



DANGERS OF THE DARK WEB

CHRISTOPHER B. HOPKINS
MCDONALD HOPKINS LLC





CHRISTOPHER B. HOPKINS

McDonald Hopkins

CHOPKINS@MCDONALDHOPKINS.COM



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

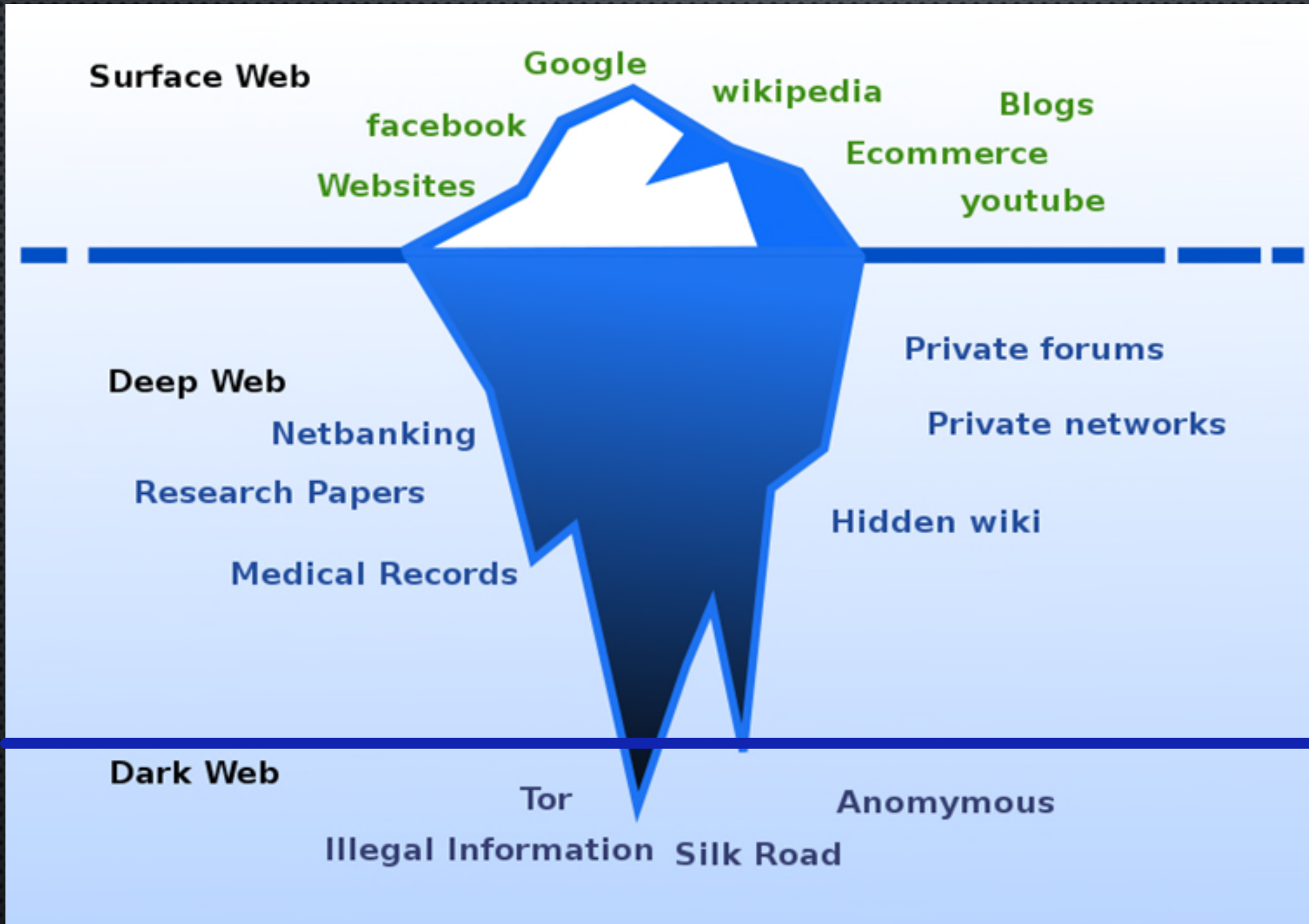


www.linkedin.com/in/cbhopkins/

InternetLawCommentary.com

PART I

What is the Dark Web?



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

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
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

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

PART II

Let's Go to the Dark Web



www.TorProject.org



Donate Now

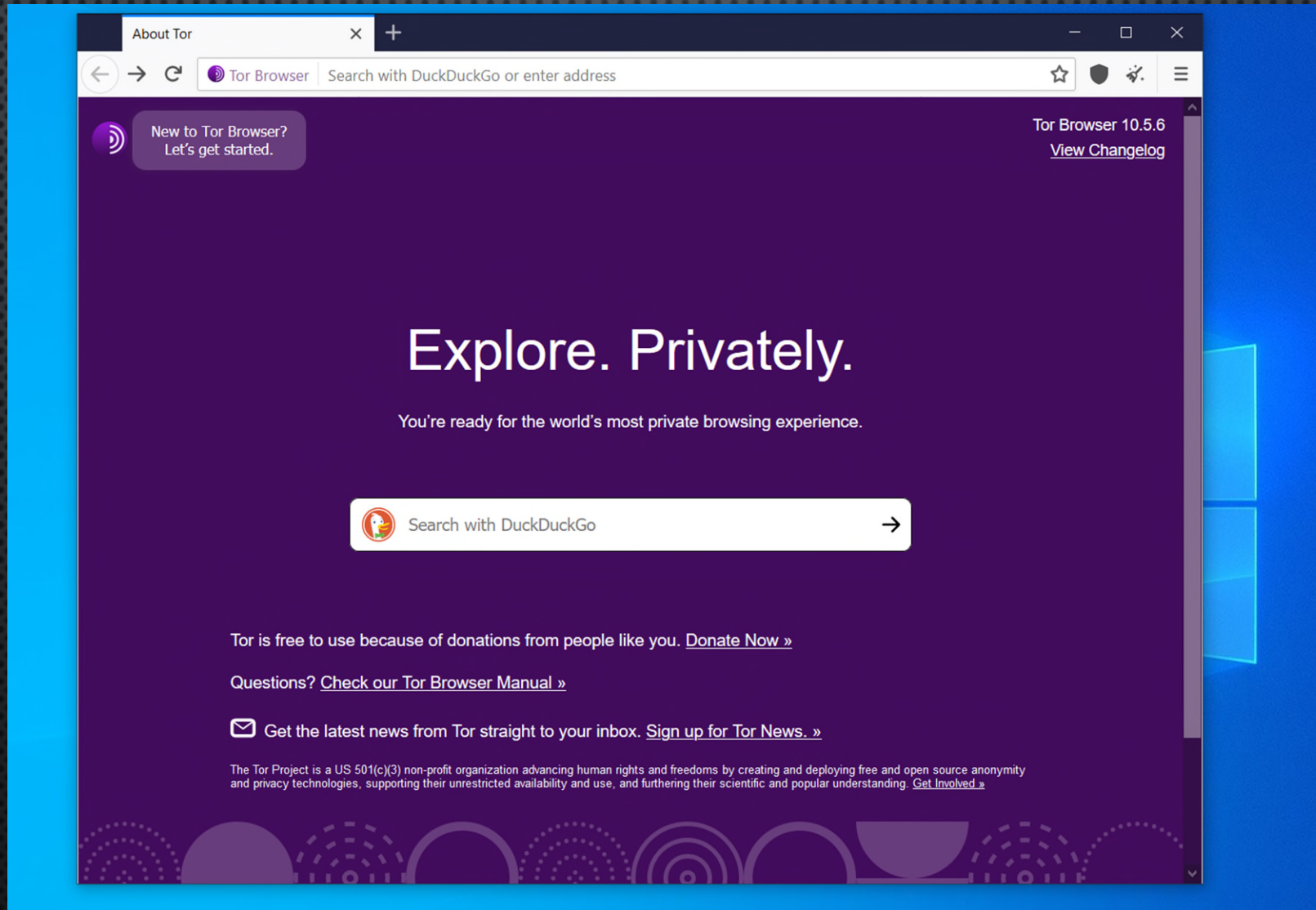
[About](#) [Documentation](#) [Support](#) [Community](#) [Blog](#) [Donate](#)

Browse Privately. Explore Freely.

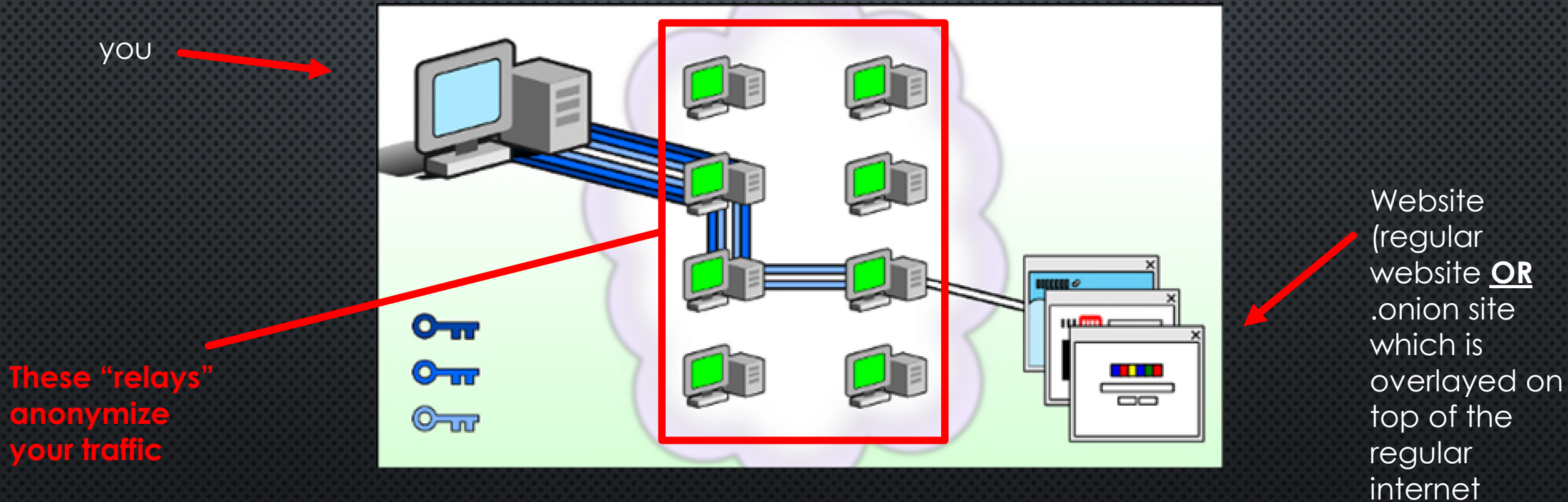
Defend yourself against tracking and surveillance. Circumvent censorship.

Download Tor Browser ↓

Tor looks like a regular browser

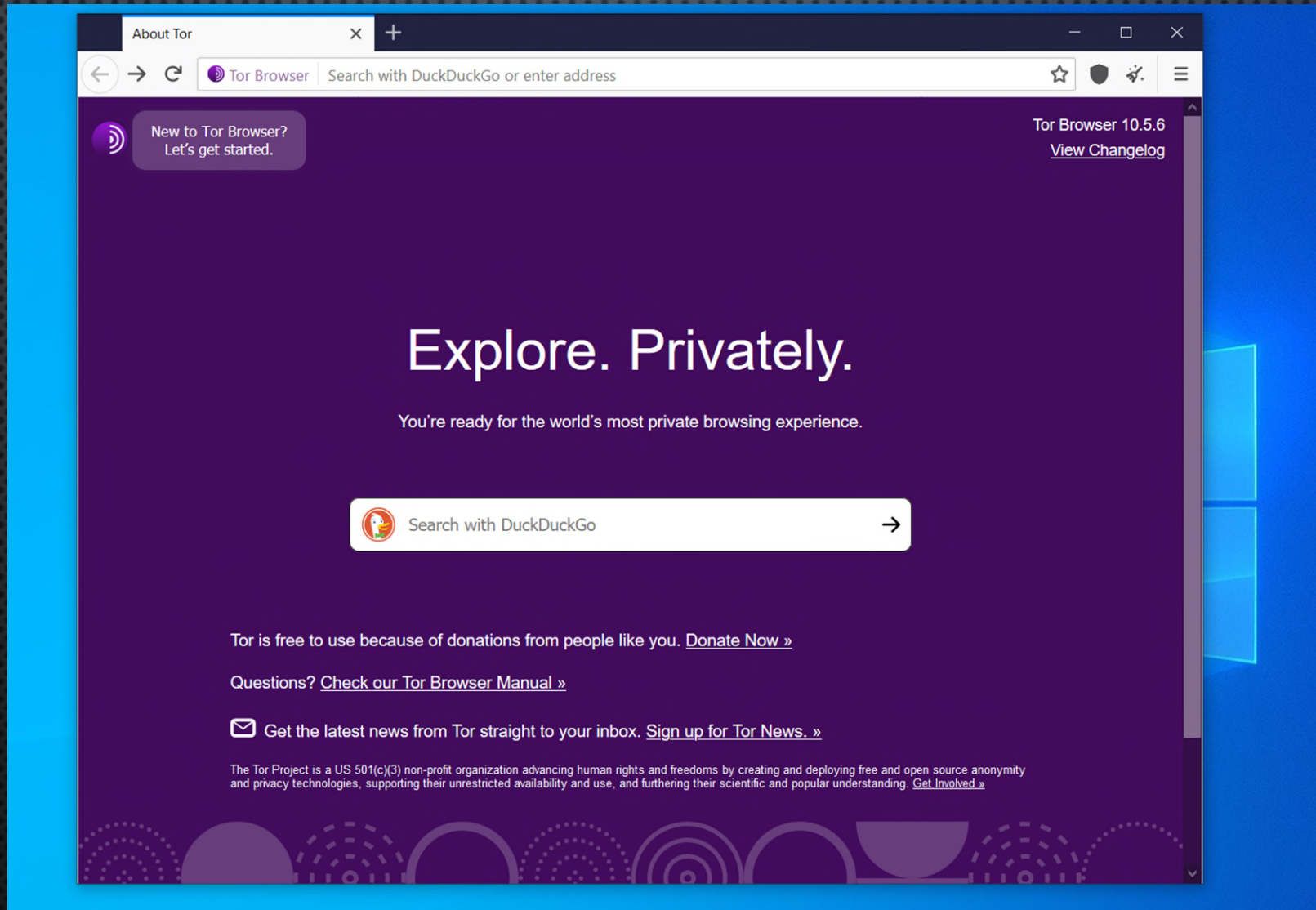


TOR acts like a regular browser
(it just can see .onion sites too)



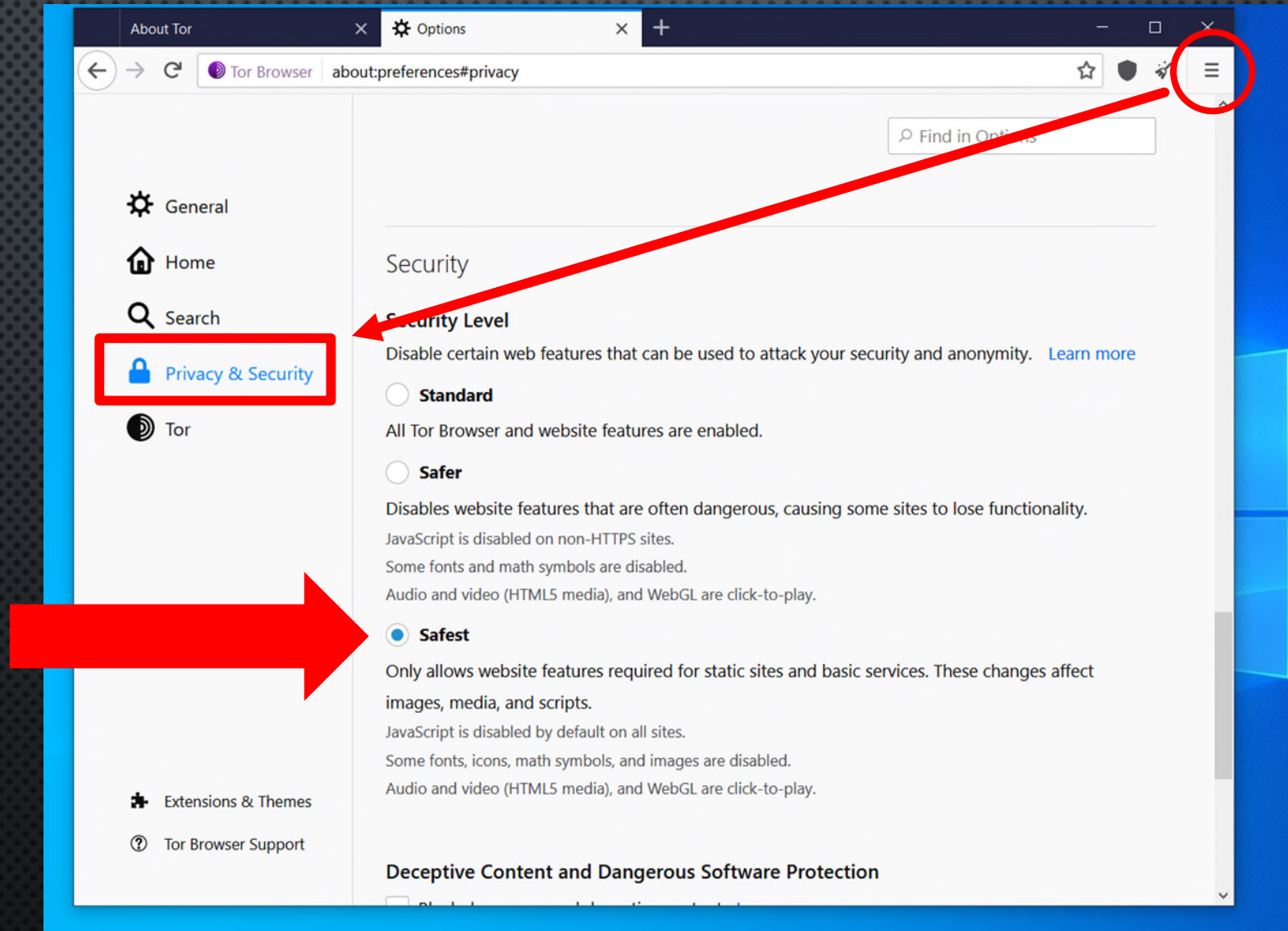
... and it is anonymized
(your ISP sees your on Tor, that's it)

OK, I'm on Tor. Now what?

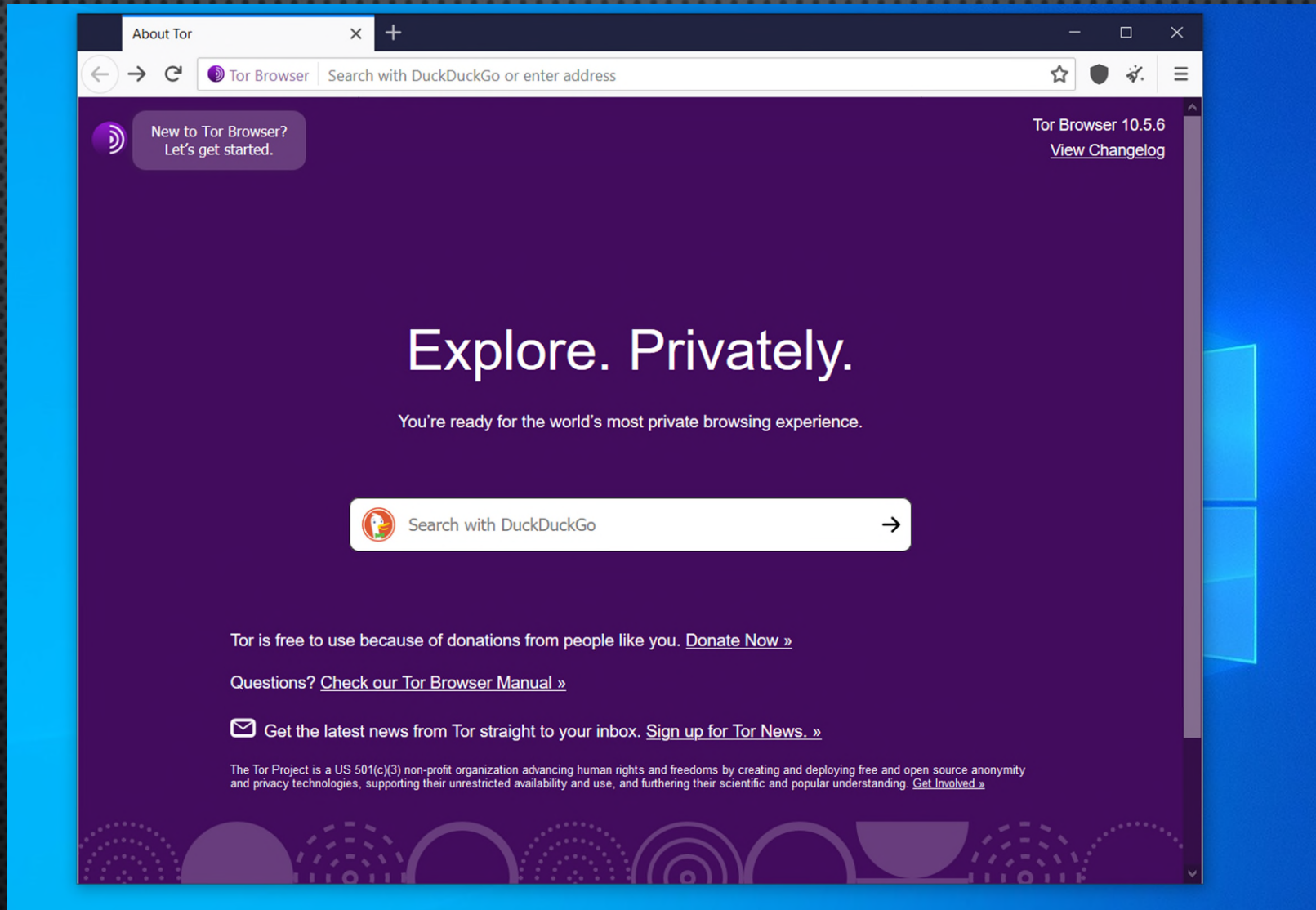


“Safest” Setting on Tor

Inside Tor settings,
go here



OK, I'm on Tor. Now what?




[tor.taxi - your ride to the darkn](#)
[The New York Times - Breaking](#)

[https://www.nytimes3xbfgragh.onion](#)

Fed Signals It Will Soon Pull Back From Pandemic Stimulus Measures

- The Federal Reserve said it could soon slow its large-scale purchases of government-backed debt and indicated it might raise interest rates in 2022.
- The statement suggests policymakers are preparing to pivot away from full-blast monetary help as the business environment recovers from the pandemic.



Jerome Powell, the Federal Reserve chair. Sarabeth Maney/The New York Times

Economy Updates


- Follow the Elizabeth Holmes trial with our reporters in the courtroom.
- Wall Street rebounds from a four-day slump as the Fed signals its next move.

In a day of meetings with Democrats, President Biden sought to bridge party chasms over his economic agenda.

LIVE

Biden Urges Global Leaders to 'Go Big' on Covid Response

President Biden called on other world leaders, pharmaceutical executives and philanthropists to band together to fight the pandemic. Here's the latest.



A coronavirus vaccination drive in Medan, Indonesia, last week. Dedi Simuhaji/EPA, via Shutterstock

Some activists say that President Biden's plan for donating an additional 500 million vaccine doses is not enough.

Moderna vs. Pfizer: Both vaccines are highly effective, but one seems to be more protective over the long term.

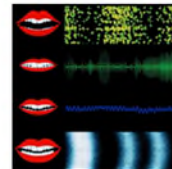
Opinion

BRET STEPHENS

New York's Superstar Progressive Isn't A.O.C.

CHAR ADAMS

Voice Assistants Don't Understand



<https://www.nytimes3xbfgragh.onion/2021/09/22/business/economy/fed-taper-interest-rate-increase.html>

CIA



A screenshot of a web browser window displaying the Central Intelligence Agency (CIA) website. The browser's address bar shows a Tor onion address: 'ciadotgov4sjwzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/index.html'. The website header features the CIA seal on the left, the text 'Central Intelligence Agency' in the center, and a 'CAREERS' button on the right. The main content area has a dark background. On the left, the text 'We are the Nation's first line of defense.' is displayed in a large, white, serif font. Below this, in a smaller white font, is the tagline 'We accomplish what others cannot accomplish and go where others cannot go.' and a paragraph: 'A career at CIA is unlike any other. We are looking for people from all backgrounds and walks of life to carry out the work of a Nation'. On the right side of the main content area is a large, high-contrast, black and white portrait of a woman with dark, curly hair, looking directly at the camera.

Anonymous Conversations

(mostly “noobs” and scams)



Frontpage - Dread x Problem Loading Onionsite x +

dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion

dread frontpage all dread 🔍 Login or Register

0 comments Hide

▲ 1
▼ % of people using proper opsec
by /u/newandnoided • 42 minutes ago in /d/CafeDread
0 comments Hide

▲ 1
▼ Low activity. Opening up my PMs again.
by /u/just_no • 2 hours ago in /d/CafeDread
0 comments Hide

▲ 1
▼ Looking for users to try our hash products for free and leave a detailed review about it
by /u/Hash2GO • 2 hours ago in /d/CannaHome
0 comments Hide

▲ 1
▼ Experience with Vendor Kimono??
by /u/prpl33w21 • 3 hours ago in /d/WhiteHouseMarket
0 comments Hide

▲ 1
▼ Exchanging crypto, what is considered "safe"
by /u/stackoftwenties • 3 hours ago in /d/DarkNetMarkets
2 comments Hide

▲ 1
▼ Looking for some answers

GanjaHero Exclusive Sale
25% off With Full Escrow Only at WHM
Buds starting at \$40/oz, Concentrates \$190
Decoys with Every Order, US-US only

CARTEL MARKETPLACE
SHOP NOW

Advertise here View All

CREATE A SUBDREAD

🔗 Suggestions

- /d/Dread 357,093 subscribers
- /d/DarkNetMarkets 35,269 subscribers
- /d/DankNation 8,871 subscribers
- /d/HarmReduction 1,850 subscribers
- /d/TheMajesticGarden 2,278 subscribers
- /d/DarknetMarketsNoobs 11,386 subscribers
- /d/OpSec 15,974 subscribers
- /d/Cannazon 3,151 subscribers
- /d/Monero

A lot of the DW involves marketplaces



Kilos | Darknet Market Search

mlyusr6htlxsc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.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

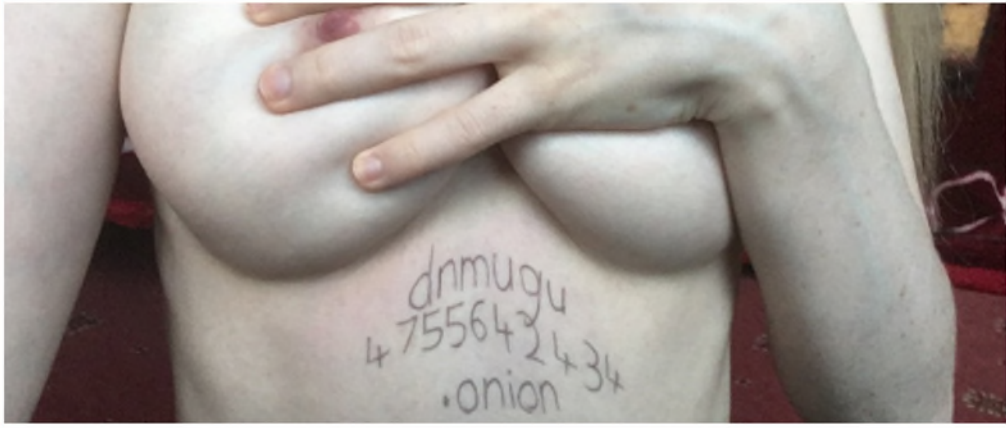
Relevance Market

Shipping origin Shipping destination Product class - any

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

Search the darknet markets

mlyusr6htlxsc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion 3 4 5 6 7 8 9 10




DRUGS



Kilos | Darknet Market Search E x


mlyusr6htlxsc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion/advanced_search?search=molly&m

Search results







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


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



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


★★★★★

Escrow | ww

3839 150

\$ 120 **Order**

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

 craftfloweraaaa

★★★★★


Escrow | ww

144 0

\$ 125 **Order**

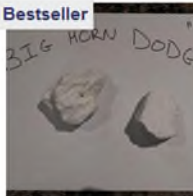
Empty Sticker

Empty stickers can be claimed by vendors.

 CLAIM THIS SPOT

0 0 0 **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


★★★★★

Escrow | NA

436 40

\$ 450 **Order**

Dark0de's Choice pressurepacks

 pressurepacks


★★★★★

Escrow | NA

3062 1.9k

\$ 9.0 **Order**

448g - budget outdoor smalls - og kush

 pacificannanw

★★★★★


Escrow | REG

116 0

\$ 199 **Order**

SKYWALKER OG SMALLS

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**

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

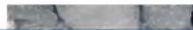
100 xanax bars - 2mg alprazolam - fas...
Bestseller **NEVER ORDER**
 grannysxani 1.2k 4.98
★★★★★ 5.0
Escrow | NA
4722 376
\$ 180 Order

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...
792 4.66

14g half - crystal cleer
 crystalclee 377 4.95

Fake Florida Driver's Licenses



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.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
The Sunshine State
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:

signature

SAFE DRIVER

motor vehicle constitutes consent to any sobriety test required

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

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



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)

Your Information



Dark0de - market

darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/search/Confidential info/all/1

DARKODE
REBORN

XMR 1.00 = \$244.19
BTC 1.00 = \$43480.4

Search for...
Search

🗨️ 🔔 👤 jenn... 🛒

blueskies 179 3.86
★★★★★ 0.0
Escrow 368 1
\$15
Order

logs 2019 - 2020 51gb+ logs

eternos 22 4.87
★★★★★
Escrow 98 0
\$300
Order

PART III

Three Ways to Get Hacked



HOW TO GET HACKED #1

Phishing

Spear Phishing

SOCIAL ENGINEERING ATTACK OR BUSINESS EMAIL COMPROMISE



- Broad range of tricks based upon relationships
- **Ask you to use firm credit card**
- **Password**
- **Transfer funds**

Phishing is a type of social engineering **attack** often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

From: [Shawn M. Riley](#) >

To: [Christopher Hopkins](#) >

[Hide](#)

SR



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](#)

SR



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

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?

SECTION 3



Let's Spot The Fakes!

(with remote working, these scams are more likely to work)



Facebook

To: Cbh >

07:51

Cb, log into Facebook with one click



Facebook

Hi Cb,

We noticed you're having trouble logging into your account. If you need help, click the button below and we'll log you in.

[Log In With One Click](#)

Why did you receive this email?

There was an unsuccessful login attempt on your account. If this wasn't you, [let us know](#).

Done



Facebook



message



call



video



mail



pay

other

security@facebookmail.com

[Add to VIP](#)

[Block this Contact](#)

[Search Mail for Contact](#)



14:20



< 39



From: Chase Bank >

To: Cbh >

Today at 14:16

Re: 2nd attempt for Cbh

Cbh, [Chase Bank Has a Surprise For](#)
[You](#) 🥰



PO Box 41529,,PMB 78292,Memphis,TN,38174

To opt-out please [click here](#)



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





[External] Customer Email Notification - Message (HTML)

File Message Kofax PDF Litera Tell me what you want to do...

Ignore Delete Reply Reply All Forward More

Move to: ? To Manager Done Create New

Rules OneNote Actions

Assign Mark Categorize Follow Up

Sun 10/25/2020 3:03 PM


Wells Fargo Online <mail@ioleads.com>

[External] Customer Email Notification

To: Hopkins, Christopher

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

Action Items

 wellsfargo.com

Dear Customer:

Recently, we discovered unusual activity or updates on your account that we believe may be unauthorized. For your protection, we have temporarily suspended use of this account until you verify the activity; you will not be able to use the ATM/Debit Card linked to this account also for withdrawals or purchases until we hear from you.

What you need to do

Please contact us as soon as possible to confirm your recent activity or to let us know if you think this account was used without your permission.

- In person:** Visit any Wells Fargo branch and speak to a banker. To find a branch near you, visit us online.
- Online :** Go to [review and verify account activities](#) to continue using your account .

Thank you,

Wells Fargo

Customer Fraud Protection Services

- Irregular Activity -ID# 142114



• SunTrust <ey@fuse.net>



Dear SunTrust Online,

We're sorry,

Our account security specialists have noticed unusual activity on your account ,Someone was trying to access your account earlier.We have taken the right security steps to ensure your safety,Your account is locked till you identify your account information for your safety.

To restore your account, please Sign in to Online Banking.

<https://onlinebanking.suntrust.com/UI/login>

Your account will work as normal after the processed.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care



- Irregular Activity -ID# 142114



• SunTrust <ey@fuse.net>



Dear SunTrust Online,

We're sorry,

Our account security specialists have noticed unusual activity on your account ,Someone was trying to access your account earlier.We have taken the right security steps to ensure your safety,Your account is locked till you identify your account information for your safety.

To restore your account, please Sign in to Online Banking.

<https://onlinebanking.suntrust.com/UI/login>

Your account will work as normal after the processed.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

From: [Netflix](#) >

To: [REDACTED]

[Hide](#)

N

re: Your account is on hold [Case ID : ID-046-EG0-DWL-EG05RC4ZQM]

Yesterday at 7:20 PM

Please update your payment details

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

[Go to Billing](#)

Need help? We're here if you need it. Visit the [Help Center](#) or [contact us](#) now.

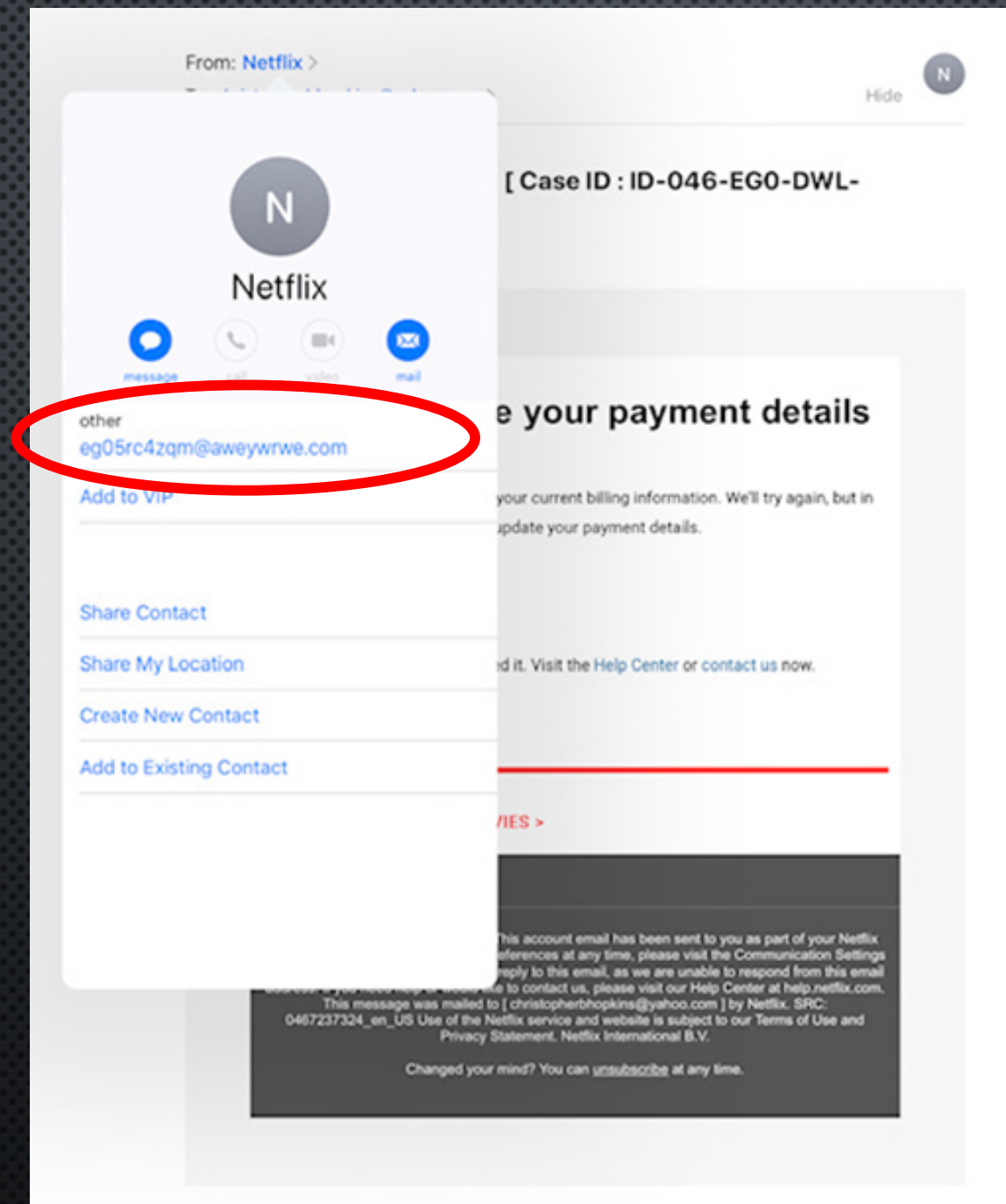
-Your friends on Netflix

[VIEW ALL TV SHOWS & MOVIES >](#)

Questions? Call 007-803-321-2130 This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the Communication Settings page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our Help Center at [help.netflix.com](#).

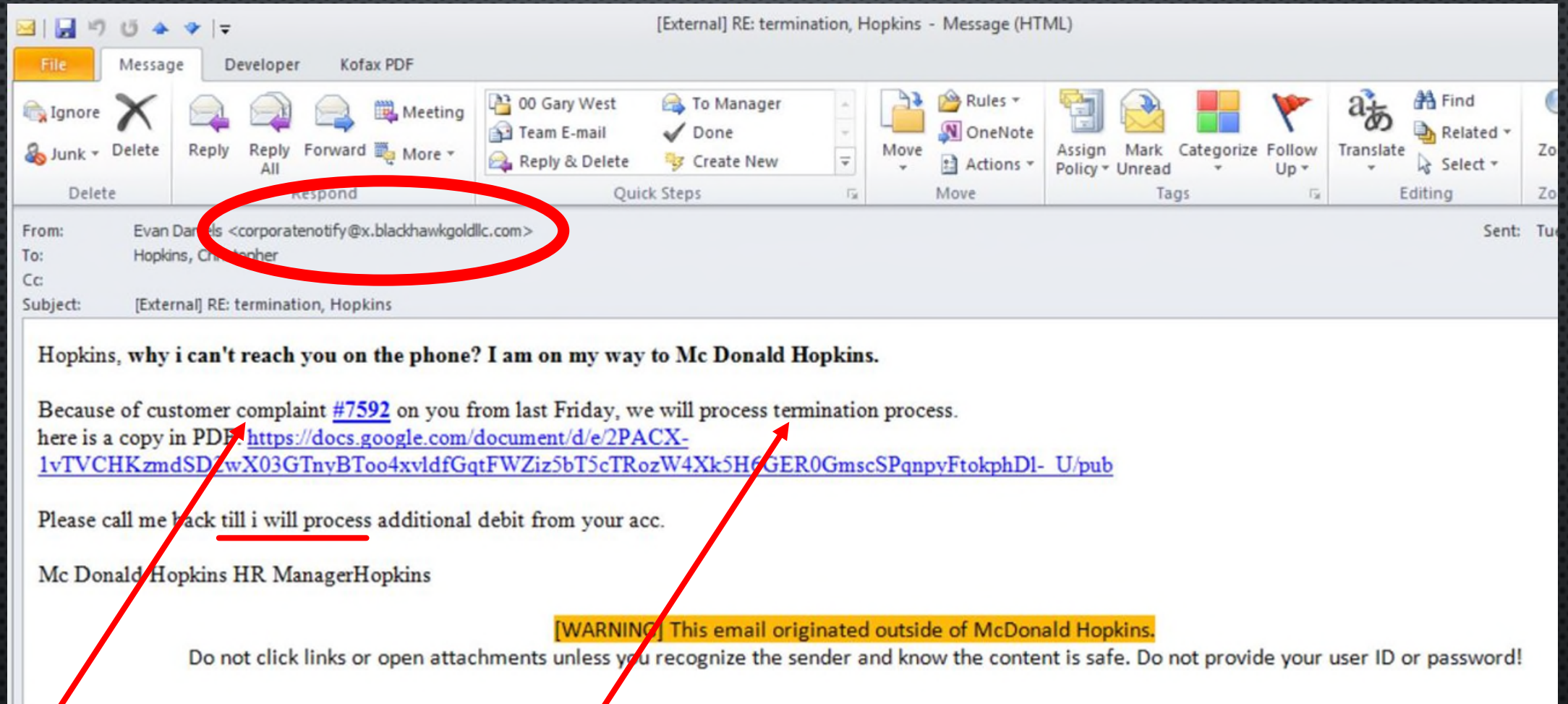
This message was mailed to [christopherbhopkins@yahoo.com] by Netflix. SRC: 0467237324_en_US Use of the Netflix service and website is subject to our Terms of Use and Privacy Statement. Netflix International B.V.

Changed your mind? You can [unsubscribe](#) at any time.

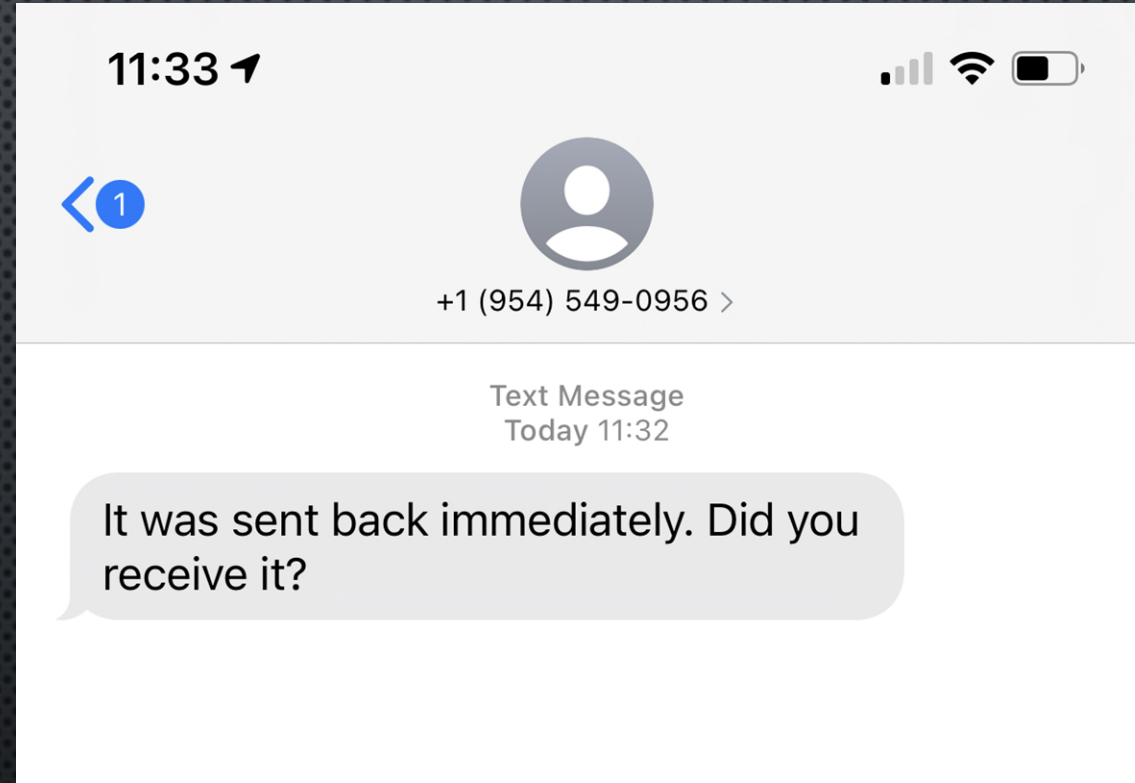


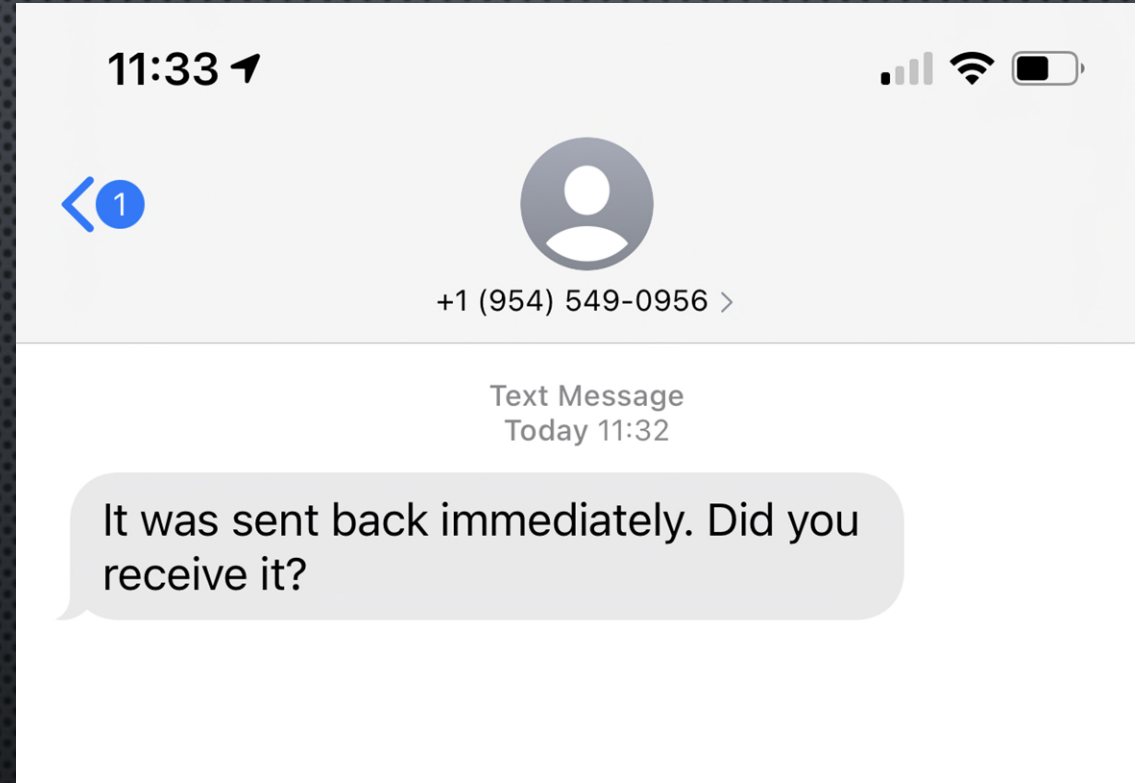
This one was good...

Hit "reply" and make
sure you look at the
address!



Urgency is a hallmark
of a scam





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



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



[Redacted]

12 messages

Melissa [Redacted] <closingagent2519@gmail.com>

Tue, [Redacted] at 11:19 AM

To: [Redacted]

Cc: [Redacted] <jd4659491@gmail.com>

Good morning,

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.



[Redacted]

12 messages

Melissa [Redacted] <closingagent2519@gmail.com>

Tue, [Redacted] at 11:19 AM

To: [Redacted]
Cc: [Redacted] <jd4659491@gmail.com>

Good morning,

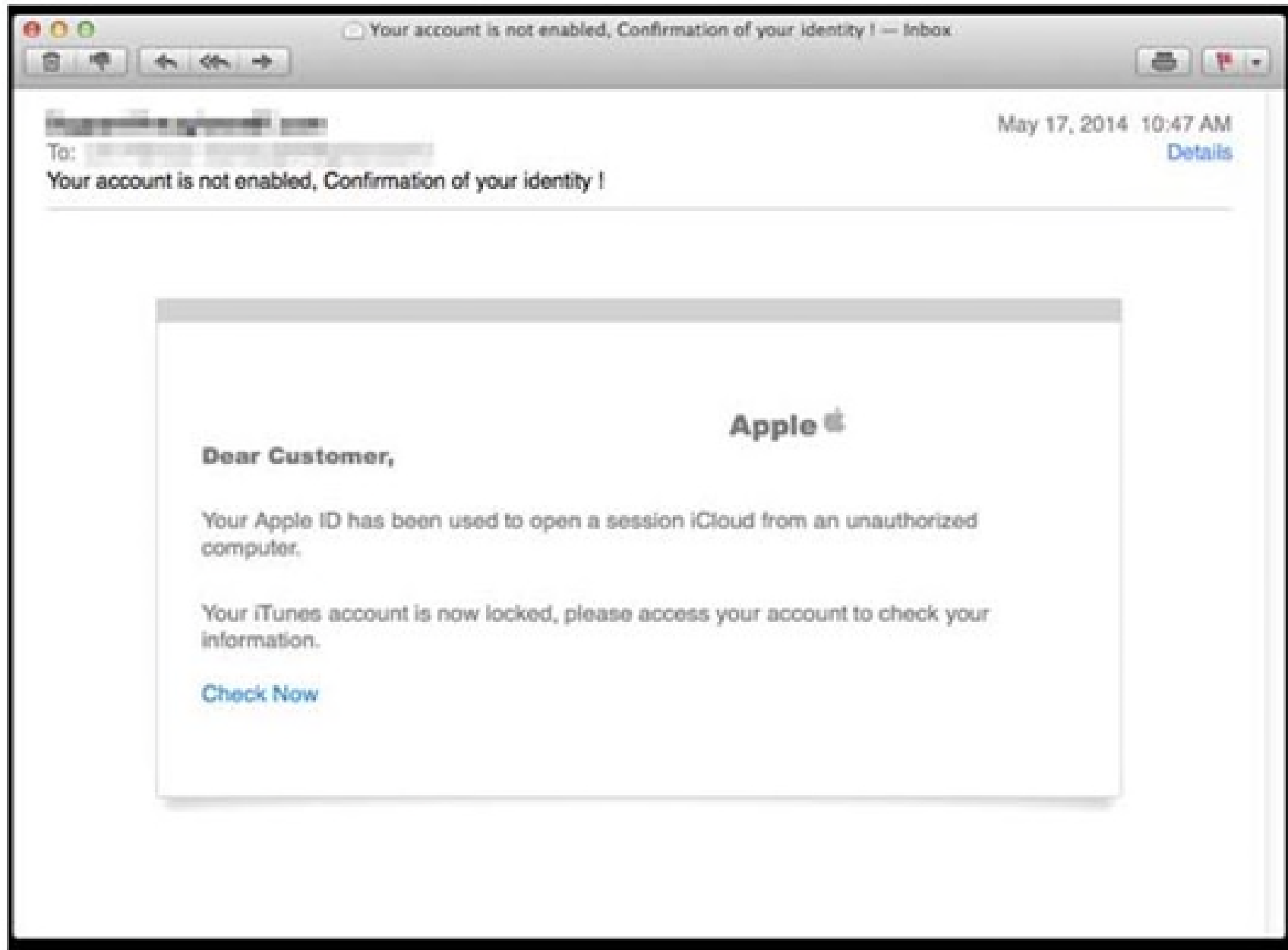
Your closing disclosure has been finalized and we're clear to close, You need to have the cash to close wire to our trust account today to avoid closing delay let me know if you can take care of it so i can forward you the wiring instructions.


Even Well-Protected People Get Hacked


(hint: you don't need to be famous to be hacked)



'Celebgate' attack leaks nude photos of celebrities








iCloud


John Appleseed

j.appleseed@icloud.com

Account details...


☒


iCloud Drive

☒



Photos

Options...

☒


Mail, Contacts, Calendars, and Tasks

With Outlook

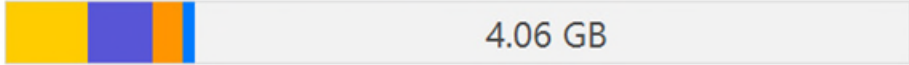
☒


Bookmarks

With Internet Explorer

Options...

You have 5.00 GB of iCloud storage.



4.06 GB

Storage

Sign out

Apply

Cancel

iCloud Help

Ways To Get Hacked #2

(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



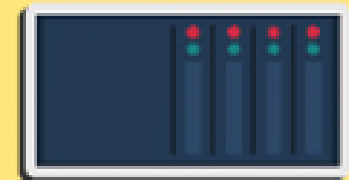
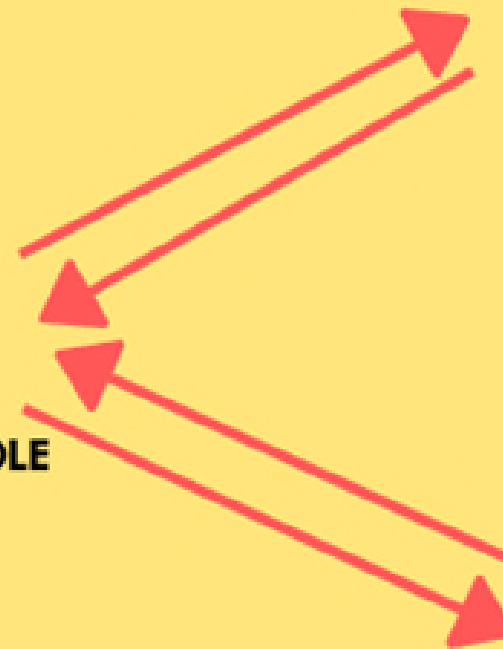
CLIENT



MAN IN MIDDLE CONNECTION



MAN IN THE MIDDLE



SERVER



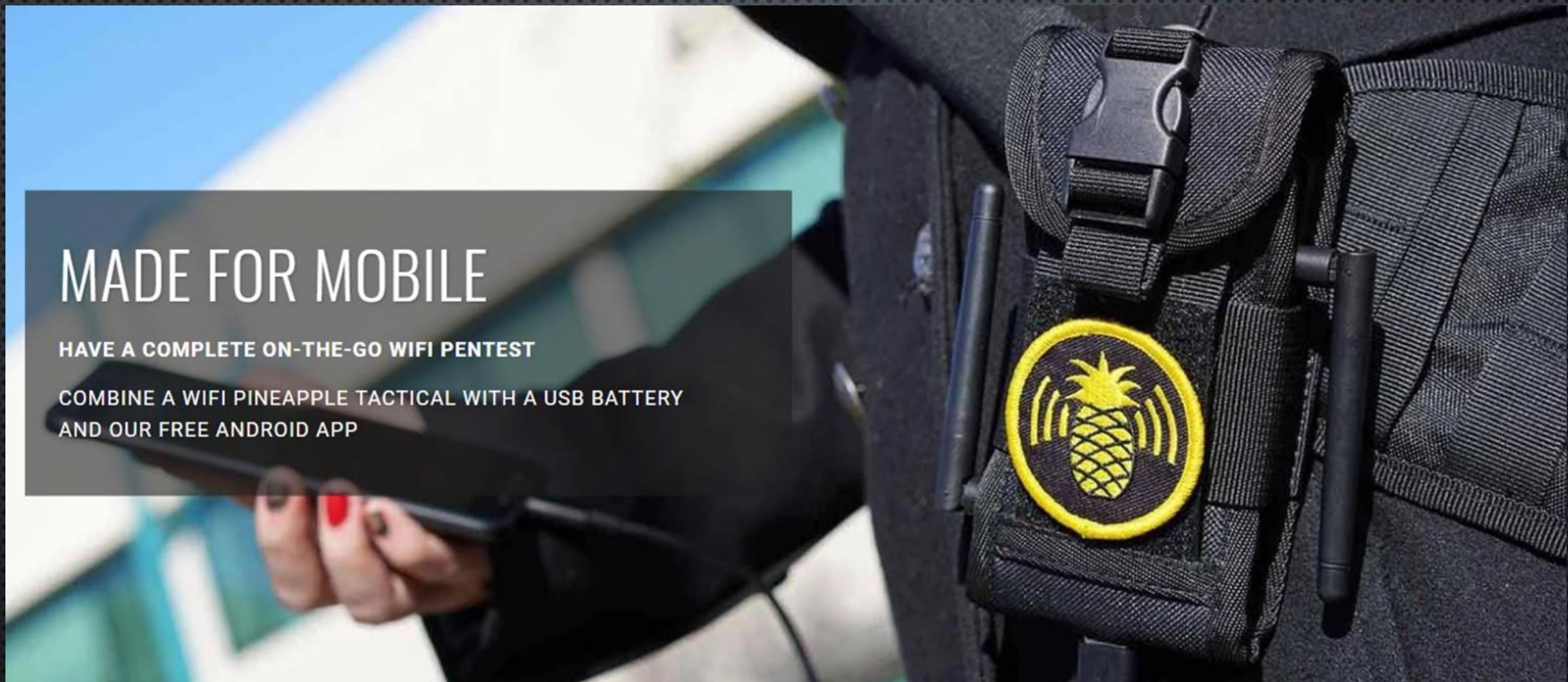
CLIENT



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



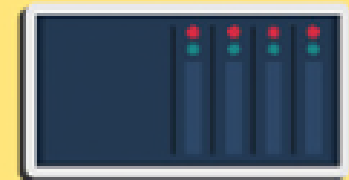
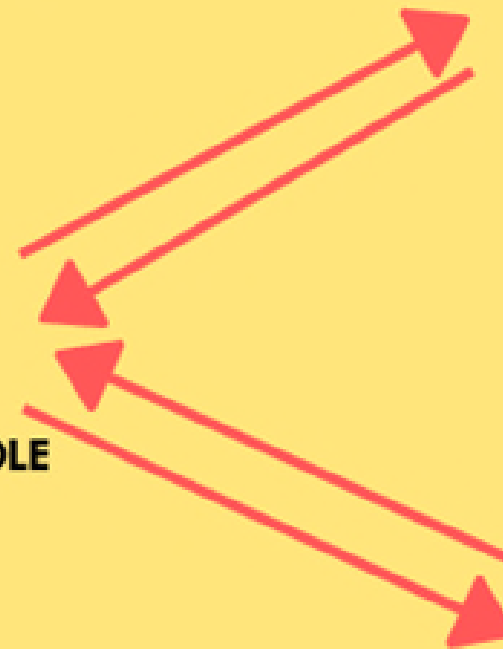
CLIENT



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](#)



- WIFI PINEAPPLE TETRA -

ULTIMATE AMPLIFIED DUAL-BAND POWERHOUSE

\$200



- WIFI PINEAPPLE NANO -

SIMPLE POCKET-SIZED WIFI PENTEST COMPANION

\$100

Ways To Get Hacked #3

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

Data Breach!



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & C

HAVE I BEEN PWNED? EPIKALLY SO —

Epik data breach impacts 15 million users, including non-customers

Scraped WHOIS data of NON-Epik customers also exposed in the 180 GB leak.

AX SHARMA - 9/20/2021, 8:32 AM

◆ WSJ NEWS EXCLUSIVE

T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'

A 21-year-old American said he used an unprotected router to access millions of customer records in the mobile carrier's latest breach

60M records exposed: Fitbit, Apple, Google health info leaked in massive data breach

BY CHARLIE FRIPP, KOMANDO.COM • SEPTEMBER 14, 2021 SHARE:

September 7, 2021
4:56 PM EDT
Last Updated 16 days ago

Litigation Data Privacy

Financial institutions clear hurdle in Sonic data breach case

Wearable Fitness Trackers the Target of a Data Breach

In Compliance September 22, 2021

TOP 10 WORST DATA BREACHES IN 2021

LATEST NEWS TECH NEWS

by Madhurjya Chowdhury / September 23, 2021

OPINION

Florida's lagging effort on cybersecurity puts us all at risk | Editorial

Staff vacancies and a lack of urgency leave the state vulnerable.

Not Just Liability: ETHICS

4-1. CLIENT-LAWYER RELATIONSHIP

RULE 4-1.1 COMPETENCE

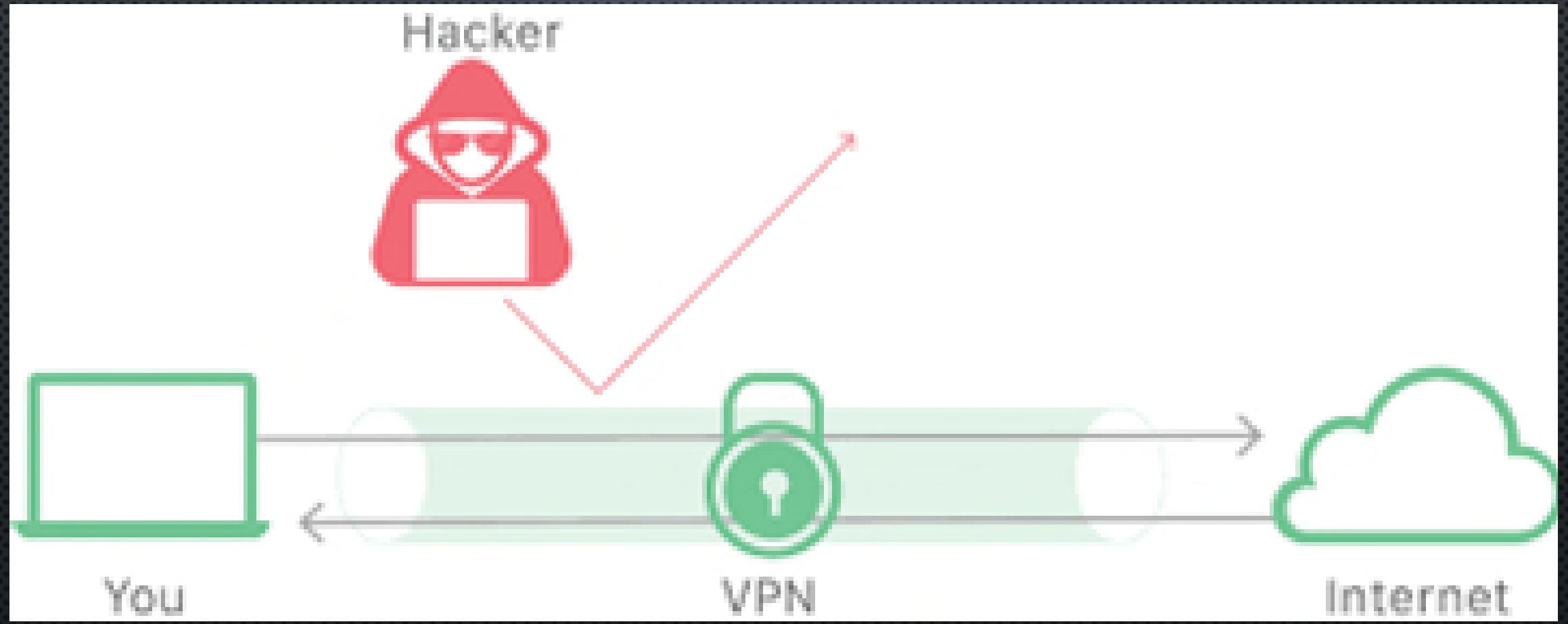
A lawyer must provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

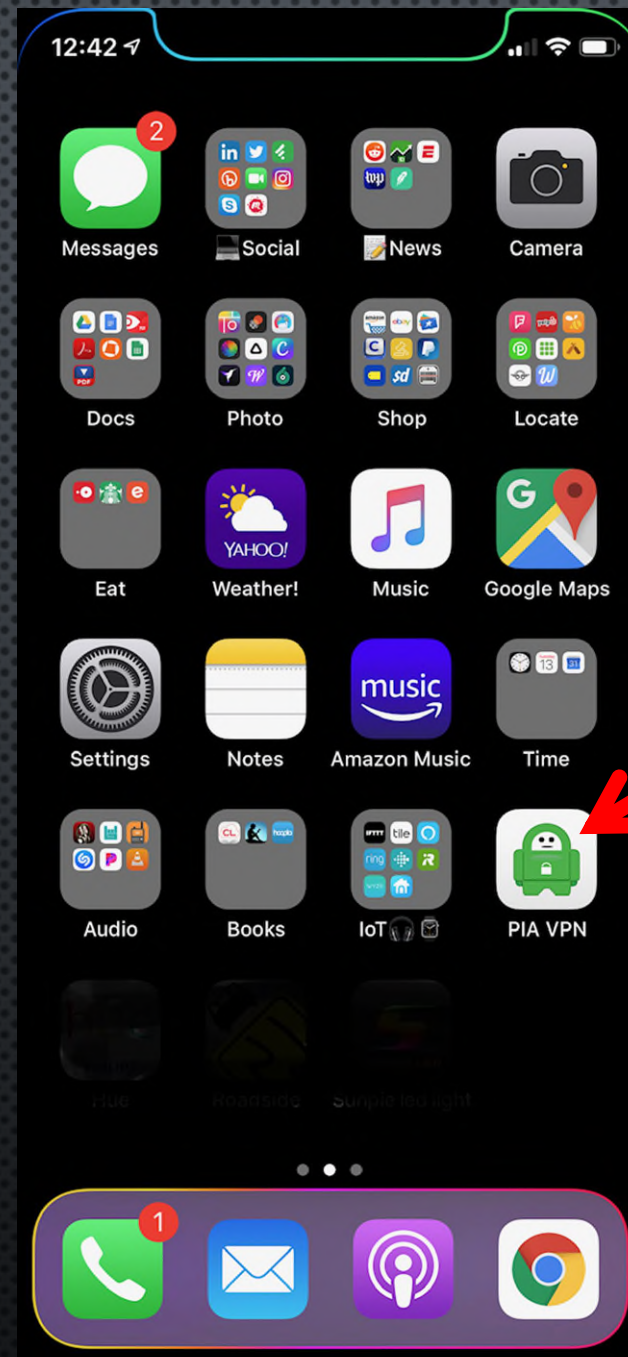
Maintaining competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education, including an understanding of the benefits and risks associated with the use of technology, and comply with all continuing legal education requirements to which the lawyer is subject.

SOLUTION #1:

Virtual Private Network (VPN)





12:44



Settings



Christopher Hopkins

Apple ID, iCloud, iTunes & App Store



Airplane Mode



Wi-Fi

MH >



Bluetooth

On >

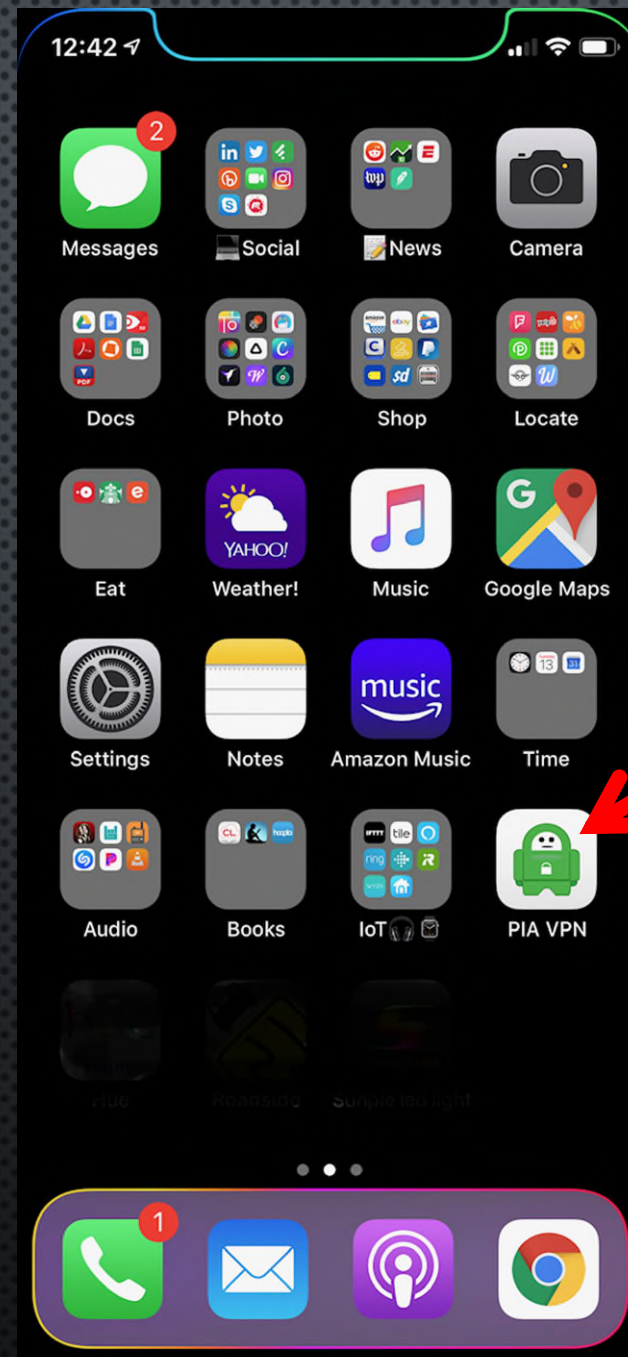


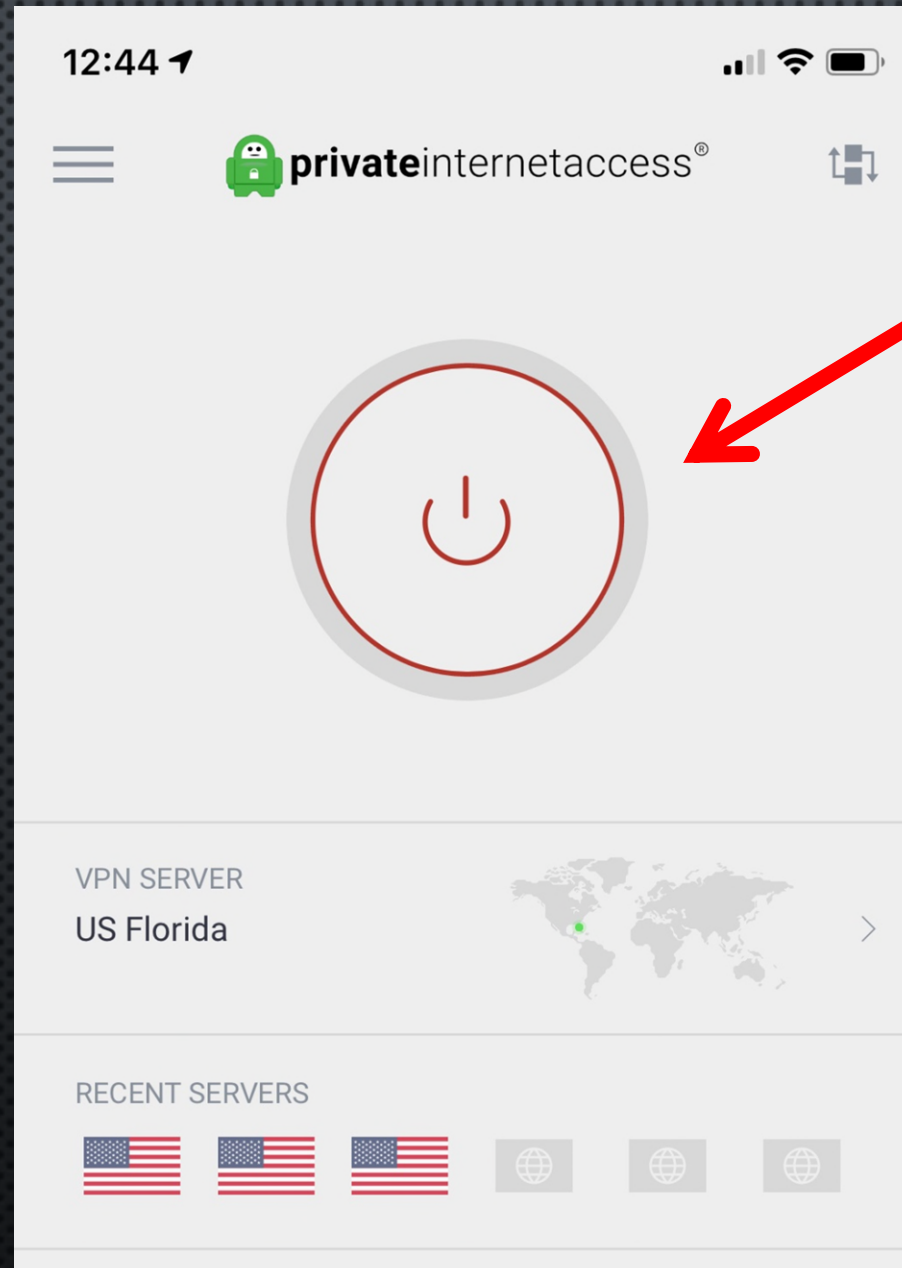
Cellular

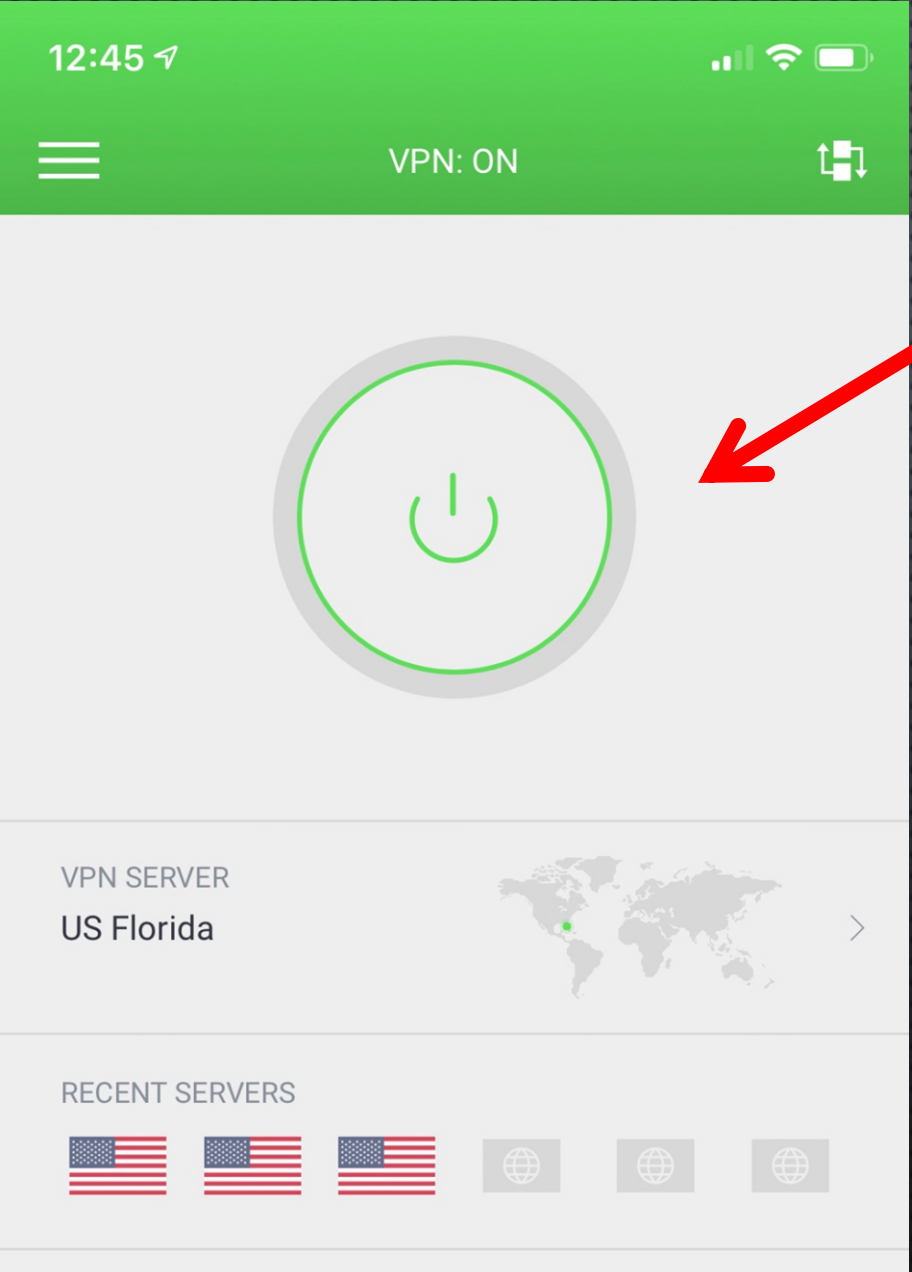


VPN











SOLUTION #2:

Outsmart the Business Email Compromise



Here's How the Hackers Are Finding You

Find a Victim's Website



McDonald Hopkins

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

MH2020 CAREERS



ABOUT

INSIGHTS

EVENTS

TEAM

EXPERTISE

▼ CONTACT

▼ OFFICES

MH2020 | CELEBRATING 90 YEARS

Honoring the past | Embracing the future →



ALERTS

President Biden's Six Prong COVID-19 Action Plan: What employers need to know about the Path out of the Pandemic

Friday, September 10, 2021

[Learn more](#)


A Website Tells A Lot!



McDonald Hopkins Attorney **Insight. Business Foresight.** MH2020 CAREERS

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

MH2020 | CELEBRATING 90 YEARS Honoring the past | Embracing the future →



ALERTS
President Biden's Six Prong COVID-19 Action Plan: What employers need to know about the Path out of the Pandemic
Friday, September 10, 2021

[Learn more](#)

Let's Gather 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.

Here's How the Dark Web Makes it Worse



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

(remember all those data breaches?)

[Link](#) ▲ 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

```
rexmundi412@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$12$mn5HZtecVpptcb7GzJKoAu8QZsSdu0G4LifSEPTBruu9kMvXw$2014-01-06  
carolinelaine:carrye58@hotmail.com:02988cb139bdc97fa0e18ead002dea  
carolinelambie:caroline_lambie@yahoo.co.uk:6cf60b614a06f7e4124696003f1e2b1d  
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.e61OzXmkaL5w8Pu/M.QtoJ7qCrS.EL8D2ZS$2014-01-06
```

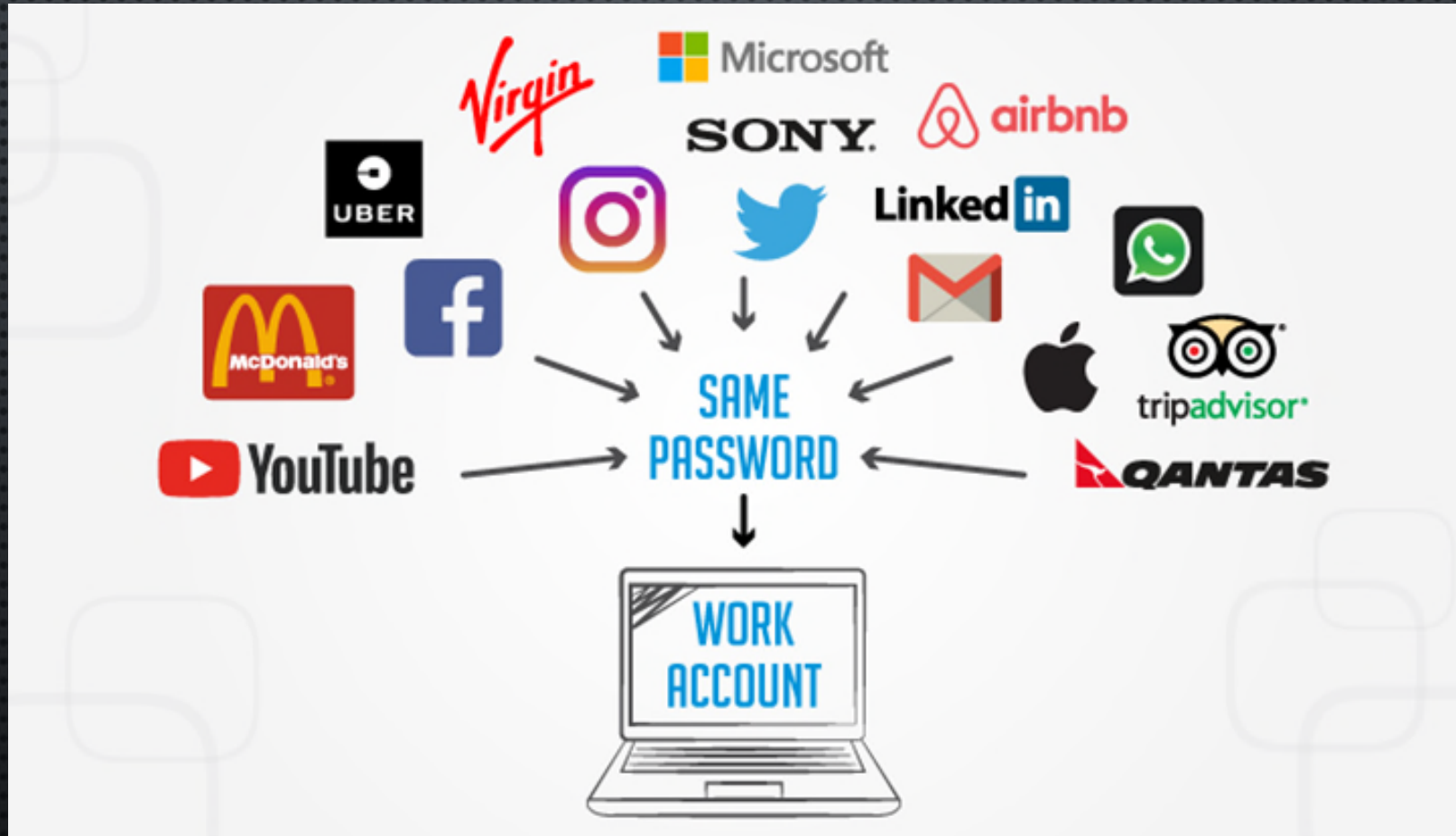
[Full Data](#)

[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)





Protect You & Your Firm



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 [Online Spambot accounts](#)

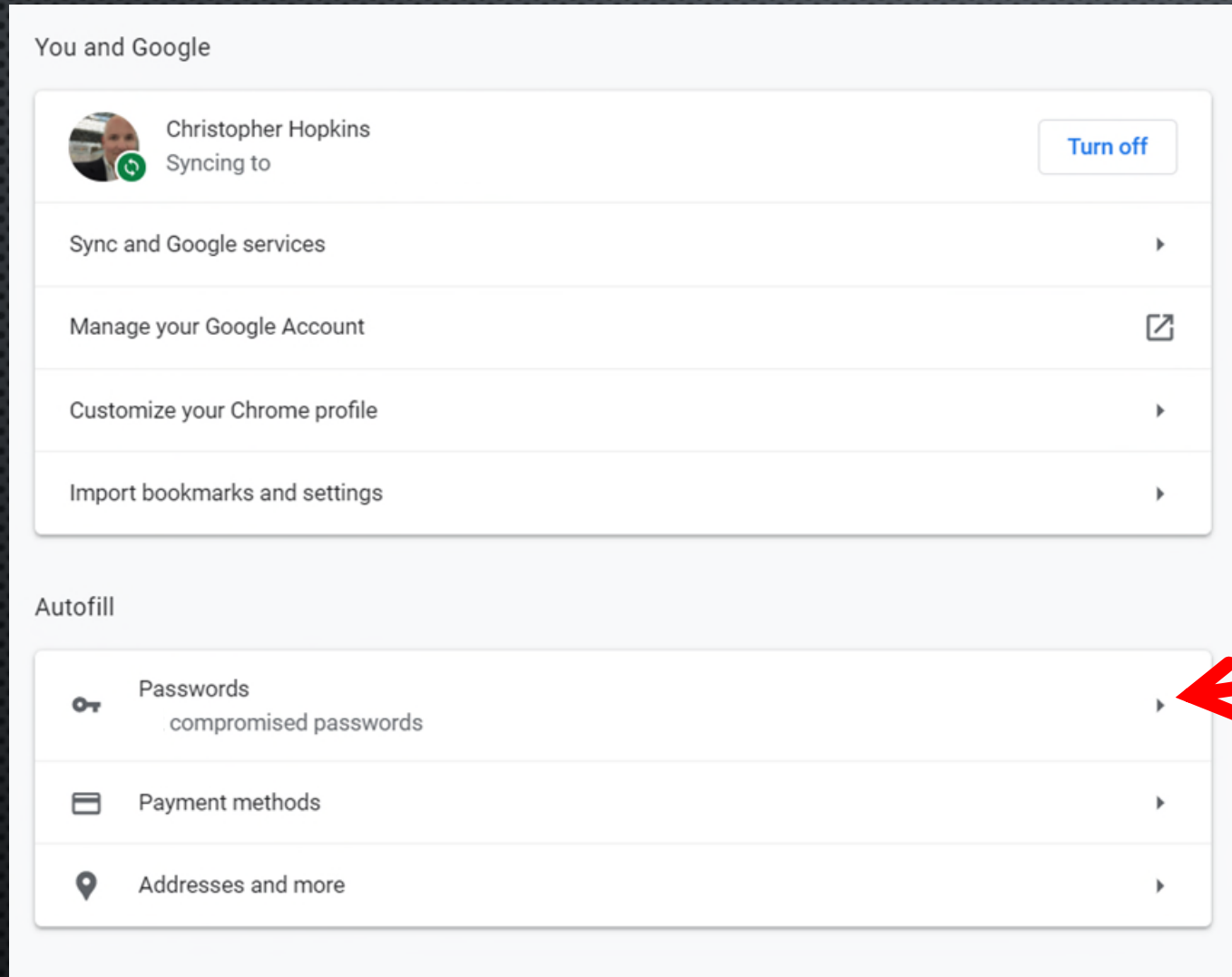
Recently added breaches

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

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

 878,209 [Imavex accounts](#)

Gmail Searches for Your Hacked Accts



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 “Fake” Emails... 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.

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:

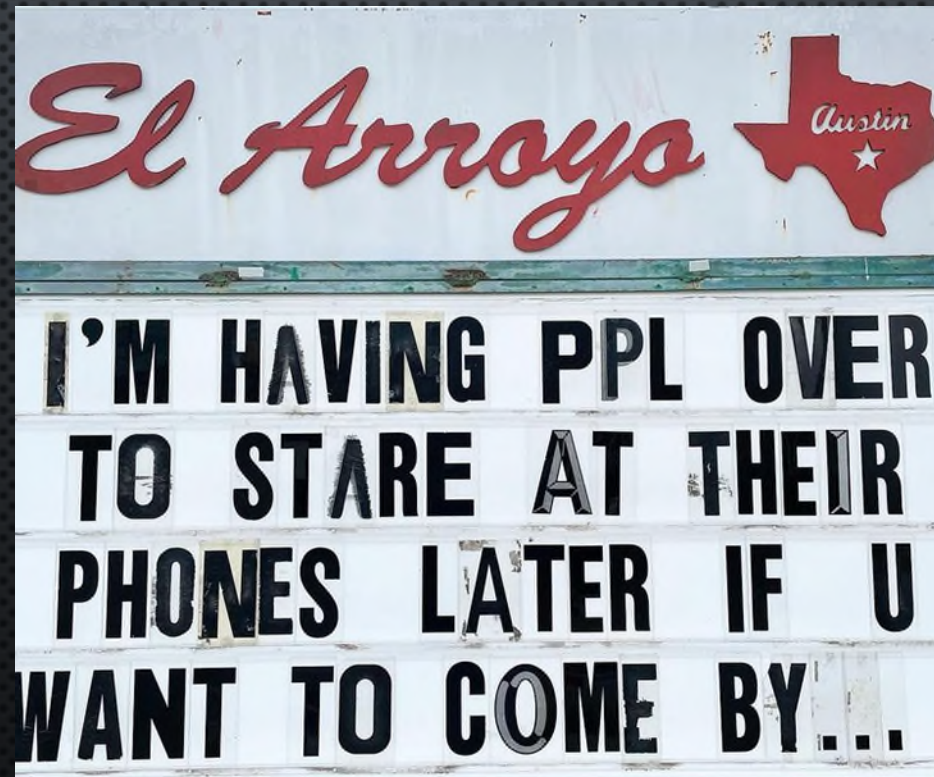
- don't re-use passwords*
- training*
- MFA*
- sign up for HIBP (all employees)*
- password managers*
- e-retention policies*

- **Data Breaches** (your system)

SOLUTION:

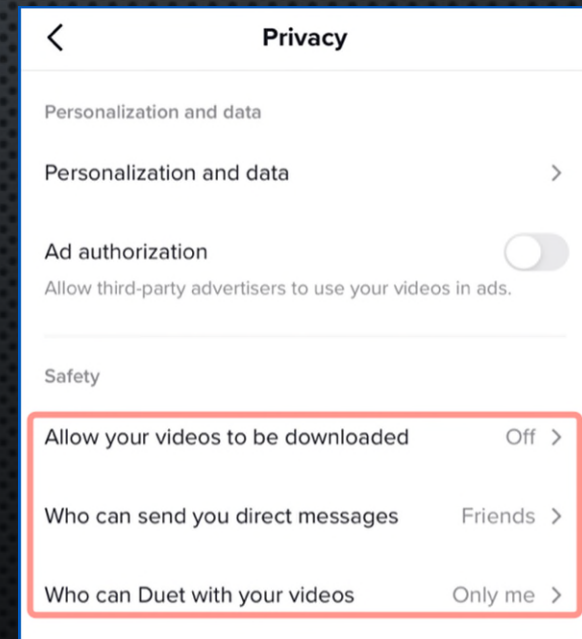
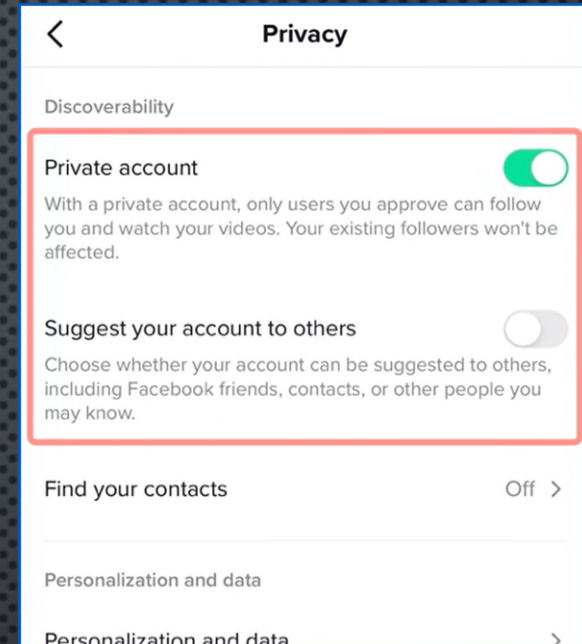
- MFA*
- Anti-malware*
- Backups*
- IT to limit incoming IP addresses (monitor traffic)*
- Don't give admin level access*
- E-retention policies*
- Routine searches for your info on dark web*

Protect Your Social Media Profiles



Protect Your Accounts & Profiles – Tik Tok

- **Make Your Account Private**
 - Settings / Privacy and Safety / Discoverability
 - Turn on “private account”
- **Don't Be “Suggested”**
 - Settings / Privacy and Safety / Discoverability
 - Turn off “suggest your account to others”
- **Don't Interact**
 - Settings / Privacy
 - Turn off “allow your videos to be downloaded”
 - Turn off “send you messages” and “Duet”



Credit: [Naked Security](#)

Protect Your Accounts & Profiles – Facebook

- What Apps have access?
 - Apps and Websites page, view Active apps
- Privacy section
 - Go through each setting
- Limit Past Posts
 - Privacy / Limit the audience for posts you've shared
 - Then click "limit last posts"
- Who Has Been Logging in?
 - Security and Login page / Where You've Logged In
 - This will tell you what devices logged in and ability to delete all posts

Protect Your Accounts & Profiles – Instagram

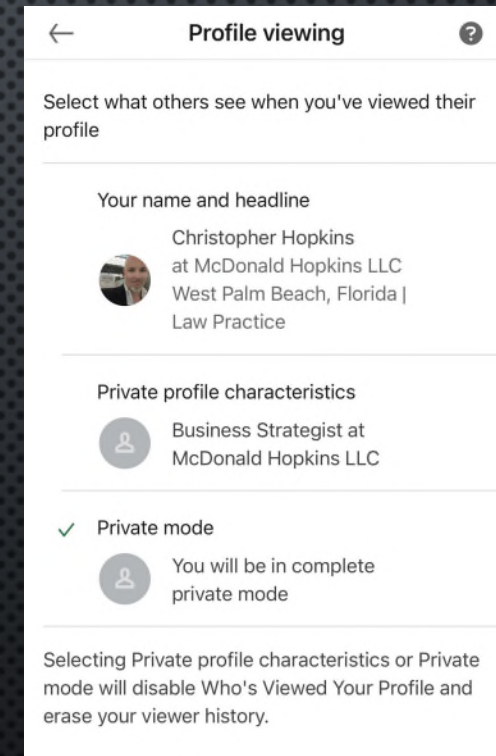
- Location
 - Settings / Privacy / Location Services / Instagram / never
- Posts Only Shared With Friends
 - Profile (bottom right) / three lines upper right / Settings / Privacy / Private Account - on
- Disconnect Apps
 - Same steps / Settings / Security / Apps and Websites / Active
- Opt Out of Personal Ads
 - Settings / Ads / Data About Your Activity from Partners - off

Protect Your Accounts & Profiles – Twitter

- **Location**
 - Three lines upper left / Settings and Privacy / Privacy and Safety
Precise location - disabled
- **No Birthdate**
 - Three lines / profile pic / Edit Profile / delete bday
- **Opt Out of Personal Ads**
 - Three lines upper left / Settings and Privacy / Privacy and Safety
Personalization and data - off

Protect Your Accounts & Profiles – LinkedIn

- **Personal Data**
 - Profile pic upper left / Settings / Data Privacy Manage Your Data and Activity (see what LI has been doing w your info)
- **Advertising Data**
 - Settings / Advertising data / Location – off
 - ... Data Collected by LI – (make your choices)
 - ... Third Party Data – turn off all four
- **Visability**
 - Settings / Visibility / Profile viewing options



Finally... be careful what else is in your photo



Christopher Hopkins

@cbhopkins

Don't post photos of your desk (😬), your work badge (👤), even your house keys...



Subtle Information Hackers Find in the Background of Your Social Media Photos
And how you can better protect yourself against accidentally exposing personal information

medium.com

Some Handouts



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



[Article](#)



CHRISTOPHER B. HOPKINS

Privacy Settings for Zoom Video and Alexa

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.

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

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).

[Click for full article](#)



CHRISTOPHER B. HOPKINS

McDonaldHopkins

CHOPKINS@MCDONALDHOPKINS.COM



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



www.linkedin.com/in/cbhopkins/

InternetLawCommentary.com