Cyber Security & Data Breach for Mediators

McDonald Hopkins LLC
Attorneys at Law

chopkins@mcdonaldhopkins.com

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 SHARE SHARE EMAIL PRI

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

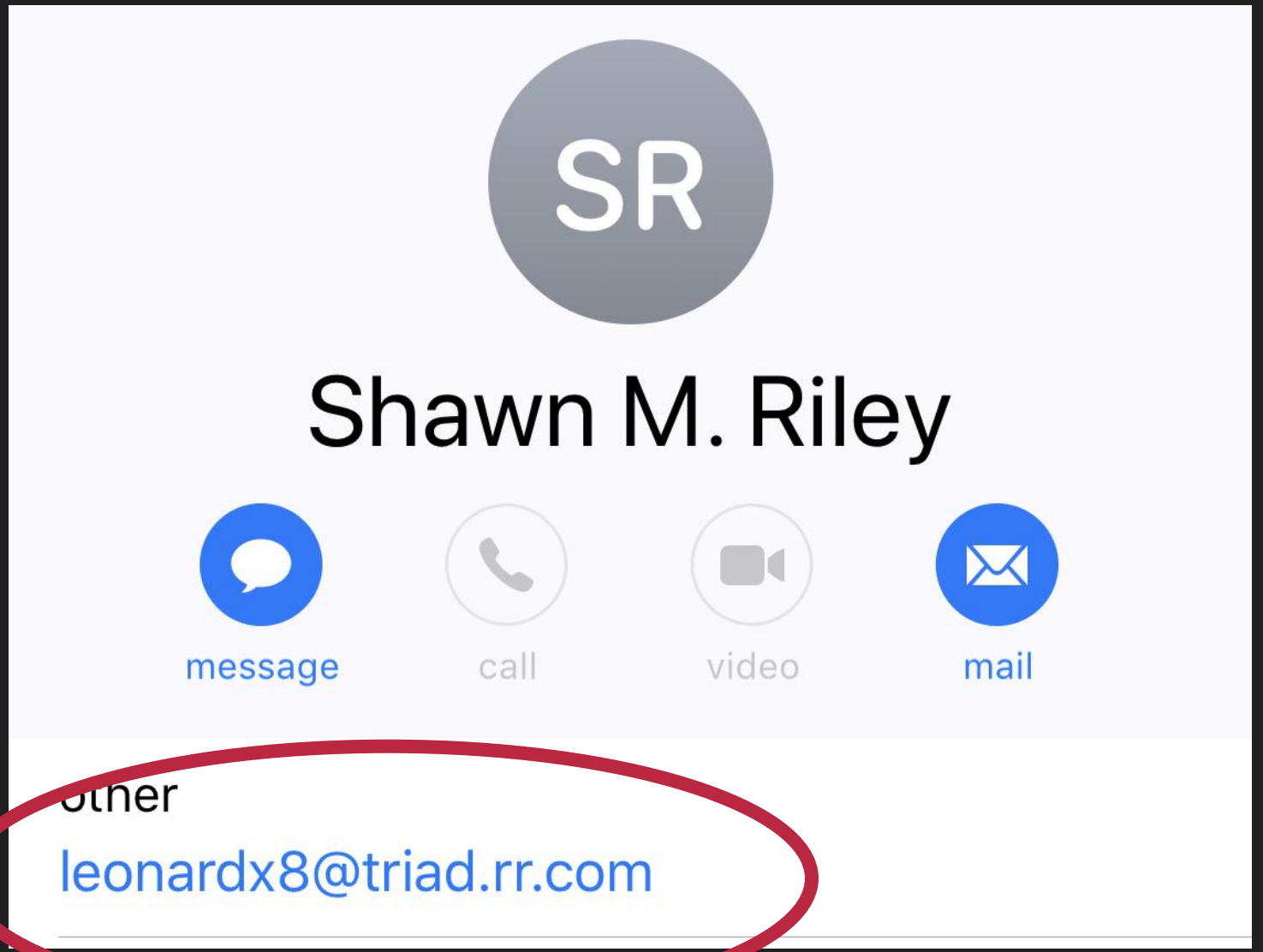
Hide

SR

Re: Request

Today at 8:12 AM

Can you help me with a quick task please?


SR
Shawn M. Riley
message
call
video
mail
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?

Social Engineering Attack

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

TOPICS:

1. What is a Data Breach
2. Ways To Get Hacked
3. Man in the Middle, VPN, Phishing, 2FA
4. Ransomware
5. U.S. Government’s Malware
6. Paul Manafort & PDF Redactions
7. Protecting You, Your Firm, Your Clients

What is Data Breach?

Definition: "A **data breach** is a security incident in which sensitive, protected or confidential **data** is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so."

Data breach - Wikipedia, the free encyclopedia

What are Hackers Trying to Steal?

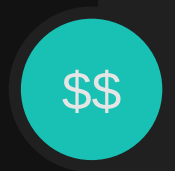
Personally Identifiable Information PII

FIRST name + LAST name +

Social, driver's license, credit card number, banking info, DOB, email and user names, security questions/answers, and biometrics (anything that leads to $$$)

Protected Health Information PHI

Medical records, health status, provision of health care, payment for health care



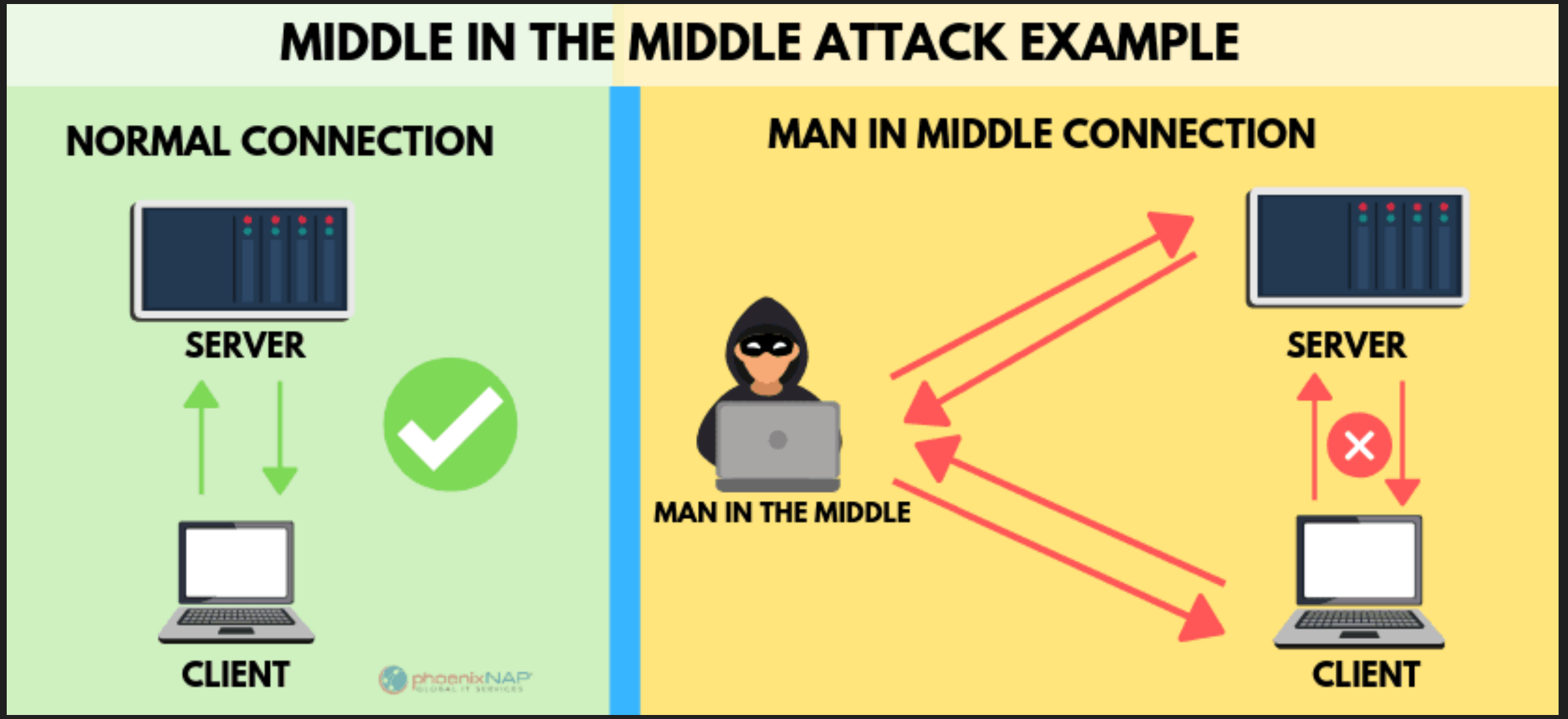
Money & Account Information

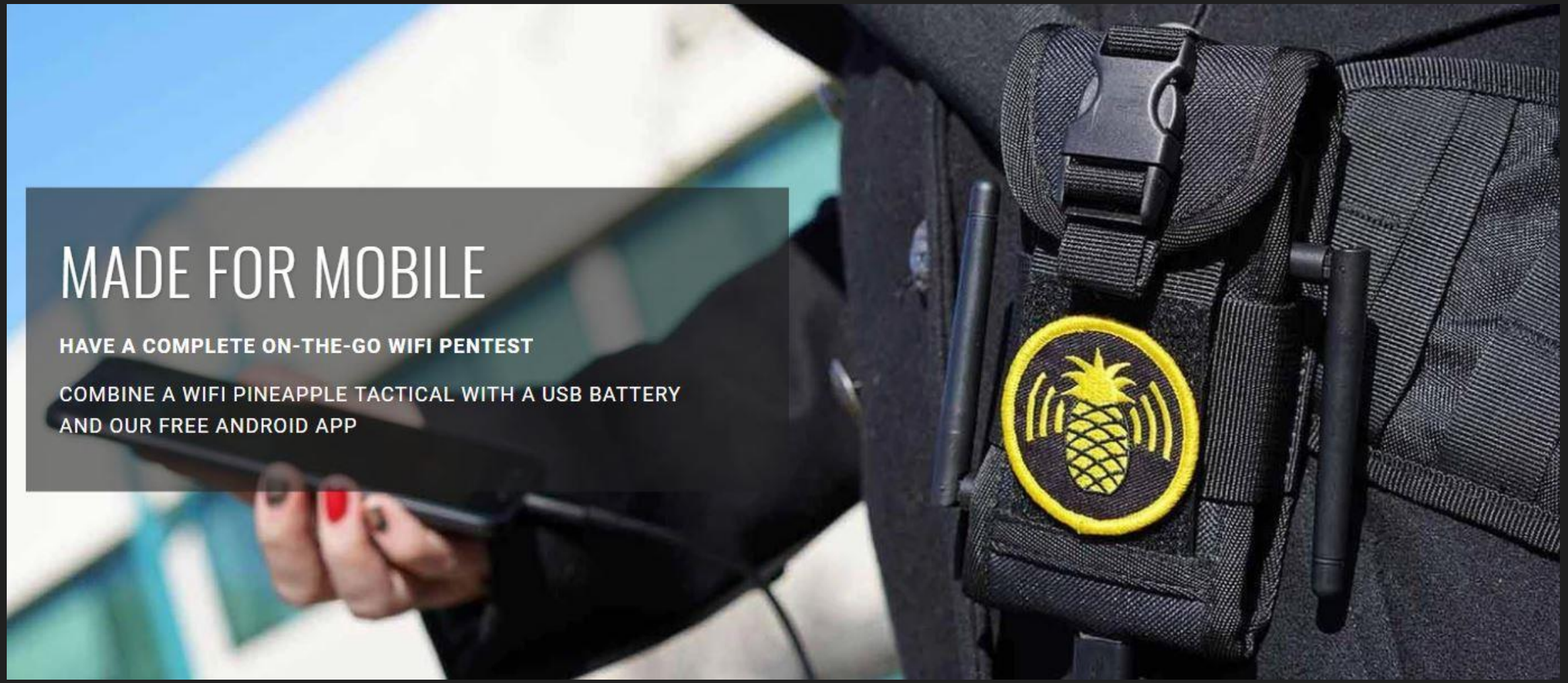
Account information. Ransomware.

Ways To Get Hacked

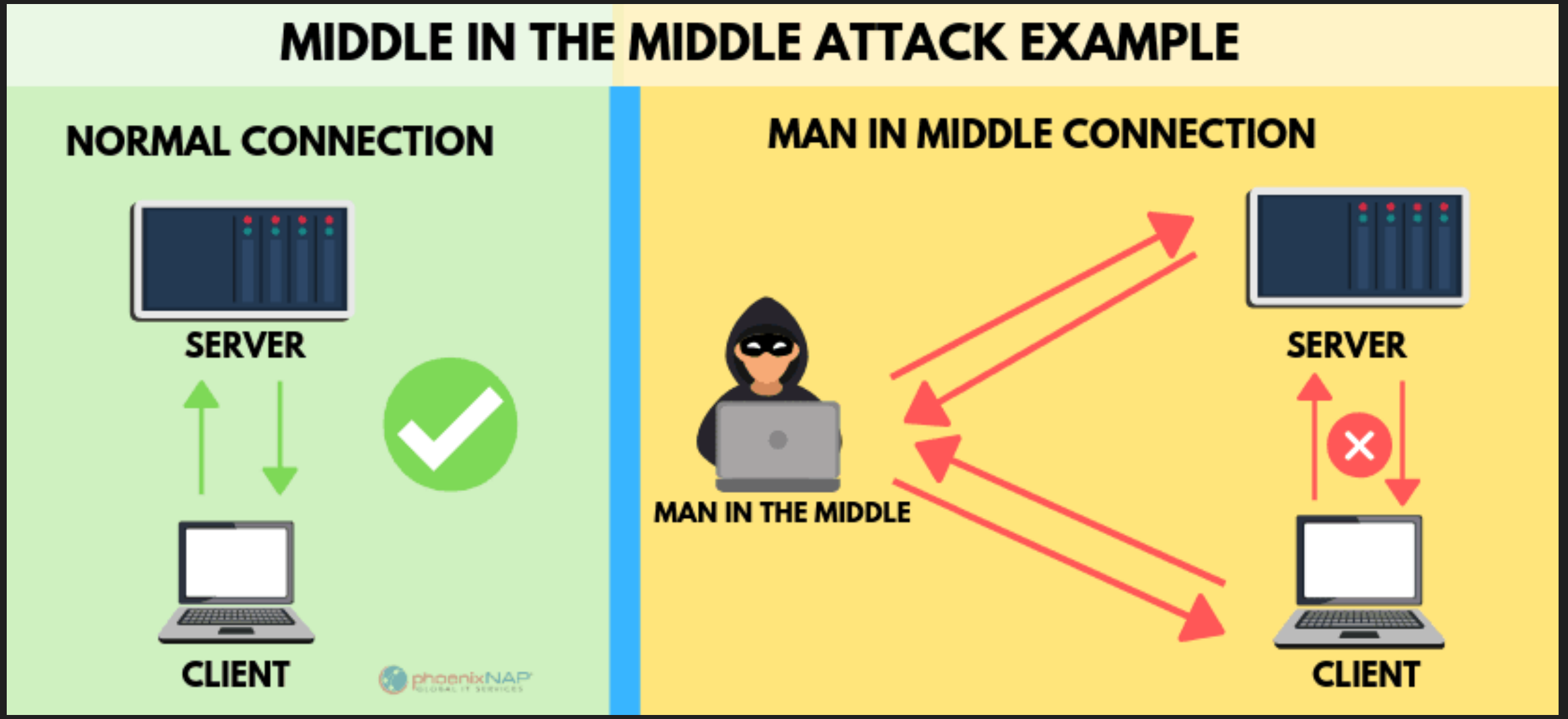
WiFi Pineapple

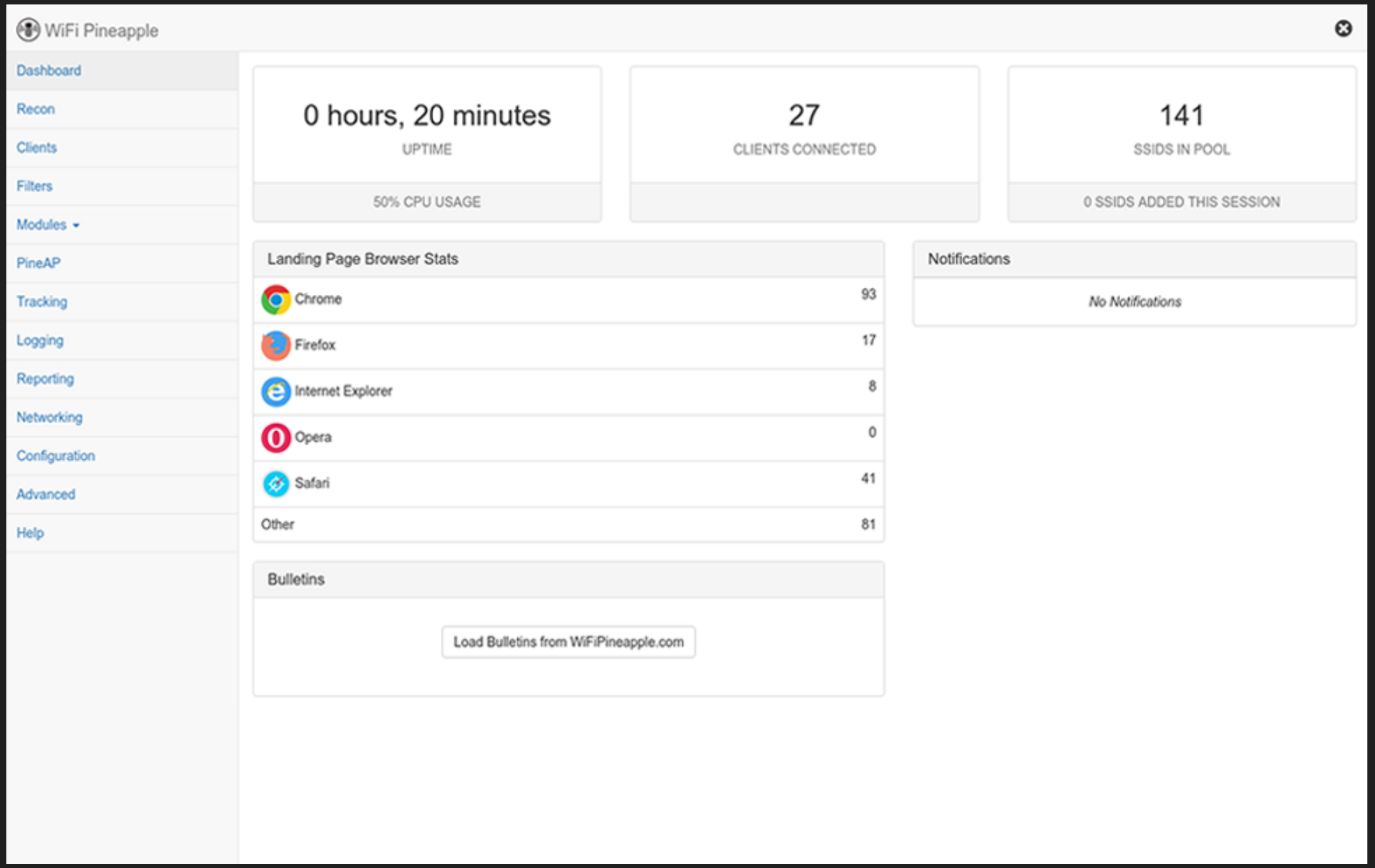
(Man In The Middle Attack)


MIDDLE IN THE MIDDLE ATTACK EXAMPLE
NORMAL CONNECTION
SERVER
CLIENT
phoenixNAP
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
phoenixNAP
MAN IN MIDDLE CONNECTION
MAN IN THE MIDDLE
SERVER
CLIENT


WiFi Pineapple
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

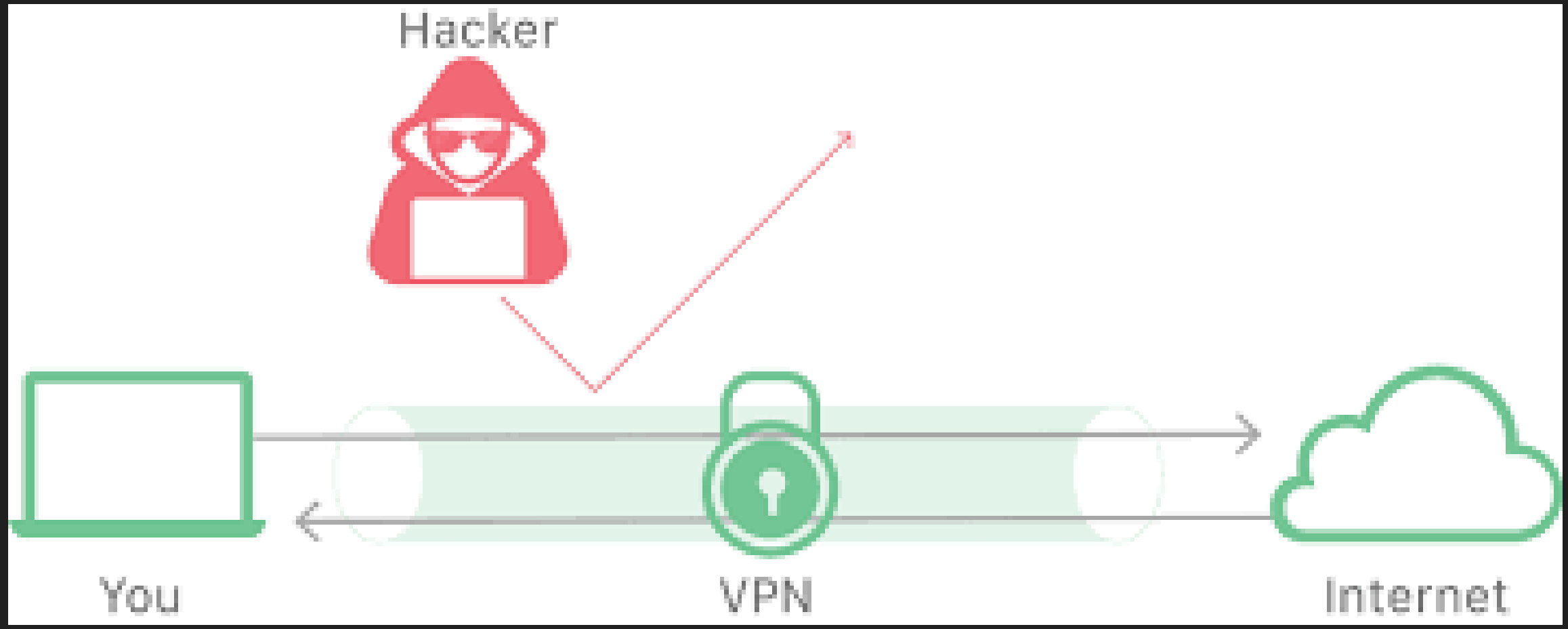
$100

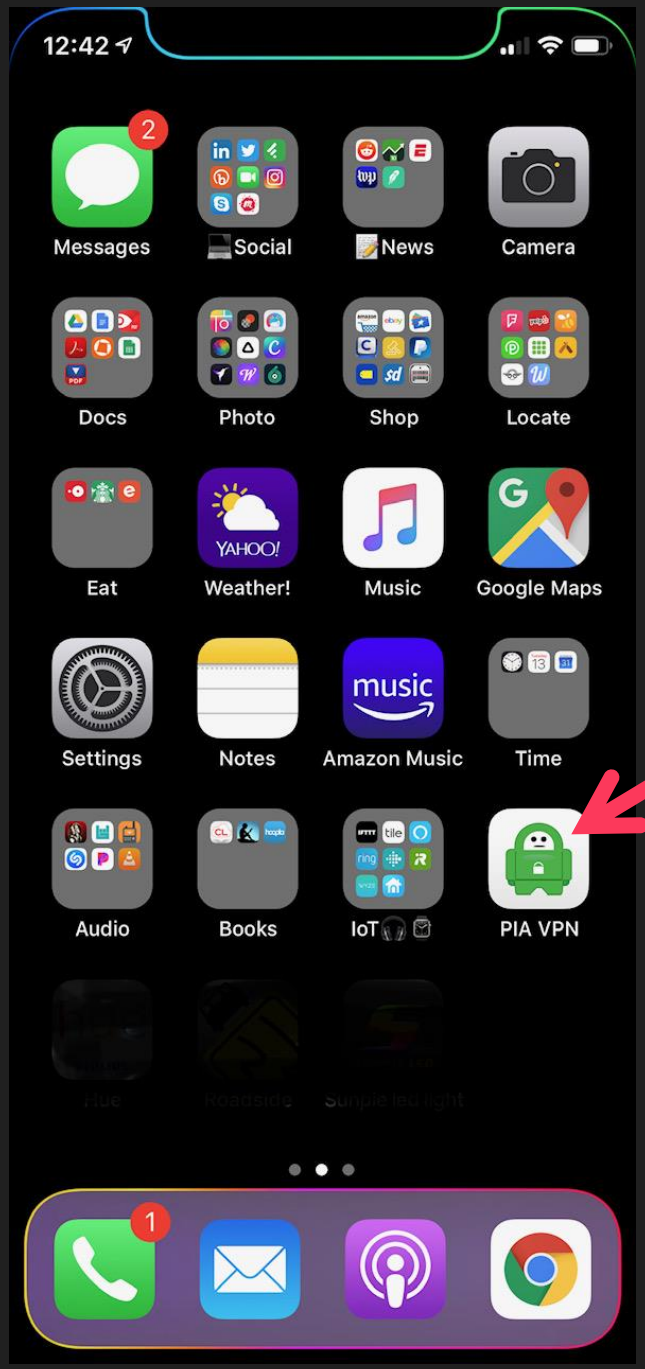
Did you connect to the conference wifi?

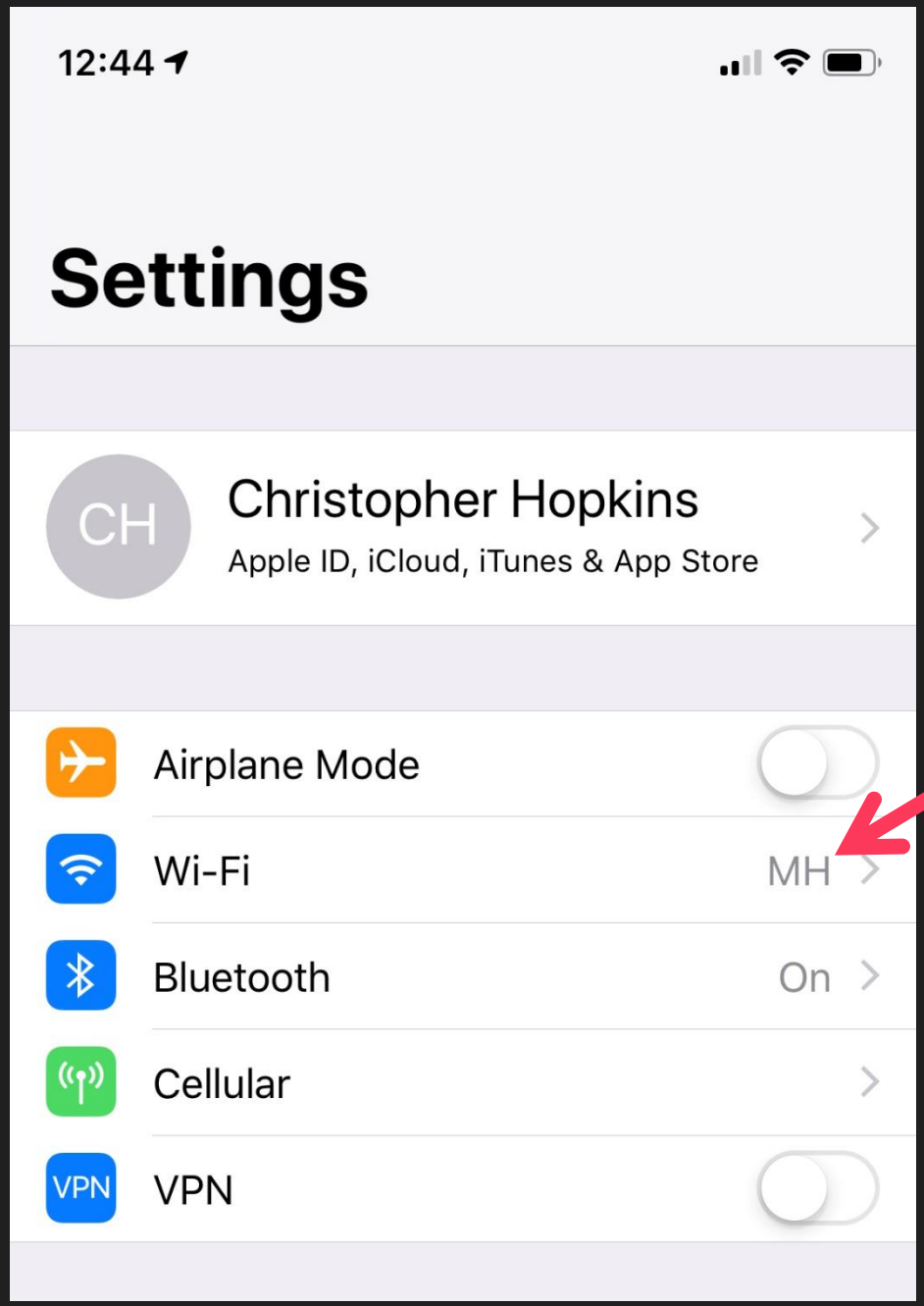
SURVEY #1

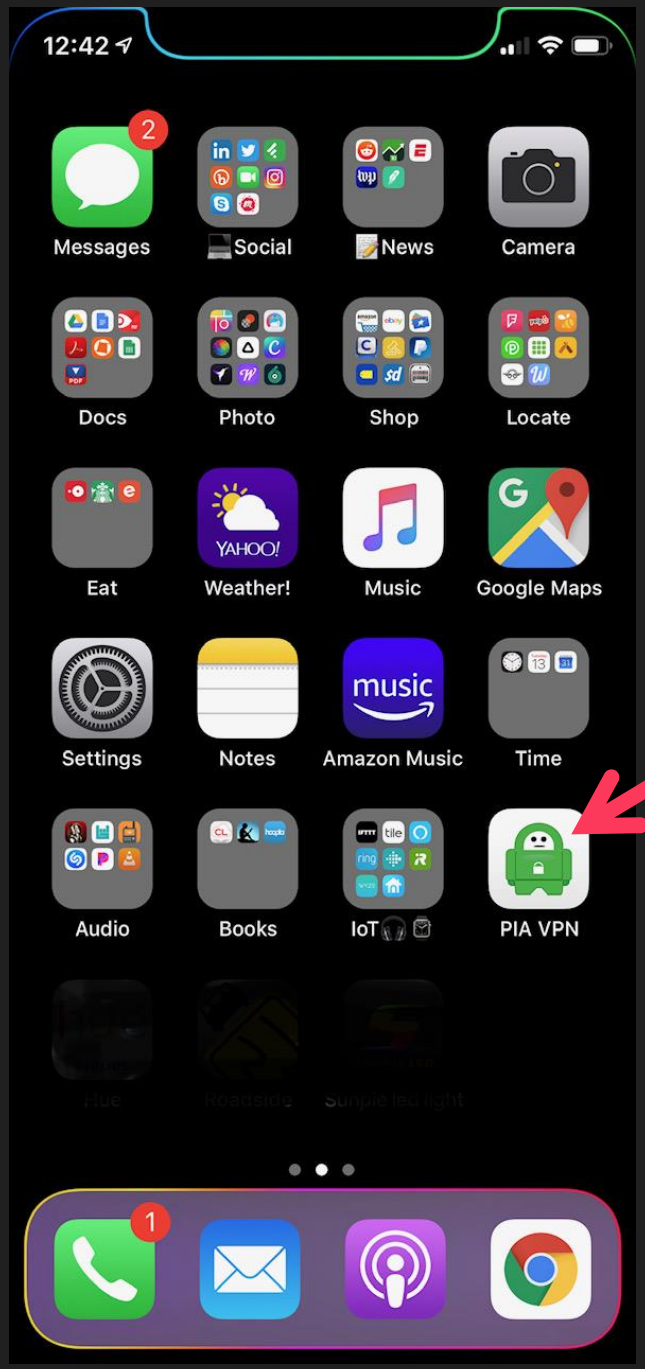
1. I connected to the wifi
2. I have not connected to the wifi
3. I did not connect to wifi due to security concerns
4. I connected to wifi and used VPN

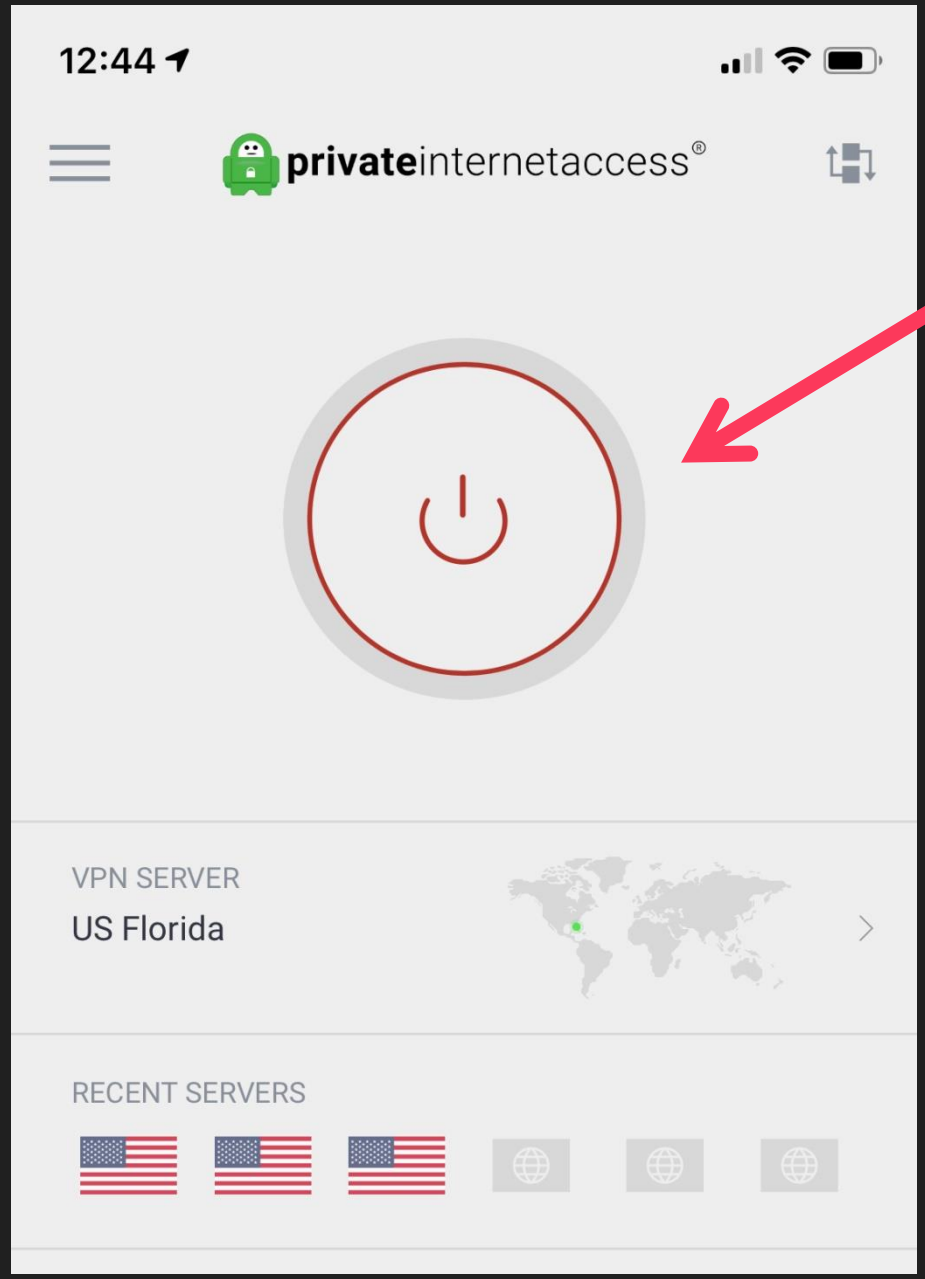
SOLUTION:
Virtual Private Network (VPN)

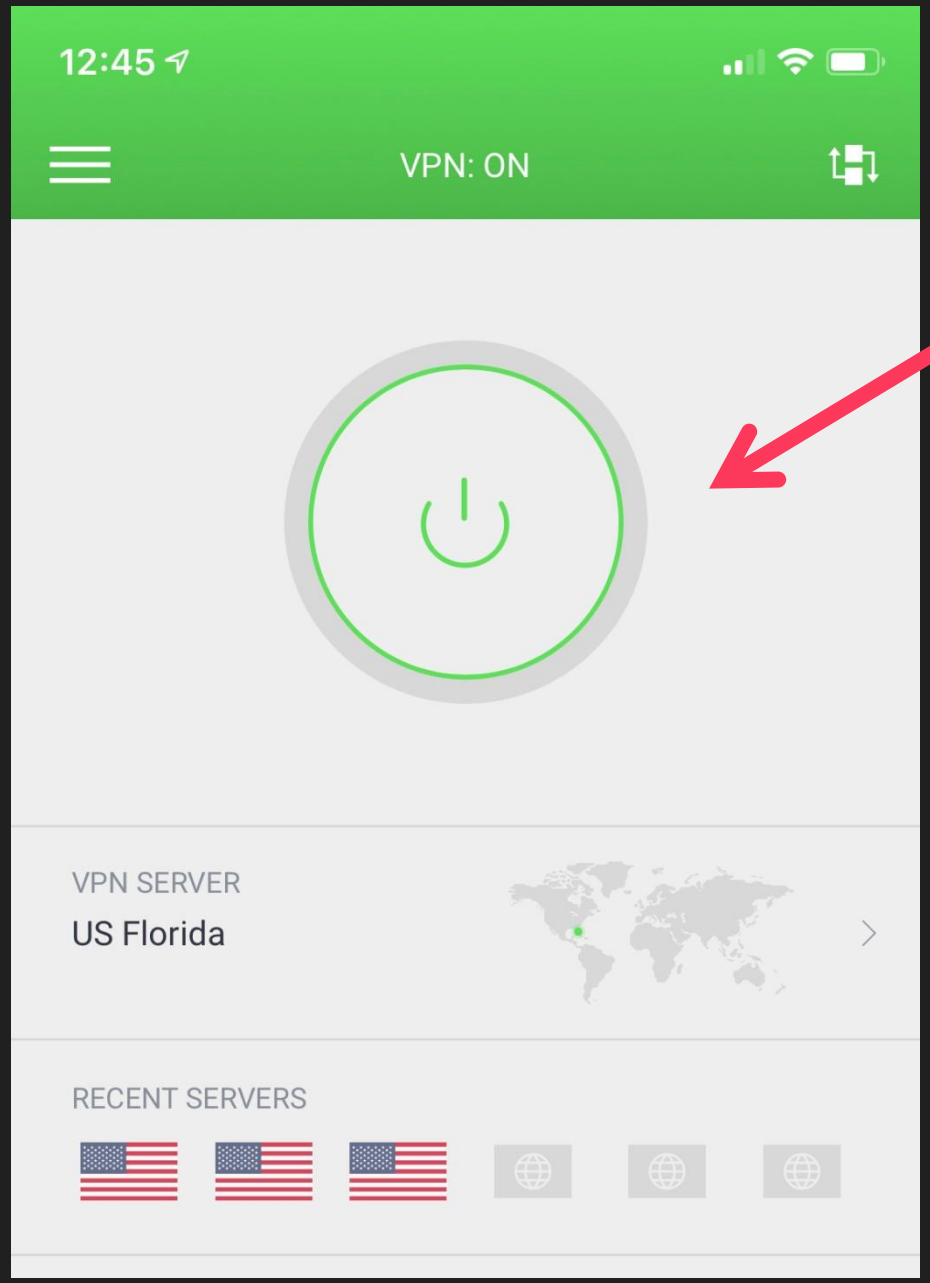

Hacker
You
VPN
Internet

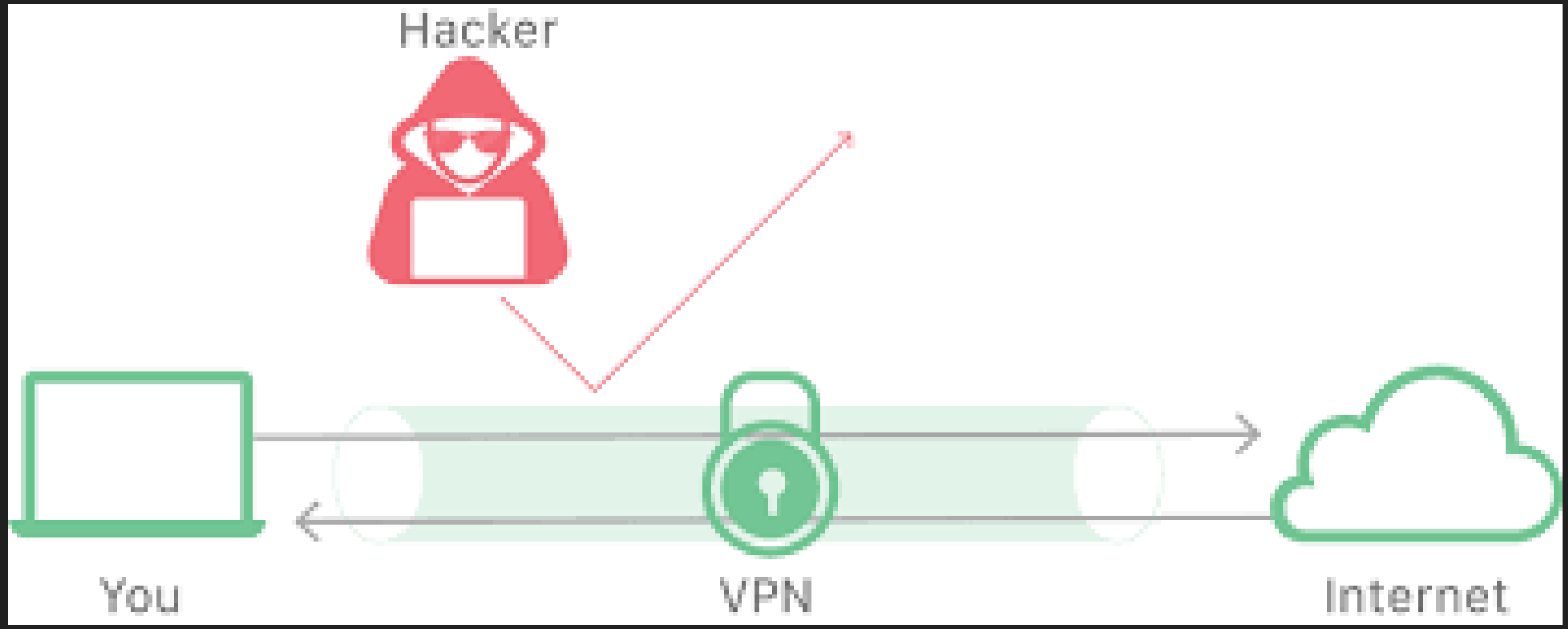

12:42
Messages
Social
News
Camera
Docs
Photo
Shop
Locate
Eat
Weather!
Music
Google Maps
Settings
Notes
Amazon Music
Time
Audio
Books
IoT
PIA VPN


12:44
Settings
CH
Christopher Hopkins
Apple ID, iCloud, iTunes & App Store
Airplane Mode
Wi-Fi
MH
Bluetooth
On
Cellular
VPN
VPN


12:42
Messages
Social
News
Camera
Docs
Photo
Shop
Locate
Eat
Weather!
Music
Google Maps
Settings
Notes
Amazon Music
Time
Audio
Books
IoT
PIA VPN


12:44
privateinternetaccess®
VPN SERVER
US Florida
RECENT SERVERS


12:45
VPN: ON
VPN SERVER
US Florida
RECENT SERVERS


Hacker
You
VPN
Internet

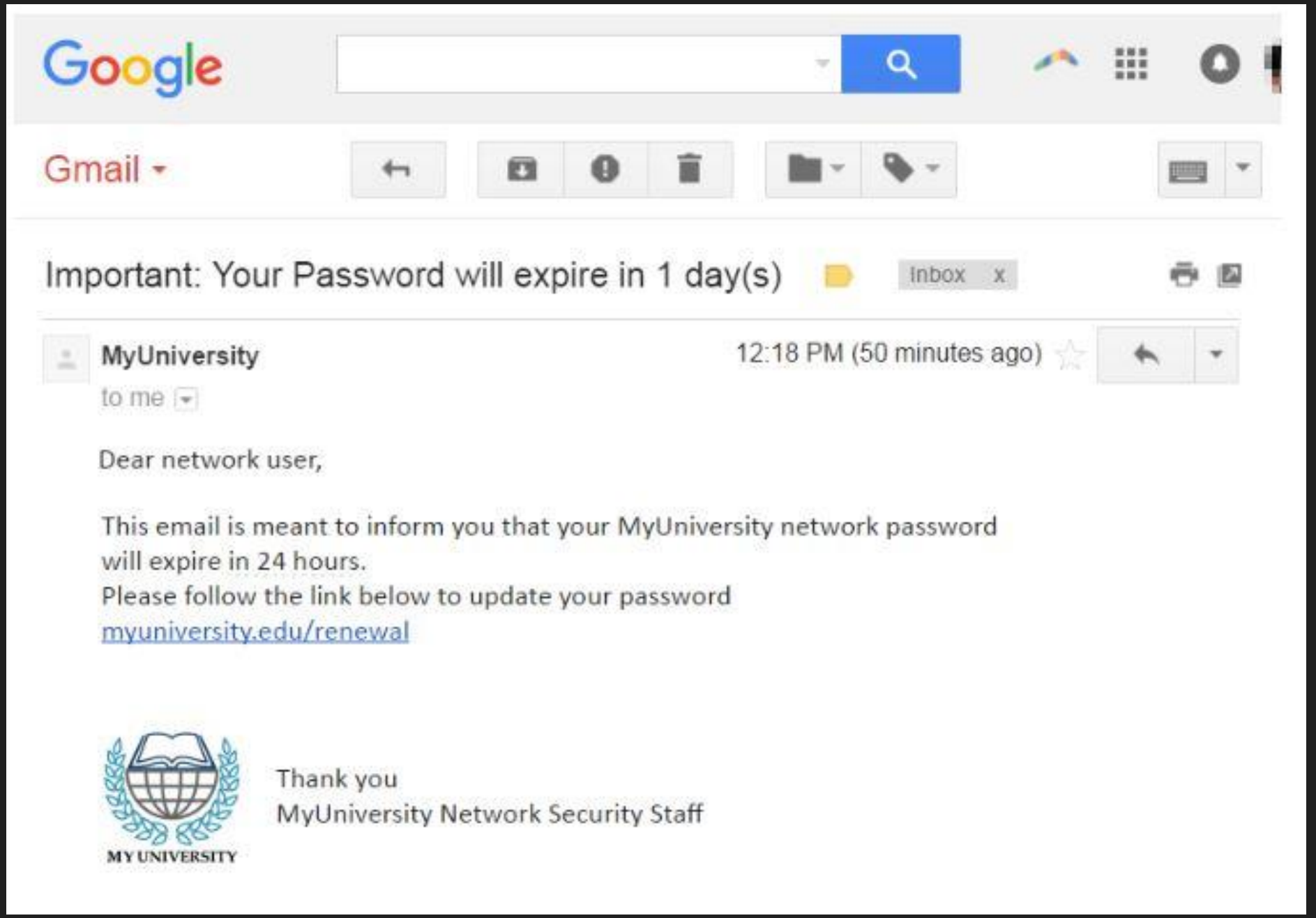
SECTION 3

Phishing

Spear Phishing

(& other ways to be hacked)

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.


Google
Gmail
Important: Your Password will expire in 1 day(s)
Inbox x
MyUniversity
12:18 PM (50 minutes ago)
to me
Dear network user,
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal
MY UNIVERSITY
Thank you
MyUniversity Network Security Staff


eFax Corporate
World Leader in Digital Faxing
Fax Message [Caller-ID: 1-887-749-9459
You have received a 1 page fax at Tue, 27 May 2014 09:23:19 GMT.
* The reference number for this fax is atl_did1-1400166434-28389721850-154
Click here to view this fax using your PDF reader.
DO NOT click this link or download/run the file
Please visit www.efax.com/en/efax/twa/page/help if you have any questions regarding this message or your service.
Thank you for using the eFax service!
j2 eFax eVoice FuseMail campaigner KeepItSafe onebox
2014 j2 Global, Inc. All rights reserved.
eFax is a registered trademark of j2 Global, Inc.

From: Netflix >

To: 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

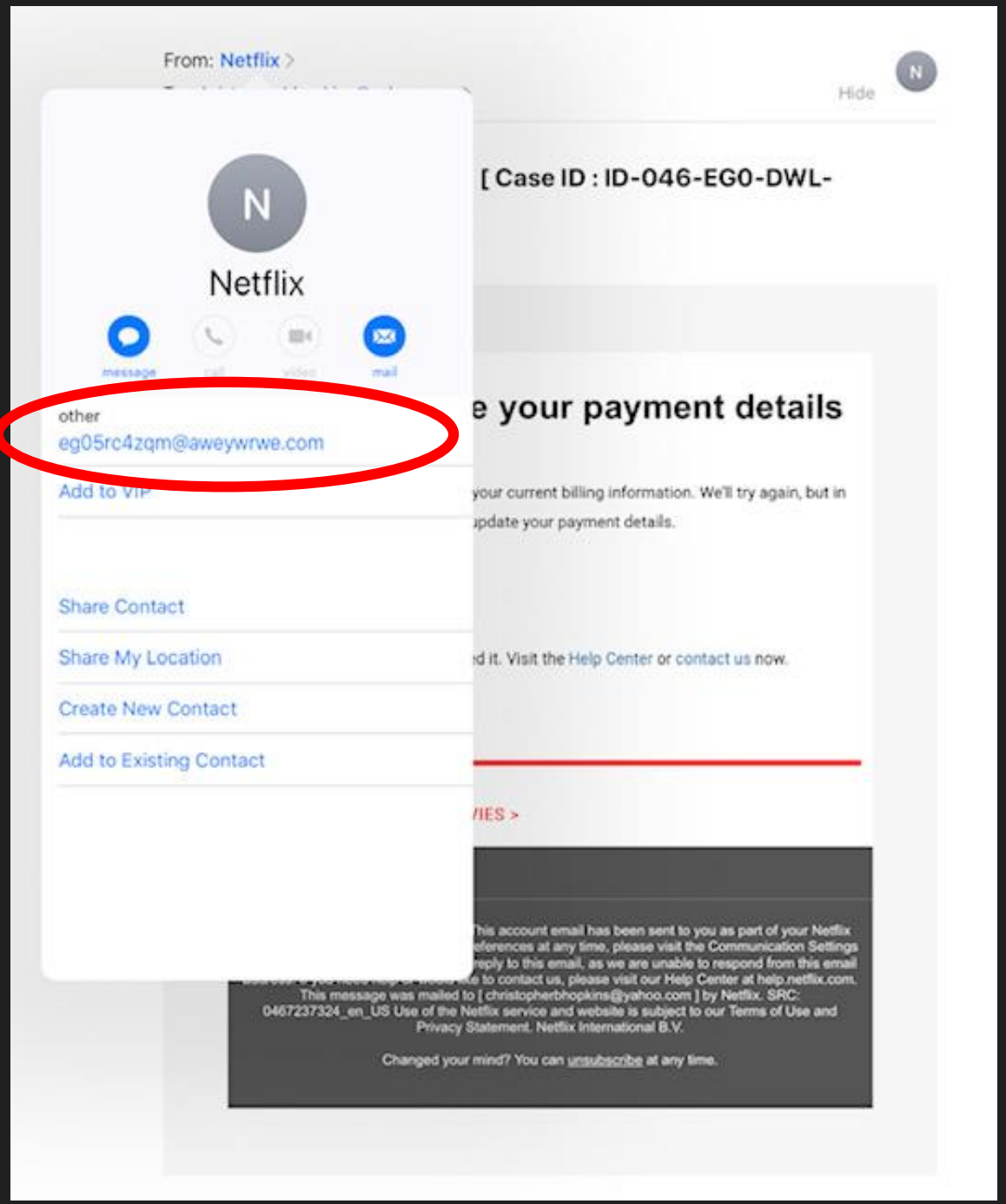
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

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 >


From: Netflix
Hide
[Case ID : ID-046-EG0-DWL-
N
Netflix
message
mail
other
eg05rc4zqm@aweywrwe.com
Add to VIP
Share Contact
Share My Location
Create New Contact
Add to Existing Contact
e your payment details
your current billing information. We'll try again, but in
update your payment details.
d it. Visit the Help Center or contact us now.
/IES >
This account email has been sent to you as part of your Netflix
eferences at any time, please visit the Communication Settings
eply to this email, as we are unable to respond from this email
e 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.

From: Jessica Bloomfield

To: Christopher Hopkins Hide

JB

Litigation representative required

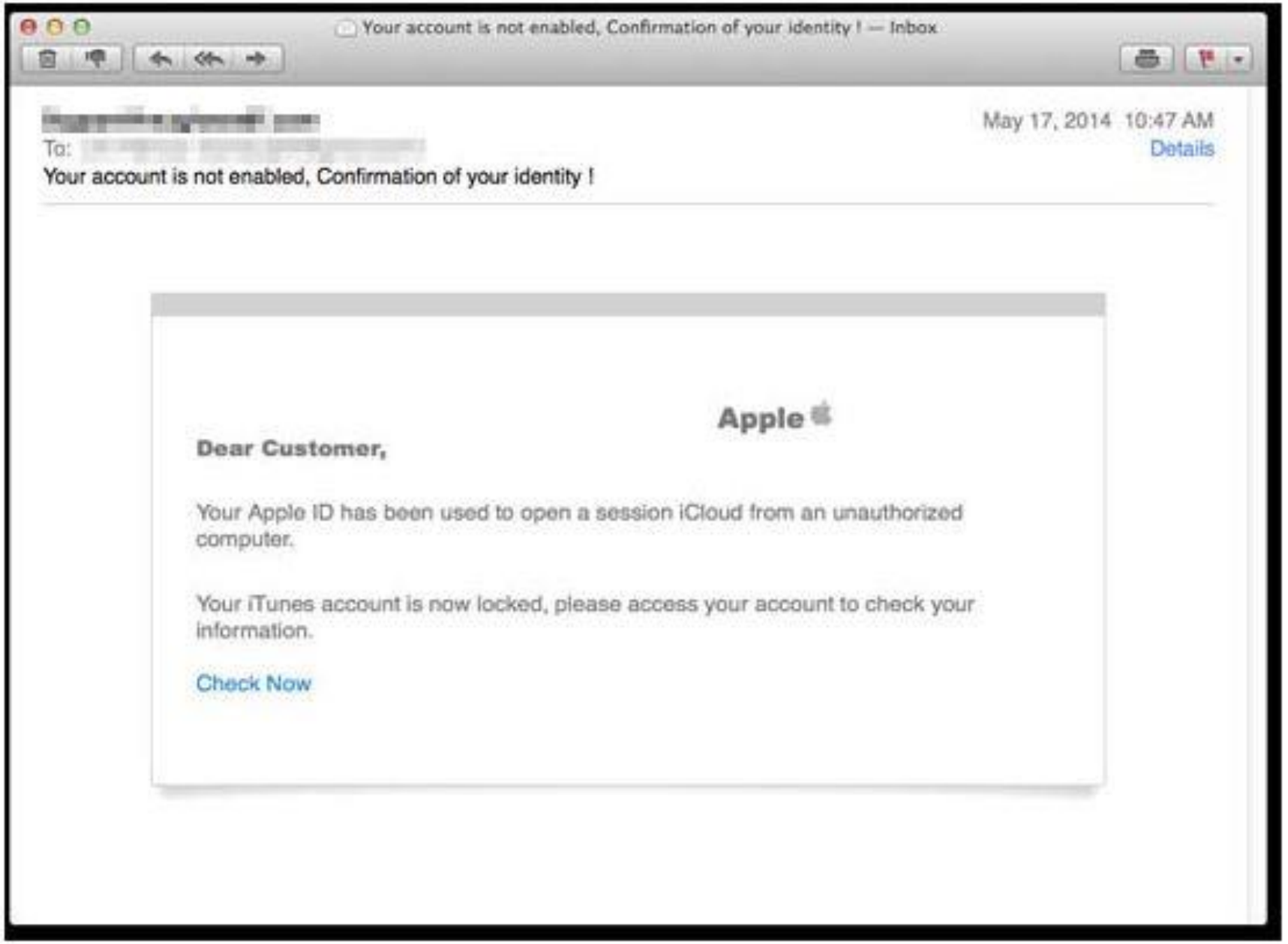
Today at 4:22 PM

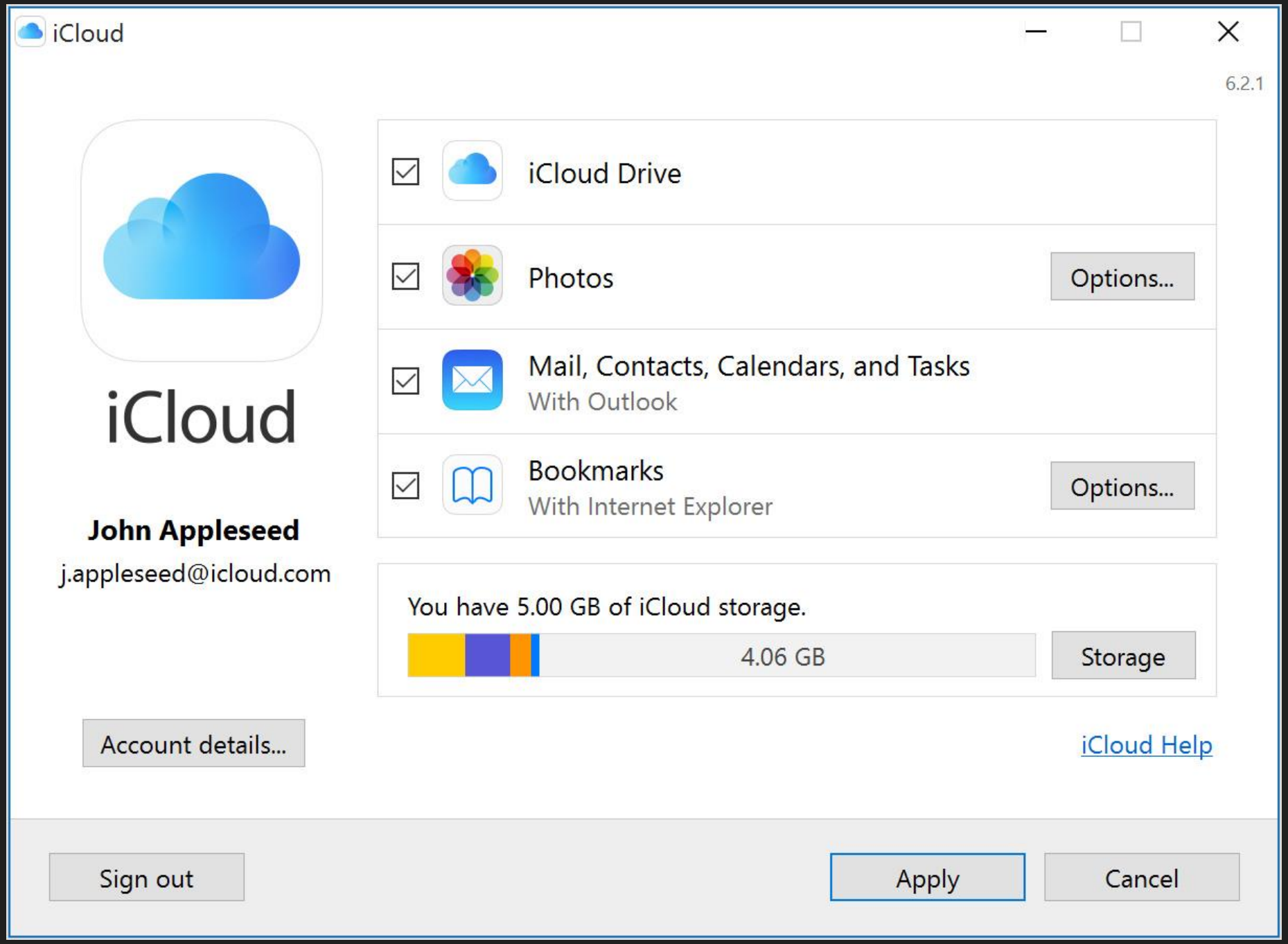
Hello,
My name is Jessica Bloomfield . I would like to retain your firm
on a
civil litigation matter . Kindly advice if you can take my
case.Please let me know if i should send supporting documents so
you can review to understand .

Thanks
J.Bloomfield

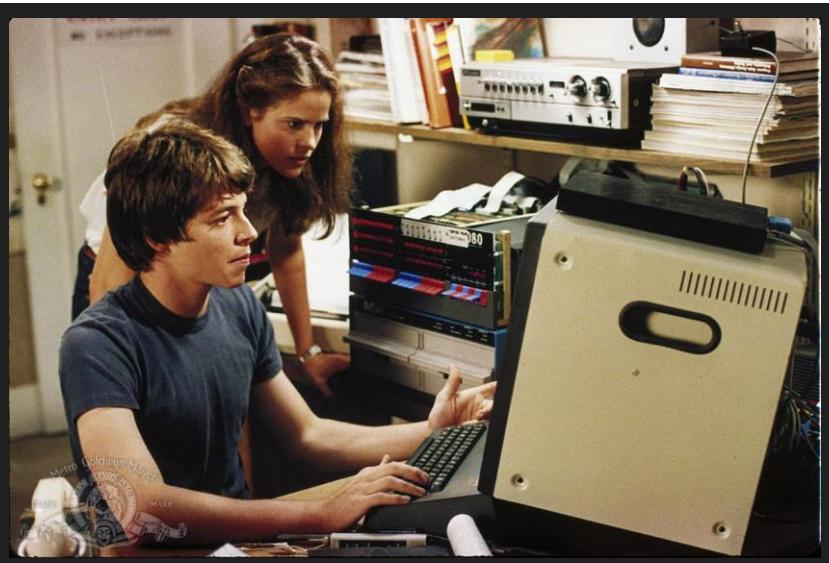

JB
Jessica Bloomfield
message
call
video
mail
other
anglais@evoice.co.uk

'Celebgate' attack leaks nude photos of celebrities


Your account is not enabled, Confirmation of your identity ! — Inbox
[redacted]
To: [redacted]
May 17, 2014 10:47 AM
Details
Your account is not enabled, Confirmation of your identity !
Apple
Dear Customer,
Your Apple ID has been used to open a session iCloud from an unauthorized computer.
Your iTunes account is now locked, please access your account to check your information.
Check Now


iCloud
6.2.1
iCloud
John Appleseed
j.appleseed@icloud.com
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
Account details...
iCloud Help
Sign out
Apply
Cancel

Brute Force: In the 1983 thriller WarGames, young Matthew Broderick sets up his modem to dial every phone number in Sunnyvale, California hoping to find a way to access a game developer's system. Instead, he hits upon WOPAR, a government supercomputer. Broderick's dauntless "war dialing" is a form of brute force attack where a hacker repeatedly tries combinations to hack passwords or otherwise obtain access to an account.



Reverse Brute Force: Instead of testing a number of passwords on one account, "reverse" brute force involves testing one or just a few passwords across multiple accounts. In the wake of large hacks, long lists of widely used passwords are available online. A hacker who tries "123456" or "password" against several hundred usernames is bound to get lucky.

Distributed Denial of Service: If you try to log into an account several times, at some point, the system will lock you out. Imagine now that hackers bombard a website with thousands of login attempts which intentionally fail and, at some point, overload the website which prevents everyone from access. That is a denial of service attack. Hackers then use multiple IP addresses to avoid being blocked (that's the "distributed" part of the hack). At a higher level, more sophisticated attacks can coax the beleaguered website to cough up data.

Over 50% increase in DDoS attacks recorded in Q1 2018: Verisign

More than 65 per cent of customers who experienced DDoS attacks in Q1 of this year were targeted multiple times, report said.

IANS | July 02, 2018, 18:10 IST

Physical Access: You can probably name a few infamous hackers such as Snowden, Manning, and Anonymous. But what is the name of the cleaning service company which enters your office every night? Hacking is not just virtual. Physical access – where a hacker gets direct access to your computer – remains the most convenient way to steal data. These are often "inside jobs." This includes installing keyloggers (devices which record your keystrokes) which function like credit card skimmers on ATMs and gas pumps.

SURVEY #2

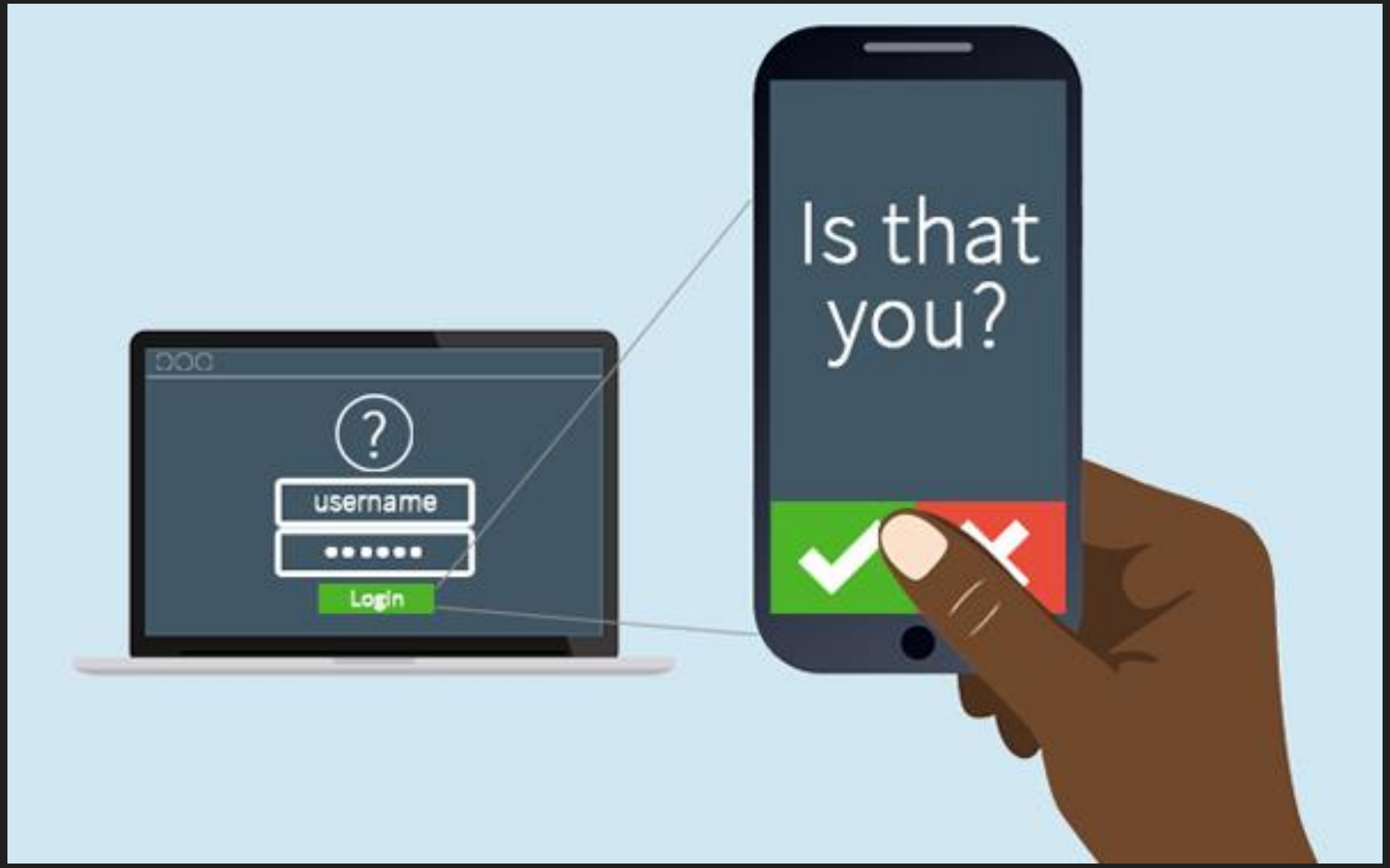
1. I know the name of the vendor which cleans our offices at night.
2. I have no idea.

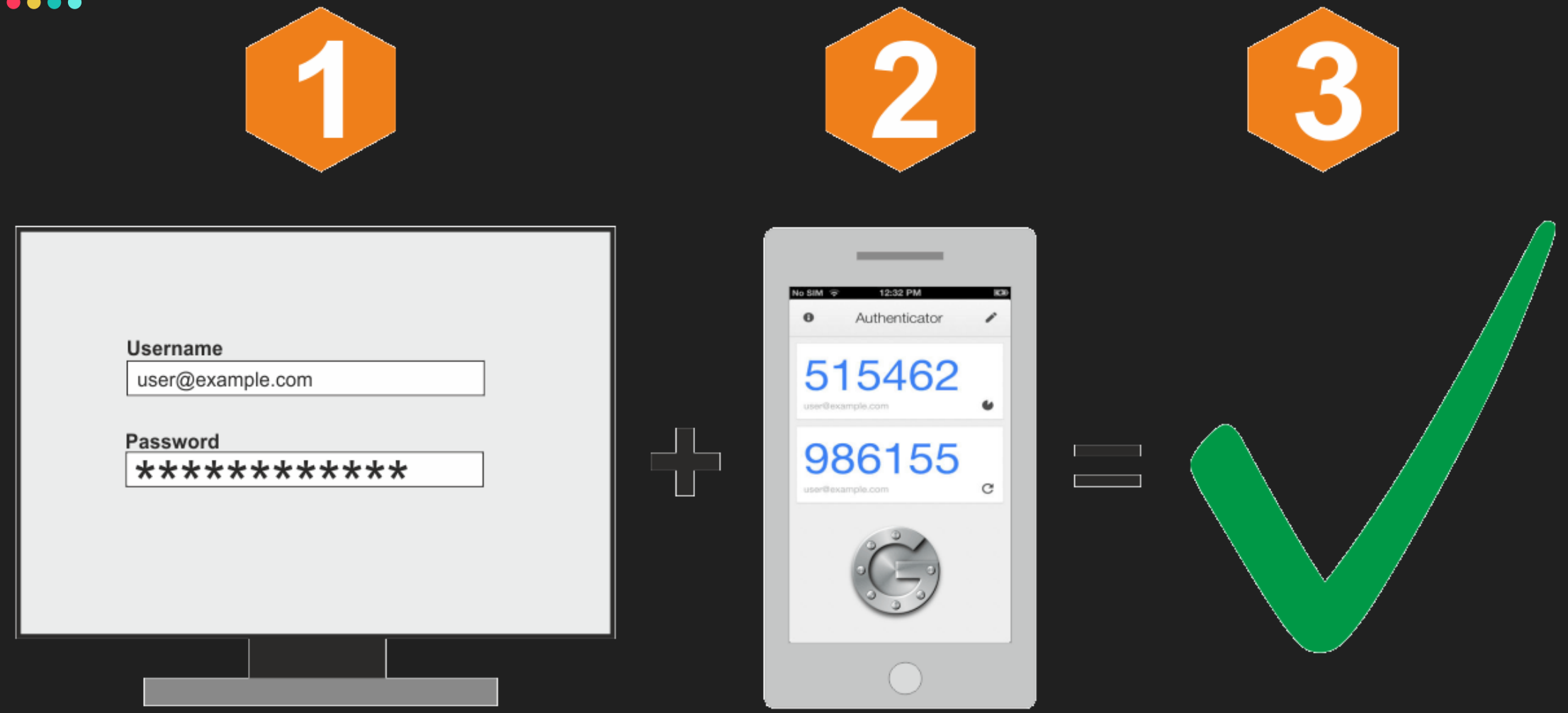
HOW TO PROTECT YOURSELF

1. Check before you click
2. 2FA (or MFA)
3. Spam filter
4. Webfilter
5. Training

SOLUTION:

Two / Multifactor Authentication (2FA / MFA)


Is that you?
username
Login


1
2
3
Username
user@example.com
Password
****
No SIM
12:32 PM
Authenticator
515462
user@example.com
986155
user@example.com

Ransomware

Riviera Beach computer outage will take weeks to fix, IT director says

by Sabrina Lolo | Monday, June 3rd 2019

City of Riviera Beach

RIVIERA BEACH, Fla. (CBS12) — A citywide computer outage in Riviera Beach is going to take weeks to fix, according to the city's interim IT director.

A city employee opened a bad email in late May, spreading a virus that took down the entire computer network for the city.


YOU ARE HACKED
ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!
IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!
CONTACT US: no-reply@gmail.com

Riviera Beach Manager: City has most of its data back after ransomware attack

by Danielle Waugh | Wednesday, August 7th 2019

*Riviero Beach City Manager (WPEC)
*

RIVIERA BEACH, Fla. (CBS12) — The city of Riviera Beach is recovering from a ransomware attack in May and has 90 percent of its data back, according to City Manager Jonathan Evans.

Council members made the controversial decision in June to meet the hacker's ransom demands and use a cyber insurance policy to pay $600,000.

Evans said they're fortunate the ransom payment resulted in decryption keys that worked.

HOW TO PROTECT YOURSELF

1. Check before you click
2. 2FA (or MFA)
3. Spam filter
4. Webfilter
5. Training

SURVEY #3

1. I would tell clients to pay ransomware.
2. I would call FBI but if they could not solve I would recommend the client pay.
3. I would NOT recommend that a client pay.
4. Our firm is full-service; we have (or would find) the ability to accept payment from the client, convert to bitcoin, and send to the hackers on behalf of the client.

SECTION 5

U.S. Government's NIT Malware

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-14915

D.C. Docket No. 2:16-cr-00203-KOB-JEO-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

JAMES RYAN TAYLOR,

US v. Taylor - NIT Malware

On the Internet, websites can see your IP address.

Internet browsing, therefore, isn't quite as private as most people think—it's actually pretty easy, for instance, for law enforcement to find out who visited what sites, when, and for how long simply by subpoenaing IP-address logs from service providers.

US v. Taylor - NIT Malware

Not so when it comes to the “dark web”…

Tor, which was the brainchild of the U.S. Navy but has since been released to the public, works by routing a user’s webpage requests through a series of computer servers operated by volunteers around the globe, rendering the user’s IP address essentially unidentifiable and untraceable.

US v. Taylor - NIT Malware

Not so when it comes to the “dark web”…

you might think of what Tor does as “using a twisty, hard-to-follow route in order to throw off someone who is tailing you—and then periodically erasing your footprints.”[2]

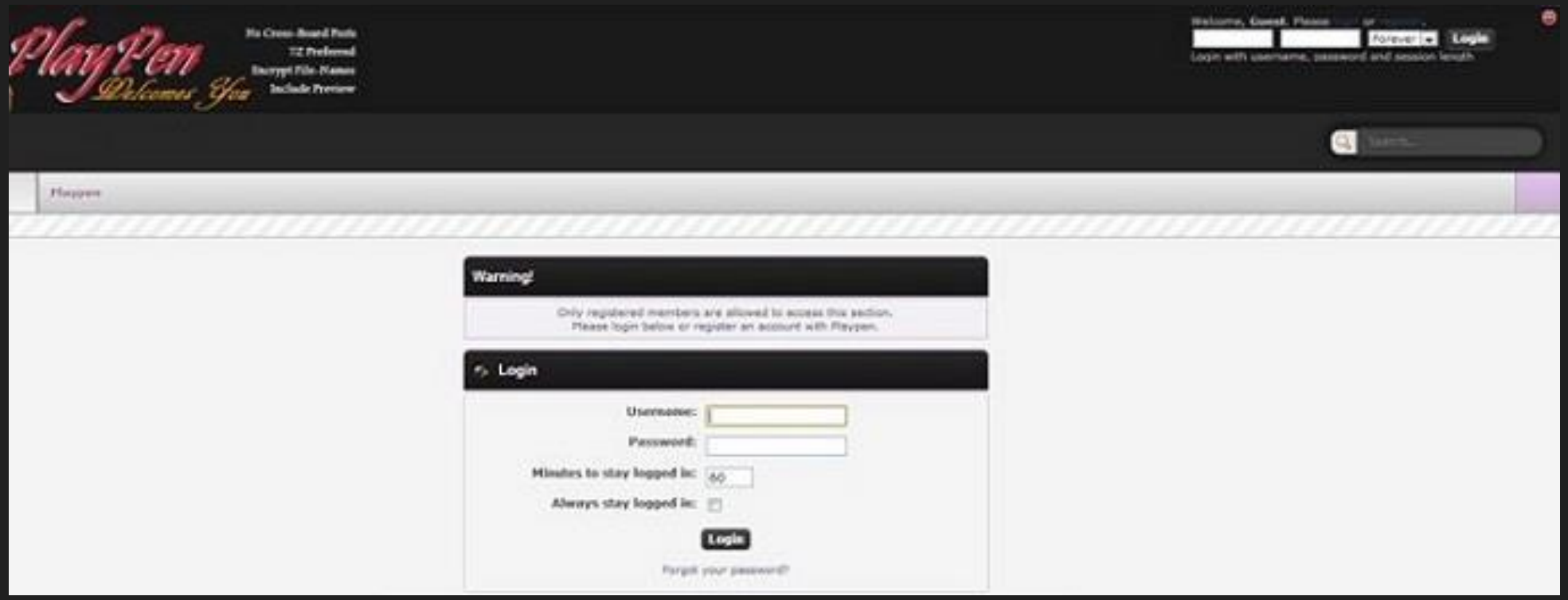
US v. Taylor - NIT Malware

Not so when it comes to the “dark web”…

“hidden services,” *i.e.*, sites accessible *only* through Tor. You can’t just Google a hidden service; rather, a user can access one of these Tor-specific sites only by knowing its exact URL address. Most Tor-site addresses comprise a random jumble of letters and numbers followed by the address “.onion”—in place, say, of “.com” or “.org”—and are shared via message-board postings on the regular internet or by word of mouth.

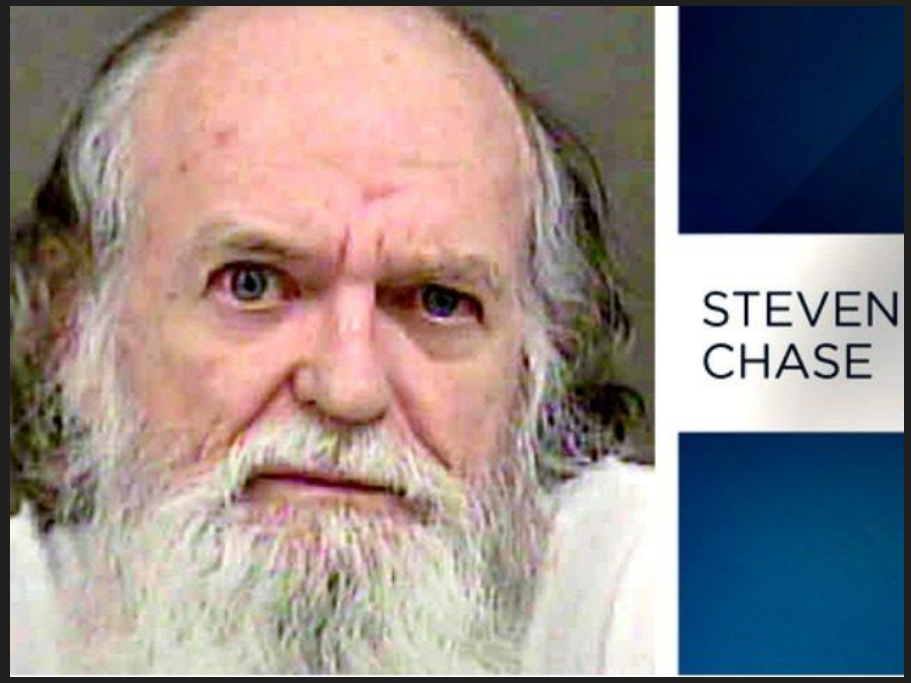
US v. Taylor - NIT Malware

Playpen website



US v. Taylor - NIT Malware

Playpen website



US v. Taylor - NIT Malware

Playpen website

US v. Taylor - NIT Malware

As a means of ferreting out Playpen visitors whose identities were masked by Tor, the FBI sought to deploy government-created malware—specifically, a computer code called the Network Investigative Technique ("NIT")—that would transmit user information back to the FBI.

US v. Taylor - NIT Malware

Here's how the NIT worked: When a Playpen user downloaded images from a Tor-based site, the NIT would essentially "hitchhike" along, invade the host computer, and force it to send to the FBI (among other information) the computer's IP address, the computer's host name, and the username associated with the computer. Based on that information, the FBI could identify the user's internet service provider and the computer affiliated with the account that accessed Playpen, thereby unmasking the user and providing probable cause for the FBI to seek a warrant to seize computers and hard drives.

US v. Taylor – NIT Malware

Warrant:

Goal of NIT was to obtain information "of any user… who logs into [Playpen]"

US v. Taylor – NIT Malware

Affidavit:

NIT may cause an activating computer – *wherever located* – to send to send IP address to a government computer

US v. Taylor - NIT Malware

Not long thereafter, NIT-transmitted data revealed to the FBI that a certain Playpen user was linked to a computer with the host name "RyansComputer." After the user accessed several images of child pornography, the FBI sent an administrative subpoena to the user's internet service provider and discovered that the IP address associated with the computer was assigned to James Taylor in Birmingham, Alabama.

US v. Taylor – NIT Malware

1. This was a 4th Amendment “search”
2. No exigent circumstances
3. Warrant from Virginia not valid in Alabama
4. Warrant = “Void at issuance”
5. Search is effectively warrantless and therefore violated the 4th Amendment

US v. Taylor - NIT Malware

So long as an officer could reasonably have thought that the warrant was valid, the specific nature of the warrant's invalidity is immaterial.

US v. Taylor - NIT Malware

In so holding, we join every court of appeals to consider the question, all of which have agreed that the good-faith exception applies—and the exclusionary rule doesn't—in a situation like this. *See United States v. Eldred*, No. 17-3367-cv, 2019 WL 3540415, at *8 (2d Cir. Aug. 5, 2019); *United States v. Ganzer*, 922 F.3d 579, 587–90 (5th Cir.), *petition for cert. filed*, No. 19-5339 (2019); *United States v. Moorehead*, 912 F.3d 963, 971 (6th Cir.), *petition for cert. filed*, No. 19-5444 (2019); *Werdene*, 883 F.3d at 216–17; *United States v. McLamb*, 880 F.3d 685, 691 (4th Cir.), *cert. denied*, 139 S. Ct. 156 (2018); *United States v. Kienast*, 907 F.3d 522, 527–28 (7th Cir. 2018), *cert. denied*, 139 S. Ct. 1639 (2019); *Henderson*, 906 F.3d at 1118; *United States v. Levin*, 874 F.3d 316, 323–24 (1st Cir. 2017); *Horton*, 863 F.3dat 1050; *United States v. Workman*, 863 F.3d 1313, 1319 (10th Cir. 2017), *cert. denied*, 138 S. Ct. 1546 (2018).

SECTION 6

Redacting PDF Documents

LOUISE MATSAKIS SECURITY 01.09.19 12:02 PM

PAUL MANAFORT IS TERRIBLE WITH TECHNOLOGY

Paul Manafort keeps getting in trouble thanks to subpar digital security practices.

ERIC THAYER/THE NEW YORK TIMES/REDUX

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 17-201 (ABJ)
	)	
PAUL J. MANAFORT, JR.,	)	
	)	
Defendant.	)	

DEFENDANT PAUL J. MANAFORT JR.'S RESPONSE TO THE SPECIAL COUNSEL'S SUBMISSION IN SUPPORT OF ITS BREACH DETERMINATION

Defendant Paul J. Manafort, Jr., by and through counsel, respectfully submits this response

D. The Areas Identified by the Government

1. Mr. Manafort's Interactions with Konstantin Kilimnik

It is accurate that after the Special Counsel shared evidence regarding Mr. Manafort's meetings and communications with Konstantin Kilimnik with him, Mr. Manafort recalled that he had – or may have had – some additional meetings or communications with Mr. Kilimnik that he had not initially remembered. The Government concludes from this that Mr. Manafort's initial responses to inquiries about his meetings and interactions with Mr. Kilimnik were lies to the OSC attorneys and investigators. [redacted]

It is not uncommon, however, for a witness to have only a vague recollection about events that occurred years prior and then to recall additional details about those events when his or her recollection is refreshed with relevant documents or additional information. Similarly, cooperating witnesses often fail to have complete and accurate recall of *detailed* facts regarding specific meetings, email communications, travel itineraries, and other events. Such a failure is unsurprising here, where these occurrences happened during a period when Mr. Manafort was managing a U.S. presidential campaign and had countless meetings, email communications, and other interactions with many different individuals, and traveled frequently. [redacted]

D. The Areas Identified by the Government

1. Mr. Manafort's Interactions with Konstantin Kilimnik

It is accurate that after the Special Counsel shared evidence regarding Mr. Manafort's meetings and communications with Konstantin Kilimnik with him, Mr. Manafort recalled that he had – or may have had – some additional meetings or communications with Mr. Kilimnik that he had not initially remembered. The Government concludes from this that Mr. Manafort's initial responses to inquiries about his meetings and interactions with Mr. Kilimnik were lies to the OSC attorneys and investigators. [redacted]

It is not uncommon, however, for a witness to have only a vague recollection about events that occurred years prior and then to recall additional details about those events when his or her recollection is refreshed with relevant documents or additional information. Similarly, cooperating witnesses often fail to have complete and accurate recall of *detailed* facts regarding specific meetings, email communications, travel itineraries, and other events. Such a failure is unsurprising here, where these occurrences happened during a period when Mr. Manafort was managing a U.S. presidential campaign and had countless meetings, email communications, and other interactions with many different individuals, and traveled frequently. [redacted]

D. The Areas Identified by the Government

1. Mr. Manafort's Interactions with Konstantin Kilimnik

It is accurate that after the Special Counsel shared evidence regarding Mr. Manafort's meetings and communications with Konstantin Kilimnik with him, Mr. Manafort recalled that he had – or may have had – some additional meetings or communications with Mr. Kilimnik that he had not initially remembered. The Government concludes from this that Mr. Manafort's initial responses to inquiries about his meetings and interactions with Mr. Kilimnik were lies to the OSC attorneys and investigators. [redacted]

It is not uncommon, however, for a witness to have only a vague recollection about events that occurred years prior and then to recall additional details about those events when his or her recollection is refreshed with relevant documents or additional information. Similarly, cooperating witnesses often fail to have complete and accurate recall of *detailed* facts regarding specific meetings, email communications, travel itineraries, and other events. Such a failure is unsurprising here, where these occurrences happened during a period when Mr. Manafort was managing a U.S. presidential campaign and had countless meetings, email communications, and other interactions with many different individuals, and traveled frequently. [redacted]

(See, e.g., Doc. 460 at 5 (After being shown documents, Mr. Manafort "conceded" that he discussed or may have discussed a Ukraine peace plan with Mr. Kilimnik on more than one occasion); id. at 6 (After being told that Mr. Kilimnik had traveled to Madrid on the same day that Mr. Manafort was in Madrid, Mr. Manafort "acknowledged" that he and Mr. Kilimnik met while they were both in Madrid)).

D. The Areas Identified by the Government

1. Mr. Manafort's Interactions with Konstantin Kilimnik

It is accurate that after the Special Counsel shared evidence regarding Mr. Manafort's meetings and communications with Konstantin Kilimnik with him, Mr. Manafort recalled that he had – or may have had – some additional meetings or communications with Mr. Kilimnik that he had not initially remembered. The Government concludes from this that Mr. Manafort's initial responses to inquiries about his meetings and interactions with Mr. Kilimnik were lies to the OSC attorneys and investigators. [redacted]

It is not uncommon, however, for a witness to have only a vague recollection about events that occurred years prior and then to recall additional details about those events when his or her recollection is refreshed with relevant documents or additional information. Similarly, cooperating witnesses often fail to have complete and accurate recall of *detailed* facts regarding specific meetings, email communications, travel itineraries, and other events. Such a failure is unsurprising here, where these occurrences happened during a period when Mr. Manafort was managing a U.S. presidential campaign and had countless meetings, email communications, and other interactions with many different individuals, and traveled frequently. [redacted]

Do Not Just Put a Black Line or Box over the Text… *because the Text is STILL THERE*

ABA JOURNAL

NEWS IN-DEPTH BLAWGS ABOUT

Home / Daily News / How to redact a PDF and protect your clients

CRIMINAL JUSTICE

How to redact a PDF and protect your clients

BY JASON TASHEA

JANUARY 10, 2019, 6:00 AM CST

Proper PDF Redactions

1. OCR software can read characters blacked out with a Sharpie
2. Some people try to count the spaces to guess the words
3. Best: when you are done with the document, in Word, replace the text with “[REDACTED]” rather than blacking out the text

Protect Yourself (Take-away steps)

10 WAYS TO PROTECT YOURSELF

1. Know where your data is (data map)
2. Back it up routinely
3. Unique Passwords
4. Update / patch operating sys & software
5. Anti-Malware software

10 WAYS TO PROTECT YOURSELF

6. Only give employees limited access
7. Data retention policy (*delete what you don’t need!*)
8. Consider buying insurance
9. Training
10. Terms and Conditions…

United States Court of Appeals
For the Eighth Circuit

No. 16-3426
No. 16-3542

Matthew Kuhns, Individually and on behalf of all others similarly situated

Plaintiff - Appellant/Cross-Appellee

v.

Scottrade, Inc., a Missouri Corporation

Defendant - Appellee/Cross-Appellant

Appeals from United States District Court
for the Eastern District of Missouri - St. Louis

Submitted: April 5, 2017
Filed: August 21, 2017

Kuhn's v. Scottrade (8th Cir. 2017)

- Be careful what you promise in contracts

- Contractual obligations to protect a consumer's PII = grounds for a lawsuit.

j. **Electronic Communications:** Like most businesses, the Firm will communicate with the Client primarily via unencrypted e-mail and via phone as well as, secondarily, by U.S. Mail and/or overnight service (unless you request otherwise). From time to time, we will also use IM/text, Internet portal, FTP, WiFi, Skype, cloud, and other live and/or Internet-based third party vendors and services. There is some risk of disclosure and loss of attorney-client privilege in using these forms of communication because they do not ensure the confidentiality of their contents; no guarantee can be made regarding the interception of data sent via the Internet or mail carriers. The Client agrees that, in advance, the Client will advise the Firm in writing if the nature of any communication(s) require a higher degree of security.

TECHNOLOGY Corner

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

CHRISTOPHER B. HOPKINS

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.

How safe is the PC on your desk? Whether you rely upon a valued IT professional or your office manager, Rule 4-1.1 tasks you, the lawyer, with "an understanding of the

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 unencrypted desktop, and -5 points for unencrypted laptop.

5. Is Your PC Up-To-Date? Keeping a

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.

10. What are Your Privacy Settings? Hit the windows key and select "Settings" and either "privacy" (Win 10) or Change PC Settings and Privacy (earlier versions)

TECHNOLOGY Corner

CHRISTOPHER B. HOPKINS

Protect the Privacy of Your Data on iOS Devices

In a recent cell phone privacy case, Carpenter v. U.S., the Supreme Court noted that Americans "compulsively carry cell phones with them all the time" yet, from a privacy standpoint, "there is no way to avoid leaving behind a trail of [personal] data."

Fortunately, for people who own iPhone and iPad devices ("iOS Devices"), you can limit law enforcement, advertisers, and third parties from accessing your personal data. In less than 10 minutes, with this article in one hand and your iOS Device in the other, follow these steps to protect your privacy.

Before delving in, ensure that your iOS Device is operating on iOS 11.x. You can confirm by going to Settings, General, and then tap Software Update. The most important security protection is a passcode. Go to Settings, Passcode (depending on your device, it will be "Touch ID & Passcode" or "Face ID & Passcode"). Make sure Passcode is turned on and Require Passcode is set to Immediately.

The person will be locked into that app until you enter the code again. They won't know you've locked them out unless they start snooping.

If you have Face ID, you can simplify the process under Settings/General/Accessibility/Guided Access/Passcode Settings and turn on Face ID. That way, three clicks of the side button will lock the app and two clicks will unlock, as long as it sees your face.

Quickly Turn Off Face ID to prevent law enforcement or third parties from accessing your Face ID protected iOS Device by forcing you to look at it, hold the side button and volume down button for a second. The power off / SOS page will appear. Once you hit cancel, your iOS Device will disable Face ID and require a passcode to access.

Snoopers Can Learn A Lot Just By Looking At Your Lockscreen Apps constantly communicate with you through Notifications on your lock screen. However,

Who is Looking at My Deleted Photos? When you delete a photo, it is not really deleted. In fact, it is readily accessible. You can avoid embarrassment by going to the Photos app and scrolling to the Recently Deleted folder and "double delete" any image so it is inaccessible without sophisticated software.

Who is Listening? Under Settings/Privacy, select Microphone to see which apps on your phone have access. Apps like Translate, Shazam, and Skype should stay on. You will be surprised at the games and other apps which want access. If you do not dictate into an app, turn off its access to the microphone.

Who is Watching Me? Under Settings/Privacy/Camera, turn off access to the camera to all apps except those which require the camera to function.

Protect Your Texts Your texts and instant messages are surprisingly revealing. First,

Nine Ways That Companies Are Getting Hacked

by Christopher B. Hopkins

The conventional wisdom regarding data breach and identity theft is that it is not if you will be hacked but *when*. Recent breaches such as Ashley Madison, OPM, Michaels, and Target have led to over 100 million people with potentially compromised credit card and personal information. How is this happening?

Many law firms are jumping on the cyber security bandwagon as they proclaim experience assisting with data breach management. But few lawyers understand how these hacks are being accomplished. Even if you and your client rely on competent IT professionals (as you should), it is important to possess a survey knowledge of how hacks and data breaches occur. This article provides a brief introduction to intrusion and disruption techniques.

Physical Access: You can probably name a few infamous hackers such as Snowden, Manning, and Anonymous. But what is the name of the cleaning service company which enters your office every night? Hacking is not just virtual. Physical access – where a hacker gets direct access to your computer – remains the most convenient way to steal data. These are often "inside jobs." This includes installing keyloggers (devices which record your keystrokes) which function like credit card skimmers on ATMs and gas pumps.

Brute Force: In the 1983 thriller WarGames, young Matthew Broderick sets up his modem to dial every phone number in Sunnyvale, California hoping to find a way to access

language called SQL (pronounced "sequel" or alternatively S-Q-L). By re-sending the special character and then a string of code, hackers can learn which databases exist behind the website. After that, they can again send the special character as well as an SQL command to "list tables." From there, a script can be set up to extract data from all revealed databases. Frighteningly, this can all be accomplished from the username and password screen. Recent examples reportedly include 7-11, Sony, and Johns Hopkins.

Malware / worms: Malware is a secret code which a user unknowingly downloads and installs which, in turn, begins spying or causing damage. Malware can be as simple as code which quietly runs a script after a user clicks a link or it can be more widespread, such as when malware is furtively "baked" into commercial software. Recent examples reportedly include Staples, Sony (recall the film, The Interview) and the Stuxnet attack which plagued nuclear reactors in Iran.

Phishing: A hacker may fool users into thinking that a fake website is real so that the hacker can steal usernames, passwords, and other information. The unwitting user typically hits a link upon receiving an email which insists that "you must change your password." This tricks the person into interacting with a fake version of a bank, social media, or shopping website. The fake website may also inject malware which further exploits the user's mistake. The "celeb-gate" incident in 2014, where nude celebrity cell phone images were spread across the internet, was caused by a widespread phishing scam.

The Government Can Sue Your Company for Negligent Cybersecurity

by Christopher B. Hopkins

While the risk of hackers dawned on many corporate lawyers after Target's data breach in 2013, the federal government has been actively suing corporations into cybersecurity compliance since 2005. Specifically, the Federal Trade Commission (FTC) has sued more than 50 companies for poor cybersecurity despite the lack of any specific statute on point. Even the Federal Communications Commission (FCC) has sued regulated companies for their lackluster data standards. It is not just credit card or health care data which needs to be protected, as evidenced by the recent Ashley Madison hack. All corporations need to be aware that they can be sued by injured parties (see the Seventh Circuit's *Remijas v. Neiman Marcus* opinion) as well as the federal government for what is best described as "negligent cybersecurity." The recent Third Circuit opinion in *FTC v. Wyndham* gives guidance on data practices to follow or avoid.

In April 2008, hackers broke into a Phoenix-area hotel's network and then connected to Wyndham's larger network. Using pure guesswork, the hackers paired usernames with frequently-used passwords as a brute-force method to break in. From there, hackers discovered unencrypted payment information and that Wyndam's system was practically unmonitored. Hackers repeatedly breached Wyndham's system

In *Wyndham*, the defendant was sued for failing to take these steps:

- Use firewalls at critical network points;
- Restrict access to certain IP addresses;
- Use encryption for certain customer files (not plain text);
- Monitor network for previously-discovered malware;
- Employ common protection which prevents users from selecting weak passwords;
- Employ reasonable methods to detect and prevent unauthorized access.

Along these lines, in 2007, the FTC published a guidebook, *Protecting Personal Information: A Guide for Business*, which provides these recommendations:

- Check software vendors' sites regularly for patches and alerts about new vulnerabilities;
- Set firewall controls to limit access only to trusted employees with a legitimate business purpose;
- Require employees to use strong passwords;
- Implement a data breach response plan which includes immediate investigation and steps to close off vulnerabilities.

Until the *Wyndham* case, most companies settled with the FTC which limited the amount of attention paid to the FTC's

Christopher Hopkins
McDonald Hopkins LLC – West Palm Beach

InternetLaw Commentary .com

@cbhopkins
chopkins@mcdonaldhopkins.com
Linkedin.com/in/cbhopkins