MasterCard, Amex, Discover).

Source: McAfee Labs.

Staying Safe Online



We are offering top quality cards:

All our cards come with PINs and instructions. You can use them at any ATM worldwide.

Our cards are equipped with magnetic strip and chip.

Once you purchase, we will email you a Full Guide on how to safely cash out.

Us cards - available balance \$2,500(minimum) and up to \$5,000.

usage:

- ✓ ATM
- ✓ Stores
- ✓ Online

Eu cards - available balance 2,500 Euro(minimum) and up to 4,500 Euro.

usage:

- ✓ ATM
- ✓ Stores
- ✓ Online

American Express cards - available balance \$6,000 (minimum) and up to \$8,000.

usage:

- ✓ ATM
- ✓ Stores
- ✓ Online

Daily withdrawal limits (ATM limits)

US cards have a \$700-\$1000 daily withdrawal limit.

- ✓ no limit online or in stores

Common avenues for fraudsters:

- Email
- Fake Websites (typosquatting)
- Pop ups
- Fake Facebook accounts

Fraudsters engage in *phishing*, which is
The practice of sending send fake emails

Phishing = *phony* + *fishing*

Phishing *How does it work?*

- Fraudsters create a fake email using actual logos
- Send it to perhaps millions of email addresses

Email

Phishing



Email



PNCBank_Statements@pnc.com

To: Pholland88@gmail.com

Your PNC Bank Online Statement is ready to be viewed

The Online Statement for the account listed below is now available for viewing. To view your Online Statement, you must sign on to PNC Online Banking and click on Online Statements.

This statement will continue to be available for up to 7 years through Online Banking.

If your e-mail address has changed or will change, please update our records by selecting the Customer Service tab in Online Banking and clicking Online Statements E-mail.

If you have not done so already, please add the sender of this e-mail to your e-mail address book to ensure ongoing reliable delivery.

Thank you.

Account Number (last 4 digits)	Statement Date
--------------------------------	----------------

XXXX8489	11/30/2015
----------	------------

ABOUT THIS MESSAGE: This e-mail was sent to: pholland88@gmail.com for the account ending in XXXX8489.

You received this service e-mail notice because you have enrolled in PNC Bank Online Statements. Look for an e-mail notice each time a new statement is available to be viewed.

If you discover a discrepancy on your statement, please call us at:

1-888-PNC-BANK (1-888-762-2265)

Monday - Friday: 7 a.m. - 10 p.m. ET

Saturday & Sunday: 8 a.m. - 5 p.m. ET

Virtual Wallet customers, please call 1-800-352-2255. Please have your account statement information available when you call.

PLEASE DO NOT REPLY TO THIS E-MAIL. Replies to this e-mail will not be received. If you wish to submit an account-related question electronically,

Email



Dear Customer,

We recently reviewed your account and suspect that your Chase account might have been accessed by an unauthorized third party.

Protecting the security of your account is our primary concern, therefore as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity.

Please follow the link below to proceed to confirming your account information:

<https://chaseonline.chase.com/verify/MachIdnt/SecAuthInformation.aspx?LOB=RBGLogon>

Thank you.

Sincerely,
Chase Security Team

Email



Dear Cardmember,

Upon intensive reviews on your profile. We have noticed that you need to resolve important security issues on your account to prevent temporal deactivation. It is therefore recommended that you complete this process. Your security is important to us.

Please click on the reference below to resolve this issue:

<https://www.online.americanexpress.com/default.aspx>

Sincerely,
American Express Customer Service



Please help us improve our online communication to you.
[Click here](#) to provide feedback.

The customer service e-mail was sent to you by American Express. You may receive customer service emails even if

Email



UPS Customer Service

To: Pholland88@gmail.com

Reply-To: upsdi@ups.com

UPS Package Information - R79W27

IMPORTANT DELIVERY

You have received an important delivery from UPS Customer Service.

Please pick up the ePackage at the following Web address:

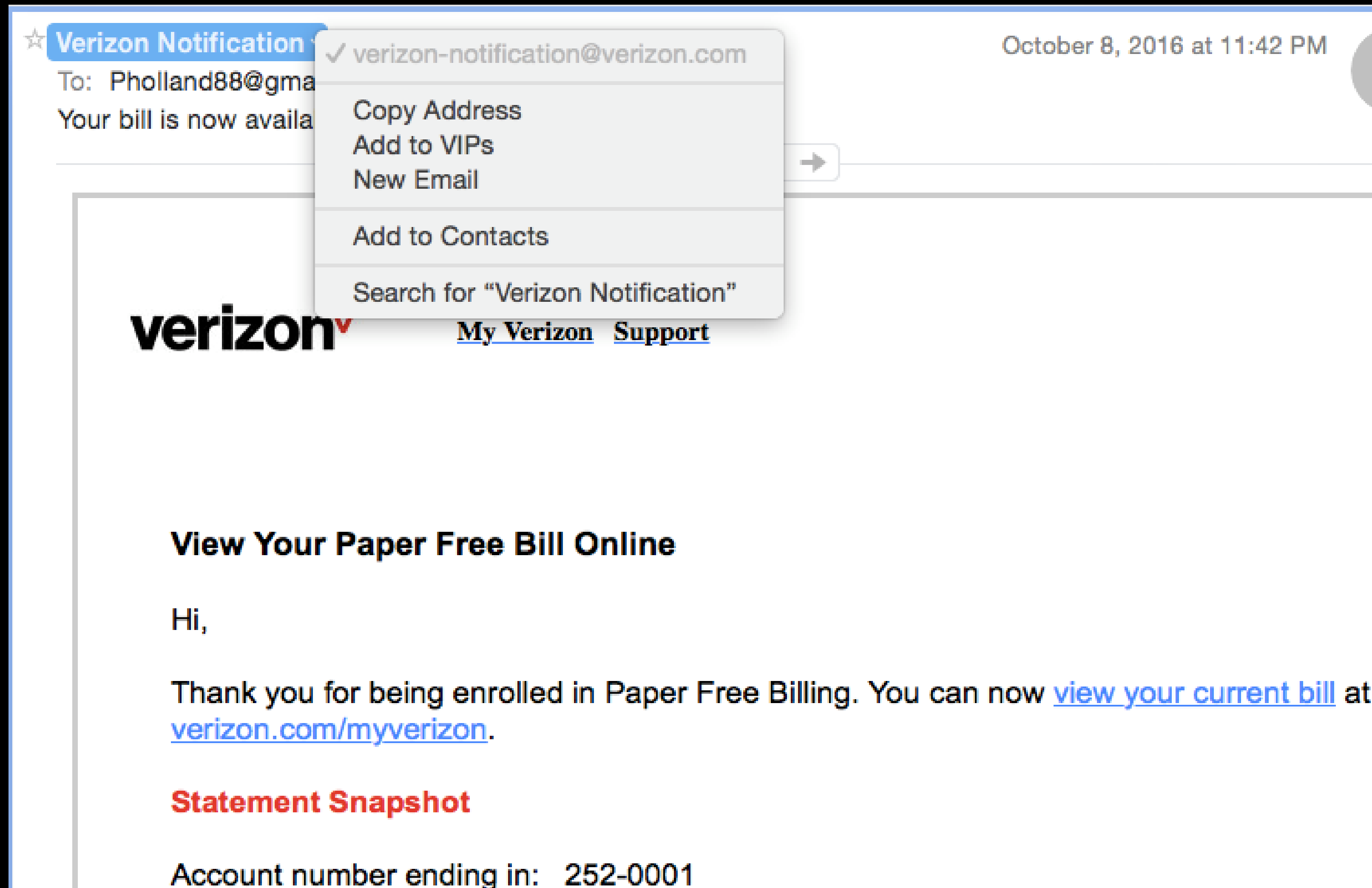
https://epackage1.ups.com/ime?x=4-153988395-93895892-67COLYO3&lang=en_US

The ePackage will expire on Saturday October 26, 2013, 00:00:00 EDT

HOW TO PICK UP YOUR ePackage

* If the Web address above is highlighted, click on it to open a browser window. You will automatically be taken to the ePackage.

Email



Email

McDonalds

To: at pholland88@gmail.com
Please Activate By: 11/18/2015

pholland88@gmail.com,

Delicious free food with
this \$100 Gift!.

[Special Bonus](#)

[Enclosed for being our
valued customer!](#)



Email

☆ **Shopping Gift to Victoria Secret**

To: Pholland88@gmail.com

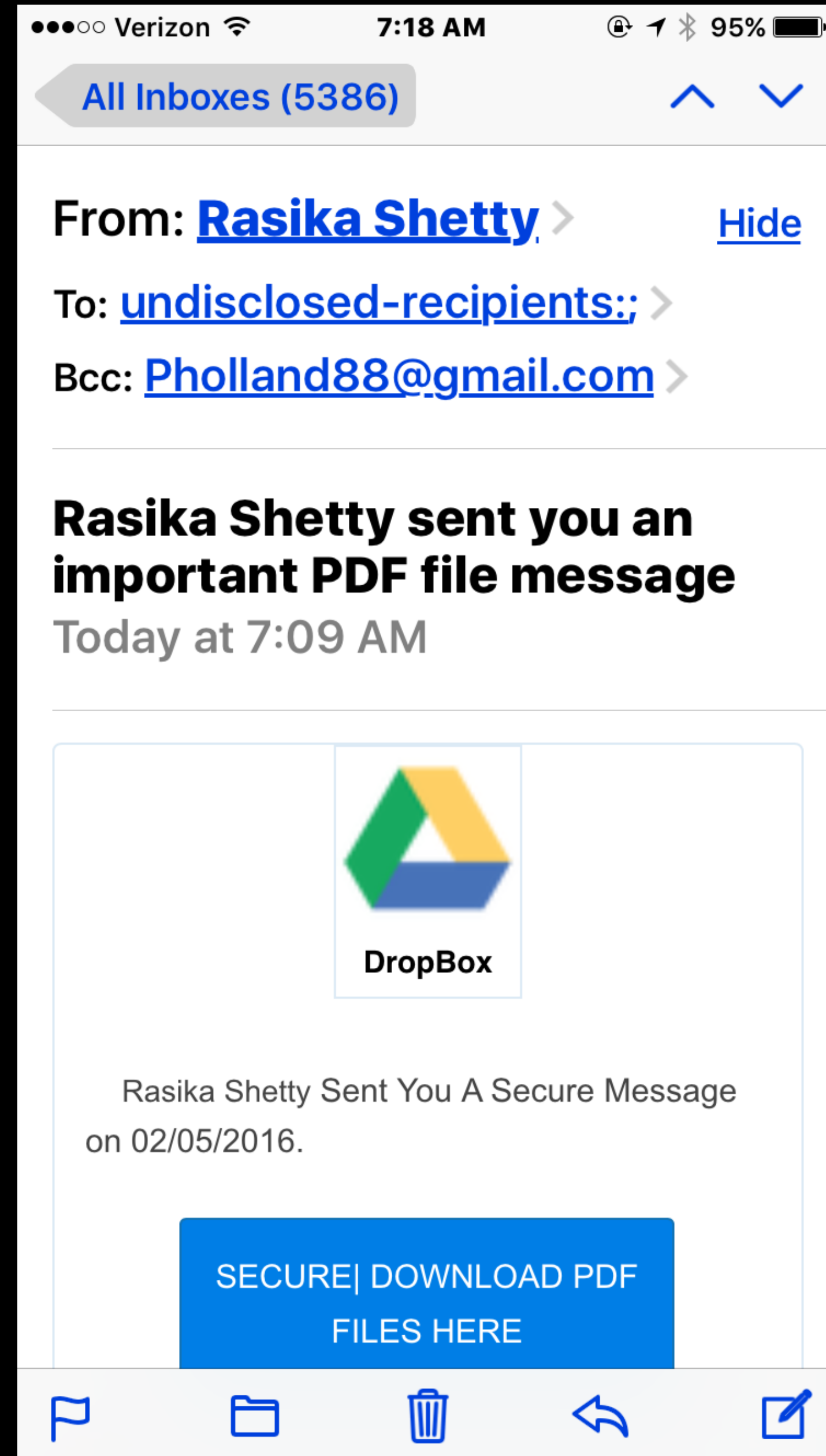
Reply-To: dickdoze

Open this immediately for your Victoria's Secret Gift

Victoria's Secret



Email



Email



Some emails may look like they came from a friend...

Camille Newell

February 23, 2015 at 7:43 AM

To: Pholland88@gmail.com, Gerald Serotta, rebecca smith, Renee Luker, roni falk, Emma Rothman, [and 14 more...](#)
from: Camille Newell

Hi!
How are you?
Breaking news <http://helloidukki.com/allowed.php> It works!

Camille Newell

[Sent from Yahoo Mail for iPad](#)

Email



☆ 'Laura Schwartz' lauraeuschwartz@aol.com [bcccommunity]

February 2, 2015 at 10:24 AM

LS

To: BCCcommunity@yahoogroups.com

Reply-To: lauraeuschwartz@hotmail.com

[bcccommunity] Need Heeeelp !!!!!!!!!!!!!!!



Hello,

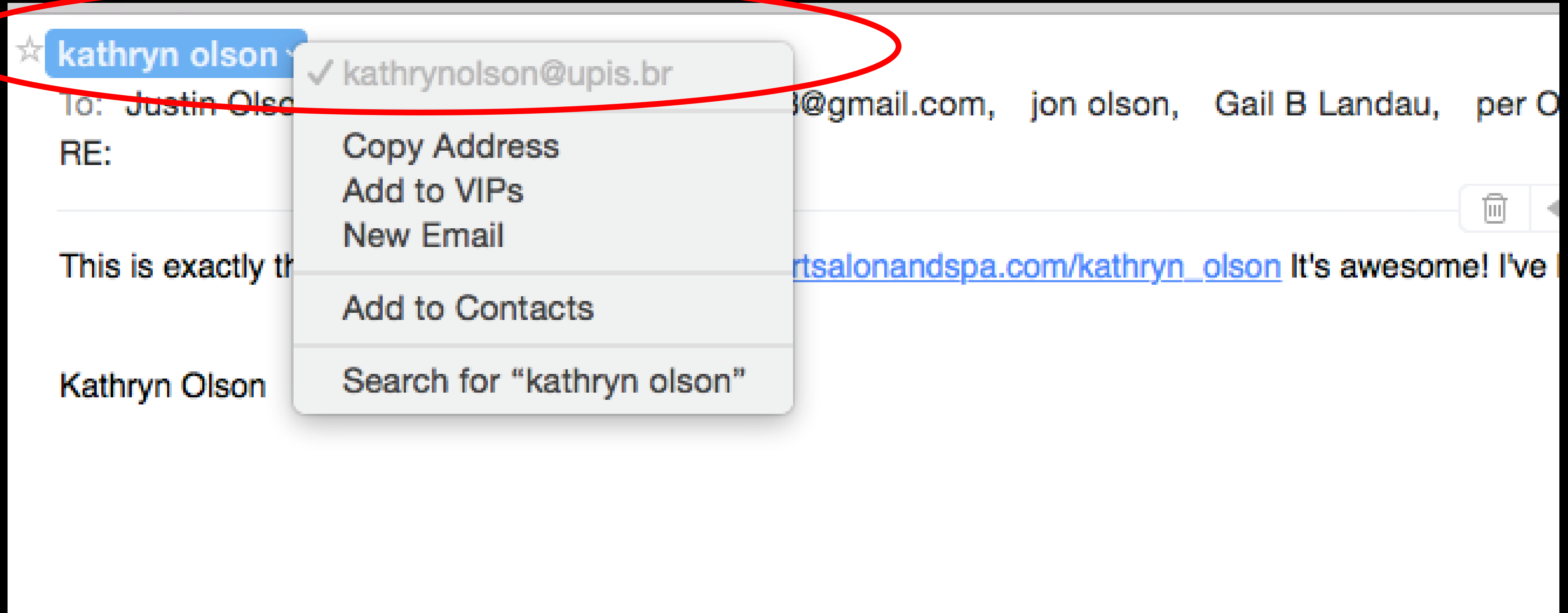
I Hope you get this on time, My family and i made a trip to Turkey and had Our bags stolen from us with Our Mobile and personal effects therein. The embassy has been helpful but We have to pay for a ticket and settle Our hotel bills with the Manager.

We have made contact with our bank but it would take 3-5 working days to access funds in our account, the bad news is Our flight will be leaving very soon but we're having problems settling the hotel bills and the hotel manager won't let us leave until we settle the bills, We need your help/LOAN financially and we promise to make the refund once we get back home, you are our last resort and hope, Please let me know if We can count on you and I need you to keep checking your email because it's the only way I can reach you.

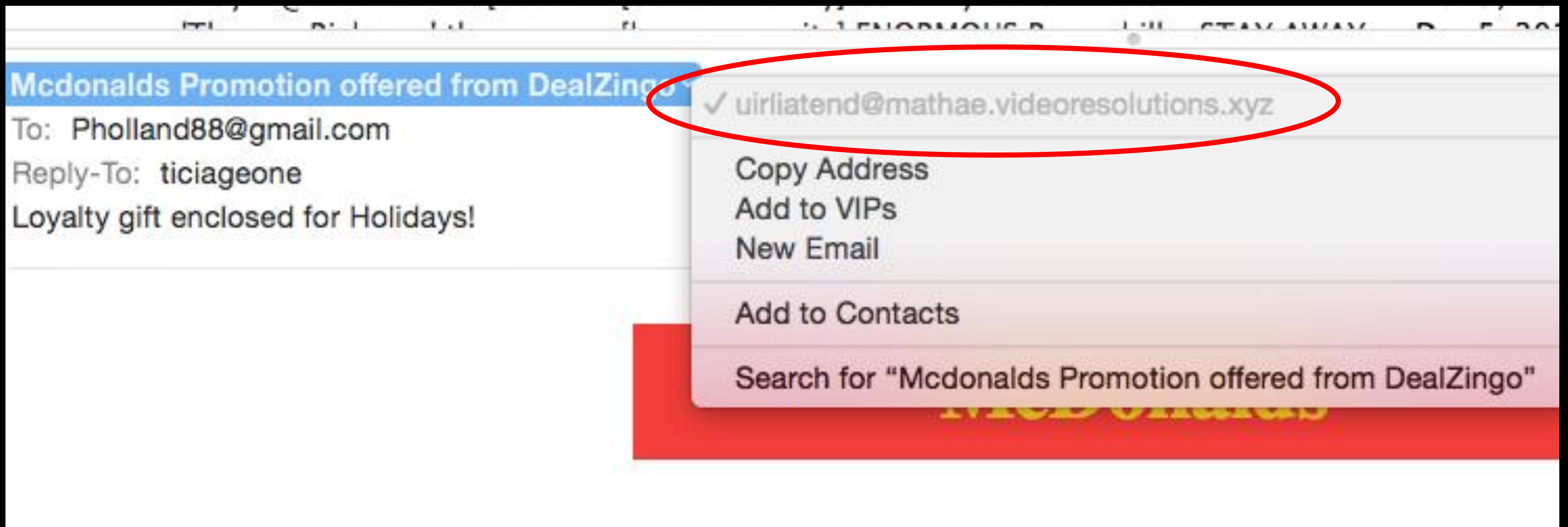
All hopes on you

Laura

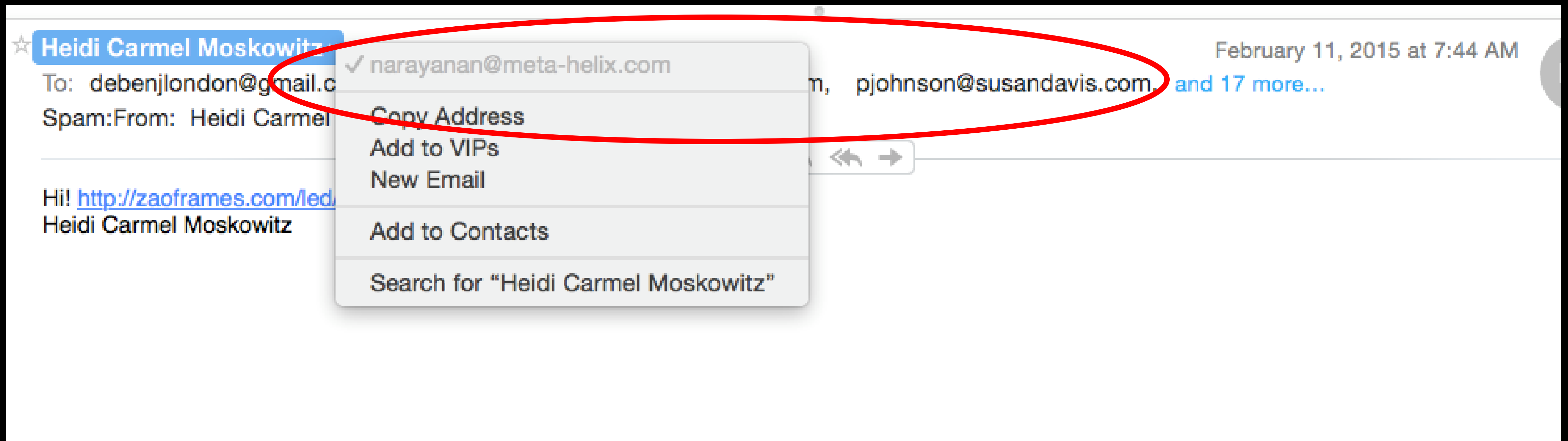
Email



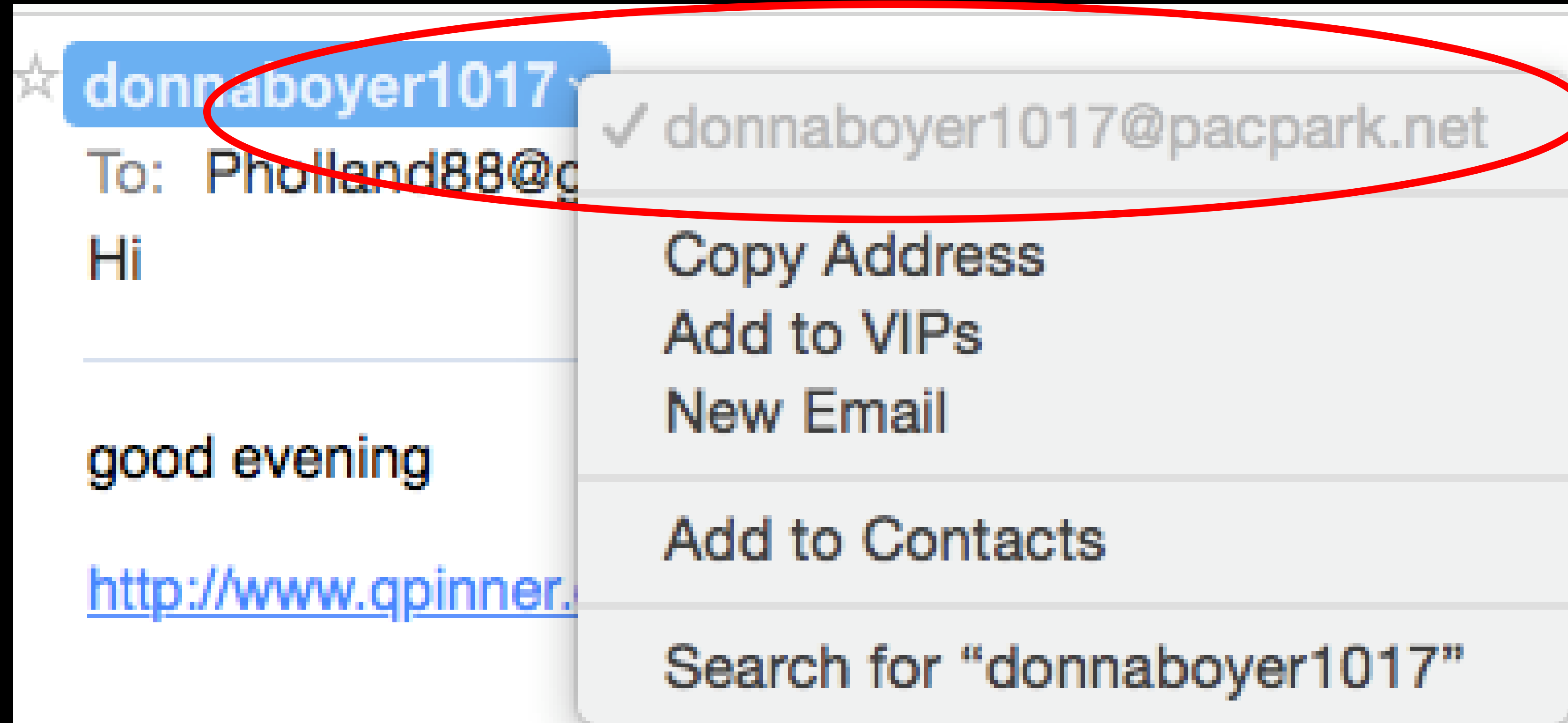
Email



Email



Email



Done



Fraud



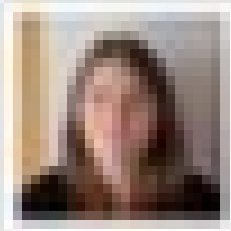
Britany Hassell

JUNE 26, 2000



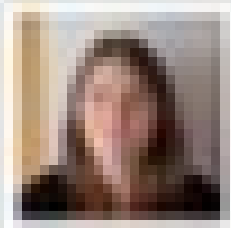
Fraud

4:51 PM

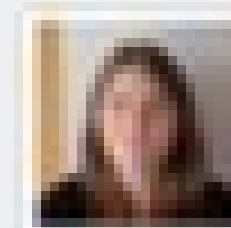


Hello how are you?

Hi there! So nice to see your name pop up. Maya is in her senior year, so getting ready to be an empty nester. Very mixed feelings! How are you? Cali still treating you well?



Good to hear from you. Am doing wonderfully great., i hope you have also been contacted by the CFDA ?



Haven't you heard about the CFDA and the fbook C.E.O made to some fb user in other for the people of the world to benefit from him, its randomly picked profile on fb \$200.000.00.. Did you get yours from him?

no

tell me more

you get money?

Viruses

Microsoft Security Essentials

WINDOWS VIRUS WARNING!

Identity Theft and Hacking Possibilities.
Contact emergency virus support now.

0-800-051-3723

The system have found (4) viruses that

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

Message from webpage

Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians
0-800-051-3723 (Toll Free)

OK

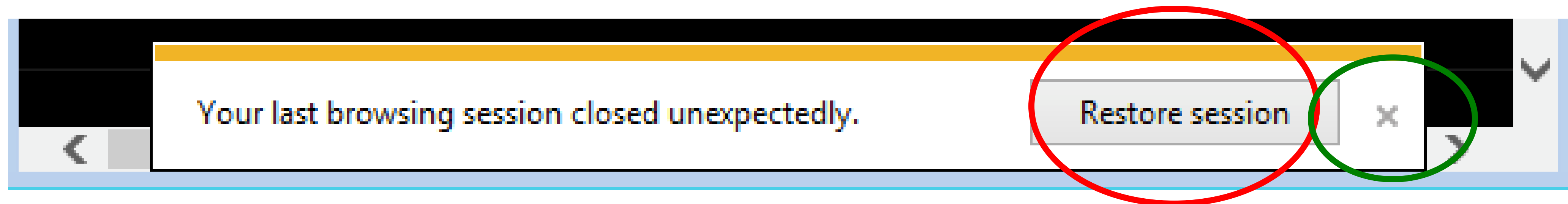
Your personal and financial information is compromised call **0-800-051-3723** to be secured.

Recommended:

Microsoft

What to do? Shut the computer down

Do not click “restore session” when rebooting



1. Keep your software up to date

2. Beware of pop up alerts that your computer needs to be “cleaned” or “repaired”

Staying Safe Online



3. Passwords...

4. Use Google search to find your website

5. Have a mental checklist to avoid clicking on 'bad stuff'

- Verify emails – be especially on guard for those that appear business like.
- Never click through an email – go to browser.
- Use google search to get to websites as it will correct typos.

6. Anti-Virus Software

- Of course, use good – up to date – anti-virus software.
- Review periodically against its competitors
- Consumer Reports is a good source for ratings

7. Backup

- Have back up that has version control and is redundant – *distinguished from cloud or other storage*
- Check reviews and company communications on response to ransomware

8. Have an action plan if suspect virus

- Know what immediate steps you will take.
- Disconnect computer from servers, online storage (e.g., dropbox), etc.

What to do if you have been scammed?

- Possibly file a police report
- If credit card used, report to the company either for replacement or to contest charges
- Change passwords if you think you've been hacked.
- Consider filing a report with FTC or state office of consumer protection.
- Look for file download with “virus” – delete.

Staying Safe Online



Thank you!

Questions?

Staying Safe Online

Pam Holland

TechMoxie, LLC

Pam@Tech-Moxie.com

www.tech-moxie.com

