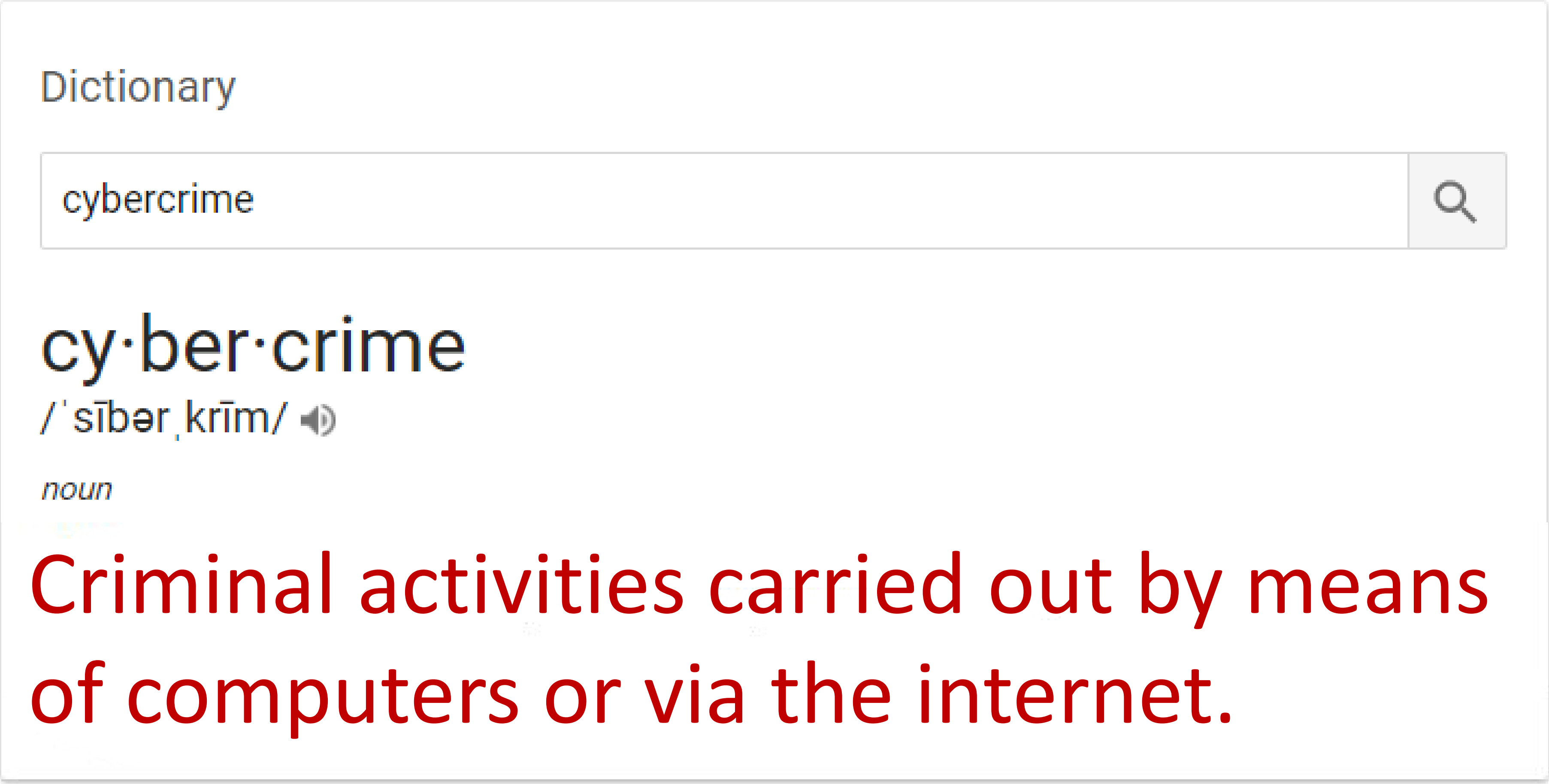
How to Avoid Becoming a Victim of Cybercrime

https://www.rayson.us/aehanson/presentations/current/psap/

My personal website

- Online outline of this presentation
  - Has ‘bonus’ information and links to articles not covered in todays presentation
- PDF version of the outline
- PDF version of my PowerPoint slides



Dictionary

cybercrime

cy·ber·crime

/ˈsībərˌkrīm/

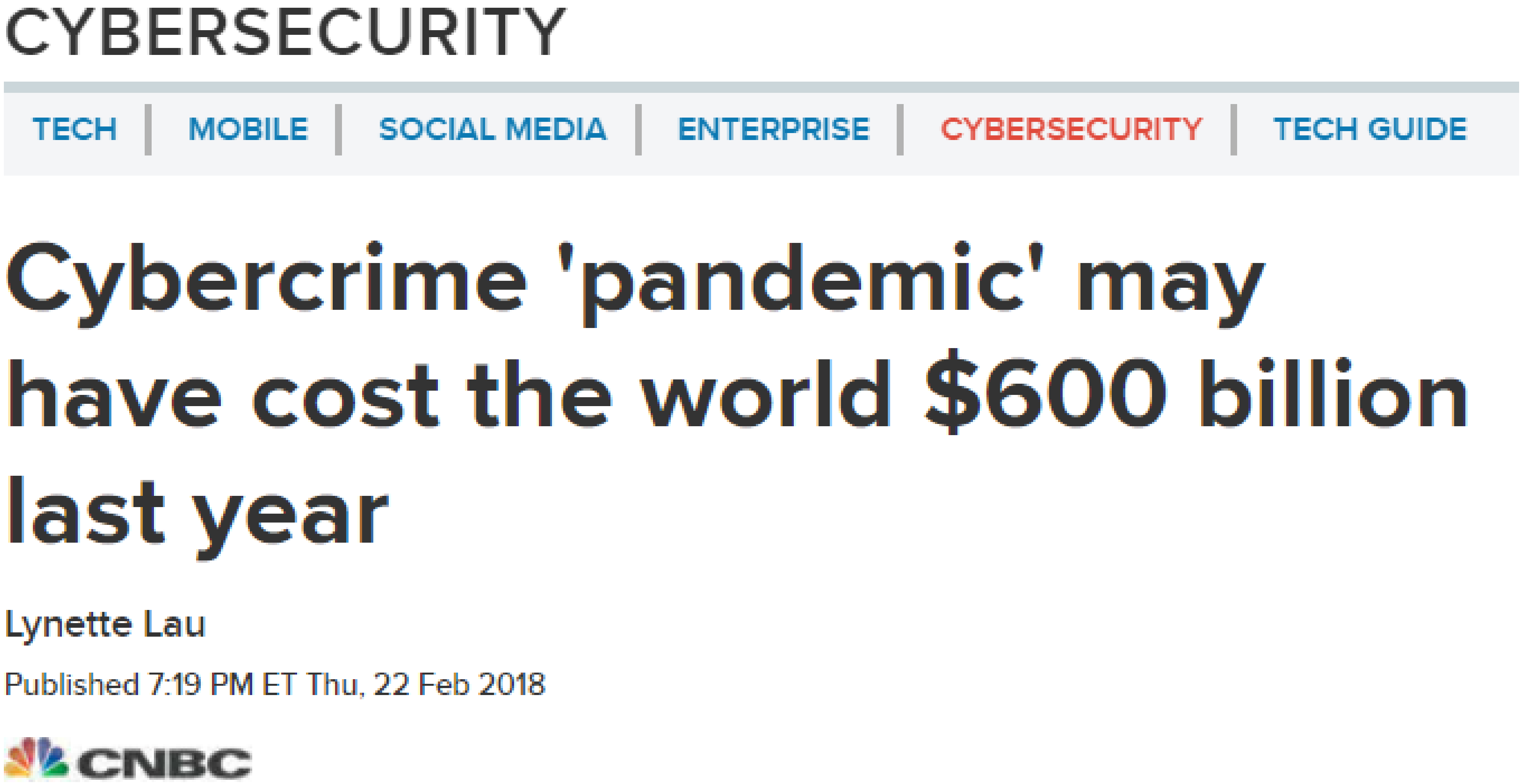
noun

Criminal activities carried out by means of computers or via the internet.

Source: **Google.com**

Hackers and scammers are actively trying to gain access to your computer and to your personal and financial information with one goal in mind:

To steal from you!



Cybercrime 'pandemic' may have cost the world $600 billion last year

Lynette Lau

Published 7:19 PM ET Thu, 22 Feb 2018

https://www.cnbc.com/2018/02/22/cybercrime-pandemic-may-have-cost-the-world-600-billion-last-year.html

Key Points:

- About 0.8 percent of global GDP
- 35% growth from 2014, when the cost was “only” $445 billion
- The rapid increase is largely due to the lower cost of entry and advancements in technology
- **North Korea**, **Iran** and **Russia** tend to go after financial services, while espionage activities are more rampant in **China**

Goals for this Presentation

1. Understand how they will try to steal from you
2. Know steps you can take to minimize your risk

Phone Calls

Social Engineering

- Utilizes knowledge of typical human behavior
- Pretending to be somebody they are not
- Tricking you into revealing private or sensitive information

Commonly Used Approaches

Social Security Scam

Goal:

- Convince you that your Social Security Number is being used by a criminal
- Get you to provide private information to clear your name

Commonly Used Approaches

Jury Duty Scam

Goal:

- Convince you that you a warrant has been issued for your arrest for failure to appear for jury duty
- Persuade you to pay a fine to clear your name

Commonly Used Approaches

Health Insurance Scam

Goal:

- Convince you that you missed the open enrollment period
- Get you to provide private/personal information
- Refer to a scam insurance agent
- Sell your information

Caller ID Cannot be Believed Anymore

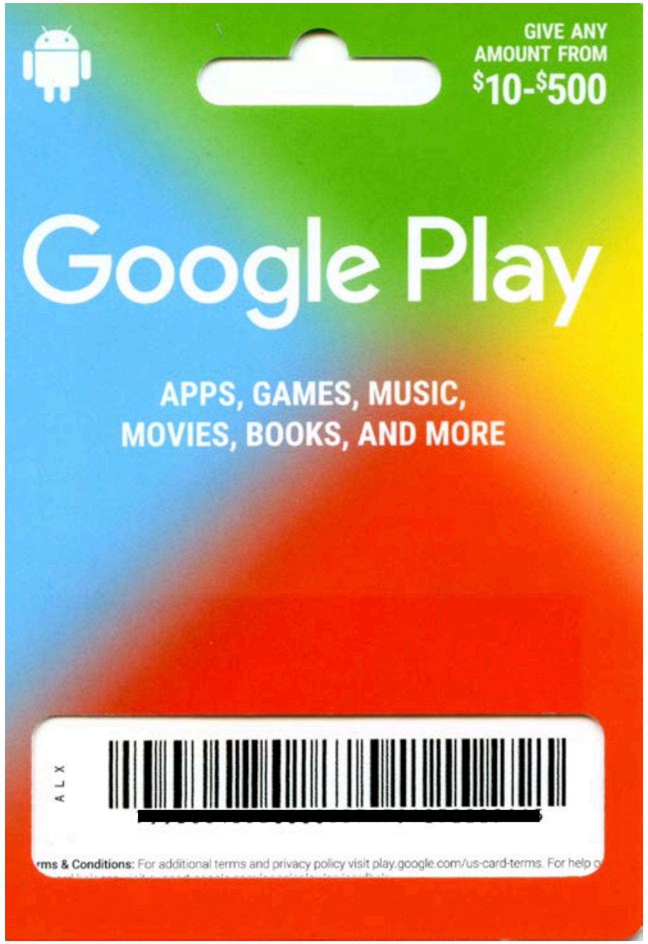
- Scammer have technology that can make your CallerID say anything they want:
  - Dallas PD
  - IRS
  - Citi Card
  - Microsoft

Other Commonly Used Approaches

- Government Representative (such as IRS)
- Financial Institution (Bank or Credit Card company)
- Microsoft Technical Support
- Blackmailer
  - Extramarital affairs
  - Pornography

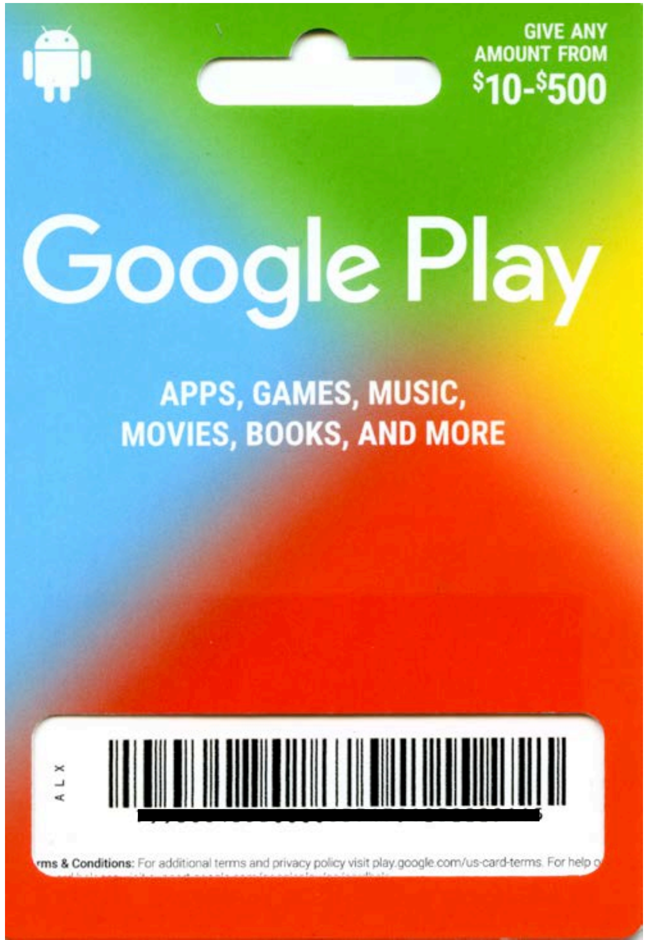
Common Themes

- They want information
- They want payment
- They want it NOW
  - Or else bad things will happen to you…


GIVE ANY
AMOUNT FROM
$10-$500
Google Play
APPS, GAMES, MUSIC,
MOVIES, BOOKS, AND MORE
A L X
[redacted]
rms & Conditions: For additional terms and privacy policy visit play.google.com/us-card-terms. For help o

Best Defense

- Be very careful about what you disclose over the telephone
- **<u>Do NOT</u>** provide personal information
- **<u>Do NOT</u>** provide financial information
- **<u>Do NOT</u>** buy gift cards!


GIVE ANY
AMOUNT FROM
$10-$500
Google Play
APPS, GAMES, MUSIC,
MOVIES, BOOKS, AND MORE
ALX
[redacted]
rms & Conditions: For additional terms and privacy policy visit play.google.com/us-card-terms. For help o

Best Defense

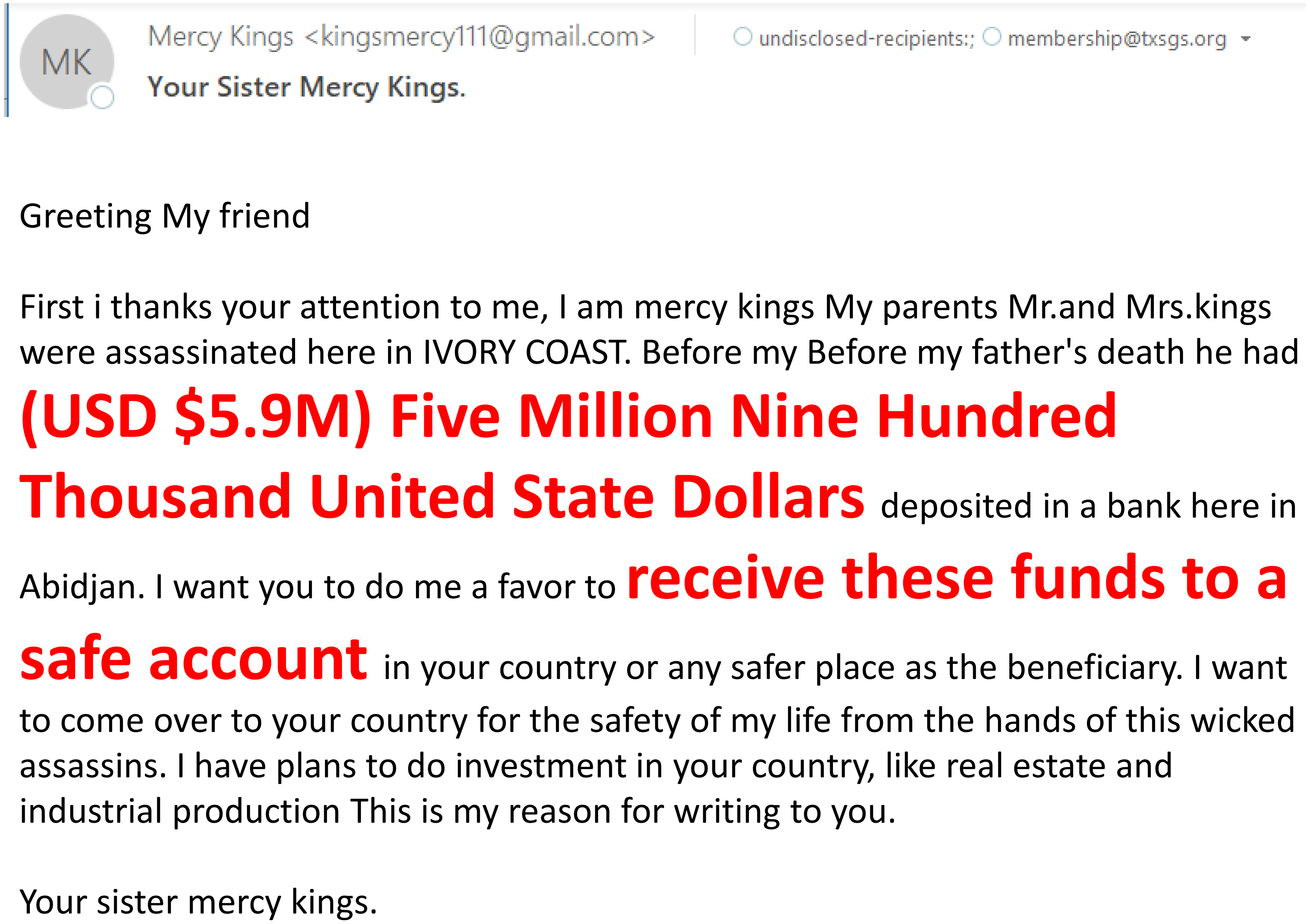
- When in doubt, **verify**
  - Hang up!
  - Obtain accurate contact information
  - Call and ask for assistance

Obtain **Accurate Contact Information**

- Use Google to find legitimate contact information
- Use your own saved Browser links
- Use your own contact information

World Wide Web (a.k.a. “The Internet”)

- Bogus business offers
- Useless Health Care Products
- Discount Software



Mercy Kings <kingsmercy111@gmail.com> ○ undisclosed-recipients:; ○ membership@txsgs.org

Your Sister Mercy Kings.

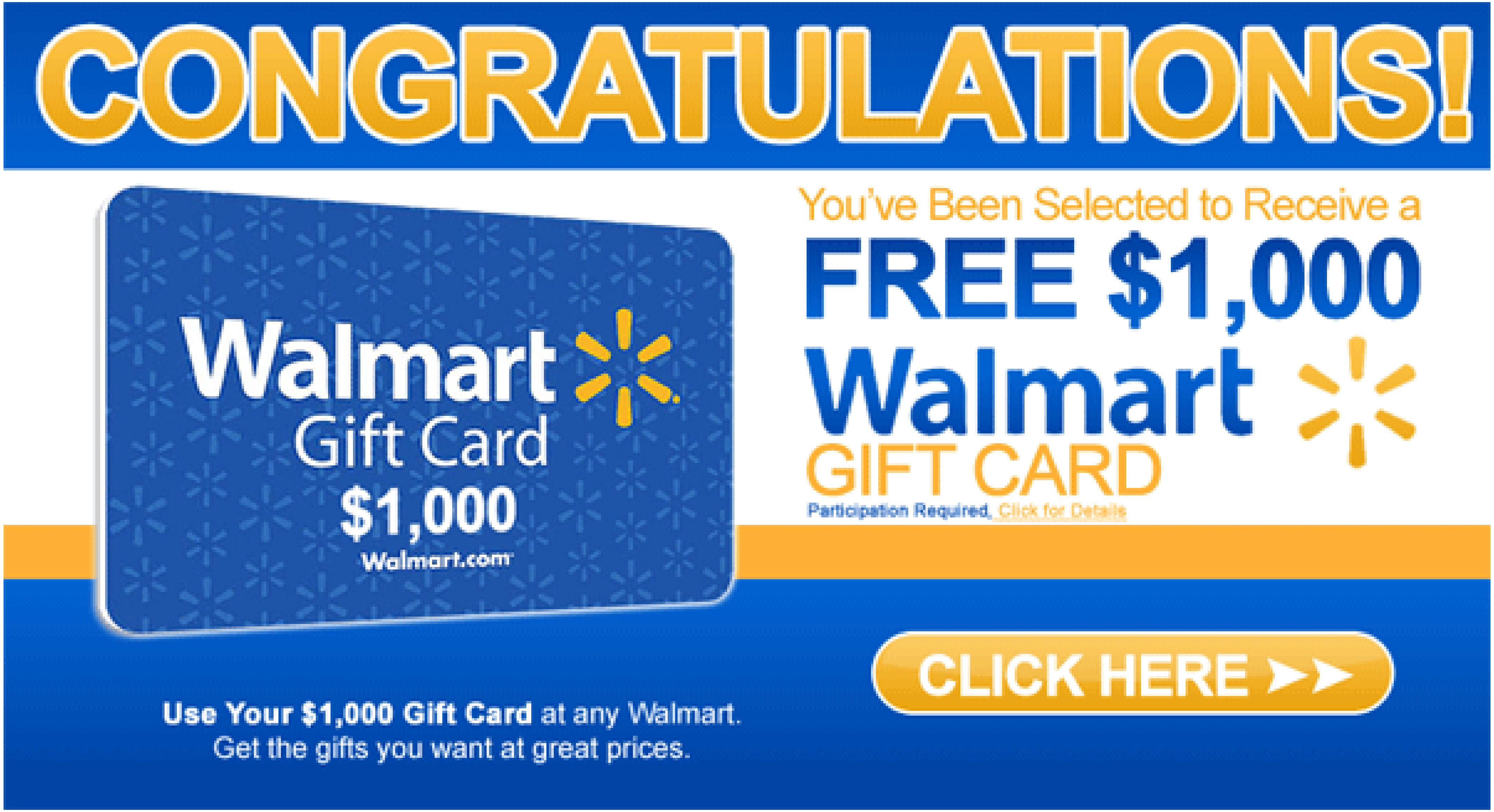
Greeting My friend

First i thanks your attention to me, I am mercy kings My parents Mr.and Mrs.kings were assassinated here in IVORY COAST. Before my Before my father's death he had **(USD $5.9M) Five Million Nine Hundred Thousand United State Dollars** deposited in a bank here in Abidjan. I want you to do me a favor to **receive these funds to a safe account** in your country or any safer place as the beneficiary. I want to come over to your country for the safety of my life from the hands of this wicked assassins. I have plans to do investment in your country, like real estate and industrial production This is my reason for writing to you.

Your sister mercy kings.

World Wide Web (a.k.a. “The Internet”)

- Bogus business offers
- Useless Health Care Products
- Discount Software
- International money transfer requests
- **Pop Ups**



CONGRATULATIONS!

You've Been Selected to Receive a

FREE $1,000

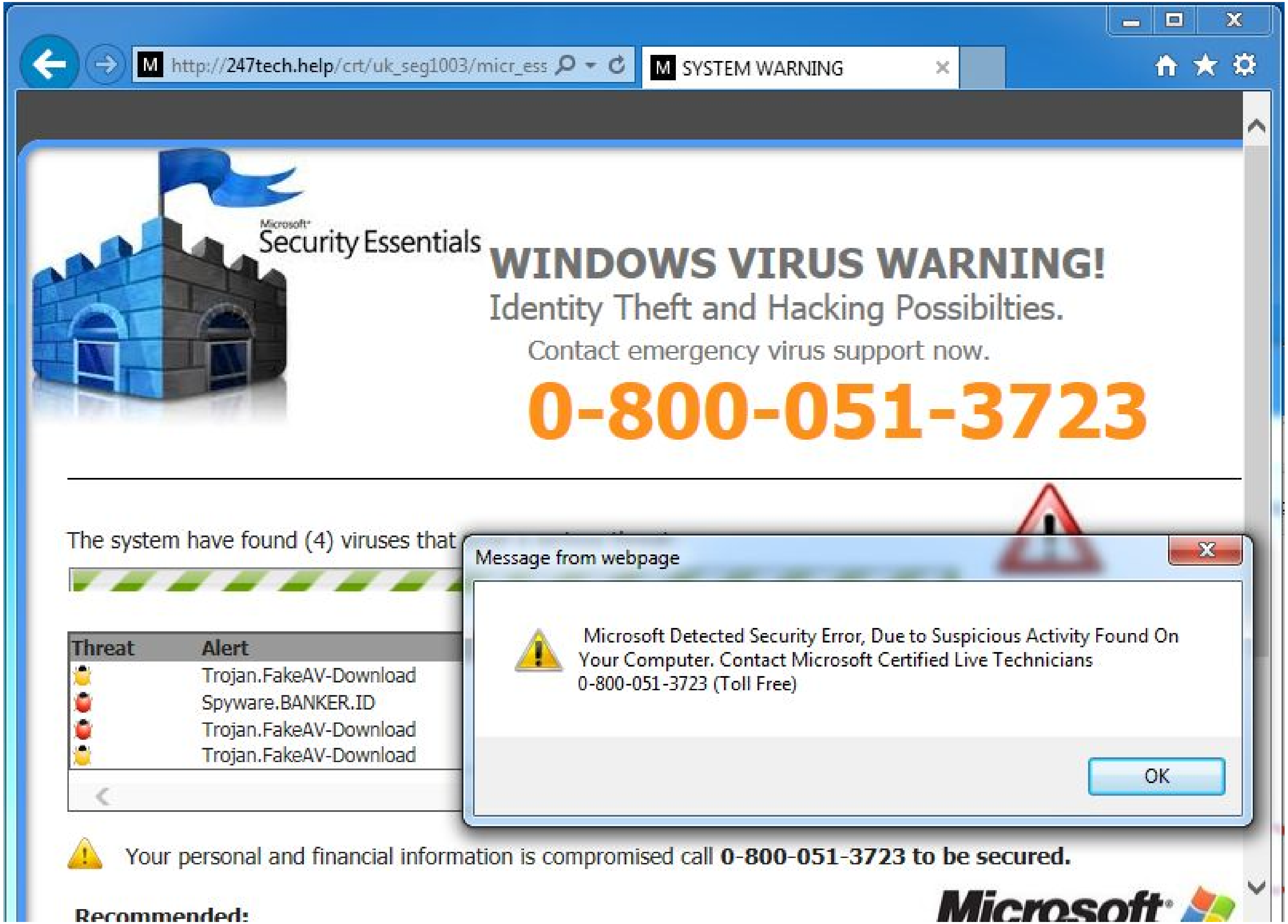
Walmart

GIFT CARD

Participation Required, Click for Details

CLICK HERE >>

Use Your $1,000 Gift Card at any Walmart.
Get the gifts you want at great prices.


http://247tech.help/crt/uk_seg1003/micr_ess
SYSTEM WARNING
Microsoft Security Essentials

WINDOWS VIRUS WARNING!

Identity Theft and Hacking Possibilties.

Contact emergency virus support now.

0-800-051-3723

The system have found (4) viruses that

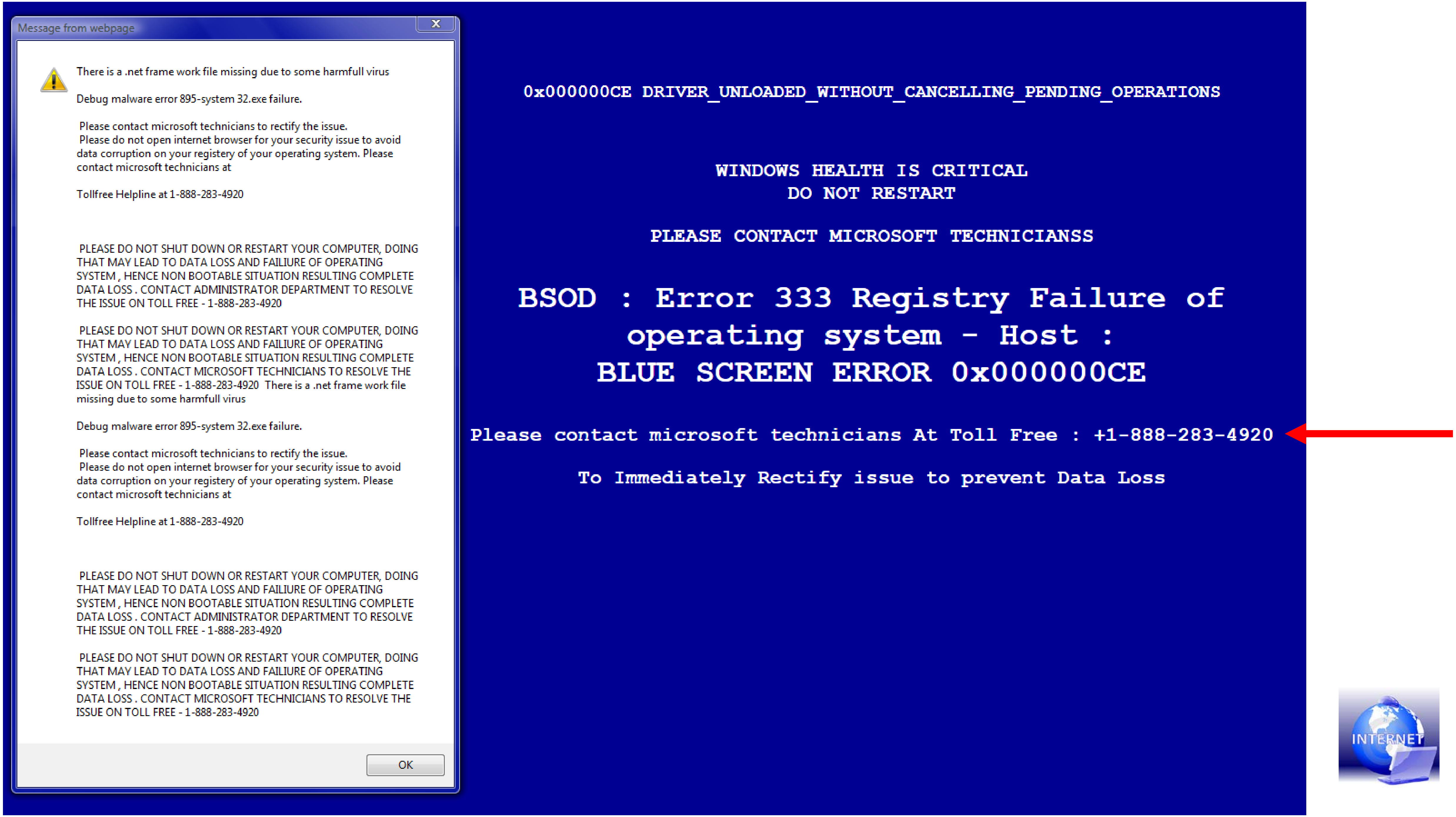
Threat	Alert
●	Trojan.FakeAV-Download
●	Spyware.BANKER.ID
●	Trojan.FakeAV-Download
●	Trojan.FakeAV-Download

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)

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

Recommended:



There is a .net frame work file missing due to some harmfull virus

Debug malware error 895-system 32.exe failure.

Please contact microsoft technicians to rectify the issue.
Please do not open internet browser for your security issue to avoid data corruption on your registery of your operating system. Please contact microsoft technicians at

Tollfree Helpline at 1-888-283-4920

PLEASE DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO DATA LOSS AND FAILIURE OF OPERATING SYSTEM , HENCE NON BOOTABLE SITUATION RESULTING COMPLETE DATA LOSS . CONTACT ADMINISTRATOR DEPARTMENT TO RESOLVE THE ISSUE ON TOLL FREE - 1-888-283-4920

PLEASE DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO DATA LOSS AND FAILIURE OF OPERATING SYSTEM , HENCE NON BOOTABLE SITUATION RESULTING COMPLETE DATA LOSS . CONTACT MICROSOFT TECHNICIANS TO RESOLVE THE ISSUE ON TOLL FREE - 1-888-283-4920 There is a .net frame work file missing due to some harmfull virus

Debug malware error 895-system 32.exe failure.

Please contact microsoft technicians to rectify the issue.
Please do not open internet browser for your security issue to avoid data corruption on your registery of your operating system. Please contact microsoft technicians at

Tollfree Helpline at 1-888-283-4920

PLEASE DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO DATA LOSS AND FAILIURE OF OPERATING SYSTEM , HENCE NON BOOTABLE SITUATION RESULTING COMPLETE DATA LOSS . CONTACT ADMINISTRATOR DEPARTMENT TO RESOLVE THE ISSUE ON TOLL FREE - 1-888-283-4920

PLEASE DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO DATA LOSS AND FAILIURE OF OPERATING SYSTEM , HENCE NON BOOTABLE SITUATION RESULTING COMPLETE DATA LOSS . CONTACT MICROSOFT TECHNICIANS TO RESOLVE THE ISSUE ON TOLL FREE - 1-888-283-4920

0x000000CE DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS

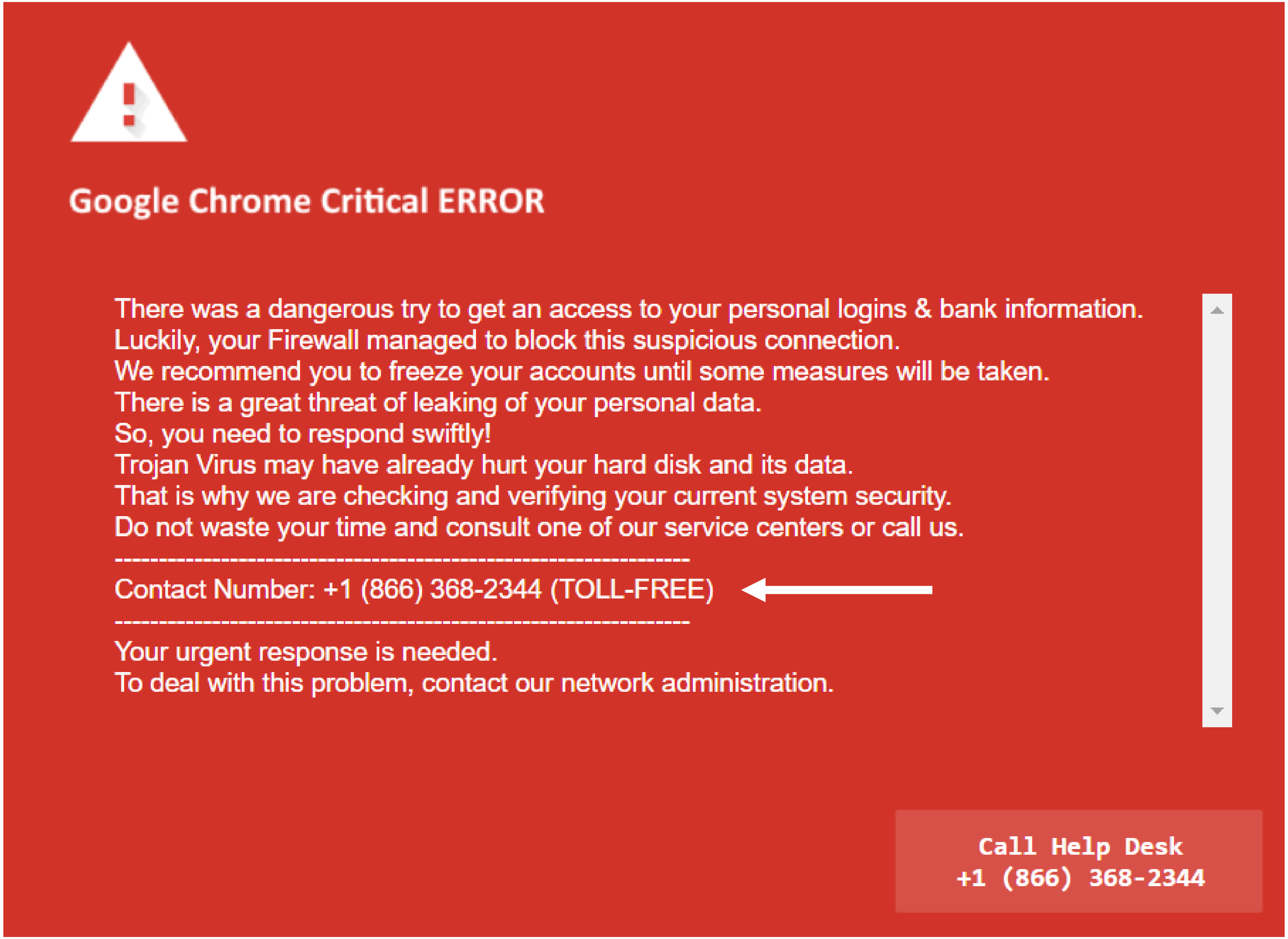
WINDOWS HEALTH IS CRITICAL
DO NOT RESTART

PLEASE CONTACT MICROSOFT TECHNICIANSS

**BSOD : Error 333 Registry Failure of operating system - Host :
BLUE SCREEN ERROR 0x000000CE**

Please contact microsoft technicians At Toll Free : +1-888-283-4920

To Immediately Rectify issue to prevent Data Loss



Google Chrome Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

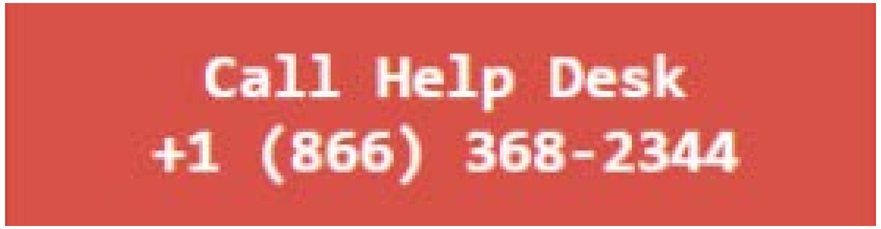
Contact Number: +1 (866) 368-2344 (TOLL-FREE)

Your urgent response is needed.
To deal with this problem, contact our network administration.

The Goal of all of These:

Convincing you to:

- **Call** their telephone numbers
- **Click** on their links



Call Help Desk
+1 (866) 368-2344

Malware

- **<u>Mal</u>**icious Soft**<u>ware</u>**
- An umbrella term used to describe software that has malicious intent
- Can be installed on your system when you click on links

What can Malware do?

- Obtain all of your email contacts
- Scan your email and files for useful information
  - Account numbers, UserIDs and Passwords

What can Malware do?

- Destroy files
- Lock your PC and demand a ransom

What can Malware do?

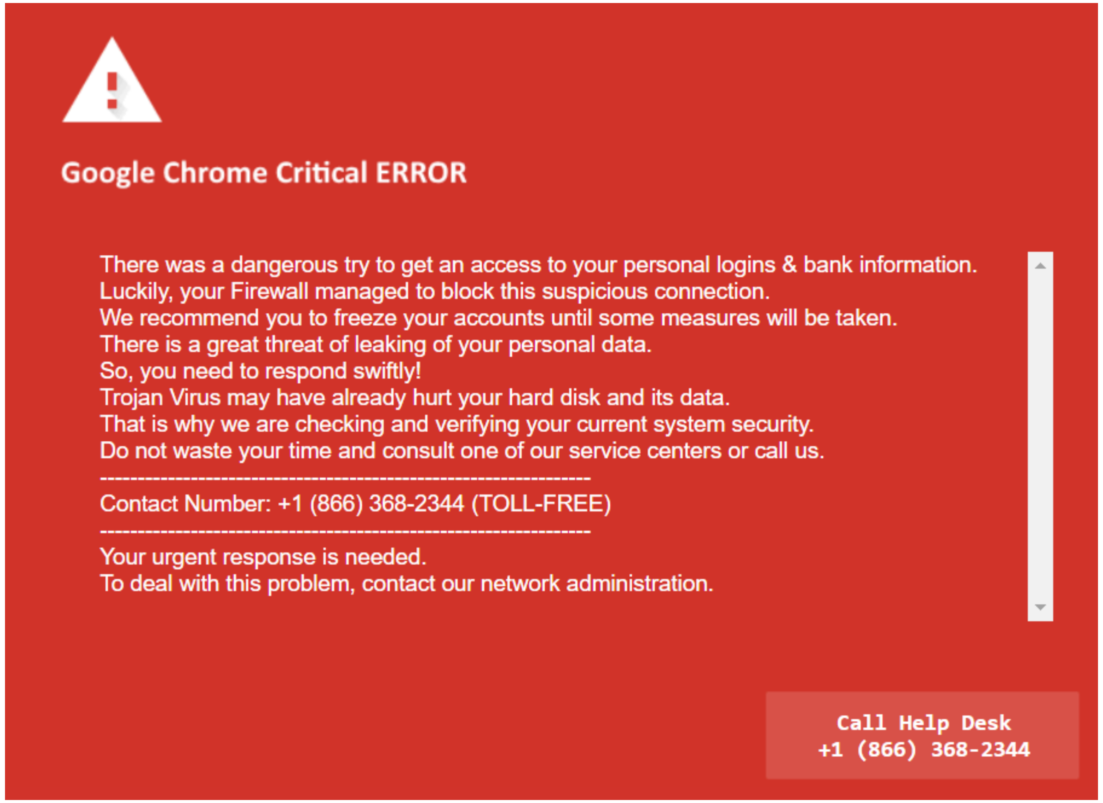
- Destroy files
- Lock your PC and demand a ransom
- Surreptitious monitoring
- Surreptitious use of storage and processor

What to do instead

It usually **looks** much more threatening that it really is…

- Clear your Browse cache
- Close your browser
- Re-Boot your system

~~Call~~ ~~Click~~



Google Chrome Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

Contact Number: +1 (866) 368-2344 (TOLL-FREE)

Your urgent response is needed.
To deal with this problem, contact our network administration.

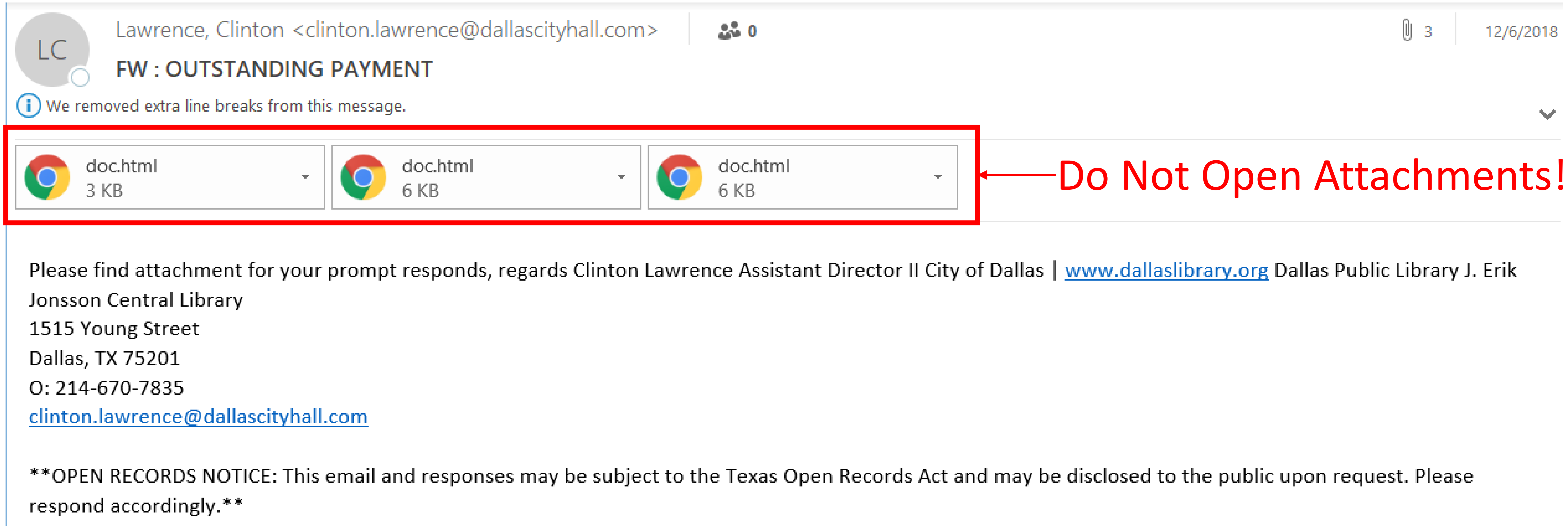
EMail

It is important to learn the signs of malicious email messages

- Spam
- Phishing

Spam

- Messages sent to a large number of recipients
- Usually caused by a virus on somebody else’s PC
- What to look for:
    - Strange or unusual topic
    - Links to webpages with long or weird URL’s
    - Attached Files
    - Weird senders email address



Lawrence, Clinton <clinton.lawrence@dallascityhall.com>

0

3

12/6/2018

FW : OUTSTANDING PAYMENT

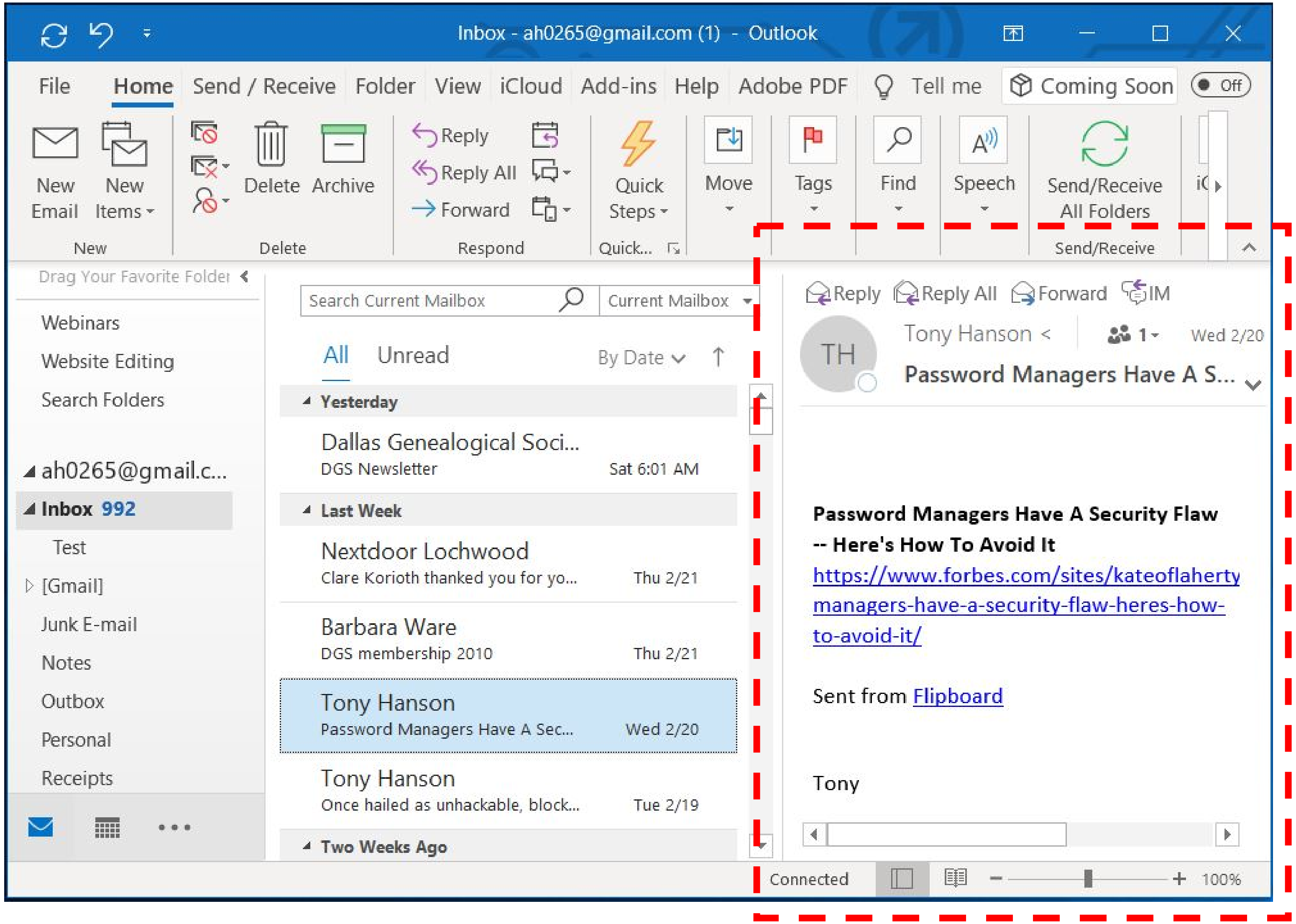
We removed extra line breaks from this message.

Do Not Open Attachments!

Please find attachment for your prompt responds, regards Clinton Lawrence Assistant Director II City of Dallas | www.dallaslibrary.org Dallas Public Library J. Erik Jonsson Central Library
1515 Young Street
Dallas, TX 75201
O: 214-670-7835
clinton.lawrence@dallascityhall.com

OPEN RECORDS NOTICE: This email and responses may be subject to the Texas Open Records Act and may be disclosed to the public upon request. Please respond accordingly.

Message Preview / Auto Preview



Dallas Genealogical Soci...
DGS Newsletter Sat 6:01 AM

Nextdoor Lochwood
Clare Korioth thanked you for yo... Thu 2/21

Barbara Ware
DGS membership 2010 Thu 2/21

Tony Hanson
Password Managers Have A Sec... Wed 2/20

Tony Hanson
Once hailed as unhackable, block... Tue 2/19

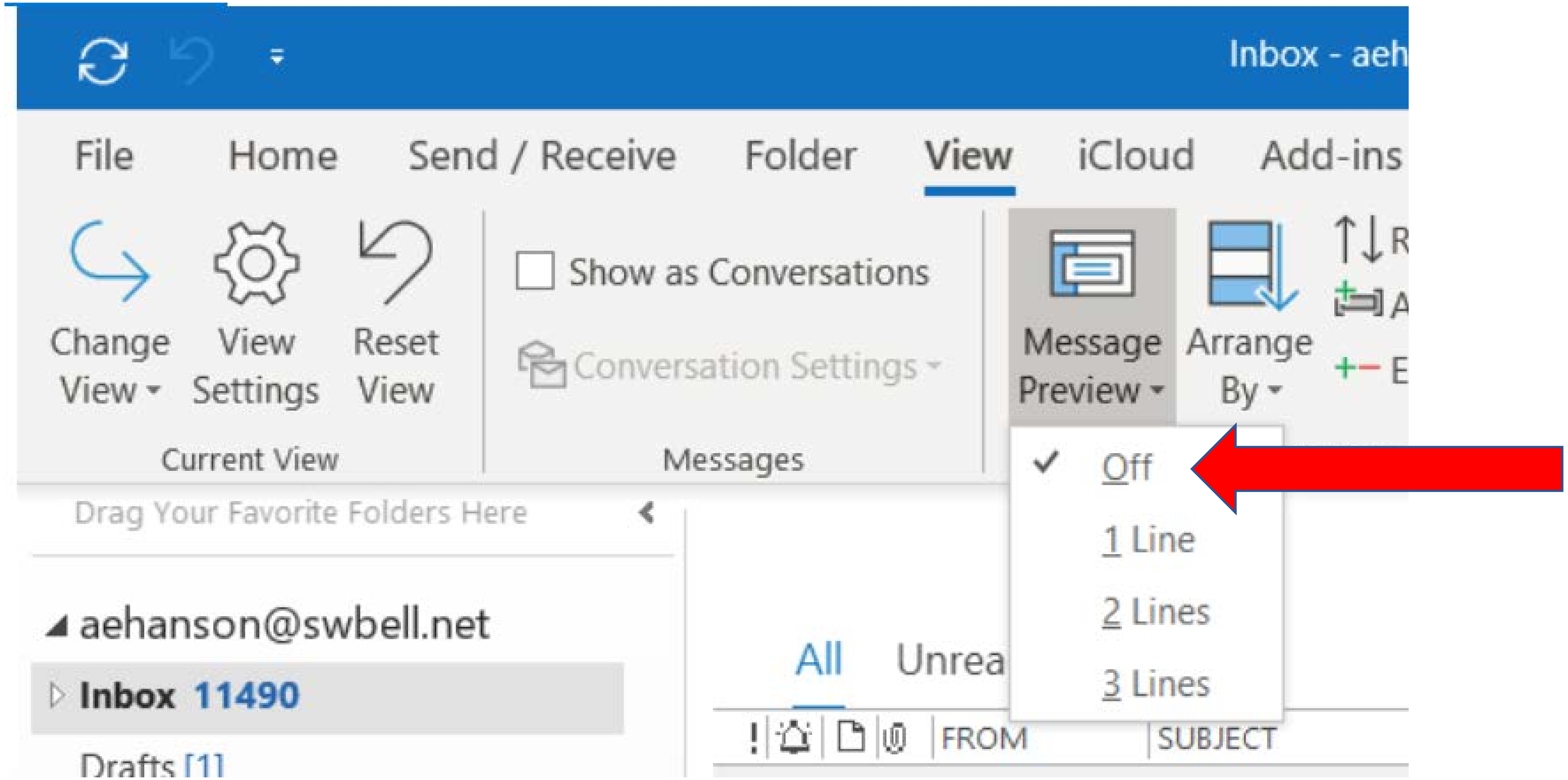
Tony Hanson < Wed 2/20
Password Managers Have A S...

Password Managers Have A Security Flaw -- Here's How To Avoid It
https://www.forbes.com/sites/kateoflaherty managers-have-a-security-flaw-heres-how-to-avoid-it/

Sent from Flipboard

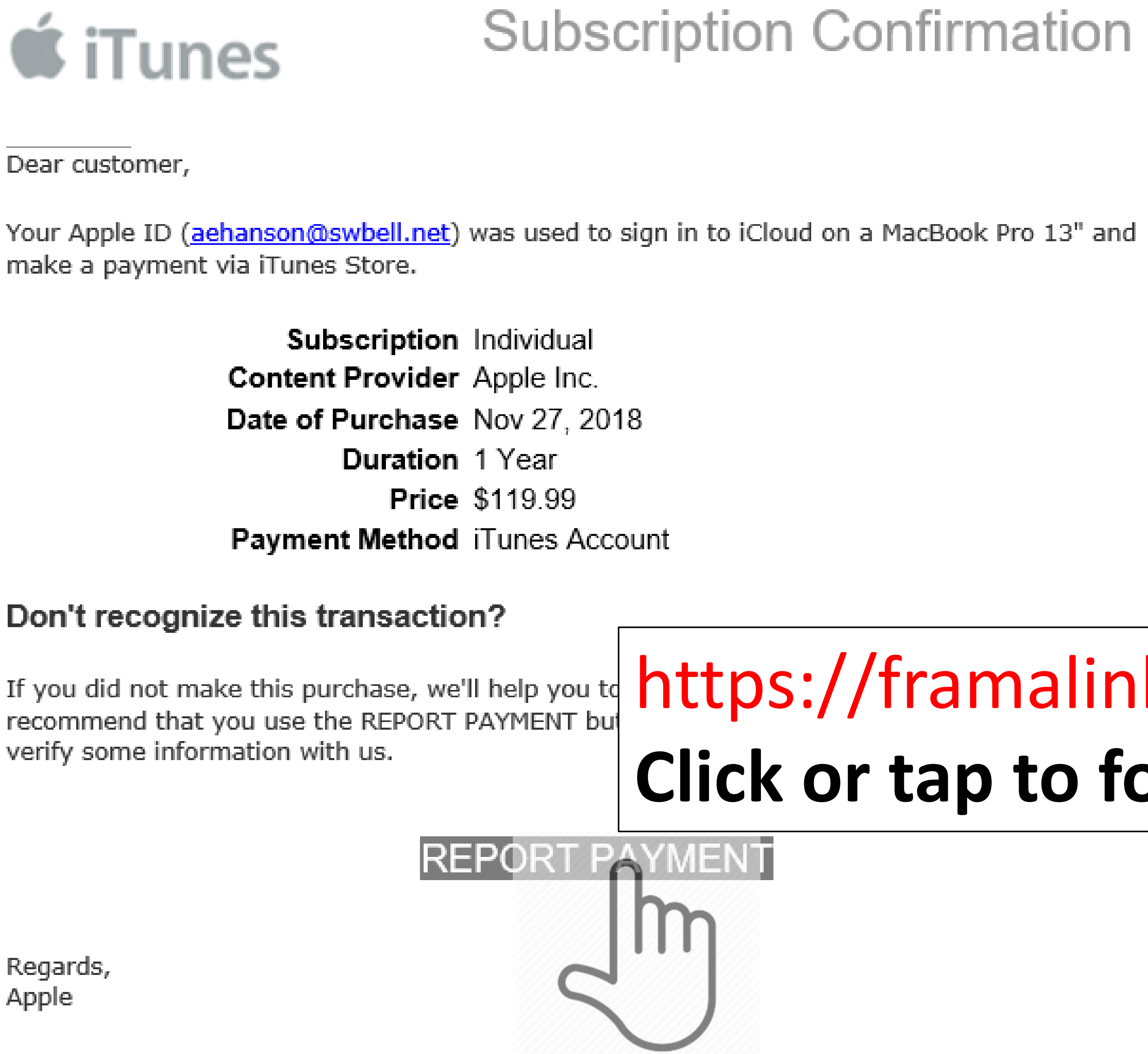
Tony

Do NOT Enable…



Phishing

- An attempt to make you believe that the email is from a legitimate company, organization, person or friend



iTunes

Subscription Confirmation

Dear customer,

Your Apple ID (aehanson@swbell.net) was used to sign in to iCloud on a MacBook Pro 13" and make a payment via iTunes Store.

Subscription	Individual
Content Provider	Apple Inc.
Date of Purchase	Nov 27, 2018
Duration	1 Year
Price	$119.99
Payment Method	iTunes Account

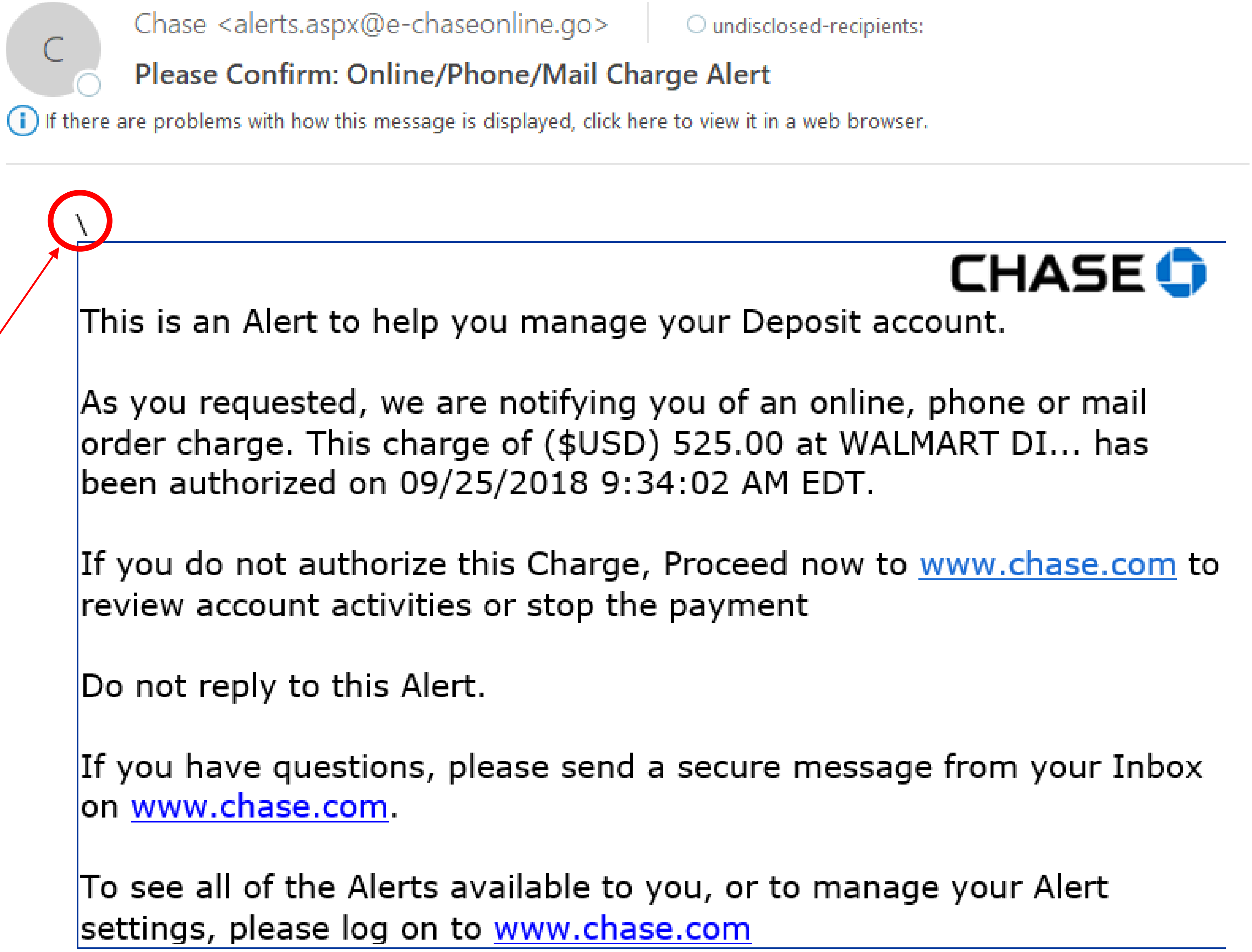
Don't recognize this transaction?

If you did not make this purchase, we'll help you to
recommend that you use the REPORT PAYMENT bu
verify some information with us.

Regards,
Apple

https://framalink.cancellation

Click or tap to follow link.



Chase <alerts.aspx@e-chaseonline.go>

○ undisclosed-recipients:

Please Confirm: Online/Phone/Mail Charge Alert

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

\

CHASE

This is an Alert to help you manage your Deposit account.

As you requested, we are notifying you of an online, phone or mail order charge. This charge of ($USD) 525.00 at WALMART DI... has been authorized on 09/25/2018 9:34:02 AM EDT.

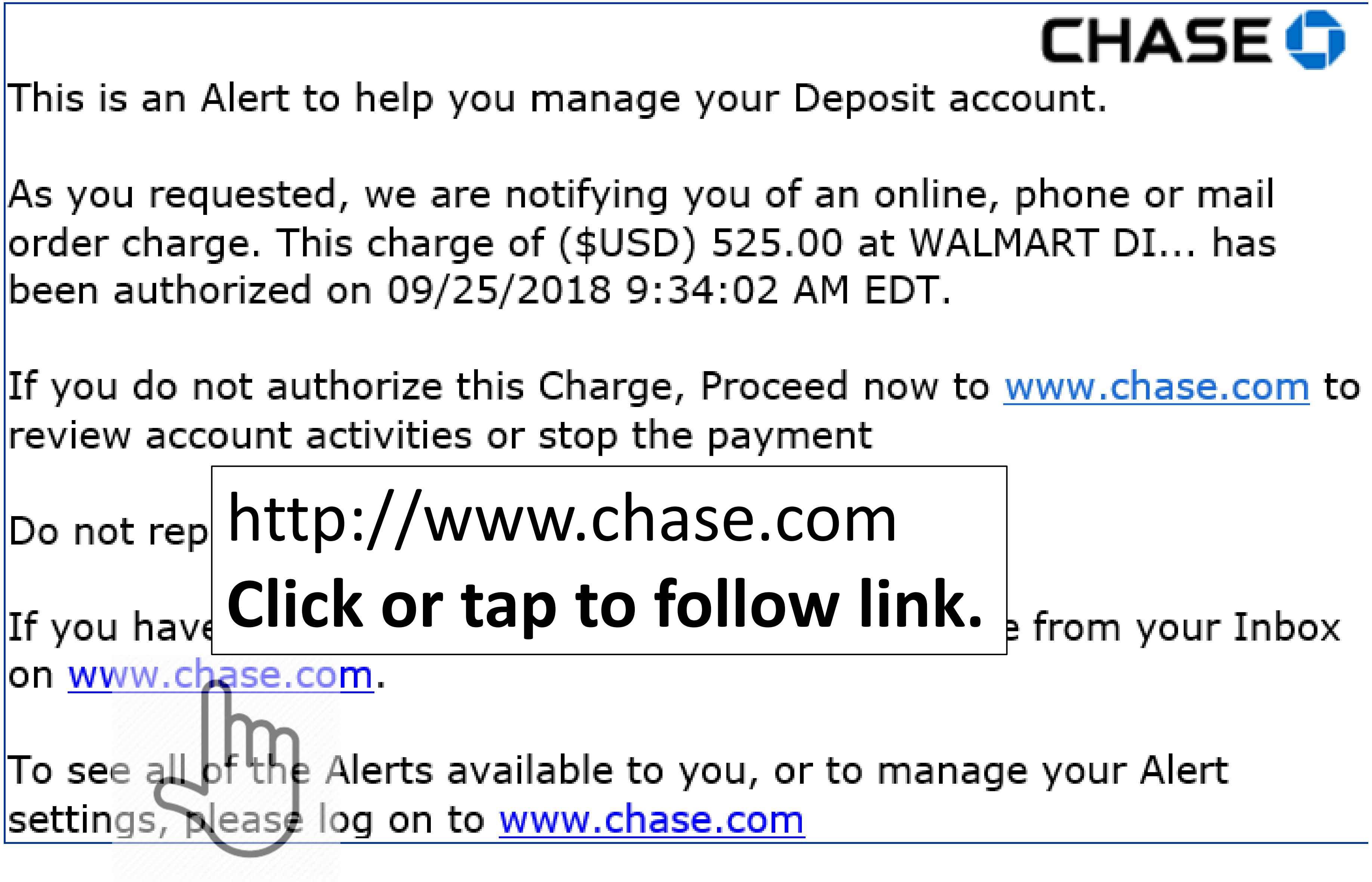
If you do not authorize this Charge, Proceed now to www.chase.com to review account activities or stop the payment

Do not reply to this Alert.

If you have questions, please send a secure message from your Inbox on www.chase.com.

To see all of the Alerts available to you, or to manage your Alert settings, please log on to www.chase.com

?



CHASE

This is an Alert to help you manage your Deposit account.

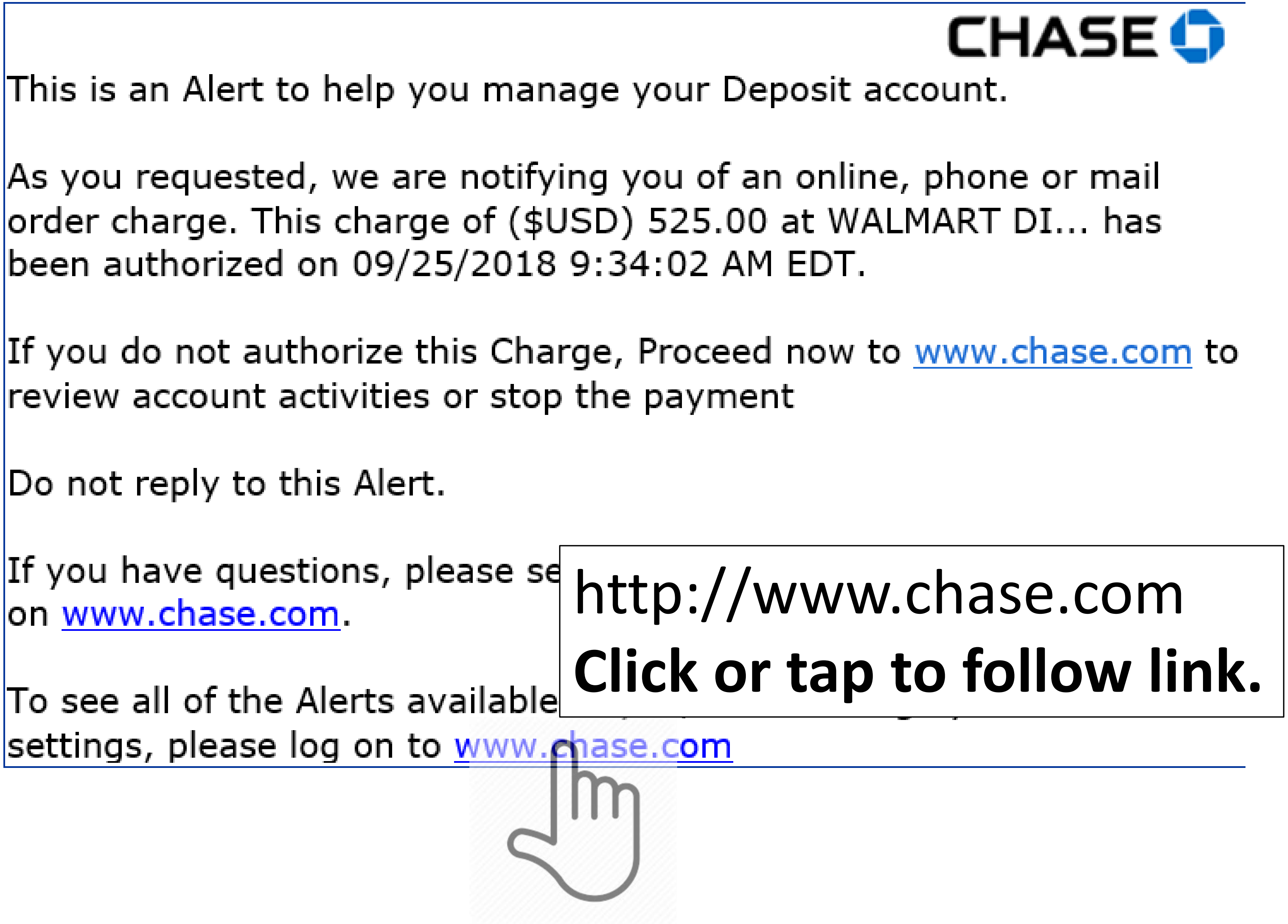
As you requested, we are notifying you of an online, phone or mail order charge. This charge of ($USD) 525.00 at WALMART DI... has been authorized on 09/25/2018 9:34:02 AM EDT.

If you do not authorize this Charge, Proceed now to www.chase.com to review account activities or stop the payment

Do not rep

If you have e from your Inbox on www.chase.com.

To see all of the Alerts available to you, or to manage your Alert settings, please log on to www.chase.com



CHASE

This is an Alert to help you manage your Deposit account.

As you requested, we are notifying you of an online, phone or mail order charge. This charge of ($USD) 525.00 at WALMART DI... has been authorized on 09/25/2018 9:34:02 AM EDT.

If you do not authorize this Charge, Proceed now to www.chase.com to review account activities or stop the payment

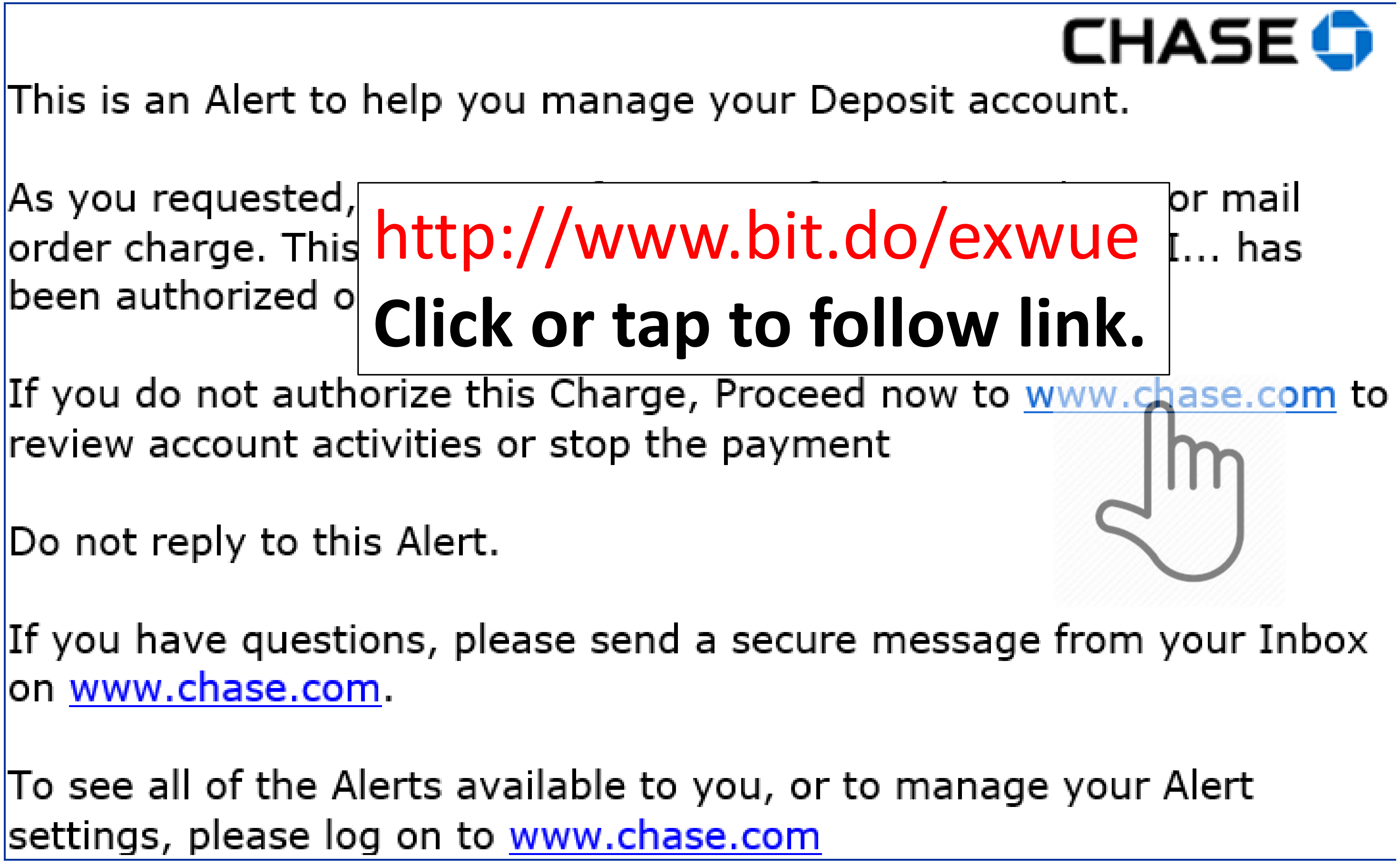
Do not reply to this Alert.

If you have questions, please se
on www.chase.com.

To see all of the Alerts available
settings, please log on to www.chase.com

http://www.chase.com

Click or tap to follow link.



CHASE

This is an Alert to help you manage your Deposit account.

As you requested, or mail order charge. This I... has been authorized o

http://www.bit.do/exwue

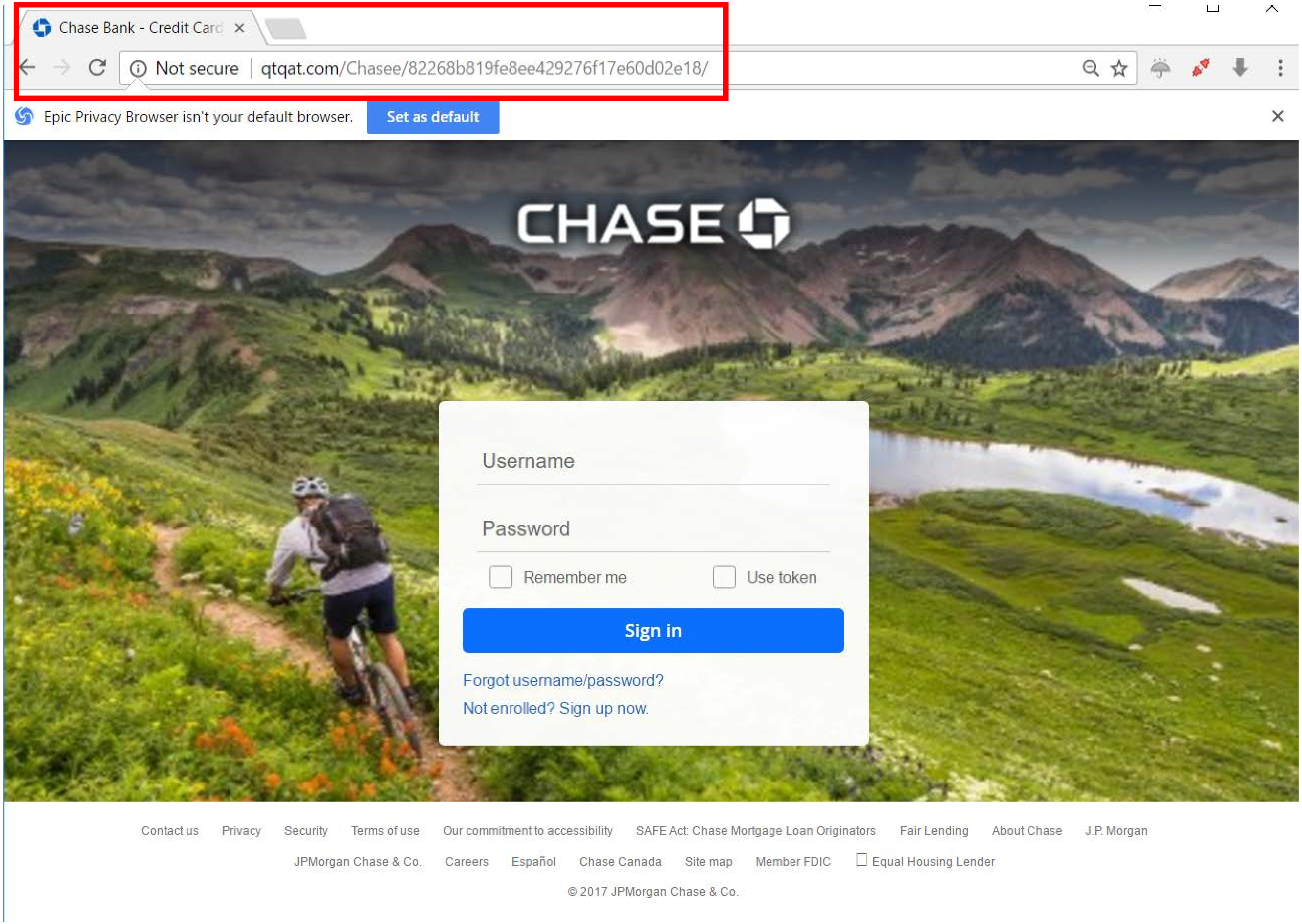
Click or tap to follow link.

If you do not authorize this Charge, Proceed now to www.chase.com to review account activities or stop the payment

Do not reply to this Alert.

If you have questions, please send a secure message from your Inbox on www.chase.com.

To see all of the Alerts available to you, or to manage your Alert settings, please log on to www.chase.com

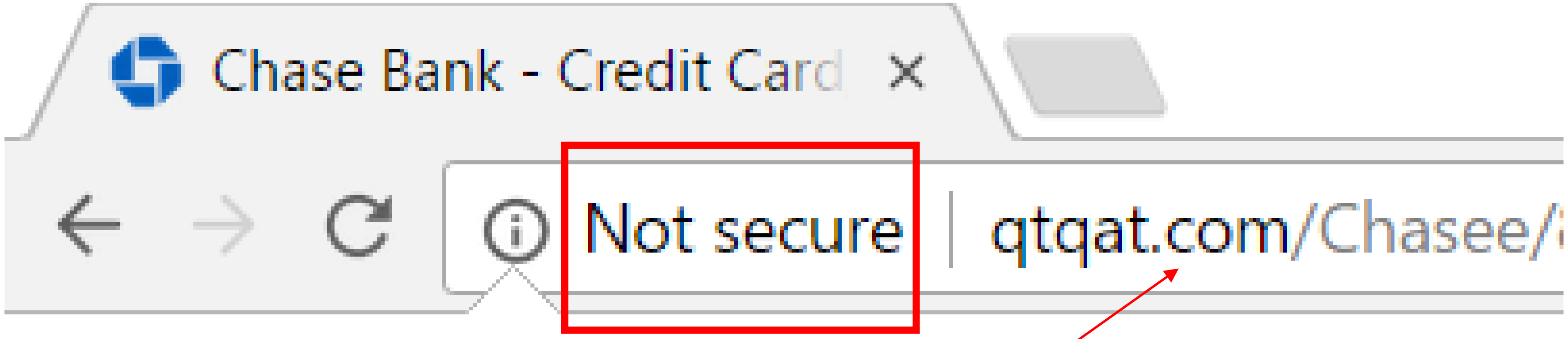


Chase Bank - Credit Card

Not secure | qtqat.com/Chasee/82268b819fe8ee429276f17e60d02e18/

Epic Privacy Browser isn't your default browser.

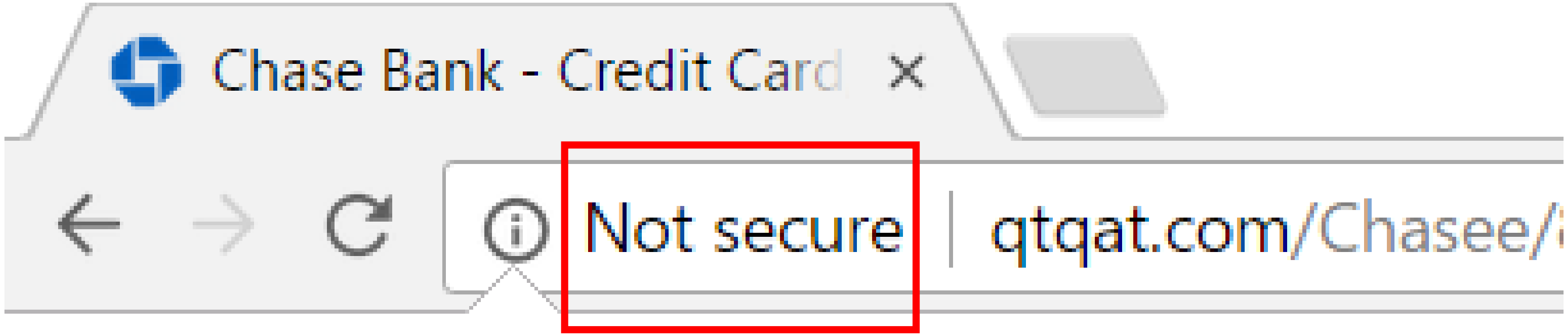
© 2017 JPMorgan Chase & Co.



qtqat.com/Chasee

http vs https

- http stands for "**H**yper **T**ext **T**ransfer **P**rotocol"
  - It is the underlying protocol used to establish connections on the internet
- http**s** provides a more secure connection
- Chrome (Google) has started identifying http connections as "Not Secure"
- The reality is that they simply are **not as secure as they could be….**

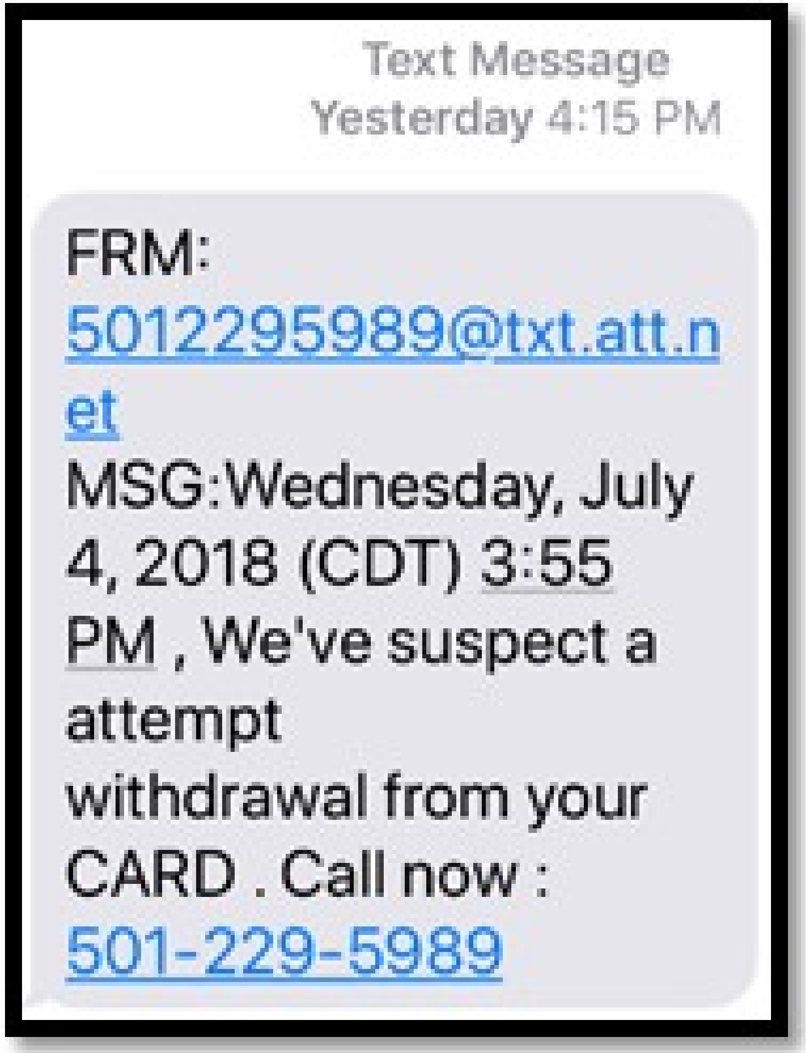


Smishing

- Phishing attempt sent via the cellular SMS network
- Phishing Text message

Click

Call



Text Message
Yesterday 4:15 PM

FRM:
5012295989@txt.att.net
MSG:Wednesday, July 4, 2018 (CDT) 3:55 PM , We've suspect a attempt withdrawal from your CARD . Call now : 501-229-5989

Public WiFi

WiFi networks that are available in public places:

- Libraries
- Airports
- Restaurants
- Hotels
- Conferences

Problems with Public WiFi

- It is a shared resource
  - With the right technology, **others may be able to see what you are typing**
- You may be connecting to a scammers fake network
  - Designed to look legitimate
  - **The scammer will be able to see what you are typing**

Good Public WiFi Habits

- Assume somebody can see the information you are typing
- Never enter private information when connected to a public Wifi network
  - UserID’s and Passwords
  - Financial information
  - Personal/private information

Public WiFi Alternative

- Mobile Phone:
  - Turn WiFi off
    - Uses your phones data network instead

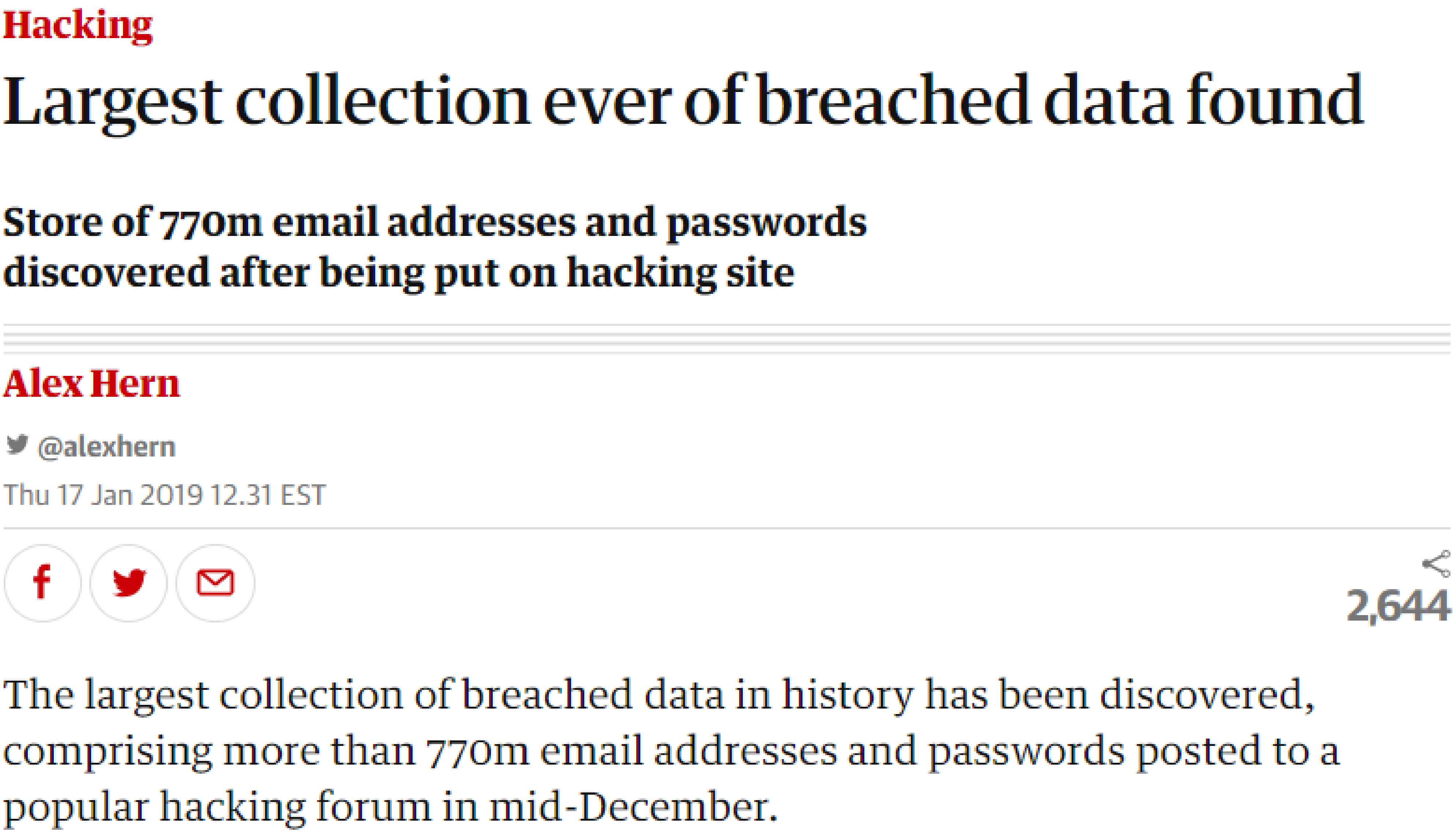
- Laptop or Tablet
  - Use the Hotspot capability on your mobile phone
    - Uses your phones data network instead

Note: Both of these options will increase your data use….

Indirect/3rd Party Attacks

Information about you is obtained from business or government systems:

- Name
- Address
- Identify Information
- Financial Information
- UserID
- Password



Hacking

Largest collection ever of breached data found

Store of 770m email addresses and passwords discovered after being put on hacking site

Alex Hern

@alexhern

Thu 17 Jan 2019 12.31 EST

The largest collection of breached data in history has been discovered, comprising more than 770m email addresses and passwords posted to a popular hacking forum in mid-December.

https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking

SCAM

Why Should You Worry?

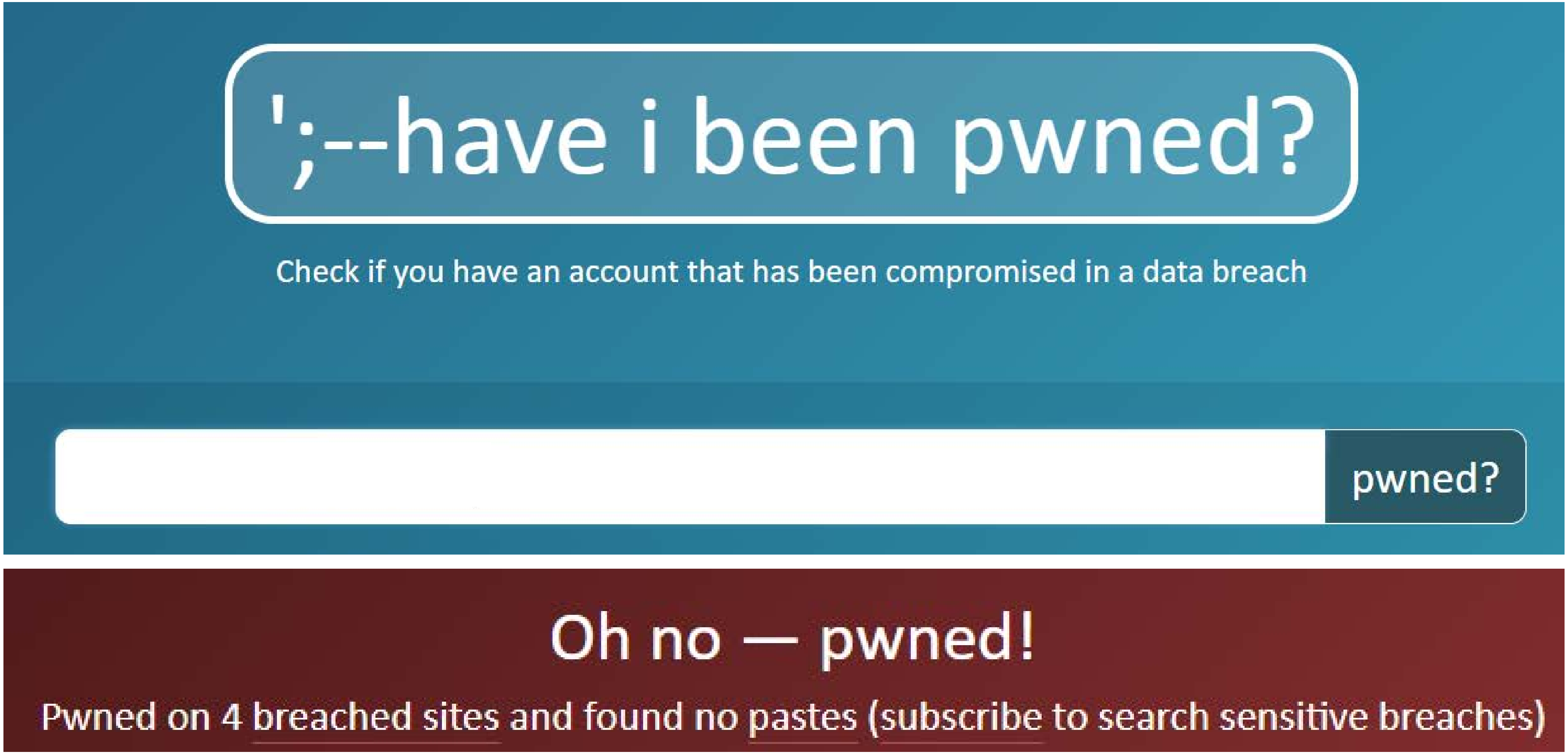
- Having specific information about you makes it easer for scammers to use the techniques we have already discussed to try to get more information from you
- If you use the same UserID and Password on multiple systems they may be able to log into your accounts without your knowledge
- If you use a weak/common password they may be able to hack into your accounts without your knowledge

Most Popular/Commonly Used Passwords

From analysis of millions of accounts that have been hacked and made publicly available

- 123456
- 123456789
- qwerty
- password
- 111111

https://haveibeenpwned.com/

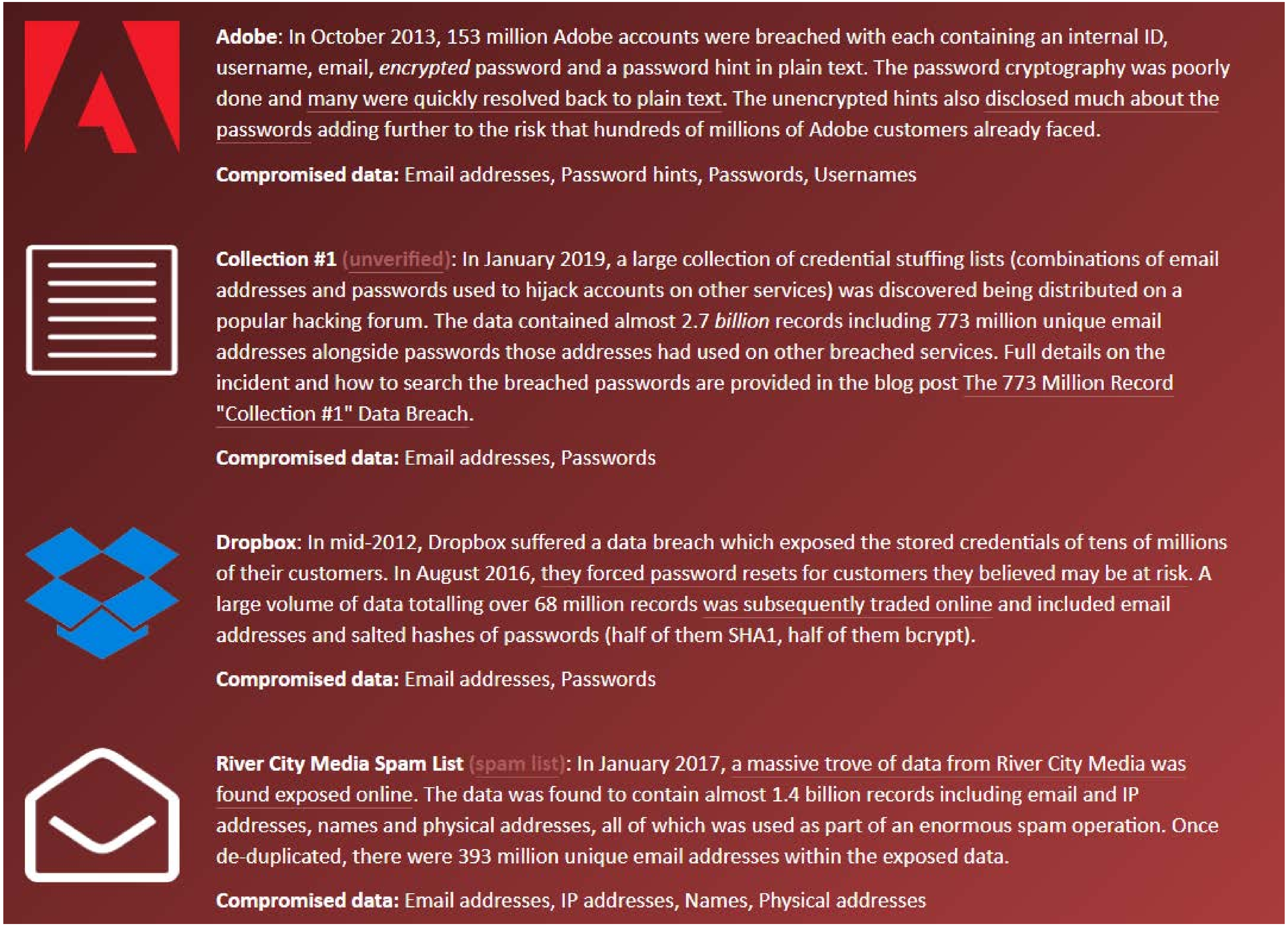


';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Oh no — pwned!

Pwned on 4 breached sites and found no pastes (subscribe to search sensitive breaches)



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

River City Media Spam List (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

Compromised data: Email addresses, IP addresses, Names, Physical addresses

Protect Yourself!

Passwords

Most People Have Bad Habits

- Identical User ID’s and Passwords are used on multiple accounts
- Passwords are changed infrequently (if at all)
- Hackers know this
  - If they get access to one of your accounts, they will try that combination on other accounts

Password Goals

- Make ***<u>every</u>*** password unique
- Change passwords on a regular basis
- Create strong/complex passwords

Characteristics of a Strong Password

- At least 10 characters in length
- Contains one or more of each of the following:
  - UPPER CASE letter
  - lower case letter
  - Number
  - Special Character (**NOT** a letter or a number)
- Does not include words found in a dictionary
- Easy for **YOU** to remember

Creating A Strong Password Is Not Hard

Pick a Phrase

Creating A Strong Password Is Not Hard

First Letter From Each Word

Creating **A** **S**trong **P**assword Is **N**ot **H**ard

caspinh

Add A **Number**

Creating A Strong Password Is Not Hard

caspinh**19**

Add A **Special Character**

Creating A Strong Password Is Not Hard

caspinh19*

Make it **Unique For Each Site**

Creating A Strong Password Is Not Hard

caspinh19***FAC**	Facebook

Make it Unique For Each Site

Creating A Strong Password Is Not Hard

caspinh19*FAC	Facebook
caspinh19***TWI**	Twitter

Make it Unique For Each Site

Creating A Strong Password Is Not Hard

caspinh19*FAC	Facebook
caspinh19*TWI	Twitter
caspinh19***VER**	Verizon

Next Year

- Pick a New Phrase
  - *‘She Turned Me Into A Newt’*
- Change the Number
- Pick a different special character

stmian20&FAC	Facebook
stmian20&TWI	Twitter
stmian20&VER	Verizon

Remembering All Those Passwords

- You probably have a lot of accounts
  - I have 169
  - My Genealogy Society has 60
  - My State Genealogical Society has more
- Many sites impose unique/different password requirement
  - Your password scheme may not work on all sites

Remembering All Those Passwords

- If you were hacked today, would you know all of the accounts you have that need to be updated with a new password?
- If you became incapacitated (or died), would your significant other (or your executor) know how to access all of your accounts?

Reasons To Use A **Password Manager**

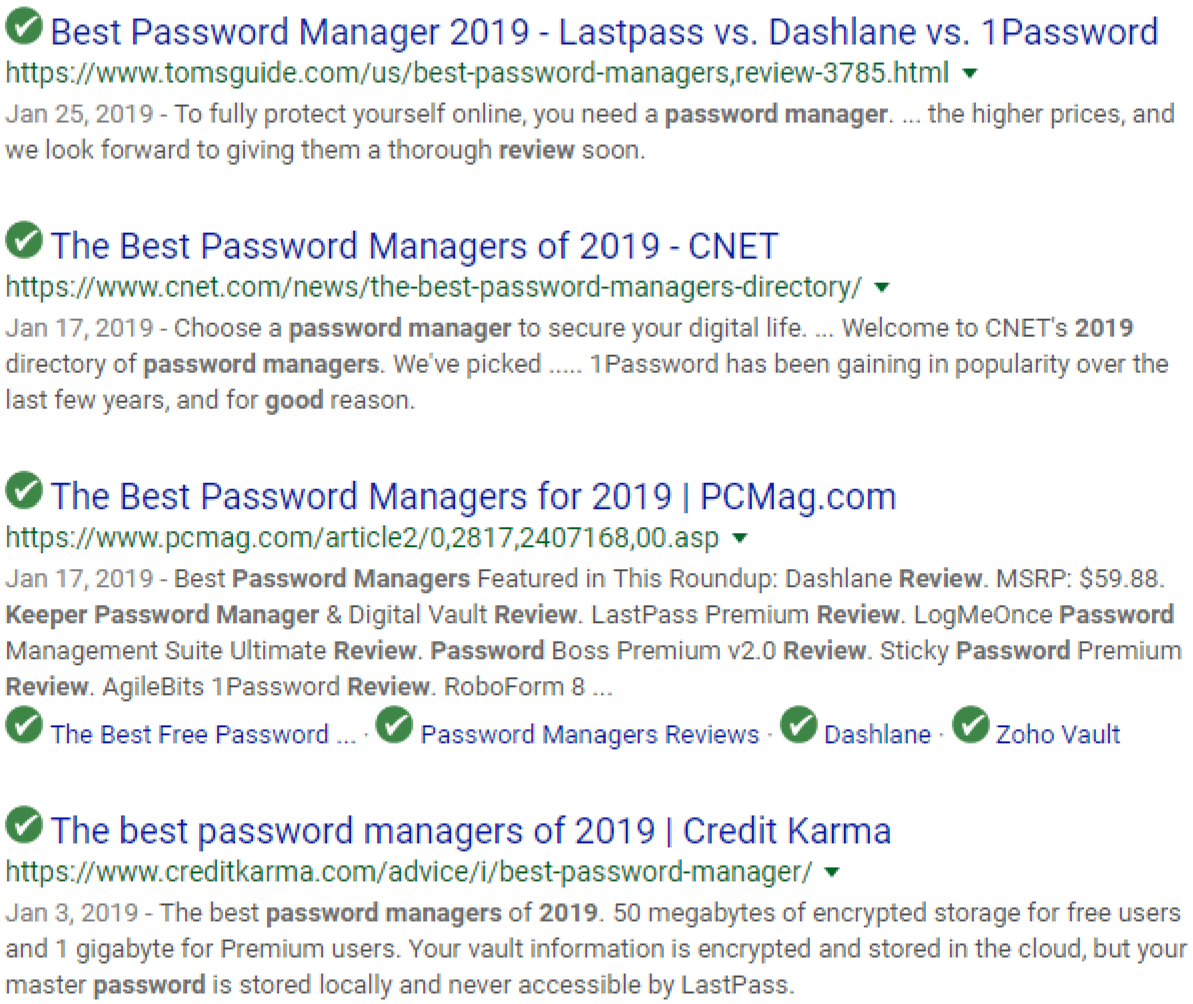
- It provides an environment that makes it easier for you to create strong, unique passwords for each site
- Can be accessed from anywhere
  - Via the internet
  - Using a mobile device App

Reasons To Use A **Password Manager**

- Most warn you when duplicate passwords are discovered
- Most have tools that allow you to quickly change passwords for each site
- Leaves a record of your accounts for your spouse or executor
  - As long as they have the password!

Google

Password manager reviews 2019



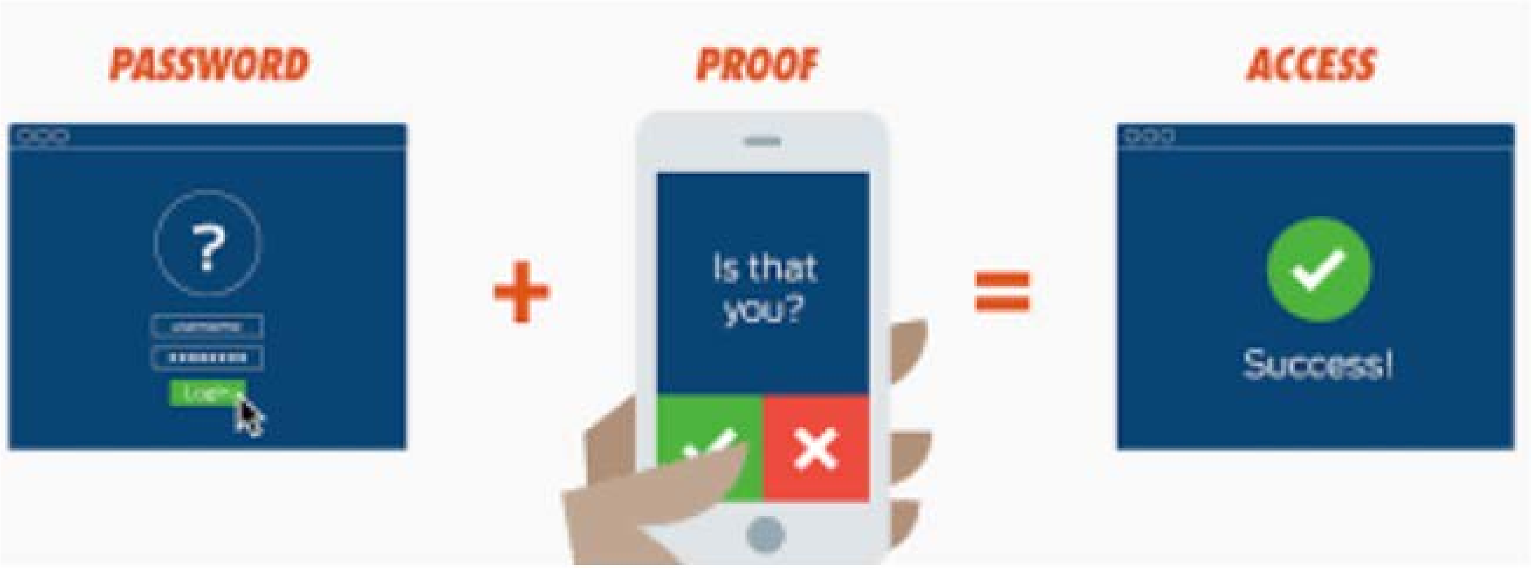
✓ Best Password Manager 2019 - Lastpass vs. Dashlane vs. 1Password
https://www.tomsguide.com/us/best-password-managers,review-3785.html ▾
Jan 25, 2019 - To fully protect yourself online, you need a **password manager**. ... the higher prices, and we look forward to giving them a thorough **review** soon.

✓ The Best Password Managers of 2019 - CNET
https://www.cnet.com/news/the-best-password-managers-directory/ ▾
Jan 17, 2019 - Choose a **password manager** to secure your digital life. ... Welcome to CNET's **2019** directory of **password managers**. We've picked ..... 1Password has been gaining in popularity over the last few years, and for **good** reason.

✓ The Best Password Managers for 2019 | PCMag.com
https://www.pcmag.com/article2/0,2817,2407168,00.asp ▾
Jan 17, 2019 - Best **Password Managers** Featured in This Roundup: Dashlane **Review**. MSRP: $59.88. **Keeper Password Manager** & Digital Vault **Review**. LastPass Premium **Review**. LogMeOnce **Password** Management Suite Ultimate **Review**. **Password** Boss Premium v2.0 **Review**. Sticky **Password** Premium **Review**. AgileBits 1Password **Review**. RoboForm 8 ...
✓ The Best Free Password ... · ✓ Password Managers Reviews · ✓ Dashlane · ✓ Zoho Vault

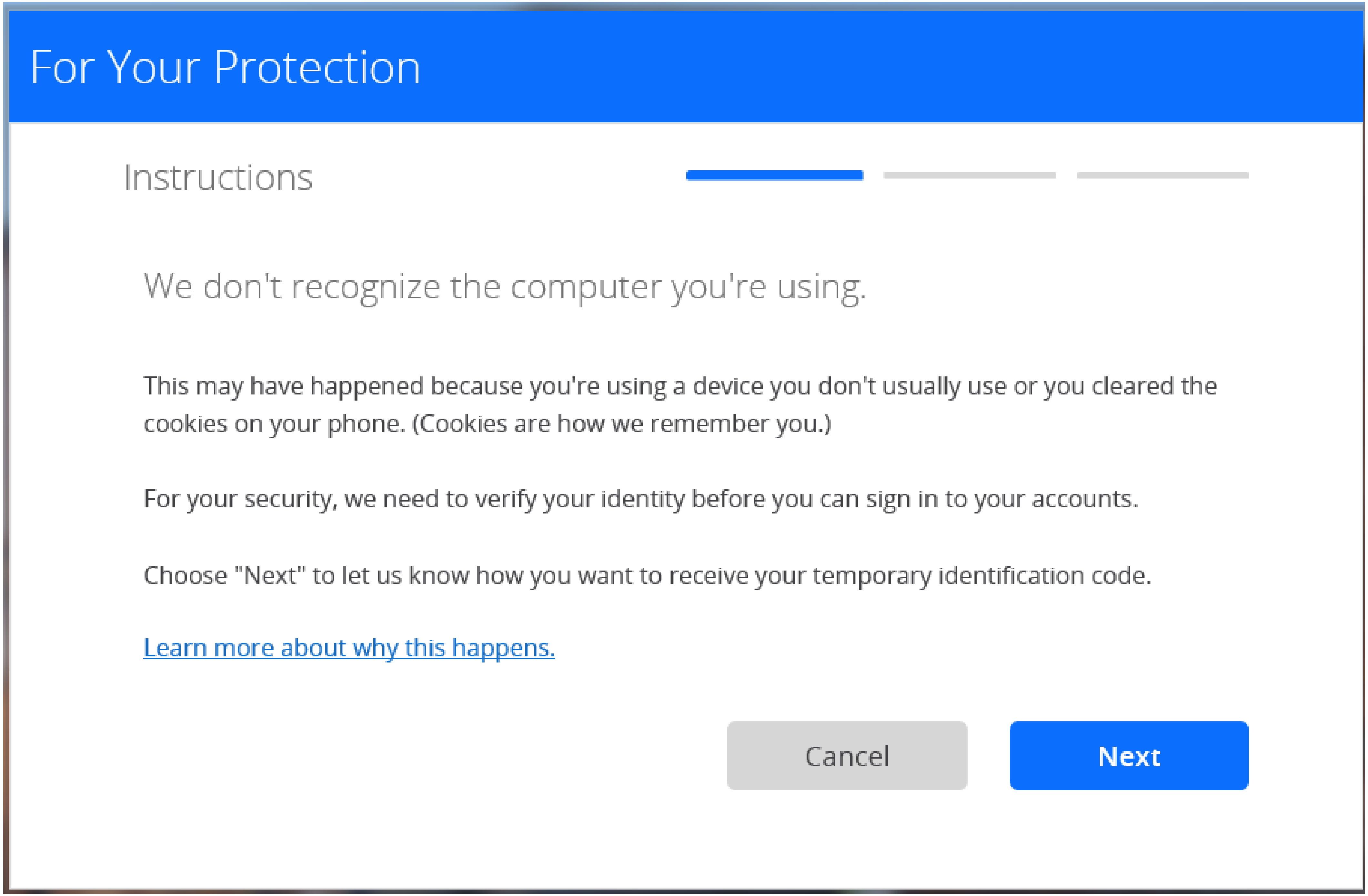
✓ The best password managers of 2019 | Credit Karma
https://www.creditkarma.com/advice/i/best-password-manager/ ▾
Jan 3, 2019 - The best **password managers** of **2019**. 50 megabytes of encrypted storage for free users and 1 gigabyte for Premium users. Your vault information is encrypted and stored in the cloud, but your master **password** is stored locally and never accessible by LastPass.

2-Step Authorization



Two-Factor (2-Step) Authentication

- Some websites allow you to link your mobile phone into your account information
- Logging in from a new location, device or using a new browser triggers a text message to your mobile phone
- You must enter the string you receive in order to log in



For Your Protection

Instructions

We don't recognize the computer you're using.

This may have happened because you're using a device you don't usually use or you cleared the cookies on your phone. (Cookies are how we remember you.)

For your security, we need to verify your identity before you can sign in to your accounts.

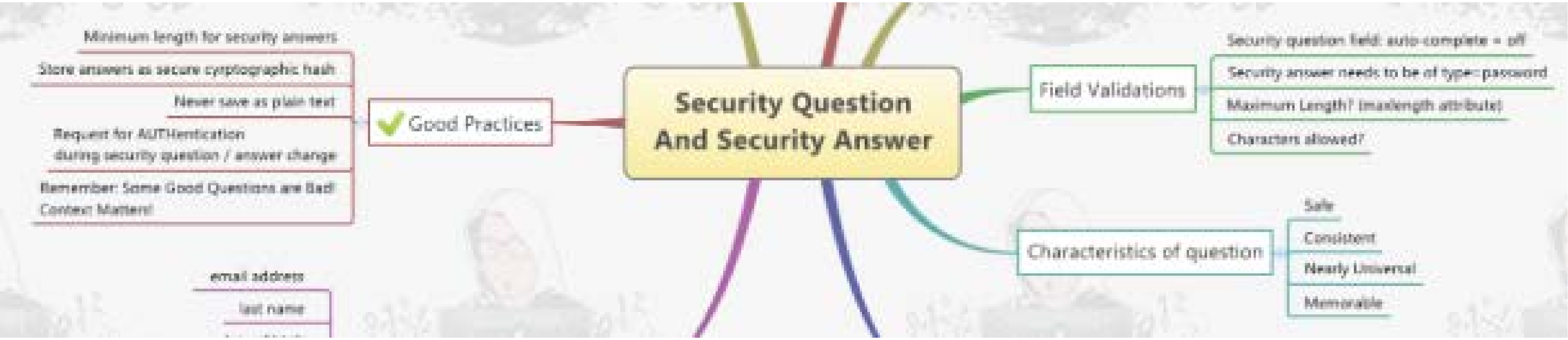
Choose "Next" to let us know how you want to receive your temporary identification code.

Learn more about why this happens.

Two-Factor (2-Step) Authentication

- Provides an additional layer of protection
- Prevents access even if your UserID and Password are compromised
  - **Bonus:** You will receive a text message if somebody else tries to access your account

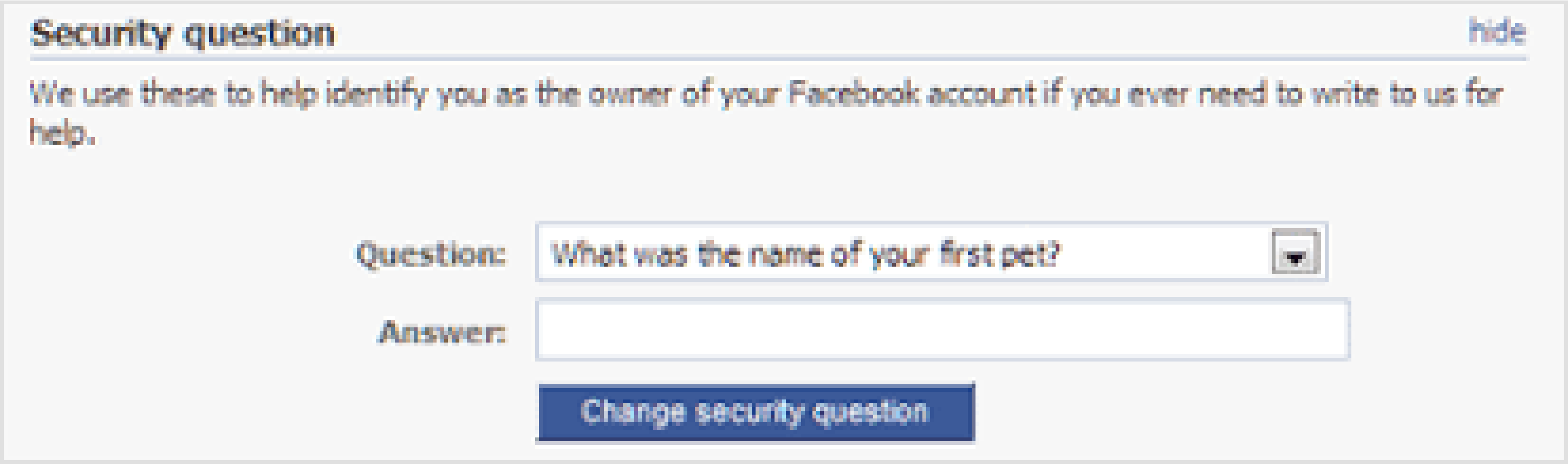
Security Questions



Security Question And Security Answer
Good Practices
Minimum length for security answers
Store answers as secure cryptographic hash
Never save as plain text
Request for AUTHentication during security question / answer change
Remember: Some Good Questions are Bad! Context Matters!
Field Validations
Security question field: auto-complete = off
Security answer needs to be of type=password
Maximum Length? (maxlength attribute)
Characters allowed?
Characteristics of question
Safe
Consistent
Nearly Universal
Memorable
email address
last name

Security Questions

Many sites ask you to provide answers to questions that will be used if you forget your UserID or Password.



Security question

We use these to help identify you as the owner of your Facebook account if you ever need to write to us for help.

Question: What was the name of your first pet?

Answer:

Security Questions

- Typical Questions:
  - Where did you go to High School?
  - What is your mothers maiden name?
  - What was your first car?
- Answers may be easily guessed or discovered

Provide Unexpected Answers

- Develop a personal strategy to **mutate your answer**
  - Enter it twice
  - Type it backwards
  - Append the number of characters

What was your first car?

~~chevy~~

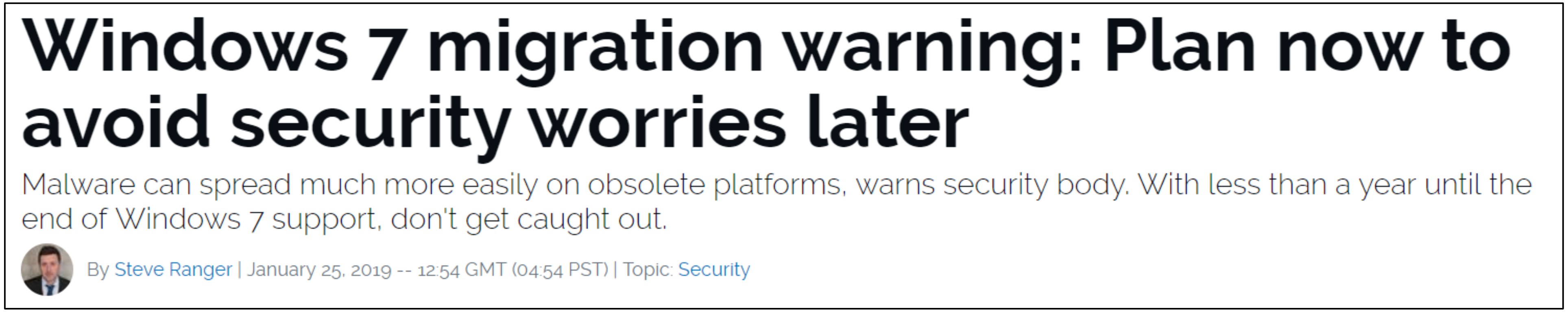
chevychevy

yvehc

chevy5

Keep Software Current

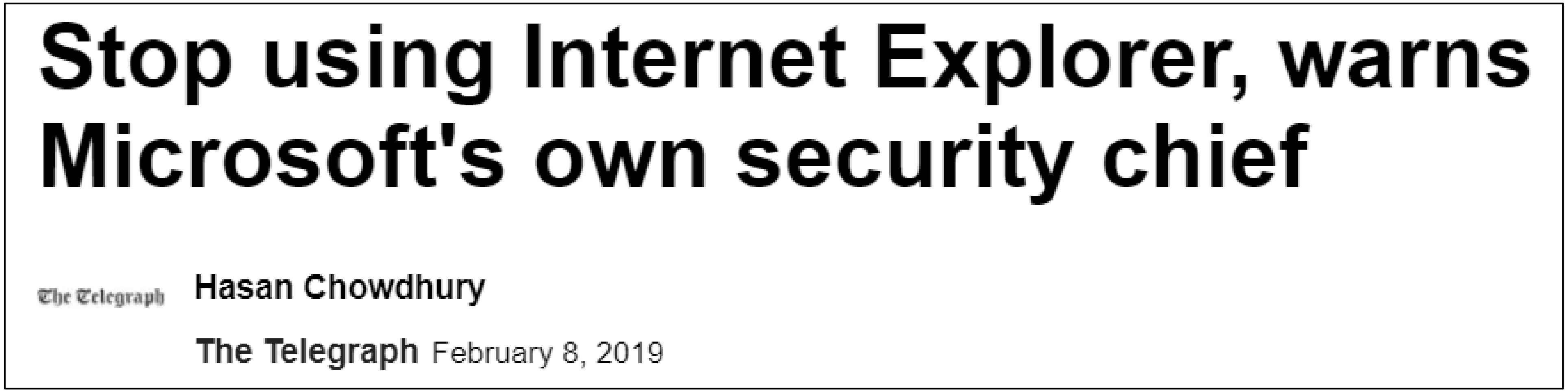
- Out of date software tends to have known vulnerabilities
- Load patches as they become available
- Fee based upgrades:
  - Best to stay current
  - Don’t let yourself fall more that one release behind



Windows 7 migration warning: Plan now to avoid security worries later

Malware can spread much more easily on obsolete platforms, warns security body. With less than a year until the end of Windows 7 support, don't get caught out.

By Steve Ranger | January 25, 2019 -- 12:54 GMT (04:54 PST) | Topic: Security



Stop using Internet Explorer, warns Microsoft's own security chief

The Telegraph

Hasan Chowdhury

The Telegraph February 8, 2019

Verify The Source!

Be sure that you are getting software upgrades from the **legitimate source**

- Don’t trust pop-up windows on the internet
- Check for updates when you are using the app
- Go to their website and check for updates

Home Phone

- National Do Not Call Registry
- Use CallerID
  - Only answer calls from people you know
- Let suspicious/unknown calls go to voicemail

Mobile/Cellular/Wireless Phone

- National Do Not Call Registry
- Keep contact list up to date
  - Only answer calls from callers you know
  - Block repeat callers who do not leave a message
- Use Provider Privacy Tools
  - AT&T: Use the **Call Protect** app (Free)
  - T-Mobile: **ScamID** (Default) & **ScamBlock** (Free)
  - Verizon: **Call Filter** ($3/month, free beginning March 2019)

Mobile/Cellular/Wireless Phone

- Load and use Apps to interact with businesses
  - Much more secure than using a browser
- Only download Apps from legitimate sources
  - Apple Store
  - Google Play Store
- Make the inactivity time required to lock your phone short
- Enable your phone’s “Find My Phone” feature

Tighten Up Mobile Phone Account Security

It is as important as you Credit Card and Bank Accounts!

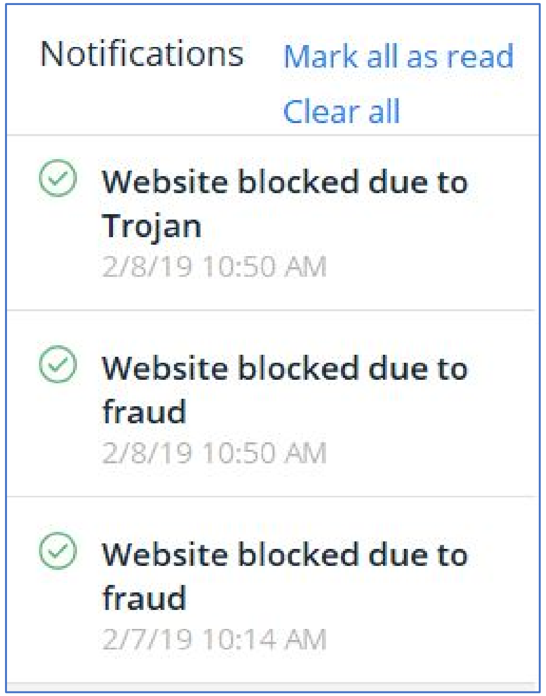
- Strong, Unique Passwords (changed often)
- Two Factor Authentication enabled
- Strong Security Question answers
- Implement any other security they offer
    - AT&T allows definition of a PIN

Suspect Sudden Cell Phone Failure

- “Slamming” cell phone accounts (unauthorized transfer of service) is becoming increasingly popular.
- Your phone number could be ported to another phone
  - Thief can use this to bypass your Two Factor Authorization

Windows User? Use Anti-Virus Software

- Windows Defender is built into the OS
  - Appears to be a good product
- Other commercial products are rated higher in some aspects of services and protection
  - Best ones appear to provide updates sooner
  - An advantage when new threats emerge
    - “Zero-Day Attacks”



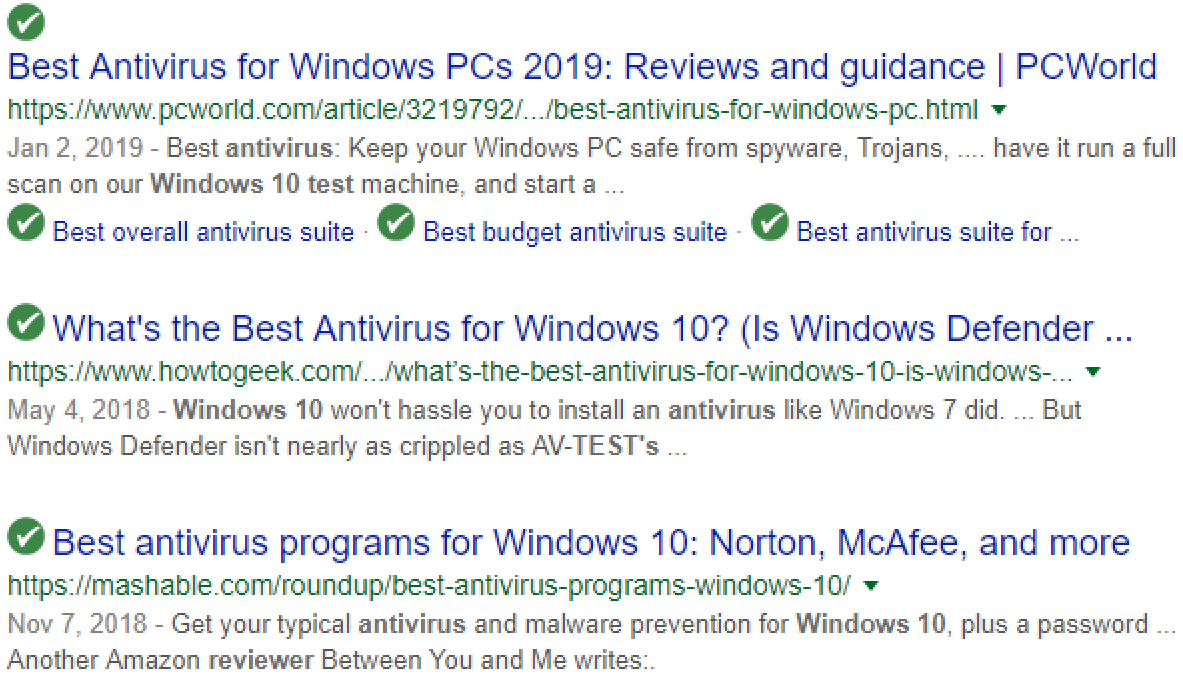
✓ Website blocked due to Trojan
2/8/19 10:50 AM

✓ Website blocked due to fraud
2/8/19 10:50 AM

✓ Website blocked due to fraud
2/7/19 10:14 AM

Which One Is The Best One?

- Google it
- Review every year
  - Consider changing if a better product becomes available



✓

Best Antivirus for Windows PCs 2019: Reviews and guidance | PCWorld

https://www.pcworld.com/article/3219792/.../best-antivirus-for-windows-pc.html ▾

Jan 2, 2019 - Best **antivirus**: Keep your Windows PC safe from spyware, Trojans, ... have it run a full scan on our **Windows 10 test** machine, and start a ...

✓ Best overall antivirus suite · ✓ Best budget antivirus suite · ✓ Best antivirus suite for ...

✓ What's the Best Antivirus for Windows 10? (Is Windows Defender ...

https://www.howtogeek.com/.../what's-the-best-antivirus-for-windows-10-is-windows-... ▾

May 4, 2018 - **Windows 10** won't hassle you to install an **antivirus** like Windows 7 did. ... But Windows Defender isn't nearly as crippled as AV-**TEST's** ...

✓ Best antivirus programs for Windows 10: Norton, McAfee, and more

https://mashable.com/roundup/best-antivirus-programs-windows-10/ ▾

Nov 7, 2018 - Get your typical **antivirus** and malware prevention for **Windows 10**, plus a password ... Another Amazon **reviewer** Between You and Me writes:.

Monitor Your Key Financial Accounts

- Review these accounts at least monthly:
  - Bank Accounts
  - Debit/Credit Card Accounts
  - Cellular Phone Accounts
- Consider using their App
- Look for questionable or fraudulent activities
  - Follow up immediately

Freeze Your Credit Reports

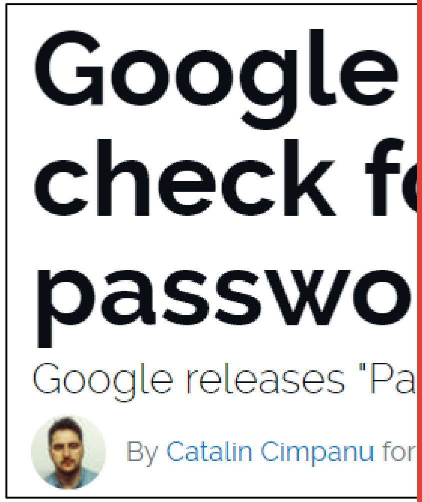
- The Big Three Credit Monitoring Companies:
  - Experian
  - Equifax
  - TransUnion
- A credit report is usually required before creditors will grant somebody credit
  - You will not normally be notified that a request has been submitted
- Freezing access to your Credit Reports may prevent somebody from establishing credit using your identity

Credit Freeze

- You need to contact each company separately to put the freeze in place
- This will be done at no cost to you (as of September 2018)
- You will need to un-freeze one of the accounts when you apply for credit

Browsers

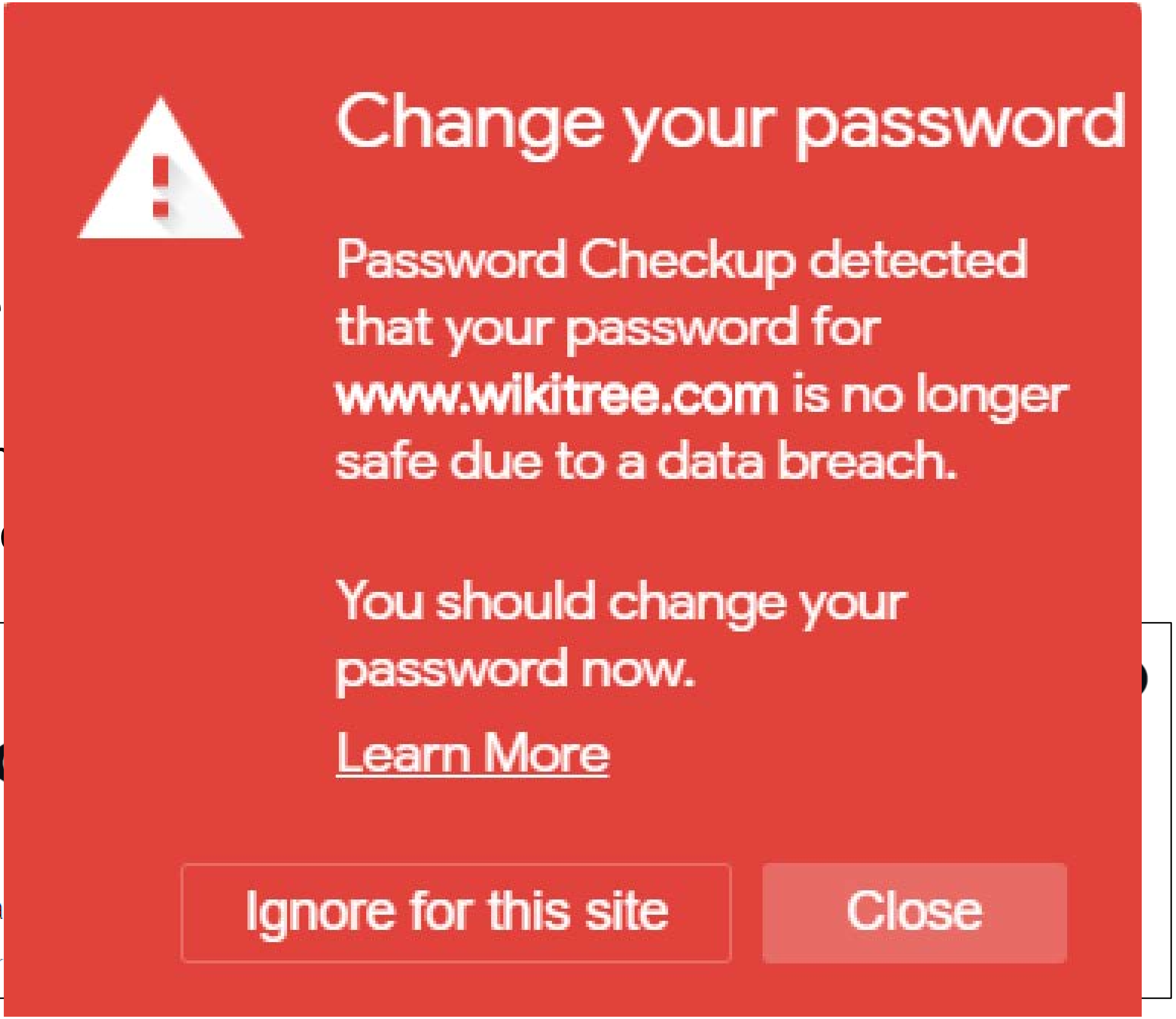
- Keep software
- Create links to
  - Use these wh
- Take advantag



Google
check f
passwo

Google releases "Pa

By Catalin Cimpanu for



Change your password

Password Checkup detected that your password for **www.wikitree.com** is no longer safe due to a data breach.

You should change your password now.

Learn More

Backups

- Good backups are your ultimate defense against a malicious virus
- You should be backing your information up 3 ways:
    - Utilize your computers native backup software
    - Pay for an online backup service such as Carbonite or Backblaze
    - Purchase a USB drive and copy files to it each month
- Be sure your SmartPhone is being backed up as well

Good Housekeeping

Malicious software is designed to search your computer to locate email and files with financial, banking and other sensitive information.

- Delete or encrypt files with sensitive information
- Delete email messages with sensitive information
  - Don’t forget your “Sent Mail” file

You Are **Not** Paranoid…

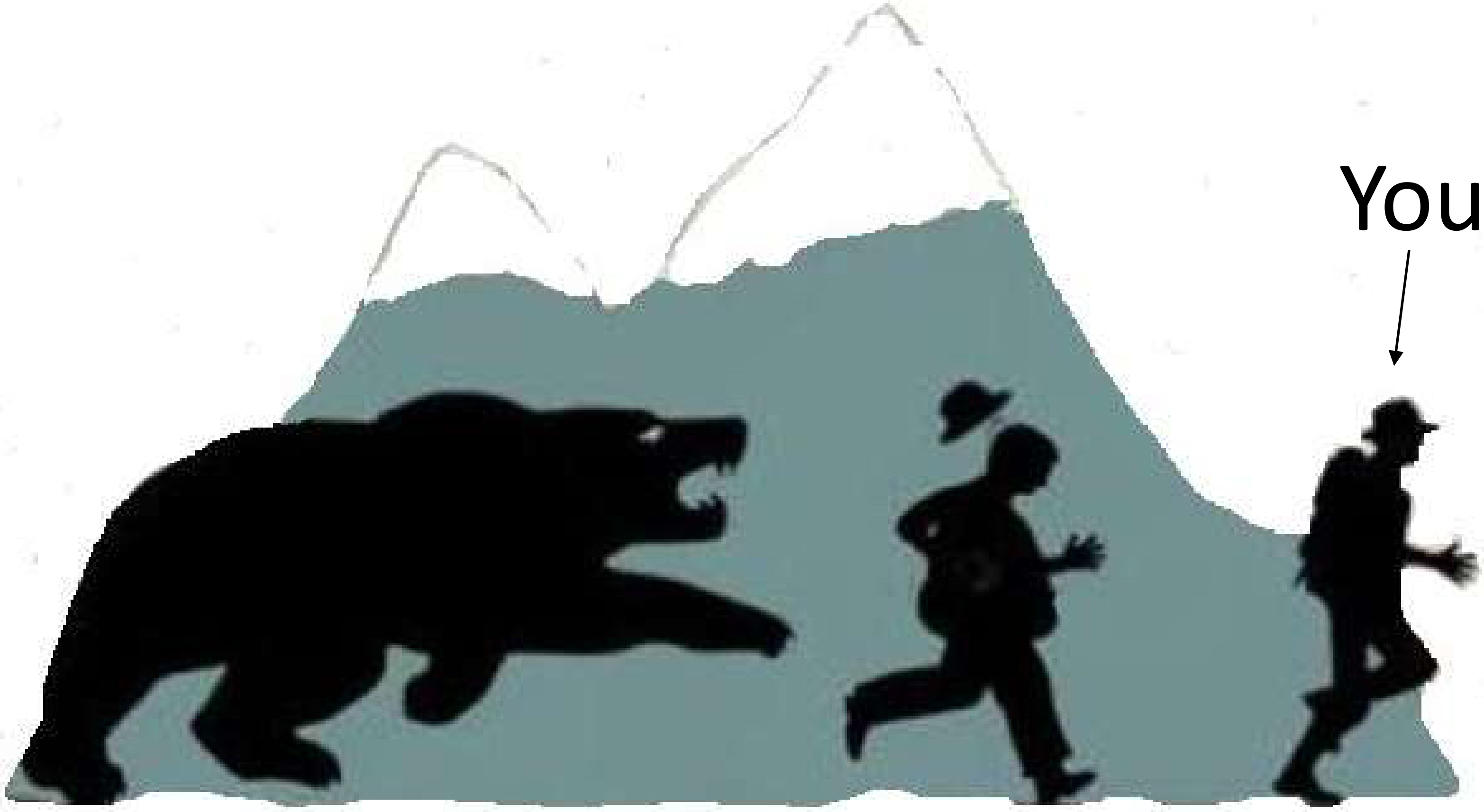
They **REALLY ARE** trying to get to you!

Summary

- Get serious about managing your passwords
- Enable 2-step authorization
- Provide weird answers to security questions
- Don’t click on suspicious links
- Use caution on public WiFi networks
- Freeze Credit Reporting
- Monitor financial and cellphone accounts
- Keep software up to date

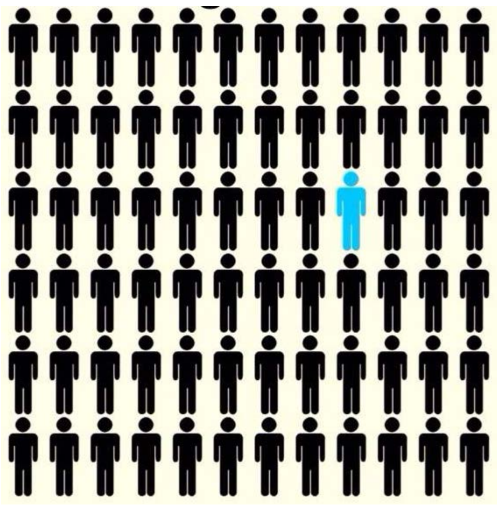
You can’t outrun a bear!

But you can outrun those around you!



Questions?

https://www.rayson.us/aehanson/presentations/current/psap/



Thank you!

PROVIDERS
STRATEGY
TRAILS
PROMOTIONS
HACKERS
DETECTION
PUBLIC
DEVICE
ISSUES
PASSWORDS
BUSINESS
LOGS
BREACH
STRATEGY
CYBER
SECURE
ATTACKS
VULNERABLE
MODEL
RESPONSE
COMPUTING
SECURITY
APPS
INSIDER
TRAILS
PROTECTION
BROWSER
PRIVACY
GOVERNMENT
MALWARE
SOFTWARE
SHARING
INFRASTRUCTURE
LEGAL
AUDIT
SECURE
INTERNET
TECHNOLOGY
NETWORK
ACCESS