

# BIG BROTHER: PROTECTING YOUR CLIENTS AND LAW PRACTICE FROM HACKERS

CHRISTOPHER B. HOPKINS  
MCDONALD HOPKINS LLC







# CHRISTOPHER B. HOPKINS



[CHOPKINS@MCDONALDHOPKINS.COM](mailto:CHOPKINS@MCDONALDHOPKINS.COM)



[@cbhopkins](https://twitter.com/cbhopkins)



[www.linkedin.com/in/cbhopkins/](https://www.linkedin.com/in/cbhopkins/)

[InternetLawCommentary.com](http://InternetLawCommentary.com)





From: **Shawn M. Riley** >



To: **Christopher Hopkins** >

Hide

---

## Re: Request

Today at 8:12 AM

---

Can you help me with a quick task please?



# McDonald Hopkins elects Shawn M. Riley as its next president

CRAIN'S CLEVELAND BUSINESS

TWEET

f SHARE

in SHARE

EMAIL

PRINT



Cleveland law firm [McDonald Hopkins LLC](#) will have a new president this fall.

The business advisory and advocacy firm said it has elected Shawn M. Riley as president, effective Oct. 1. Carl J. Grassi, the firm's current president, will become chairman and will remain on the Executive Committee, according to a [news release](#). The firm said in the release that when Riley becomes president, Grassi will have served for more than nine years as president, a position that is term-limited. "This is a carefully crafted transition that has been in the planning stages for quite some time," Grassi said in a statement. "Shawn has been an essential part of our leadership team during my tenure as president. He is dedicated to the success of our clients, our firm and our communities. We strongly believe in collaboration and the transition will be a smooth one." Riley joined McDonald Hopkins in 1995. Since 2007, he has served as managing member of the Cleveland office and has been a



From: **Shawn M. Riley** >



To: **Christopher Hopkins** >

Hide

---

## Re: Request

Today at 8:12 AM

---

Can you help me with a quick task please?





Shawn M. Riley



message



call



video



mail

other

[leonardx8@triad.rr.com](mailto:leonardx8@triad.rr.com)



Cancel

Re: Request

Send




To: Shawn M. Riley



Cc/Bcc, From: chopkins@mcdonaldhopkins.com

Subject: Re: Request

|



On May 27, 2019, at 8:12 AM, Shawn M. Riley <leonardx8@triad.rr.com> wrote:

Can you help me with a quick task please?

That is a  
“Business Email Compromise”  
Attack



# Let's Spot The Fakes!

*(with remote working, business email compromise attacks  
are more likely)*

From: [Jessica Bloomfield](#) >

To: [Christopher Hopkins](#) >

[Hide](#)



## **Litigation representative required**

Today at 4:22 PM

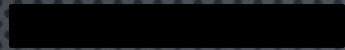
Hello,

My name is Jessica Bloomfield . I would like to retain your firm on a civil litigation matter . Kindly advice if you can take my case.Please let me know if i should send supporting documents so you can review to understand .

Thanks

J.Bloomfield





Jessica Bloomfield



message



call



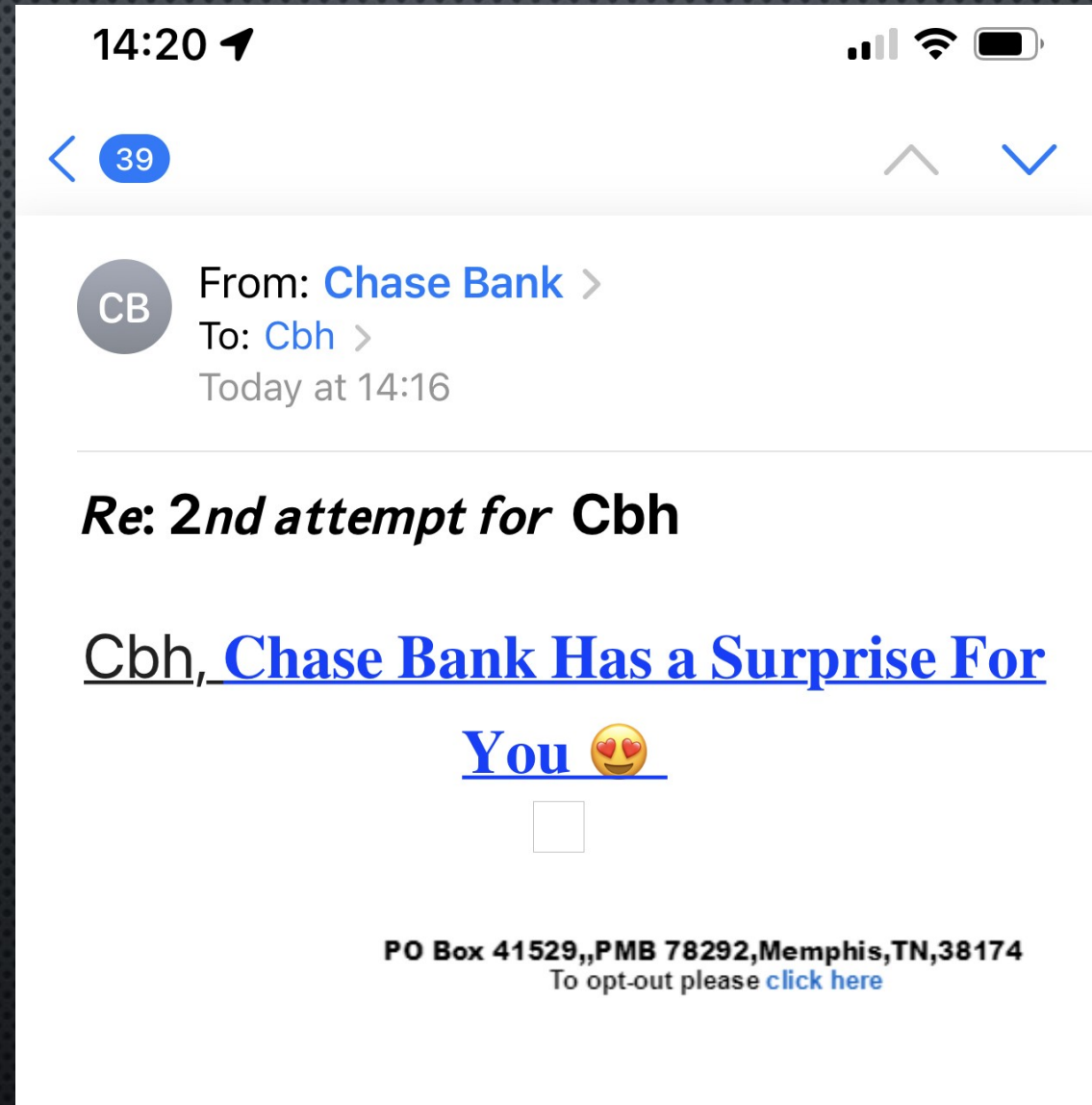
video



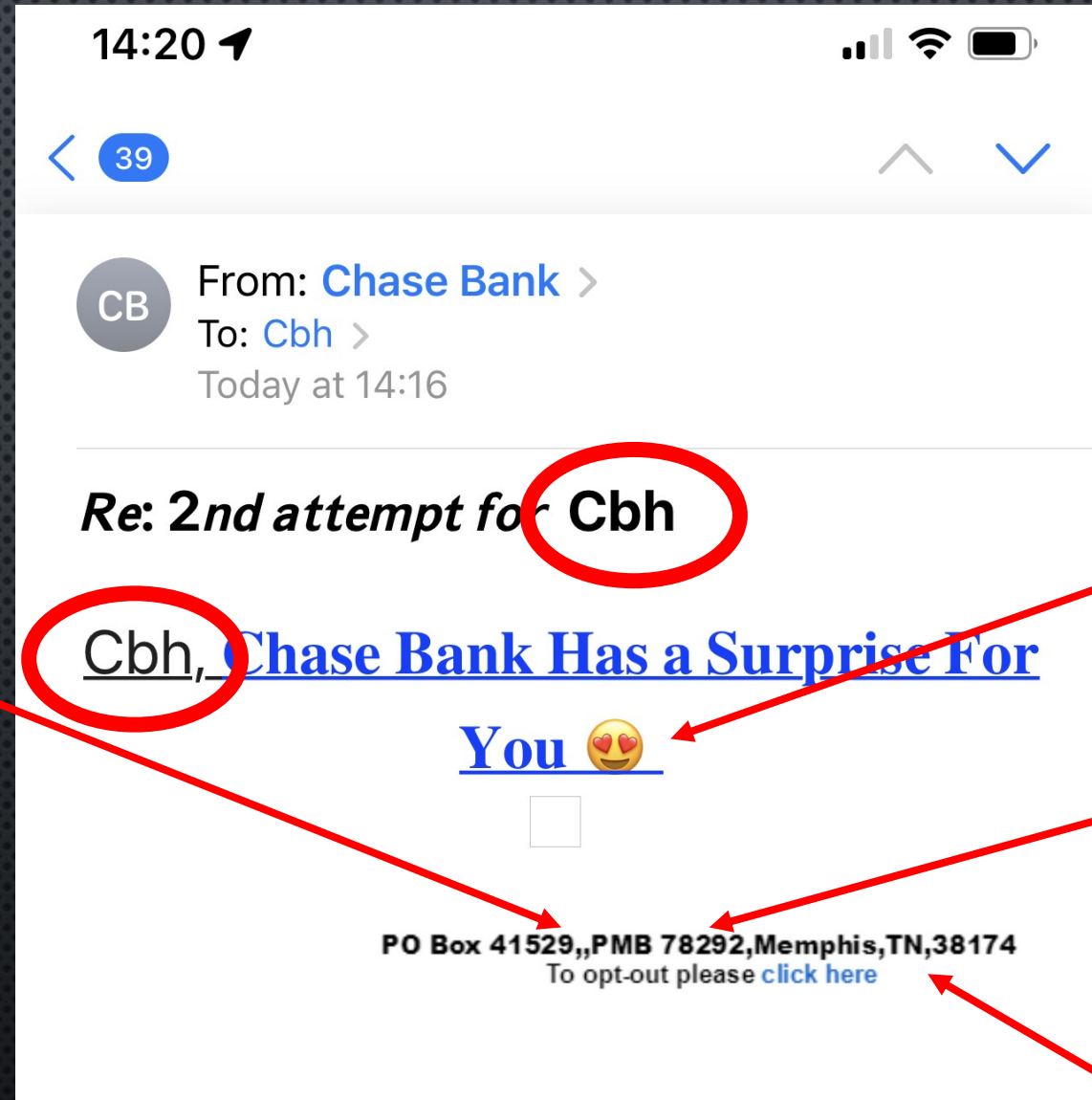
mail

other

[anglais@evoice.co.uk](mailto:anglais@evoice.co.uk)







typos

They don't  
love me that  
much

"Private Mail  
Box" gives  
you a street  
address so  
you don't  
use a PO Box

No spacing

# How many people respond??



+1 (561) 599-5794 >

Text Message  
Today 19:21

Sorry I missed the event! Maybe this  
can make up for it!





File

Message

Developer

Kofax PDF

Ignore

X

Junk

Delete

Reply

Reply All

Forward

More

Meeting

More

00 Gary West

Team E-mail

Reply & Delete

To Manager

Done

Create New

Move

Move

Rules

OneNote

Actions

Assign Policy

Mark Unread

Categorize

Follow Up

Tags

Translate

Find

Related

Select

Editing

From: Evan Daniels <corporatenotify@x.blackhawkgoldllc.com>

To: Hopkins, Christopher

Cc:

Subject: [External] RE: termination, Hopkins

Sent: Tue

Hopkins, **why i can't reach you on the phone? I am on my way to Mc Donald Hopkins.**

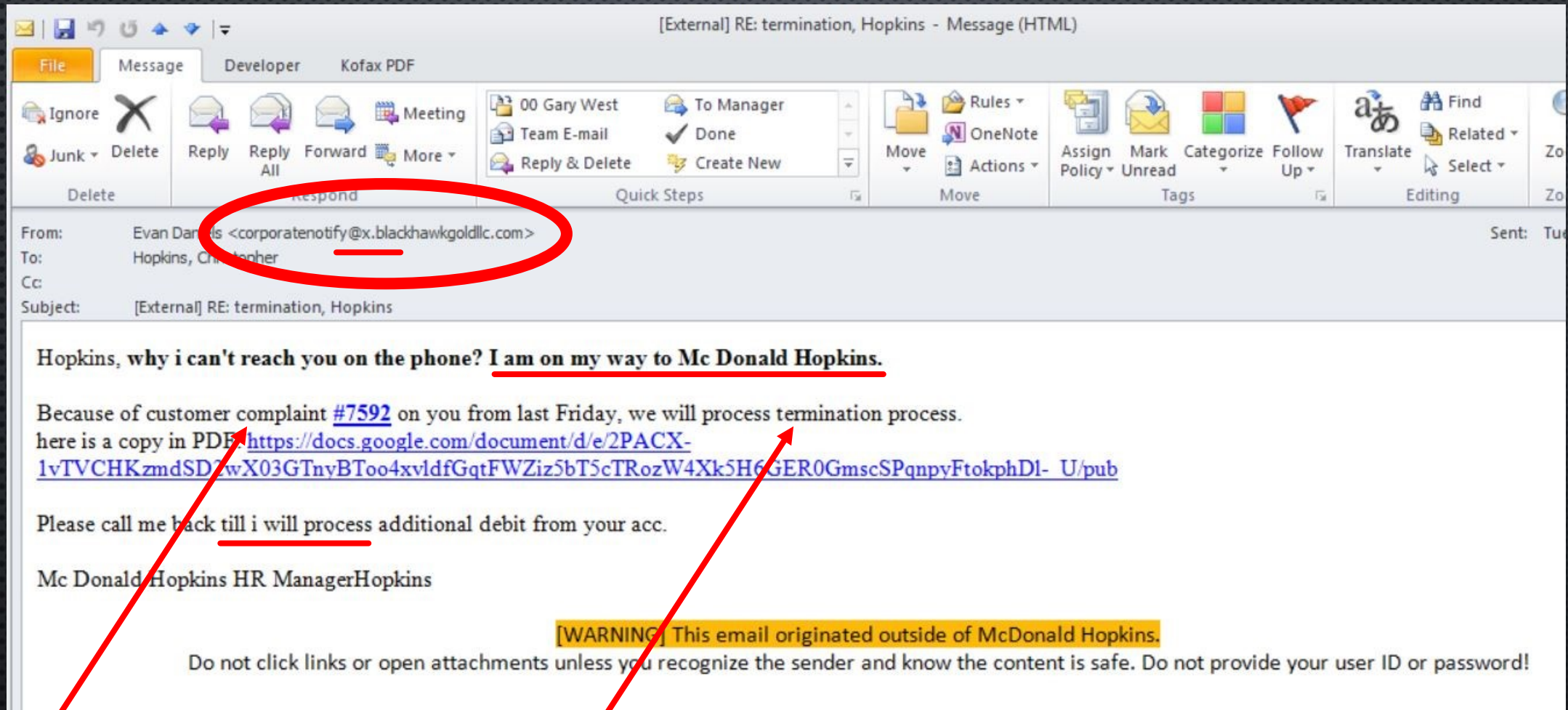
Because of customer complaint [#7592](#) on you from last Friday, we will process termination process.  
here is a copy in PDF: <https://docs.google.com/document/d/e/2PACX-1vTVCHKzmdSD2wX03GTnyBToo4xvldfGqtFWZiz5bT5cTRozW4Xk5H6GER0GmscSPqnpyFtokphDl-U/pub>

Please call me back till i will process additional debit from your acc.

Mc Donald Hopkins HR ManagerHopkins

**[WARNING] This email originated outside of McDonald Hopkins.**

Do not click links or open attachments unless you recognize the sender and know the content is safe. Do not provide your user ID or password!



Urgency is a hallmark  
of a scam





Fri 1/7/2022 10:52 AM

chopkins - Notifications <abessette@unitedscc.com>

[External] Scheduled Payment Notification

To Hopkins, Christopher



✉-chopkins.pdf.shtml

177 KB

### Action Items

This Message Is Trusted By mcdonaldhopkins.com

Kindly review the attached document for payment.

Document secured for chopkins

File name: ✉-chopkins.pdf

Sender: 16456473342

For Recipient: [chopkins@mcdonaldhopkins.com](mailto:chopkins@mcdonaldhopkins.com)

Encrypted By mcdonaldhopkins.com

---

**NEC SL4273 SharePoint**

This email was sent to [chopkins@mcdonaldhopkins.com](mailto:chopkins@mcdonaldhopkins.com).

## Step 1: Identify a Target



Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

## Step 2: Grooming



Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

## Step 3: Exchange of Information



The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

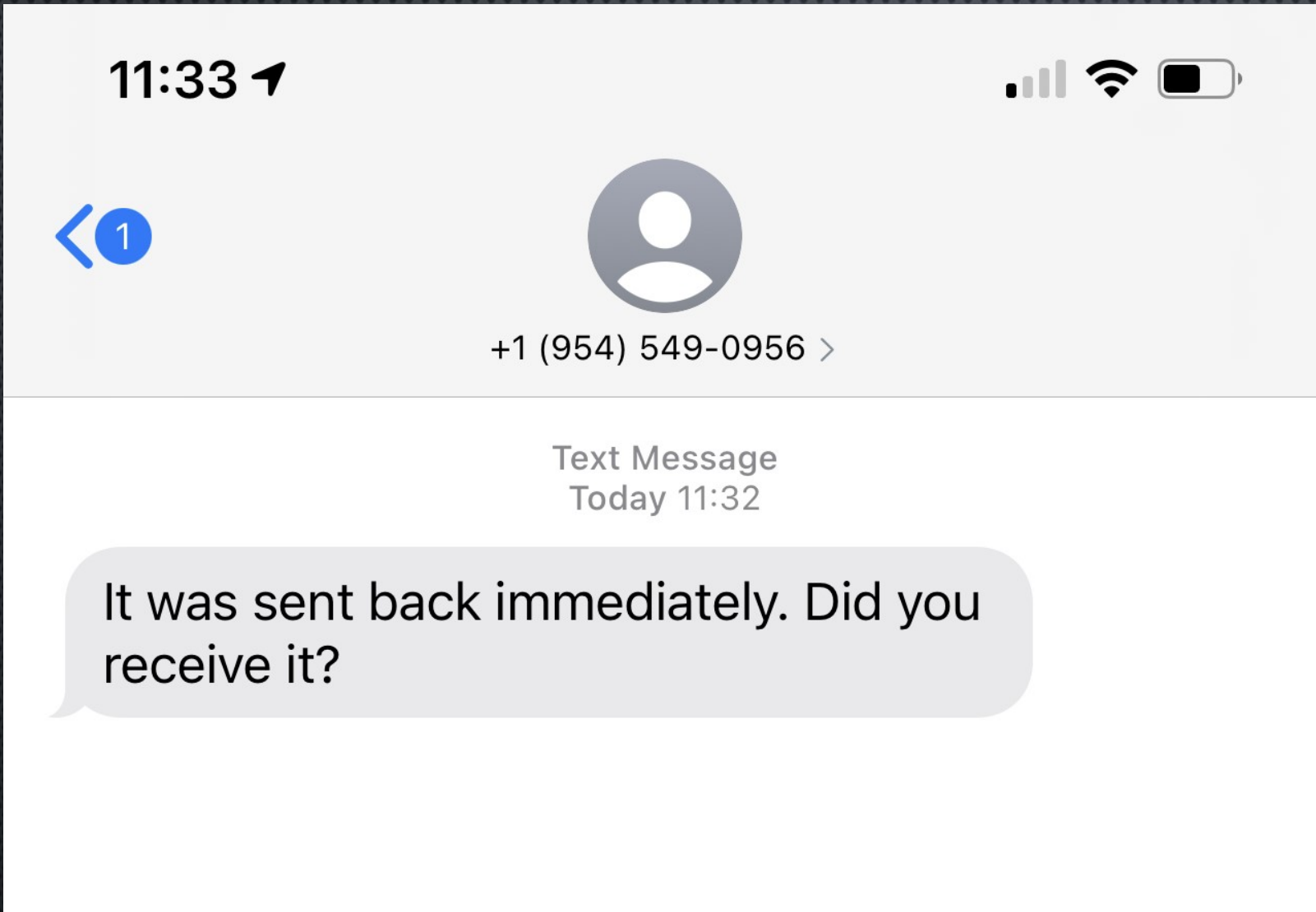
## Step 4: Wire Transfer



Upon transfer, the funds are steered to a bank account controlled by the organized crime group.\*

\*Note: Perpetrators may continue to groom the victim into transferring more funds.





Don't respond to  
unknown  
numbers or  
texts...

**Final note: watch out for emails which looks like discussions**

< Yahoo!
 Edit

# Inbox

---

me, Alex (2)

cbh01@yahoo.com

18:40 >

...

---

●

Daily Business Review Breakin...

Meet the New Justice: After Opposition, Florida Go...

View in Browser

Daily Business Review Breaking News Sep 14, 202...

18:09 >



# Ways To Get Hacked

*(let's talk about that wifi you're connected to...)*



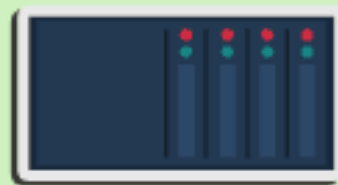


# WiFi Pineapple

## (Man In The Middle Attack)

# MIDDLE IN THE MIDDLE ATTACK EXAMPLE

## NORMAL CONNECTION



SERVER



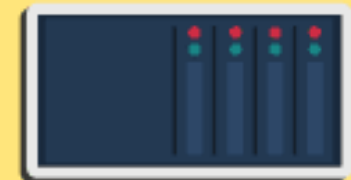
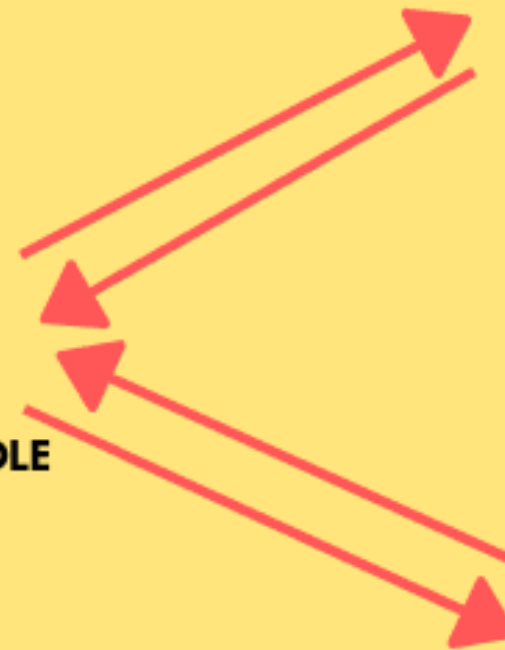
CLIENT



## MAN IN MIDDLE CONNECTION



MAN IN THE MIDDLE



SERVER



CLIENT



# HAK5

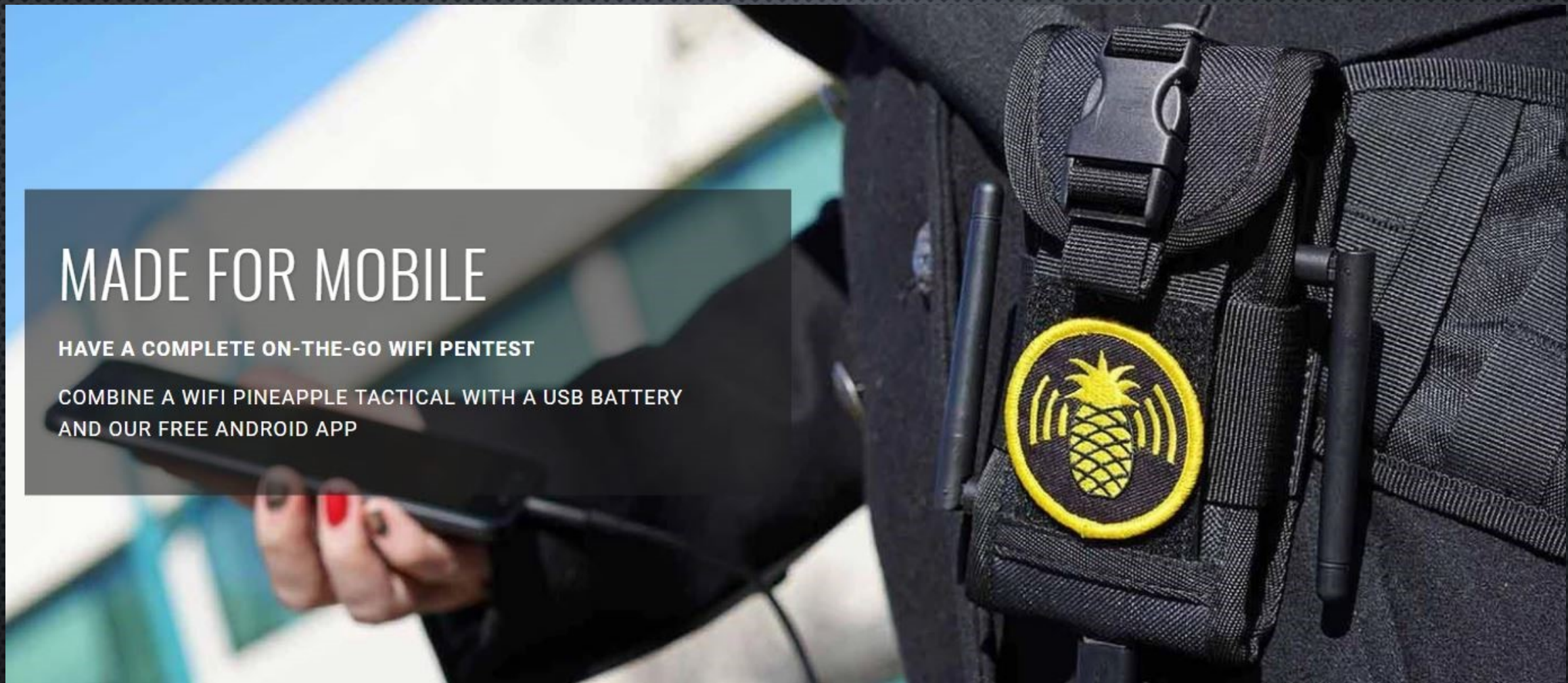




# MADE FOR MOBILE

HAVE A COMPLETE ON-THE-GO WIFI PENTEST

COMBINE A WIFI PINEAPPLE TACTICAL WITH A USB BATTERY  
AND OUR FREE ANDROID APP









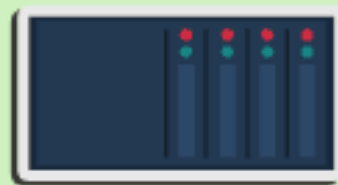
Your device  
is looking  
for familiar  
WiFi





# MIDDLE IN THE MIDDLE ATTACK EXAMPLE

## NORMAL CONNECTION



SERVER

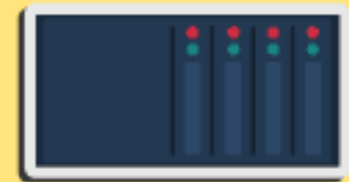
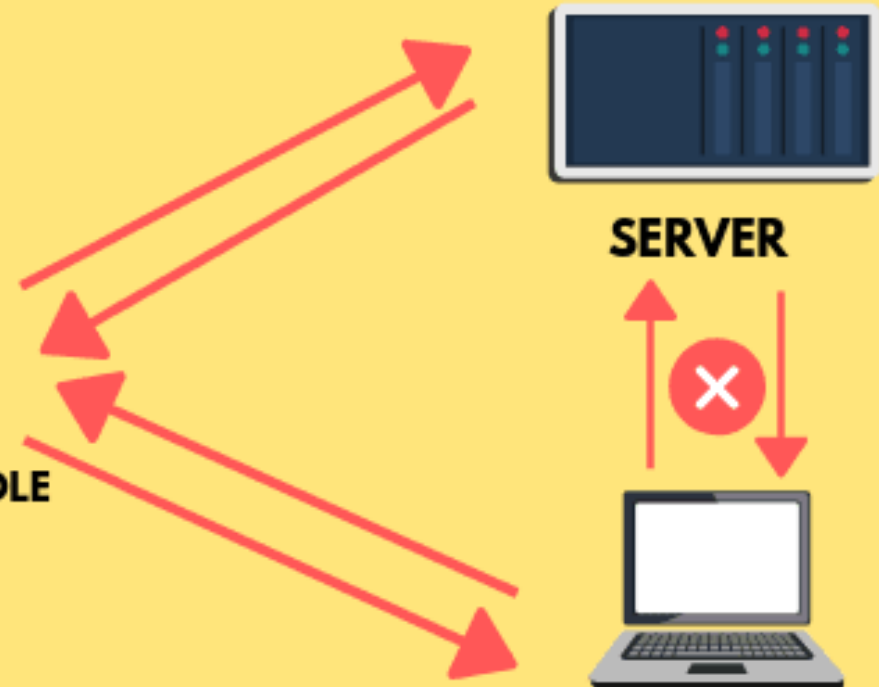


CLIENT

## MAN IN MIDDLE CONNECTION



MAN IN THE MIDDLE



SERVER



CLIENT



Dashboard

Recon

Clients

Filters

Modules ▾

PineAP

Tracking

Logging

Reporting

Networking

Configuration

Advanced

Help

0 hours, 20 minutes

UPTIME

50% CPU USAGE

27

CLIENTS CONNECTED

141

SSIDS IN POOL

0 SSIDS ADDED THIS SESSION

## Landing Page Browser Stats

 Chrome	93
 Firefox	17
 Internet Explorer	8
 Opera	0
 Safari	41
Other	81

## Notifications

No Notifications

## Bulletins

[Load Bulletins from WiFiPineapple.com](#)



**MARK VII BASIC**  
\$109.99

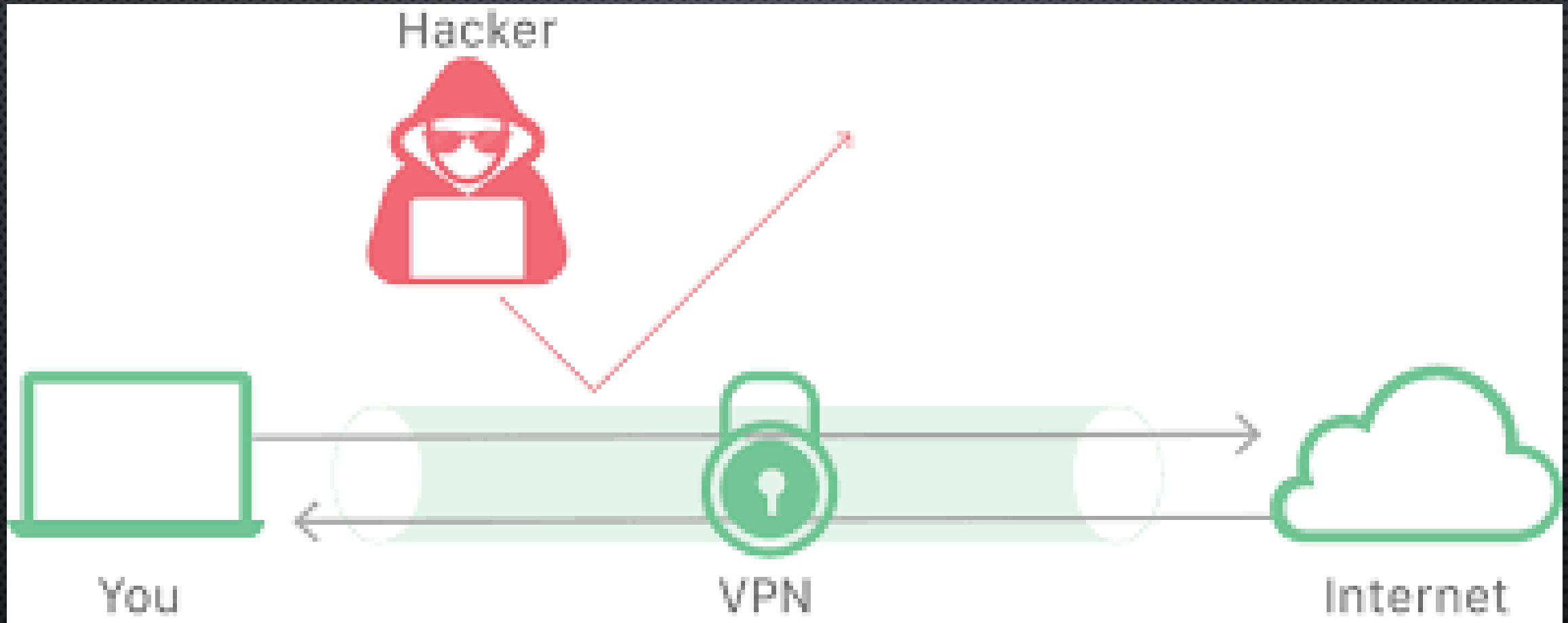


**MARK VII+AC TACTICAL**  
\$199.99

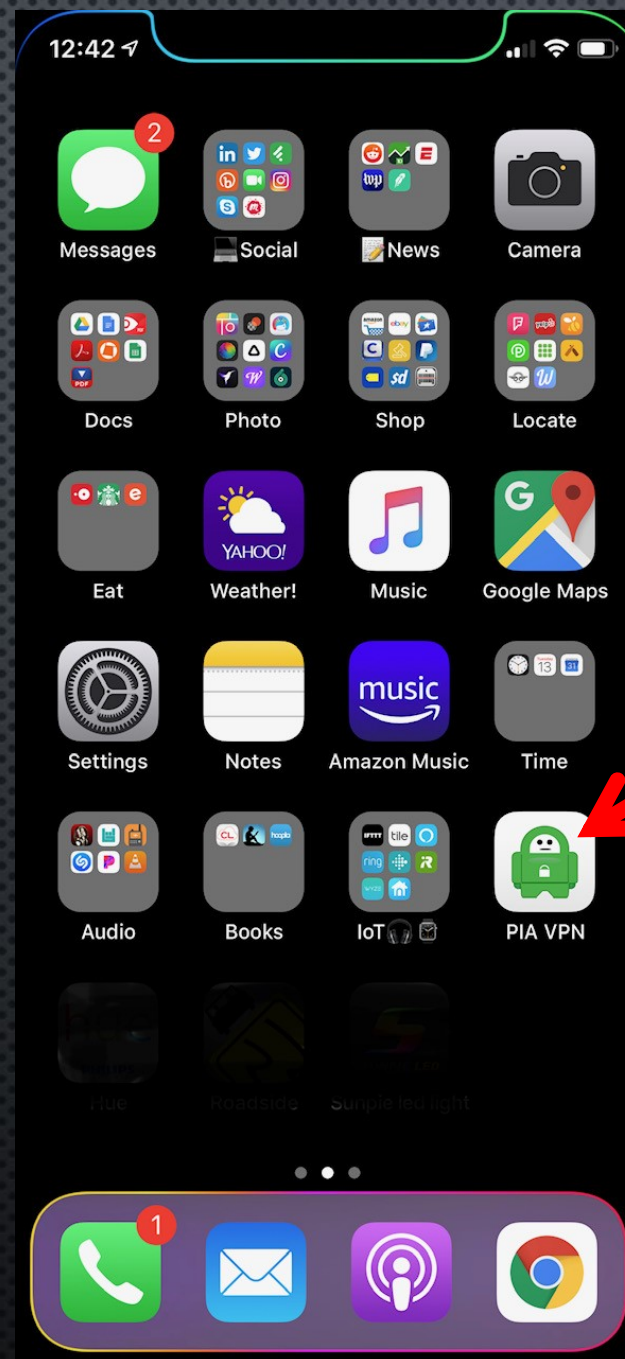


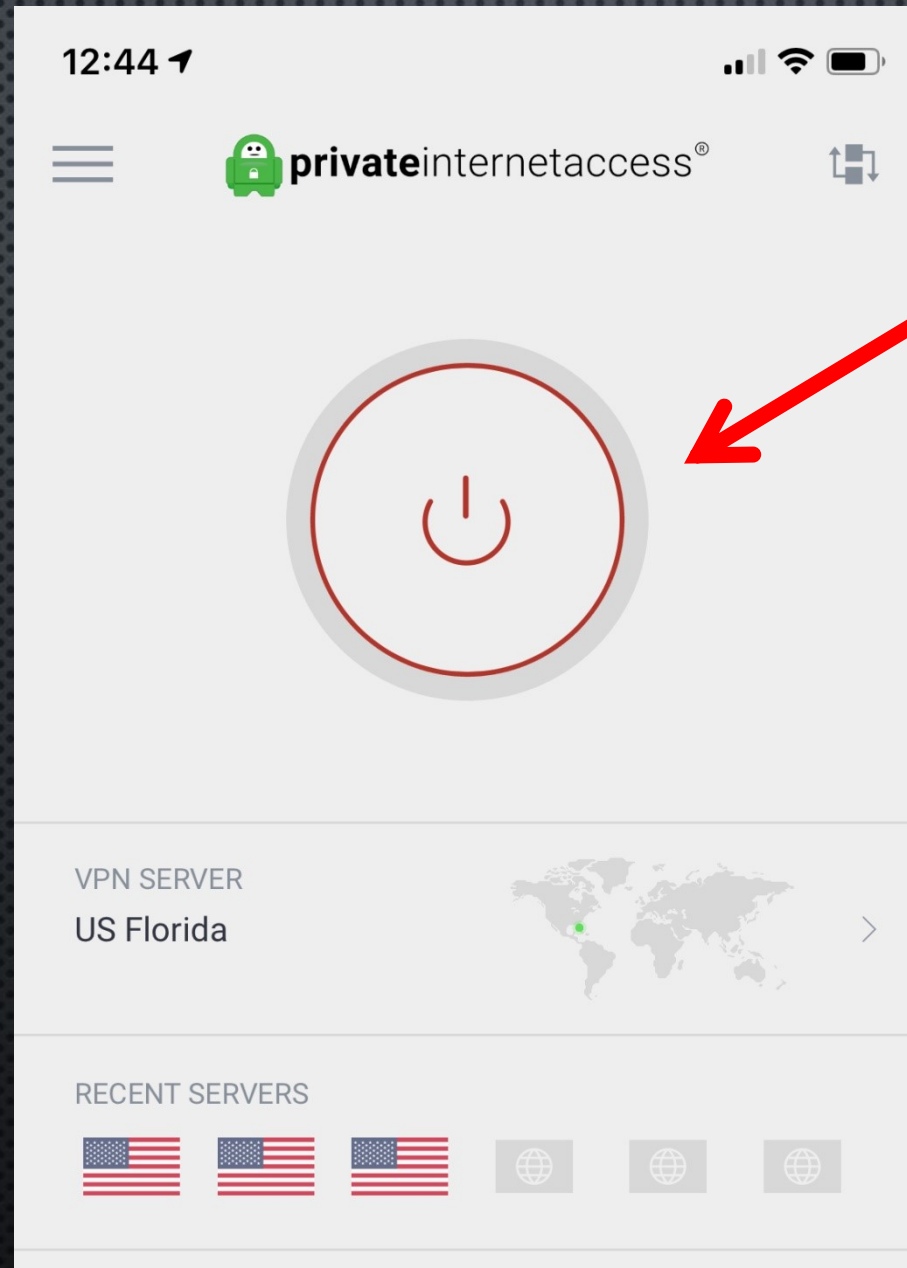
# SOLUTION:

# Virtual Private Network (VPN)

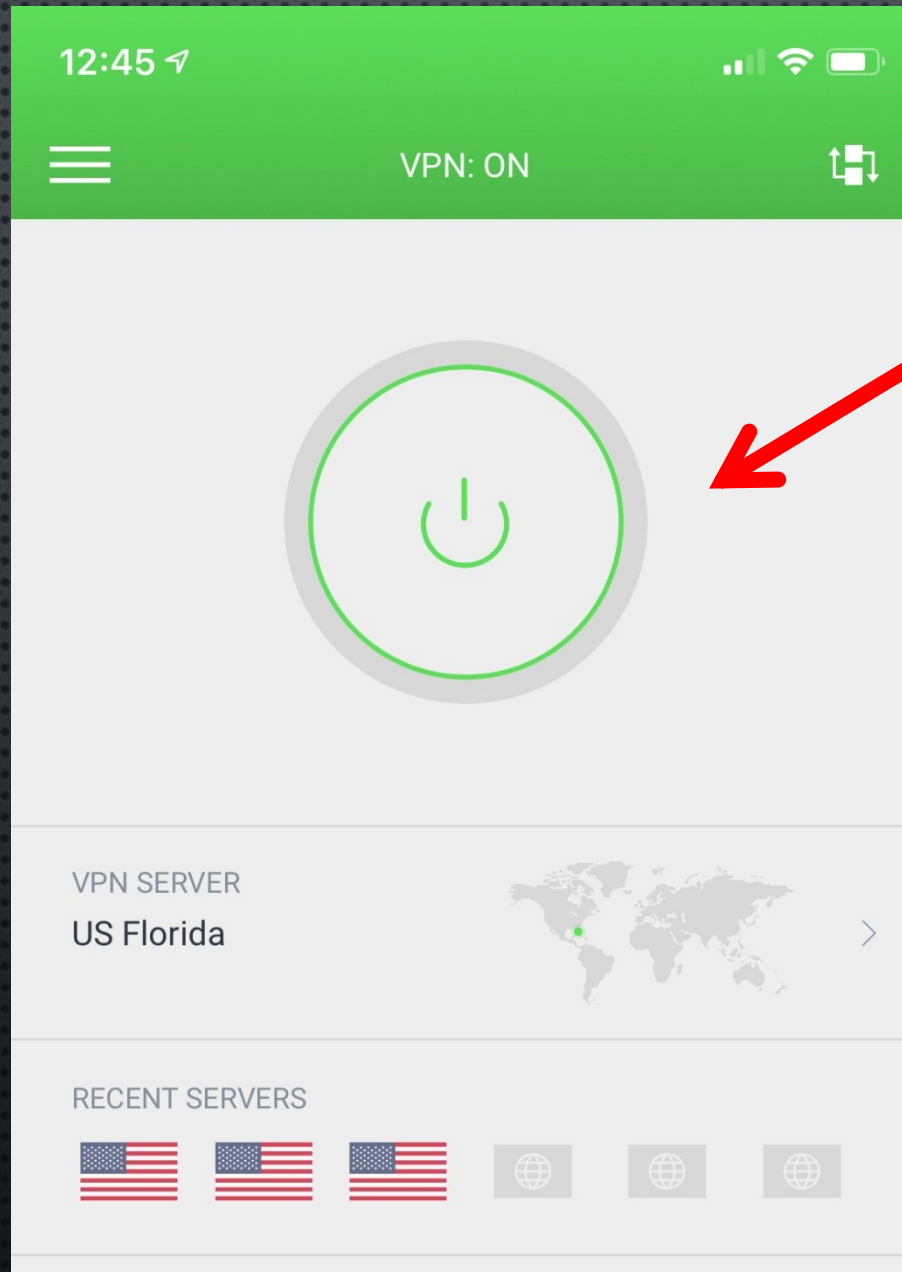












12:44



# Settings



Christopher Hopkins

Apple ID, iCloud, iTunes & App Store



Airplane Mode



Wi-Fi

MH >



Bluetooth

On >



Cellular



VPN





# PART III

## Case Examples



# Business Email Compromise Cases



# #1



**From:** .  
**Sent:**  
**To:**  
**Cc:**  
**Subject:** pending invoices  
**Importance:** High

Hello

Kindly cancel the payment because I stated to my email earlier today to that we can't receive payment to our account details which you have on records due to some issue which we have with the account currently.

So, kindly cancel the payment and let me know once it has been cancelled so that I can provide you with our updated ACH account details for payment.

Awaiting your urgent response!

# #1



**From:** .  
**Sent:**  
**To:**  
**Cc:**  
**Subject:** pending invoices  
**Importance:** High

**Email came from legit address!**

**What are the warning signs?**

**How avoid the risk?**

Hello

Kindly cancel the payment because I stated to my email earlier today to that we can't receive payment to our account details which you have on records due to some issue which we have with the account currently.

So, kindly cancel the payment and let me know once it has been cancelled so that I can provide you with our updated ACH account details for payment.

Awaiting your urgent response!

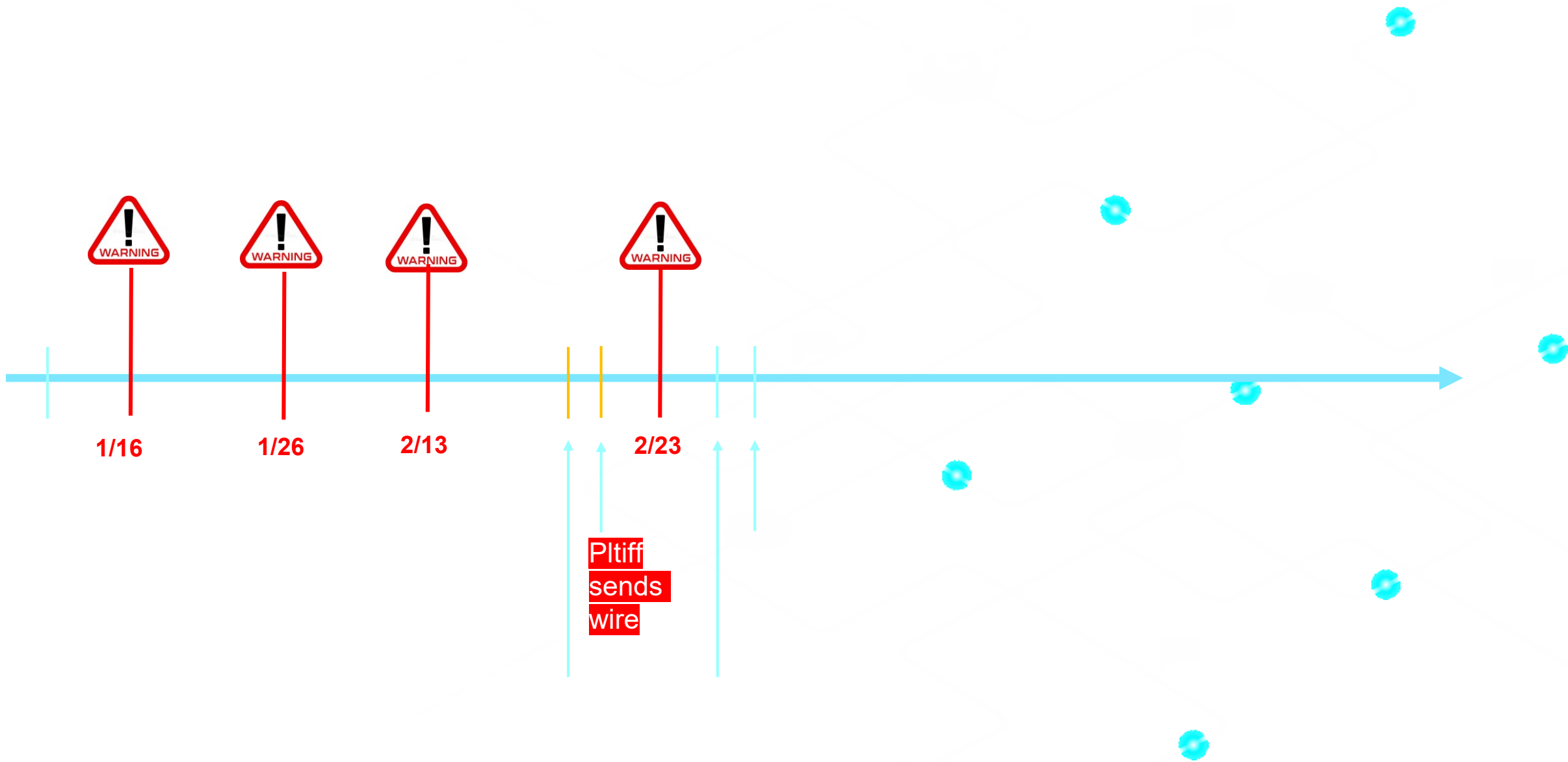


# Warnings at bottom of emails?

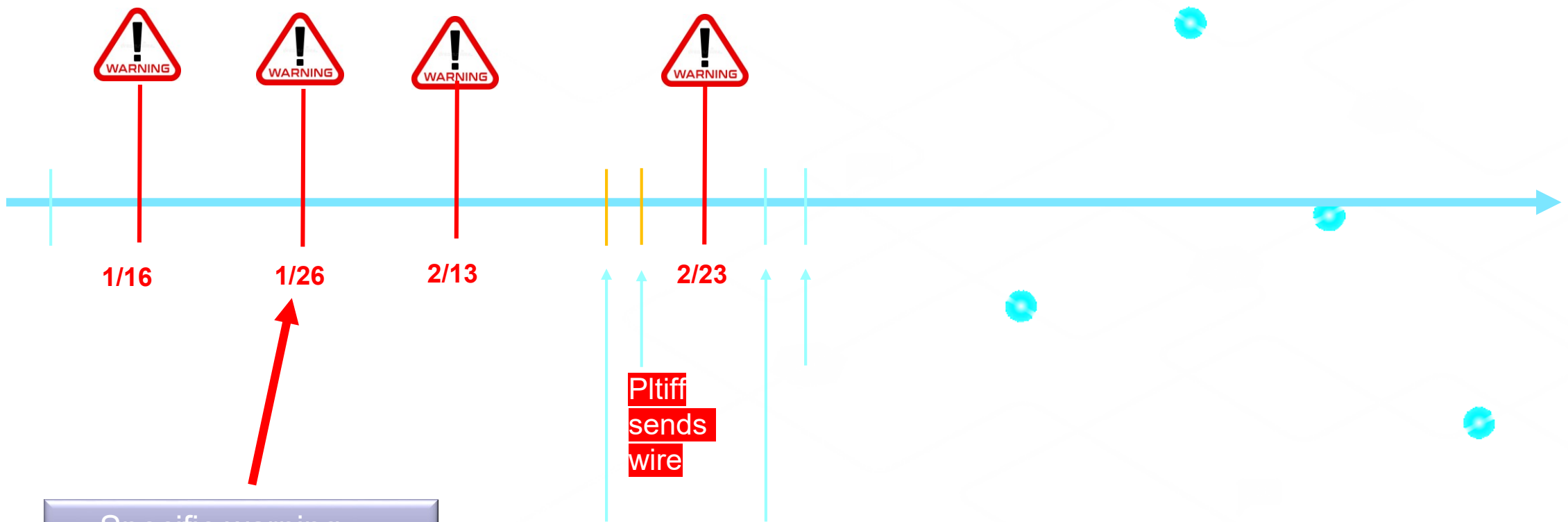
*Are these warnings in the signature block  
good enough??*



*\*\*\* Due to the risk of cyber threats, prior to wiring or depositing monies into our account, please call our office to verbally verify wiring instructions.*







- Specific warning
- In body of email

Good afternoon

Our office is facilitating the closing for . In order to start preparing closing documents, please send me the following information at your earliest convenience.

1. Your mailing address after closing (*where you would like the deed, tax bill, etc. sent*);
2. Confirm your marital status;
3. Confirm how you are taking title. Please select, sign and send back the attached title vesting sheet;
4. Will this be your primary residence?;
5. Are you able to come to our office to close? .
6. Please sign and send back the attached survey authorization; and
7. Please provide me the name and contact information for the Lender you are using.

**\*\*All funds due at closing will need to be wired to our account, wiring instructions will be sent once we have confirmed the final cash to close amount. For your protection, please call our office before sending any wires.**

Thank-you for your help and when we get closer to closing we will arrange with you the signing of closing documents. Please call or email with any questions. We look forward to a smooth transaction.





20. Upon information and belief, an unknown third party hacked into one or more email accounts used by Defendant to gain information about the real estate transaction and then used that information in order to realistically spoof the Defendant's email account and send fraudulent wire transfer instructions to the Plaintiffs. The wire transfer instructions directed Plaintiffs to transfer money to a bank account controlled by the unknown party.

2. Relative to the allegations in paragraph of the Complaint, please identify any person(s) with personal knowledge that "an unknown third party hacked into one or more email accounts used by the Defendant..."

**ANSWER: Plaintiffs have not identified any individual with personal knowledge of the facts alleged, however discovery is ongoing.**



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

# ';--have i been pwned?

Check if your email or phone is in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)


[Home](#)
[Notify me](#)
[Domain search](#)
[Who's been pwned](#)
[Passwords](#)
[API](#)
[About](#)
[Donate !\[\]\(6059a5aa8b4ca7bb793408023d6c6e42\_img.jpg\) !\[\]\(d293b9aef7d8767760396289fbc64e8a\_img.jpg\)](#)

# ';--have i been pwned?

Check if your email or phone is in a data breach

pwned?



**Good news — no pwnage found!**

No breached accounts and no pastes (subscribe to search sensitive breaches)



# ';--have i been pwned?

Check if your email or phone is in a data breach

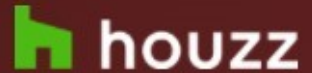
plaintiff@email.com

pwned?



Oh no — pwned!

Pwned in 9 data breaches and found no pastes (subscribe to search sensitive breaches)



**Houzz:** In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

**Compromised data:** Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames



## Thieves Fool Plaintiff into Sending Wire

Your closing disclosure has been finalized and we're clear to close, You need to have the cash to close wire to our trust account today to avoid closing delay let me know if you can take care of it so i can forward you the wiring instructions.

yes we are ready to send wire. Need amount and where/who to

See attached wiring instructions, when will wire be sent so i can watch for it.

Good morning,  
Has wire been sent?

Yes, I just got home.



## Hours Later Via SMS, Plaintiff TELLS Realtor!

Plaintiff



Realtor

The wire transfer  
has been made  
and confirmed  
by the closing  
agent.



## Hours Later Via SMS, Plaintiff TELLS Realtor!

**Plaintiff**



**Realtor**

It looks like the closing won't happen until Monday. Will you be back by then?



## Hours Later Via SMS, Plaintiff TELLS Realtor!

**Plaintiff**



**Realtor**

Yes, but Monday  
is my  
anniversary... I  
would push for  
possibly Tues or  
Wed closing



## Hours Later Via SMS, Plaintiff TELLS Realtor!

**Plaintiff**



**Realtor**

Ok, are you guys  
having fun? 😊



## Hours Later Via SMS, Plaintiff TELLS Realtor!

**Plaintiff**



**Realtor**

We're doing our best little added stress with this file to closing on time but it's fun



## ONE WEEK LATER

Plaintiff



Realtor

...should reach  
out to you shortly  
about how much  
money to wire...



## ONE WEEK LATER

Plaintiff



Realtor

Money was  
wired last week



## ONE WEEK LATER

Plaintiff



Realtor

No, you didn't  
wire any money  
to the title  
company...



# ONE WEEK LATER

Plaintiff



Realtor

Yes I did ?!?!?



## ONE WEEK LATER

Plaintiff



Realtor

[That company]  
doesn't even  
handle the wire  
and they have  
multi-layered  
system where  
they call you..



## ONE WEEK LATER

Plaintiff

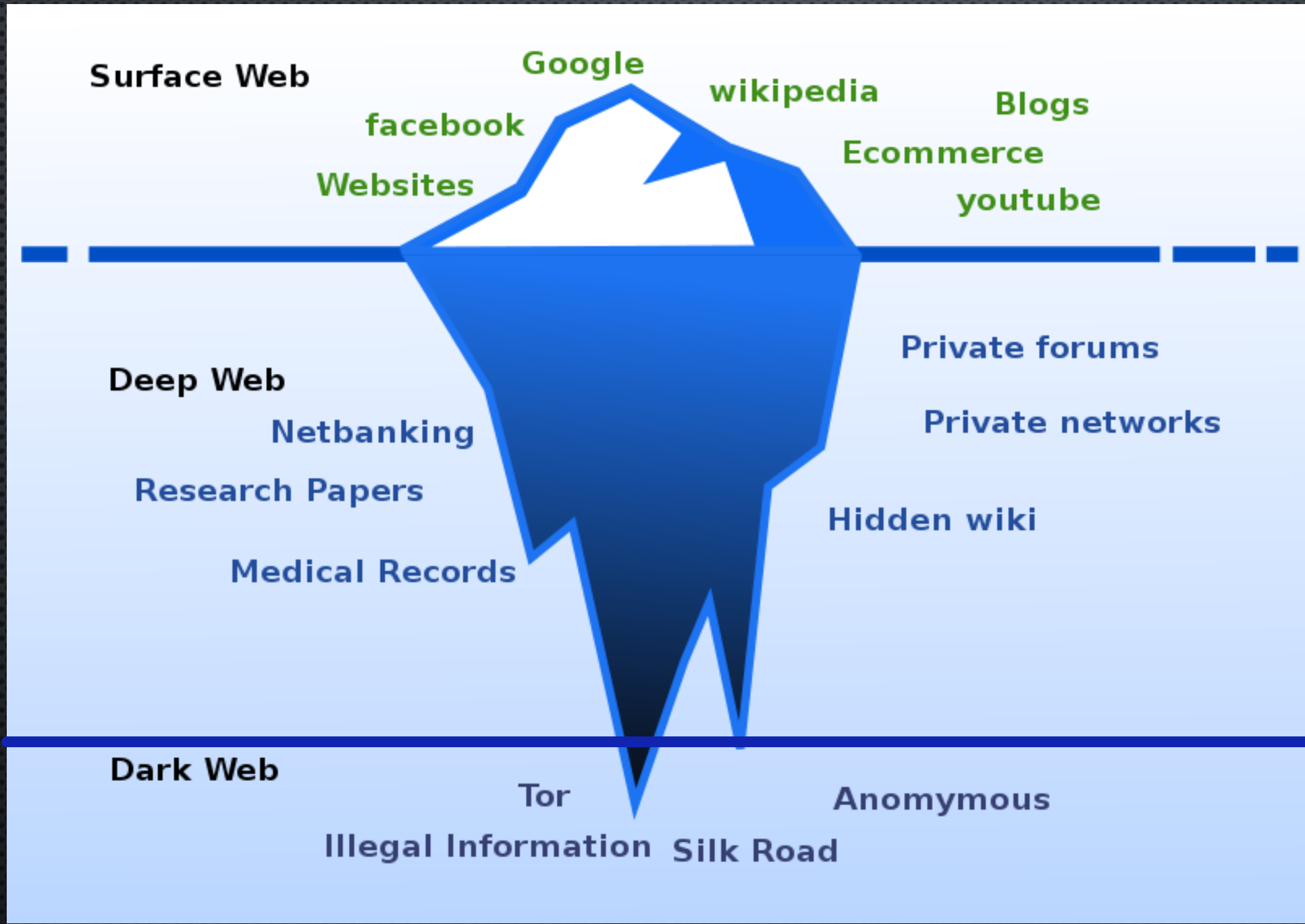


Realtor

We've got a  
problem... that's  
not even their  
real email  
address



# Quick Side Trip to The Dark Web





## Surface Web

Google  
facebook  
Websites  
wikipedia  
Ecommerce  
Blogs  
youtube

- “Regular internet”
- Clear web
- Clear net

## Deep Web

Netbanking  
Research Papers  
Medical Records  
Private forums  
Private networks  
Hidden wiki

## Dark Web

Tor  
Anomymous  
Illegal Information  
Silk Road

## Surface Web

Google  
facebook  
Websites  
wikipedia  
Blogs  
Ecommerce  
youtube

- “Regular internet”
- Clear web
- Clear net

## Deep Web

Netbanking  
Research Papers  
Medical Records

Private forums

Private networks

Hidden wiki

- Deep Web
- SE do not index
- Really big!
- If you log into acct, it's likely DW

## Dark Web

Tor  
Illegal Information  
Silk Road  
Anonymous



## Surface Web

Google  
facebook  
Websites  
wikipedia  
Ecommerce  
Blogs  
youtube

- “Regular internet”
- Clear web
- Clear net

## Deep Web

Netbanking  
Research Papers  
Medical Records

Private forums

Private networks

Hidden wiki

- Deep Web
- SE do not index
- Really big!
- If you log into acct, it's likely DW

## Dark Web

Tor  
Illegal Information  
Silk Road  
Anonymous

- Dark Web
- “Overlay Network”
- Not illegal to access
- Requires Tor

www.TorProject.org



Donate Now

[About](#) [Documentation](#) [Support](#) [Community](#) [Blog](#) [Donate](#)

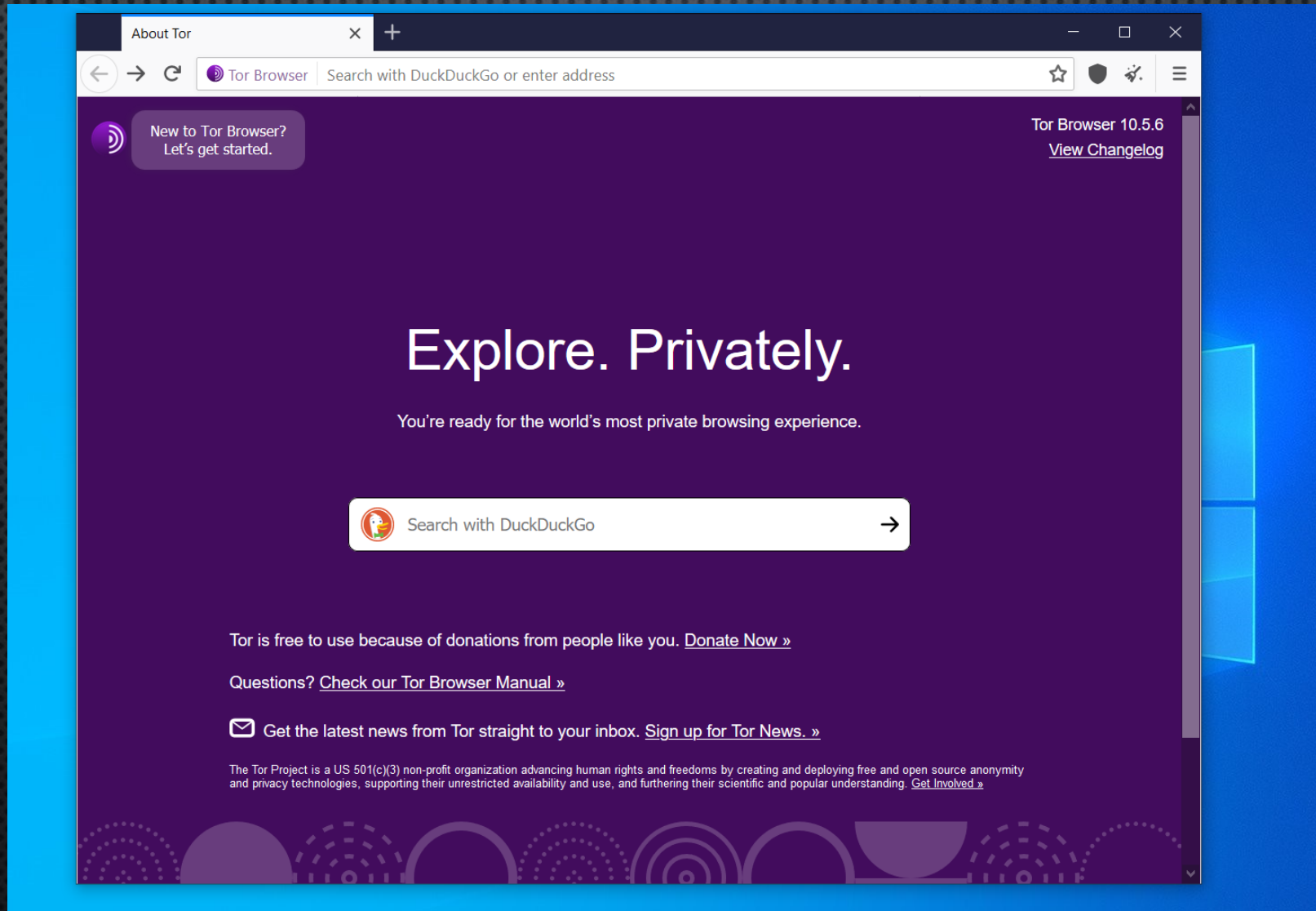
# Browse Privately. Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

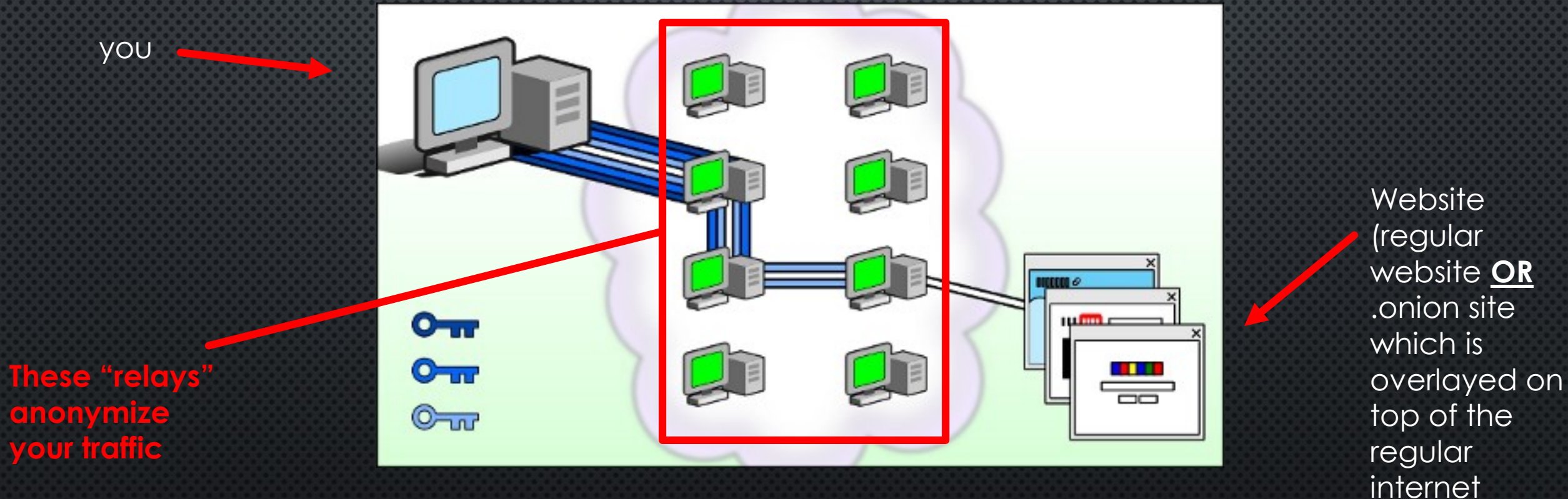
Download Tor Browser ↓



# Tor looks like a regular browser



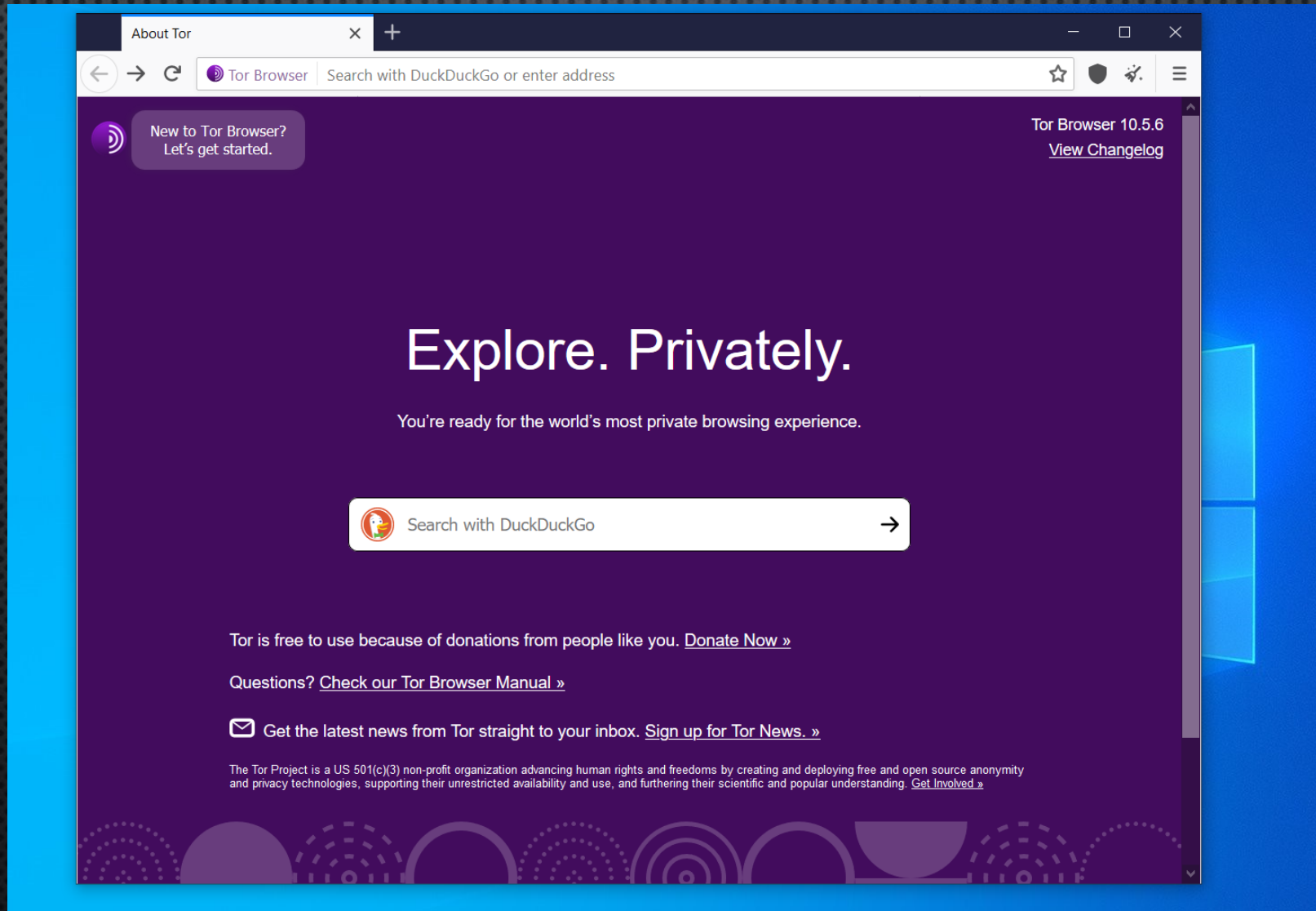
TOR acts like a regular browser  
(it just can see .onion sites too)



... and it is anonymized  
(your ISP sees you on Tor, that's it)



# OK, I'm on Tor. Now what?



# A lot of the DW involves marketplaces



Kilos | Darknet Market Search E x +

mlyusr6htlxsys7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion/advanced\_search?search=ecstasy&

Search now!

Kilos Account

Kilos Finance

Social

Education

Hosting

Misc

Kilos is supported by...

**CARTEL**  
MARKETPLACE  
SHOP NOW   
1800+ PRODUCTS LISTED  
[View all]

Search query

Minimum price Maximum price Display currency

Relevance Market

Shipping origin Shipping destination Product class - any

☐ Accepts BTC ☐ Accepts BCH ☐ Accepts LTC ☐ Accepts XMR

Search the darknet markets

mlyusr6htlxsys7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion 3 4 5 6 7 8 9 10



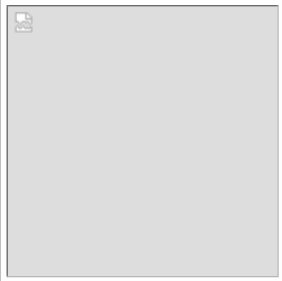
# DRUGS



Kilos | Darknet Market Search E X +


mlyusr6htlxyc7t2f4z53wdxh3win7q3qpxcrbam6jfdmua7tnzuyd.onion/advanced\_search?search=molly&m

## Search results







**500 x PURE  
MDMA Pills  
300ugs(Ecstasy/  
Molly)**


For sale by [caracolcartel](#)  
on [ToRReZ](#)

 ToRReZ

caracolcartel has 0 known  
reviews and an average  
score of 100.0%.


Origin: Austria  
Destination: Europe  
Price: 1520.0 USD  
Product type: Physical

Accepts BTC?   
Accepts BCH?   
Accepts LTC?   
Accepts XMR? 







**25g Pure MDMA  
Molly Rocks  
Dutch Import  
UNCUT 86%  
Purity**

For sale by [Combi](#) on  
[Versus](#)

 VERSUS

Origin: Liechtenstein  
Destination: Worldwide  
Price: 228.0 EUR  
Product type: Physical

Accepts BTC?   
Accepts BCH?   
Accepts LTC?   
Accepts XMR? 

# More Drugs...



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/home#

**DARKODE**  
REBORN

XMR 1.00 = \$244.11  
BTC 1.00 = \$43462.6

Search for...

Search

jenn...

ultra clean colombian cocaine 91% (1...

Dark0de's Choice

ukwhite

★★★★★

(FE) | WW

3839 150

\$ 120

Order

[DD] 24k gold top aaaa+ \$125/28 grams

craftfloweraaaa

★★★★★

(Escrow) | WW

144 0

\$ 125

Order

CLAIM THIS SPOT

0 0 0

Empty Sticker

Empty stickers can be claimed by vendors.

Claim!

28 grams rerock party/bar cocaine

Bestseller

bighornododge

★★★★★

(Escrow) | NA

628 108

\$ 750

Order

cocaine 7g m and m candy stamp \*fir...

Dark0de's Choice

stardockgalix

★★★★★

(FE) | NA

436 40

\$ 450

Order

Dark0de's Choice

pressurepacks

★★★★★

(Escrow) | NA

3062 1.9k

\$ 9.0

Order

448g - budget outdoor smalls - og kush

Pacificanna

pacificannanw

★★★★★

(Escrow) | REG

116 0

\$ 199

Order

phillip plein xtc pills 240mg 50+10 €90

drugspanda

★★★★★

(Escrow) | WW

24 2

\$ 107

Order

\*30 mg ad adderall\* 25 pack for \$99.99

Bestseller

spacebeans

★★★★★

(Escrow) | WW

4300 375

\$ 100

Order

76



# Even More Drugs...



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/home#

**DARKODE** REBORN

XMR 1.00 = \$244.11  
BTC 1.00 = \$43462.6

Search for... Search

1g x mdma marquis tested best on...  
drswole 155 5.0  
★★★★★ 5.0  
Escrow | WW  
149 20  
\$ 25 Order

tramadol 100 mg 200 tablets  
Dark0de's Choice  
milo8490 4.9k 4.99  
★★★★★ 4.97  
FE | REG  
1553 348  
\$ 360 Order

\*\*\*new vendor promo\*\*\* big bud top...  
jollygreeng 58 5.0  
★★★★★ 5.0  
Escrow | EU  
459 50  
\$ 12 Order

All Products

Best Rated Products

100 xanax bars - 2mg alprazolam - fas...  
Bestseller N EVERY ORDER  
grannysxani 1.2k 4.98  
★★★★★ 5.0  
Escrow | NA  
4722 376  
\$ 180 Order

10x-1000x good fucking xanax bars  
Bestseller  
snapdrugs 14k 4.32  
★★★★★ 5.0  
Escrow | REG  
1099 11k  
\$ 10 Order

ritalin 10 mg 60 tablets  
Dark0de's Choice  
milo8490 4.9k 4.99  
★★★★★ 5.0  
FE | REG  
1627 187  
\$ 170 Order

1gx super strong synthetic china white  
darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/product/PDKQzcQ617775788 792 4.66

1gr-50gr // crystal meth ice // ephedrin...  
crystalclee 377 4.95

14g half - crystal cleer

# Fake Florida Driver's Licenses



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmitid.onion/search/sc/5/Forgery/False Document

**DARKODE**  
REBORN

XMR 1.00 = \$244.32  
BTC 1.00 = \$43461.3

Search for... Search

Escrow 103 0

\$949

Order

**Florida**  
DRIVER LICENSE CLASS E  
L123-456-78-900-0

LAST NAME  
FIRST MIDDLE  
123 STREET DR  
CITY FL 12345-1234  
DOB: 01-01-1950 SEX: M  
ISSUED: 01-01-2013 HGT: 5-10  
EXPIRES: 01-28-2022  
REST:  
ENDORSE:  
DUPLICATE:

SAFE DRIVER

florida dl

falloutb0y 82 4.0

Escrow 119 0

\$100

Order




# Fake COVID Vaccine Cards



Dark0de - market


darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/search/Covid19 Outbreak/all/1

**DARKODE** REBORN 

XMR 1.00 = \$244.32  
BTC 1.00 = \$43461.3

Search for... **Search**

Order



COVID-19 Vaccination Record Card

Please keep this record card, which includes proof of information about your vaccine, safe and secure.

Por favor, guarde esta tarjeta de registro, que incluye información sobre su vacuna, segura y protegida.

Wickr:stonersday420

Last Name: [redacted]

Product Name/Manufacturer: [redacted]

Lot Number: [redacted]

1<sup>st</sup> Dose: [redacted]

2<sup>nd</sup> Dose: [redacted]

Admin date: [redacted]

PFIZER Lot: EL1264

Admin date: [redacted]

vaccination card certificate for sale


gambler 9 5.0

★★★★★

Escrow 297 0

\$300

Order




# Ivermectin



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/search/Covid19 Outbreak/all/1


**DARKODE** REBORN  XMR 1.00 = \$244.32  
BTC 1.00 = \$43461.3

Search for... Search

Escrow 249 0

\$178

Order



iverheal 12mg (covid 19 treatment) 200 pills

mastermeds 32 4.71

Escrow 151 2

\$90

Order



# Credit, Gift, Debit Cards



Search for Products and ... Robot Check Problem Loading Onion CC Plaza | The Tor Marketpla

2b2nmjtwycscv6hu.onion/index-2.html

CCPlaza Home

working tested methods. You will also get free support via email if you have any issues.

Contact us: authentic21@tuta.io

CC Credit Card Board (26) Updated: 2020-09-14

ID	Card	Balance (USD)	Price (USD)	You Profit (USD)	
330C3445	Yes	\$91.67	\$8.25	\$83.42	Order Now (\$8.25)
77CB1117	Yes	\$105.31	\$9.48	\$95.83	Order Now (\$9.48)
FED36EE8	Yes	\$109.90	\$9.89	\$100.01	Order Now (\$9.89)
29B6A948	Yes	\$111.39	\$10.03	\$101.36	Order Now (\$10.03)
79E0DCF4	Yes	\$157.38	\$14.16	\$143.22	Order Now (\$14.16)
D469DDD0	No	\$194.72	\$17.52	\$177.20	Order Now (\$17.52)
7DC14501	Yes	\$204.82	\$18.43	\$186.39	Order Now (\$18.43)

MH

82



# How The Hackers Find and Fool You

# Hackers Search the Dark Web For Released Databases of Hacked Emails

[📄](#) Found 24 Text Files, 7 CSV Files, 2 Email Files, 1 Excel File

[jobseeker.json.rar/jobseeker.com\\_2.txt](#) [Part 864 of 1538]

[PREVIEW](#) 2021-09-09 10:25:37

```
{"sort": [2169279], "_type": "jobseeker", "_index": "jobseeker-20190423-1556052455200", "_score": null, "_source": {"non-us-non-canada": false, "last-active": "2016-10-05T17:31:59+0000", "telephone": "", "last-login": "2014-07-30T11:41:49+0000", "security-clearance": "None", "experience": {"past-companies": ["ByteLight", "Red Bend Software", "General Dynamics Information Technology (GDIT)", "OpenReach", "Enterasys Networks", "Indus River Networks", "Dimension Enterprises", "Phillips Business Information", "Women in Communications", "Vineyard Gazette"], "past-titles": ["Marketing and Operations Consultant", "Executive Vice President of Marketing", "Vice President of Corporate Marketing", "Director of Marketing", "Director of Product Marketing & Management", "Sr. Product Marketing Manager", "Sr. Product Manager", "Product Manager", "Sr. Strategic Analyst, consulting AT&T and Global One on their I", "Manager of New Media", "Product Manager of TelecomWeb", "Editor of ISDN News", "Communica
```

[Full Data](#)

[Combolist30M.txt](#) [Part 16 of 222]

[PREVIEW](#) 2020-12-01 03:58:43

```
remmundi412@yahoo.com:poiuyt
rexuejianjian@163.com:wujian8726792
rexwolf_razvan@yahoo.com:1q2w3e4r5t
reyes.jocelyne@yahoo.com:1beauty
reyeha2@yahoo.com:10061989
reymoaquaran@yahoo.com:Flowers12
reynaldobayonon@yahoo.com:123456
reyna509@yahoo.com:Theanswer1
```

[Full Data](#)

[Bitly.com DataBase.7z/Bitly.com DataBase.txt](#) [Part 21 of 149]

[PREVIEW](#) 2020-11-24 14:24:39

```
carolinelabrie:caroline@carolabrie.com:bcrypt$2a$12$mn5HZtecVpptcb7GzJKoAu8QZzSdSuu0G4LifSEPTBruu9kNNveXW$2014-01-06
carolinelaine:carrye58@hotmail.com:02988cb139bdc97fa0e18ead002dea
carolinelambie:caroline_lambie@yahoo.co.uk:6cf60b614a06f7e412469003f1e2b1d
carolinelange:cla@seas-nve.dk:2d4d5d09f2e6390f9303379a17b714d4
carolinelangley:carolinelangleyrichardson@gmail.com:bd18f9e4f82097fe486806ce0a74a7ad
carolinelarnach:carolinelarnach@hotmail.com:8eb40c167ddb91a5bd870842cf2e5e3c
carolinelau:caroli.lau@gmail.com:5c16d2ed0135f6252ee10c542b07029f
carolinelawrence:flaviagemina@hotmail.com:bcrypt$2a$12$KuX1J3EjnVxqbwPZO.e610ZxmkaL5w8Pu/M.QtoJ7qCrS.EL8D2ZS$2014-01-06
```

[Full Data](#)

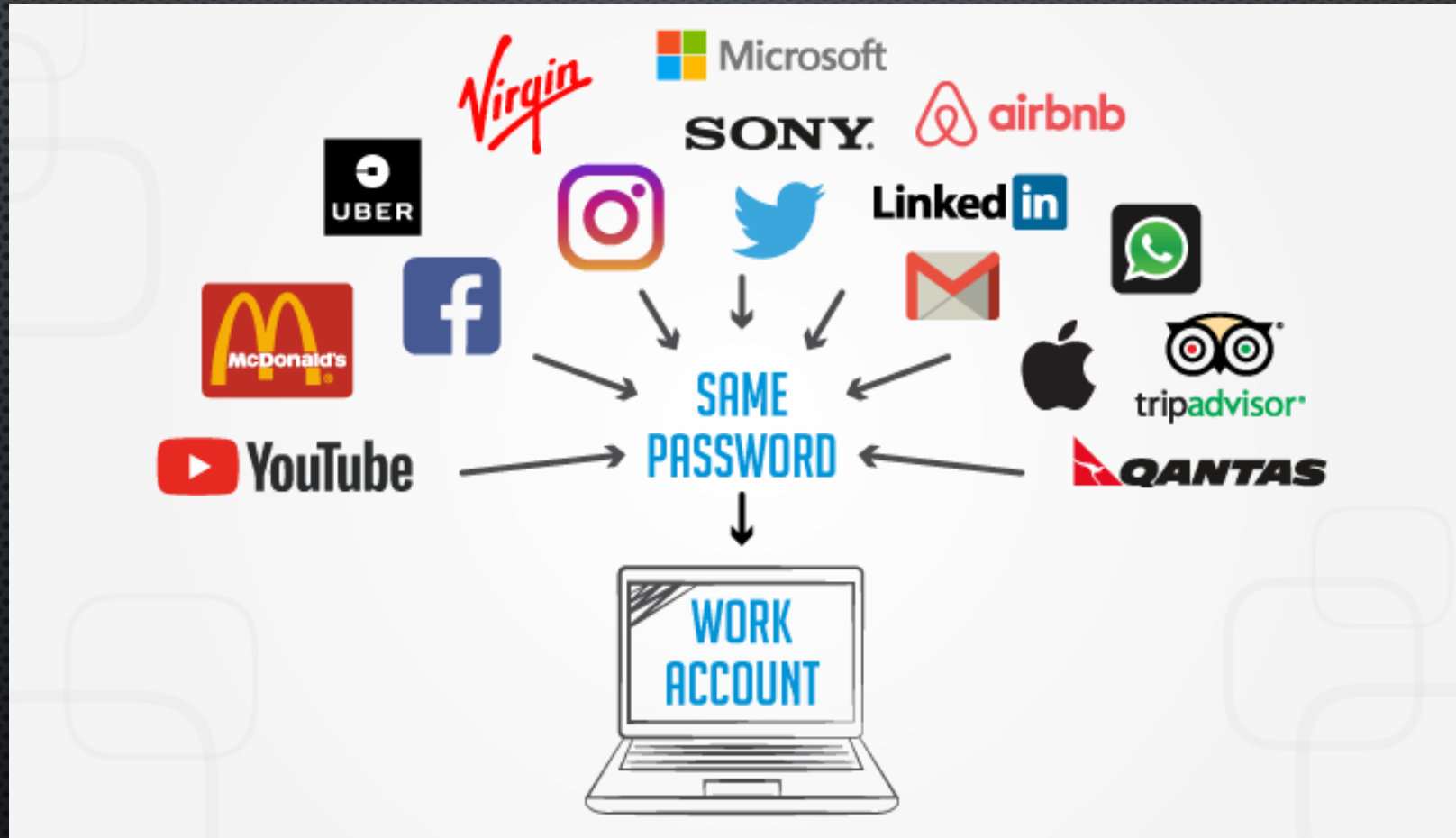
[Разбитая база 2018.18.07\\_15-23-32/35.txt](#) [Part 32 of 40]

[PREVIEW](#) 2020-03-17 19:48:45

```
sjcj_92@hotmail.com:sandro1992
zivkovicpg@gmail.com:drac55
ryanluna48@yahoo.com:tuffguy123
```



# Your Employees Re-Use the Same Password...



# Now Hackers Are in Your System

*(think: ransomware, stolen data, \$\$, fool your clients)*





# Find a Victim's Website



McDonald Hopkins

Attorney **Insight.** Business **Foresight.®**

CAREERS

ABOUT

INSIGHTS

EVENTS

TEAM

EXPERTISE

▼ CONTACT

▼ OFFICES

A wide-angle photograph of the Baltimore skyline at dusk. Several tall skyscrapers are visible, including the Baltimore Marriott Waterfront. The water in the foreground reflects the city lights. A large blue wave graphic is overlaid on the right side of the image.

NEWS

McDonald Hopkins announces expansion into Baltimore with additions of Pollock and Campbell to national Data Privacy and Cybersecurity team


Thursday, April 14, 2022

Learn More




# Find a Victim's Website



McDonald Hopkins Attorney **Insight.** Business **Foresight.** CAREERS 

ABOUT INSIGHTS EVENTS **TEAM** **EXPERTISE** ▼ CONTACT ▼ OFFICES



**NEWS**  
McDonald Hopkins announces expansion into Baltimore with additions of Pollock and Campbell to national Data Privacy and Cybersecurity team

Thursday, April 14, 2022

[Learn More](#)



# Find a Victim's Website



[McDonald Hopkins](#) / [Team](#) / John Metzger

Search by first or last name	Search by Location	Search By State Admission
Search by industry or service	Search by Law School	Search by Court of Admission
Submit		Reset all fields

ALL A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



## John T. Metzger

West Palm Beach **Managing Member; Board of Directors; Executive Committee**

West Palm Beach

P: 561.659.1799



John is the Managing Member of the firm's West Palm Beach, Florida office, a member of the firm's Executive Committee and Board of Directors, and a member of the firm's national real estate practice. John has over 30 years of experience assisting clients in complex real estate transactions and business litigation matters, and focuses on providing strategic advice and practical solutions to best meet his client's business needs in a cost effective manner. His clients include developers, lenders, contractors, title insurance companies, real estate professionals, property owners

# Find a Victim's Website



[McDonald Hopkins](#) / [Team](#) / Christopher Hopkins

<input type="text" value="Search by first or last name"/>	<input type="text" value="Search by Location"/>	<input type="text" value="Search By State Admission"/>
<input type="text" value="Search by industry or service"/>	<input type="text" value="Search by Law School"/>	<input type="text" value="Search by Court of Admission"/>
<input type="submit" value="Submit"/>		<a href="#">Reset all fields</a>

ALL A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



## Christopher B. Hopkins

Member

West Palm Beach

P: 561.847.2346



Christopher B. Hopkins is a member of McDonald Hopkins LLC, a business advisory and advocacy law firm.

He has more than 20 years of trial and appellate experience representing businesses and families in the areas of commercial, ethics, fraud investigation, legal/medical malpractice, and probate litigation.

In addition to his work in the courtroom, Christopher's practice involves a wide range of emerging

Practice Focus



# Let's Find Everyone's Email Addresses



## Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as \*.gov.uk are allowed. You are searching 34 billion records.

mcdonaldhopkins.com

Submit

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [\\*.ru](#), [\\*.gov.uk](#), [solarwinds.com](#)

- ☐ Domains
- ☒ Email Addresses
- ☐ URLs

[Intelligence X](#)

© 2020 Intelligence X. [Terms of Service](#) | [Privacy Policy](#)

# Let's Gather Everyone's Email Addresses





# Send the Phishing Email... See who bites!



From: **John T. Metzger** >

To: **Christopher Hopkins** >

Today at 07:07

Good morning,

When will you be in?


I have a request I need you to work on.

Thanks.

Send the Phishing Email... See who bites!



**NOT GOOD  
ENOUGH**

 From: **John T. Metzger** >  
To: **Christopher Hopkins** >  
Today at 07:00

Good morning  
What will you be doing today?  
I have a request I need you to work on.

Thanks.



This one is a little **TOO** heavy-handed



From: [John T. Metzger](#) >

To: [Christopher Hopkins](#) >

Today at 12:08

---

**[External] Christopher B. Hopkins**

Do you have a moment I have a request I need you to handle discreetly. I am going into a meeting now, no calls so just reply to my email.

John T. Metzger  
Managing Member  
sent from my mail

# Go to ChatGPT

(especially if English is a second language)

HO

You are a lawyer named John. You are writing to your law partner, Christopher. In a short email, explain that you are traveling, lost your wallet, need to rent a car. Ask Christopher if he can use Zelle to send money? The email you are writing should be 3-4 sentences.



# Go to ChatGPT



# Go to ChatGPT

(especially if English is a second language)



Dear Christopher,

I hope this email finds you well. I am currently traveling and unfortunately, I seem to have misplaced my wallet. I urgently need to rent a car, so I was wondering if you could possibly use Zelle to send me some money to cover the rental expenses. Please let me know if this is possible.

Best regards,

John





# Protect You & Your Practice



# HavelBeenPwned.com

(maybe dumb name... but sign up)




[Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#) 

';--have i been pwned?

Check if your email or phone is in a data breach

pwned?

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?


557  
pwned websites

11,469,730,784  
pwned accounts


114,131  
pastes

207,749,076  
paste accounts


Largest breaches



772,904,991 [Collection #1 accounts](#)




763,117,241 [Verifications.io accounts](#)




711,477,622 [Onliner Spambot accounts](#)


Recently added breaches



15,003,961 [Epik accounts](#)



20,154,583 [IndiaMART accounts](#)



878,209 [Imavex accounts](#)


100



# Gmail Searches for Your Hacked Accts



You and Google

Christopher Hopkins  
Syncing toTurn off


Sync and Google services


Manage your Google Account


Customize your Chrome profile

Import bookmarks and settings

Autofill

 Passwords  
compromised passwords

 Payment methods

 Addresses and more

Using Chrome, log into  
your Gmail account

Hit “...” in upper right

Go to Settings



# Train (and Warn) Your Employees



17. **Mandatory Avoidance of Email, Business Compromise, and Other Scams.** I am aware that it is my duty, during my employment for [REDACTED] to avoid email, business compromise scams, and other scams or tricks, including but not limited to internet hacks, viruses, malware, and phishing scams. Within the scope of my employment, I will carefully read and consider emails, attachments, documents, and hyperlinks before opening, clicking, and engaging. If I have questions, I am to ask first. If I suspect there is or was any sort of intrusion or risk of intrusion, I am to immediately report it to [REDACTED]. I acknowledge and agree that opening, clicking, and engaging with fraudulent emails, attachments, documents, and hyperlinks (or failing to report the same) can be cause for termination.



# Send Your Own “Fake” Emails... See who bites!



Dear Christopher,

Good morning. I wanted to let you know that I will be out of the office today for a personal matter. Would you be able to help me with something?

Thank you for your assistance.

Best regards,

John

# Tell Clients in Your Engagement Letter



**Electronic Communications & Storage:** Like most businesses, the Firm communicates with the Client primarily via unencrypted e-mail, phone, and, secondarily, by U.S. Mail or overnight service. We also use IM/text, internet portal, FTP, WiFi, WeTransfer, Zoom, video conferencing, cloud storage, and other physical and/or Internet-based third party vendors and services for communications and storage (unless you request otherwise). Client agrees and accepts that there is always some risk of disclosure, hacking, intrusion, and loss of attorney-client privilege when using these forms of communication and storage because of issues inherent to the internet communications, storage, and third party vendors; no guarantee can be made regarding the interception of data sent or stored on the internet or with third parties.

The Client agrees that, in advance, the Client will advise the Firm in writing if the nature of any communication or storage require a higher degree of security.



# Tell Clients in Your Engagement Letter



**Wire Transfer – Verbal Confirmation Required:** During the period in which the Firm provides legal services, the Client may wish, or possibly be required, to make electronic or wire payment to the Firm or third parties. Client acknowledges the risk of identity theft, impersonation, email compromise, phishing, and other scams. Relative to payments relating to this matter, Client confirms it has sole responsibility to obtain verbal verification from Mr. Hopkins before making any electronic or wire payments to the Firm or third parties.



# Stay Safe #1



- **Unsecured WiFi** (while traveling) – hackers can access all your transmitted info  
*SOLUTION: VPN (free to employees?)*
- **Phishing/BEC** (easier when we're remote) – hackers fool people into giving out info  
*SOLUTION:*
  - train employees to spot fakes*
  - test them*
  - attorneys... don't answer "cold" emails*
  - don't go to bad sites*
  - anti-malware*



# Stay Safe #2



- **Data Breaches** (not your fault) – until you or your employees re-use passwords  
*SOLUTION:*
  - don't re-use passwords*
  - training*
  - MFA*
  - sign up for HIBP (all employees)*
  - password managers*
  - e-retention policies*
- **Data Breaches** (your system)  
*SOLUTION:*
  - MFA*
  - Anti-malware*
  - Backups*
  - IT to limit incoming IP addresses (monitor traffic)*
  - Don't give admin level access*
  - E-retention policies*
  - Routine searches for your info on dark web*



# Further Reading

[InternetLawCommentary.com](http://InternetLawCommentary.com)





CHRISTOPHER B. HOPKINS

# Is Your PC Keeping Your Information Private? Take This 10-Question Quiz

What entity was the victim of the largest data breach in history? According to *The Guardian*, the "biggest [hack] in history" involved 11.5 million documents known as the Panama Papers stolen from... a law firm. "BigLaw" firms are not alone – small firms and solo lawyers frequently suffer ransomware attacks while, according to Verizon, in-house lawyers are, "far more likely to actually open a [phishing] email than all other [corporate] departments." Lawyers are particularly susceptible targets for data breach because we often hold clients' confidential and financial information. Worse, we can be a weak link: lawyers are quick to answer client inquiries and we respond quickly and at all hours from our mobile devices.

new software. Unless it is a personal computer, few users need full "admin rights." Tap the Windows key and type "control panel." Select User Accounts (twice). 5 points if "administrator" does not appear under your name. If it says "administrator," and it is not your personal PC, subtract 5 points.

**4. Is Your Hard Drive Encrypted?** An encrypted drive should render your drive unreadable if it is stolen. Tap the Windows key and type "control panel." Select "Security and Systems" and look for BitLocker encryption to be "on." Admittedly, there is more than one encryption method; hit the Windows key and type "PGP" to see if you find PGP Whole Disk Encryption. 5 points for encryption, no points for an

**8. Can Someone Else Remotely Access my PC?** Hit the Windows key and R, then type "SystemPropertiesRemote.exe." It should open a new dialog box with the title "Remote Access." If "Allow Remote Assistance" is unchecked, give yourself 5 points. If your IT department allows remote access limited to "Network Level Authentication," add no points. If remote access is allowed without restriction, subtract 5 points.

**9. Do I Have Any Unknown Programs on my PC?** Tap the Windows key and type "control panel." In the upper right corner, type, "program" in the search box, and select "show which programs are installed." Add 3 points if you recognize all apps; -1 for each app you cannot identify.



[McDonald Hopkins](#) / [Insights](#) / Don't connect your phone to rental cars

**BLOG POSTS**

## Don't connect your phone to rental cars







CHRISTOPHER B. HOPKINS

In March 2020, as professionals worked from home due to COVID-19, Zoom video conferences surged in popularity while, conversely, lawyers cast weary glances at the Alexa device in their home office, wondering if it was recording confidential communications.

As of this writing, rumors abound on social media about the security of both platforms. With little hard evidence, a BigLaw firm publicly broadcast its ban on these devices. While society struggles with its relationship with ubiquitous communication devices, let us at least properly configure our Zoom and Alexa privacy settings.

### Zoom Video: Recommended Settings

As a brief primer, Zoom throws a few numbers at you which can be confusing. A Personal Meeting ID (PMI) is a virtual room assigned to you alone; this is visible on the URL, called a Personal Link, when you invite someone to your personal meeting room. Your Meeting ID is a temporary number for a scheduled meeting. The Meeting ID typically expires after your meeting unless you create a recurring meeting. These links and IDs may be confusing but the important point is that, without proper precautions, they can be hacked, re-used, or simply guessed by third parties.

## Privacy Settings for Zoom Video and Alexa

**Is This Being Recorded?** - Zoom reports that all participants will see a red notification (upper left on desktop and upper right on iOS) if the meeting is being recorded.

**Only the Host Has Certain Abilities** - On the website, go to Settings and turn OFF "Join Before Host," "Use Personal Meeting ID," "Annotation," "Remote Control," and "Allow Removed Participants to Rejoin." Meanwhile, turn ON "Allow host to put attendees on hold" and "host only" under screen sharing.

**Hypervigilance Against Zoom-Bombing** - To really lockdown meetings, on the website, turn off "Join Before Host" and "File Transfer" but turn on "Require Password for... Phone" and, towards the bottom, turn on "Waiting Room." You will need to Google how to use Waiting Rooms.

The following steps will assist in protecting your privacy during a Zoom meeting:

**Spacebar To Mute** - press and hold spacebar to temporarily mute yourself.

**Set a Virtual Background** - The benefit of a virtual background is that participants cannot see the room behind you, whether that includes privileged information on a wall calendar or... a snoring pug. Select a high definition shot of the Enterprise, the

**Look Your Best** - While not strictly a privacy issue, on the desktop app, tap the cog wheel, then video, then Touch Up My Appearance. On iOS, select "more," then Meeting Settings, and turn on Touch Up My Appearance.

### Alexa: Recommended Settings

According to Amazon, "you'll always know when Alexa is recording... because a blue light indicator will appear or an audio tone will sound..." What is less clear is what third parties are doing with your data or if voice apps have the power to control the microphone.

**What Has Alexa Heard?** - In the Alexa app, tap the three lines in the upper left corner and then go to Settings / Alexa Privacy / Review Voice History. Scroll through (and delete) the recent commands she recorded.

**Set Up Delete By Voice Command** - Following those same steps, toggle on "Enable deletion by voice." Then later you can instruct Alexa "delete what I [just said][said today]."

**Auto Delete Old Recordings** - Follow the same instructions but choose Manage Your Alexa Data and set auto delete to either after 3 or 18 months.

**Turn Off "Use Voice Recordings to Improve Amazon Services"** - Again, using the same



## TECHNOLOGY CORNER



CHRISTOPHER B. HOPKINS

# Protect The Privacy of Your iOS 13 Device

It has been two years since we covered iPhone and iPad security in this column. The risks have only increased while several privacy settings have become more difficult to find. To echo the Fourth District's recent assessment in a real-time cell phone tracking case: "[t]his presents significant privacy concerns." Make sure your device is running iOS 13.x (Settings / General / Software Update) and then check the following:

**Apple Is Tracking You:** Under Settings / Privacy / Location Services, scroll all the way down to System Services. Location-Based Apple Ads, Location-Based Suggestions, iPhone Analytics, Popular Near Me, and Routing & Traffic should be off. Turn off Significant Locations.

**Google Maps Is Tracking You:** Open Google Maps and select your profile in the upper right corner. Select Your Data in Maps, then

prevent this intrusion, go to Settings / Mail and toggle Load Remote Images to off. If an email contains an image you want to see, just click the banner at the top when you open the email.

**I See When You Opened My Text:** Under Settings / Messages, turn off "Send Read Receipts."

**I See You Are Not in Your Office:** Why broadcast that you are out of the office? Turn off "sent from my iPhone" under Settings / Mail / Signatures (leave it blank). There is still another trick. When sending a reply, your email will be entitled "Re:" when you reply on a mobile device whereas it will be "RE," with a capital E, if you are logged in via computer. So an email which is entitled, "Re: [title]" is coming from a handheld device. When it matters, you can manually capitalize the letter "e" to prevent leaking

able to keylog what you type because you granted them "all access." Make sure you know which apps can read your texts under General / Keyboard / Keyboards. Delete anything which is unfamiliar.

**Are Text Messages Going to Other Devices?** Are iMessages being pushed to other devices on your Apple account? Maybe. To keep your chats private, make sure Settings / Messages / Send & Receive is set to your phone only and no other devices or email.

**Health:** Unless you intended an app to access this feature, only Health should be listed under Settings / Health / Data.

.....  
*Christopher B. Hopkins handles privacy and cybersecurity matters with McDonald Hopkins LLC ([chopkins@mcdonaldhopkins.com](mailto:chopkins@mcdonaldhopkins.com)).*





# CHRISTOPHER B. HOPKINS



[CHOPKINS@MCDONALDHOPKINS.COM](mailto:CHOPKINS@MCDONALDHOPKINS.COM)



[@cbhopkins](https://twitter.com/cbhopkins)



[www.linkedin.com/in/cbhopkins/](https://www.linkedin.com/in/cbhopkins/)

[InternetLawCommentary.com](http://InternetLawCommentary.com)