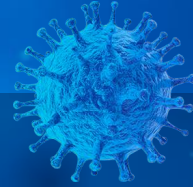




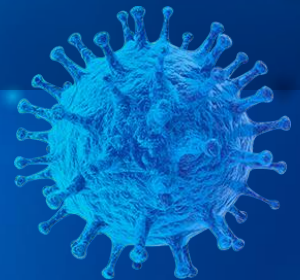
# CORONAVIRUS

DATA PRIVACY AND CYBERSECURITY



McDonald Hopkins

A business advisory and advocacy law firm®





Christopher B. Hopkins

McDonaldHopkins

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

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

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



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

CancelRe: RequestSend

To: Shawn M. Riley

Cc/Bcc, From: chopkins@mcdonaldhopkins.com

Subject: Re: Request

May 27, 2019, at 8:12 AM, Shawn M. Riley <leonardx8@triad.rr.com> wrote:  
Can you help me with a quick task please?



# 1. Spearphishing Attack

## Social Engineering Attack

- Broad range of tricks based upon relationships
- Ask me to use Firm credit card
- Password(s)
- Transfer funds
- Fake urgency





**Send routine emails to remind employees  
to be wary of impersonations and fake  
emails**

**Or...**

**Send your own  
“fake” emails and see who clicks.**

# 2. Phishing Emails

Business Email Compromise



**2114 Villa [REDACTED], FL**

12 messages

[REDACTED] <closingagent2519@gmail.com>

To: [REDACTED]

Cc: [REDACTED]

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.

Email me if you need anything else!

Thank you,



2114 Villa [REDACTED], FL

[REDACTED] <closingagent2519@gmail.com>

To: [REDACTED]  
Cc: [REDACTED]

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.


Email me if you need anything else!





Thank you,








**How did thieves find out  
about this transaction?**

**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.






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](http://myuniversity.edu/renewal)



Thank you  
MyUniversity Network Security Staff



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 >](#)

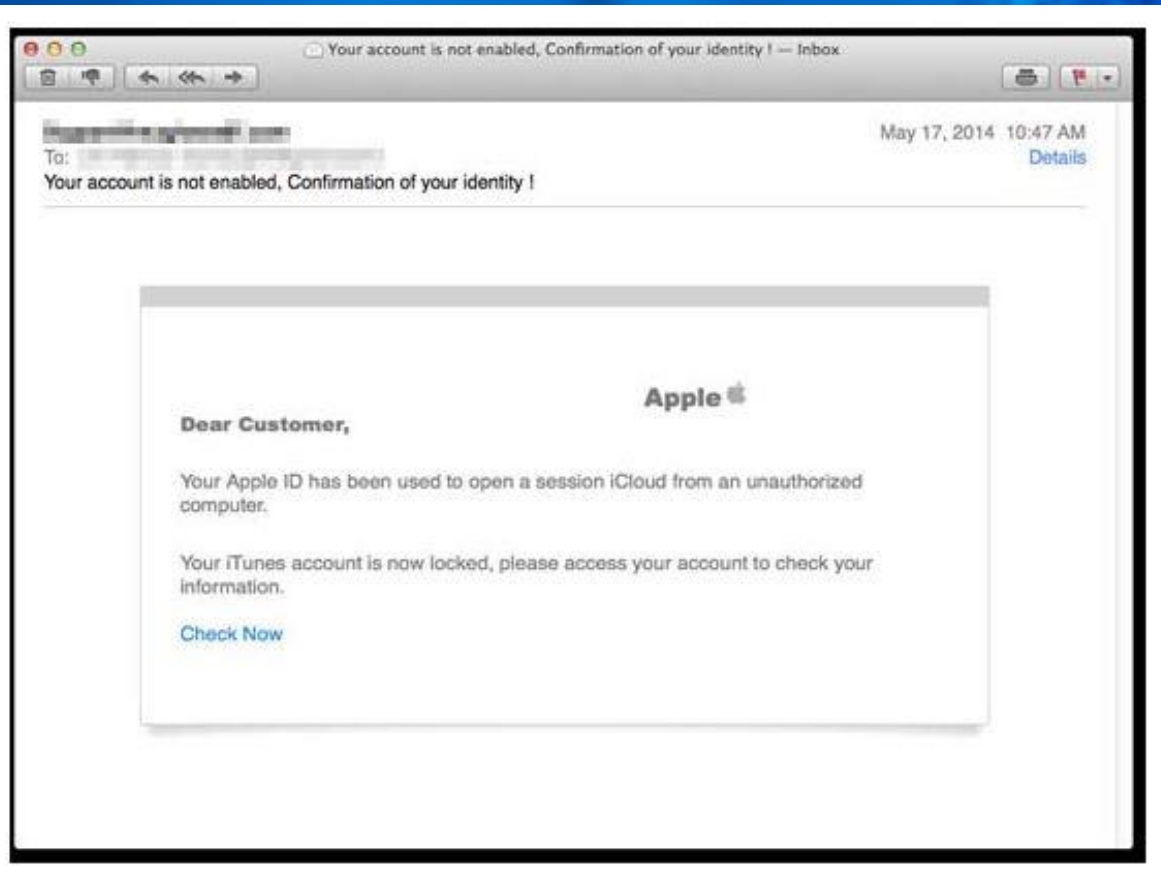
Questions? Call 007-800-321-2130 This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the [Communication Settings](#) page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our [Help Center](#) at [help.netflix.com](#).

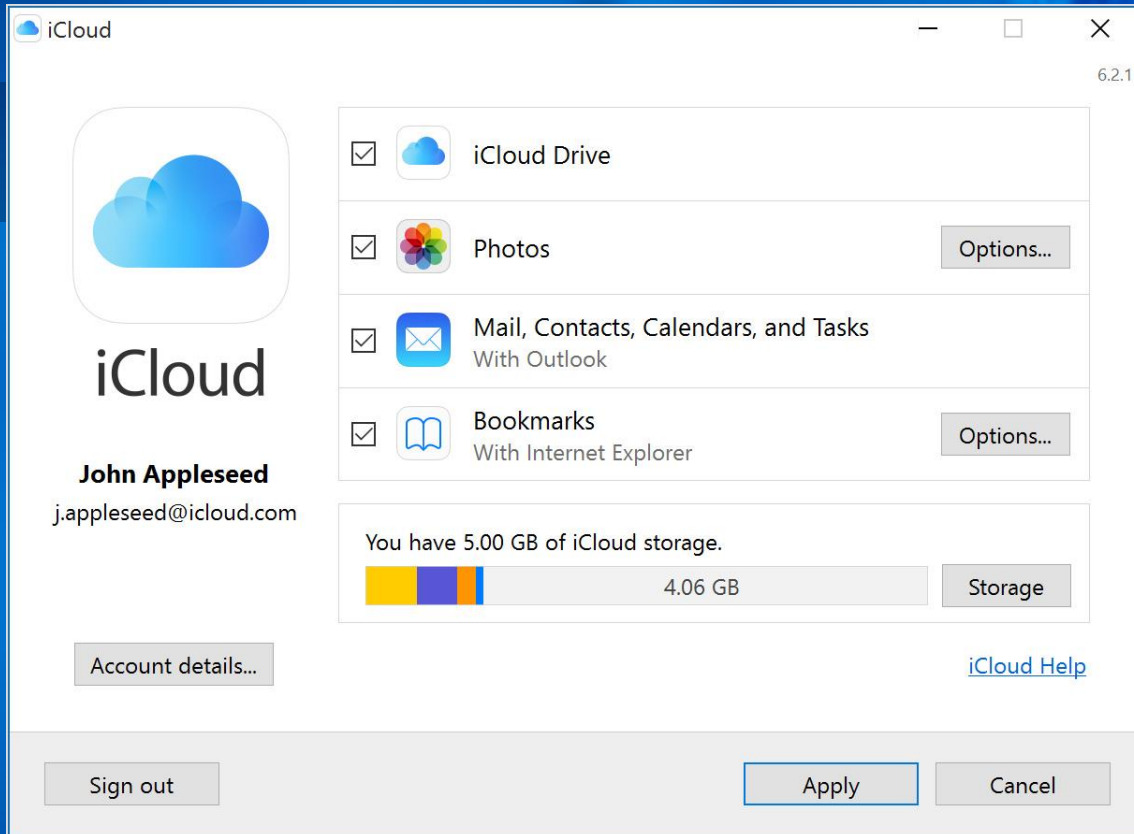
This message was mailed to [christopherhopkins@yahoo.com] by Netflix. SRC: 0467237324\_en\_US Use of the Netflix service and website is subject to our [Terms of Use](#) and [Privacy Statement](#). Netflix International B.V.

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



**'Celebgate' attack leaks nude photos of celebrities**







## Step 1: Identify a Target



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

## Step 2: Grooming



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

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

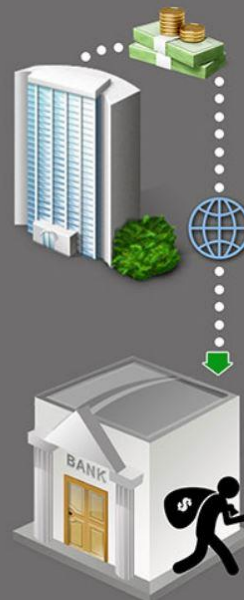
Grooming may occur over a few days or weeks.

## Step 3: Exchange of Information



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

## Step 4: Wire Transfer



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

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





# **Protection from Phishing Scams While Working from Home**

## EDUCATE YOUR EMPLOYEES (create a policy!)

- Current versions of Windows or Mac OS at home
- Keep your system up to date
- Use Anti-Virus / Malware protection – even free versions
- Check email addresses carefully
- Use Multifactor authentication (MFA / 2FA) – this includes Gmail, Yahoo, & social media
- And...

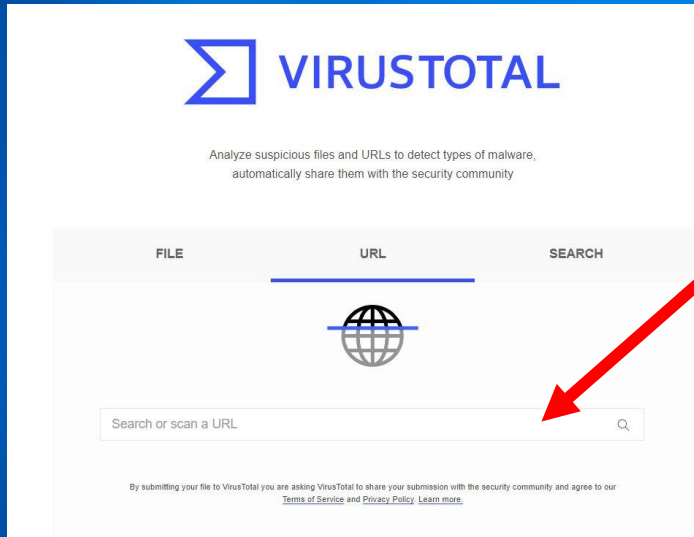


# BIG CONCEPT



DO NOT WIRE OR SEND MONEY  
WITHOUT A VERBAL CONFIRMATION

# VirusTotal.com



- COPY a suspicious link from any email
- PASTE into VirusTotal.com
- It will check security/validity of link
- FREE. Owned by Google's parent co.

# 3. Public Wi-Fi

How Your Data is Stolen at Hotels, Airports, etc.



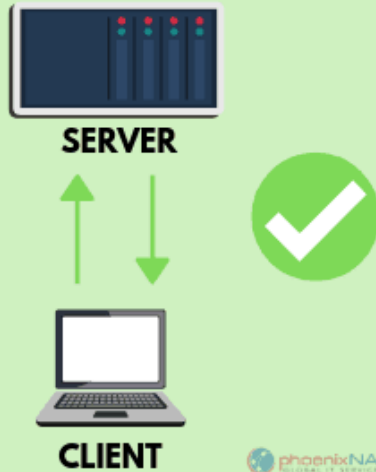


# **Wi-Fi Pineapple**

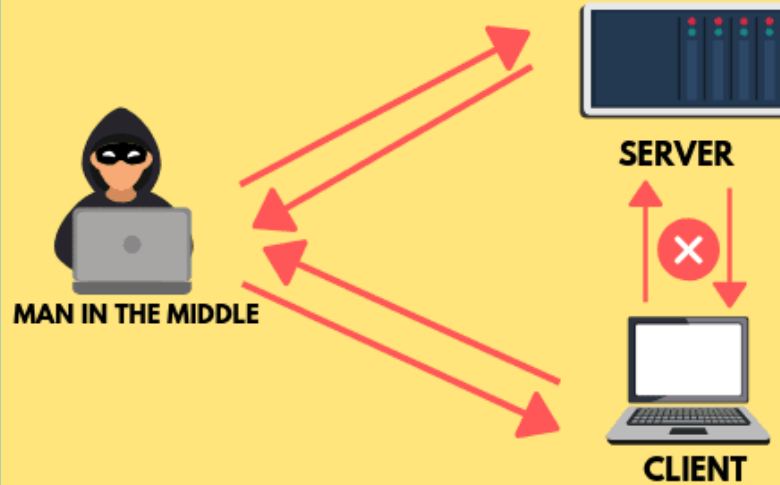
## **(Man-In-The-Middle Attack)**

## MIDDLE IN THE MIDDLE ATTACK EXAMPLE

### NORMAL CONNECTION



### MAN IN MIDDLE CONNECTION

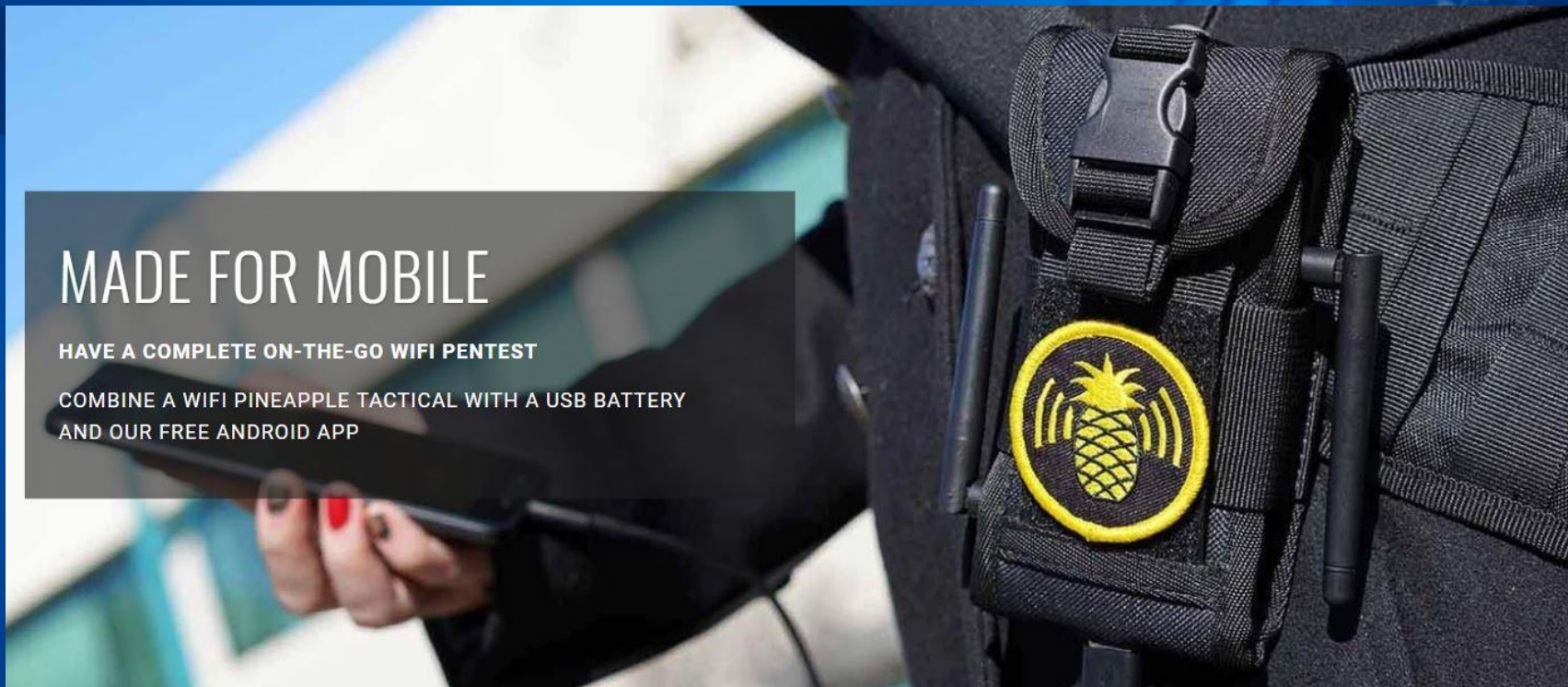




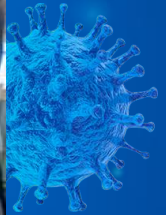
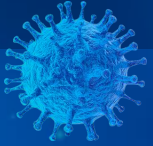
# MADE FOR MOBILE

HAVE A COMPLETE ON-THE-GO WIFI PENTEST

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



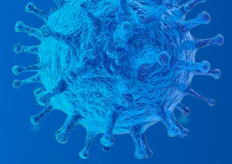






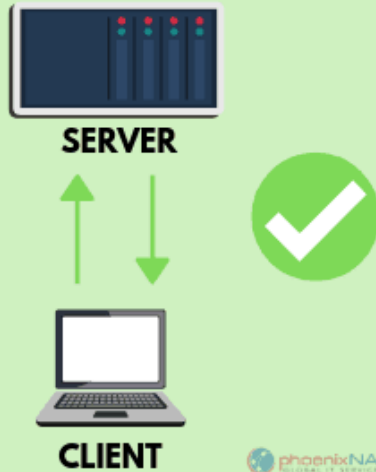
Your device  
is looking  
for familiar  
Wi-Fi



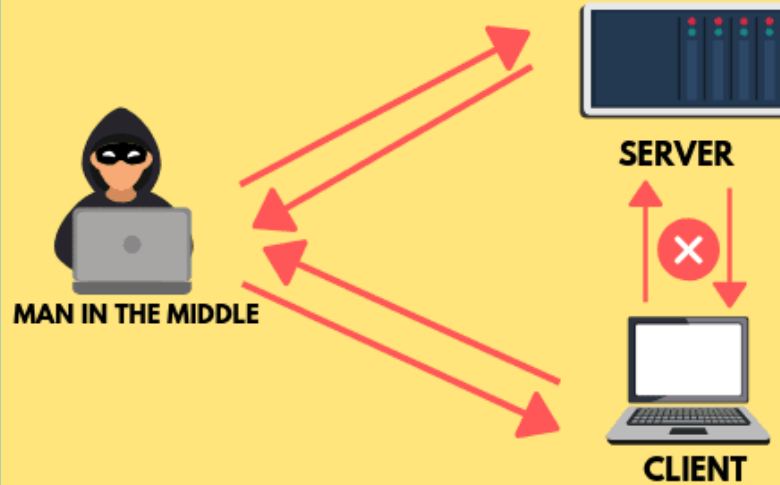


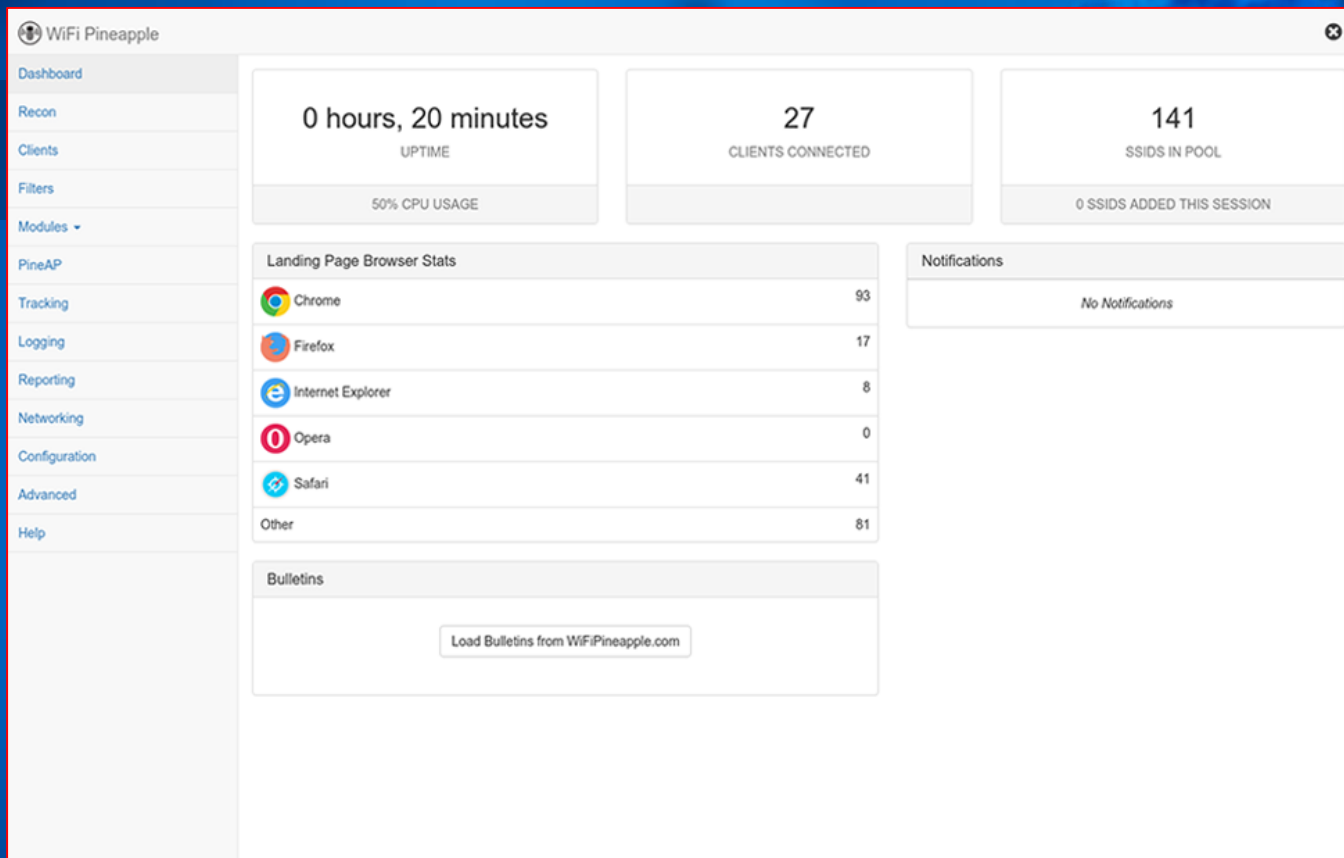
## MIDDLE IN THE MIDDLE ATTACK EXAMPLE

### NORMAL CONNECTION



### MAN IN MIDDLE CONNECTION







**- WIFI PINEAPPLE TETRA -**

ULTIMATE AMPLIFIED DUAL-BAND POWERHOUSE

\$200



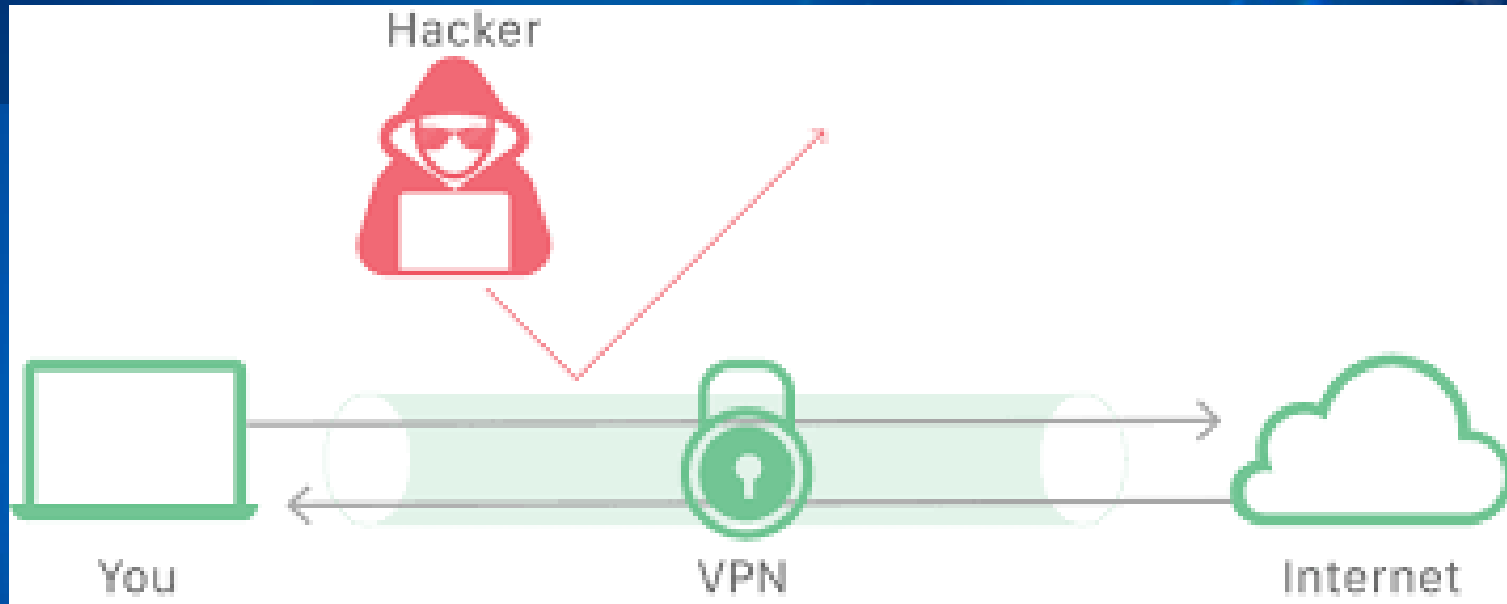
**- WIFI PINEAPPLE NANO -**

SIMPLE POCKET-SIZED WIFI PENTEST COMPANION

\$100

# 4. Virtual Private Network (VPN)

How to Use Public Wi-Fi Safely (and Easily)



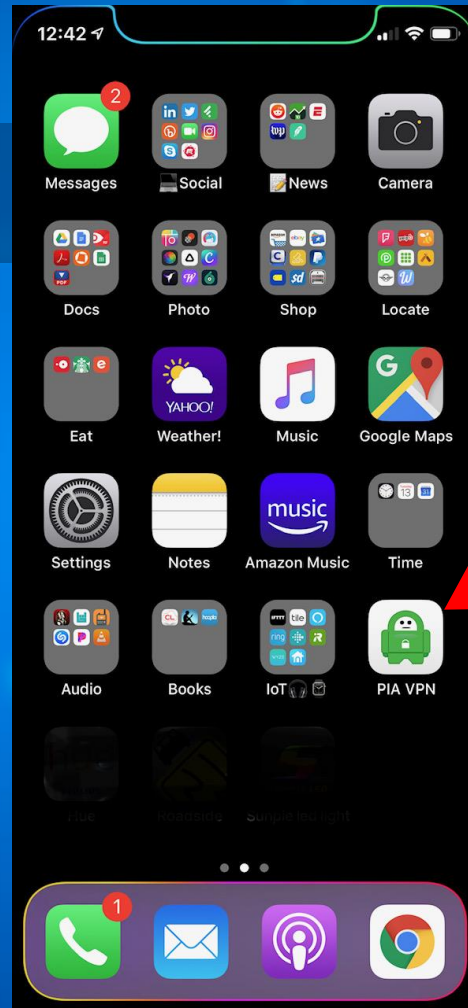


## EDUCATE YOUR EMPLOYEES

- Don't use public wi-fi
- Employees use a VPN
- Employers use a VPN
- Use Multifactor authentication (MFA / 2FA)



**How easy is VPN...?**



12:44



# Settings



Christopher Hopkins

Apple ID, iCloud, iTunes & App Store



Airplane Mode



Wi-Fi

MH >



Bluetooth

On >

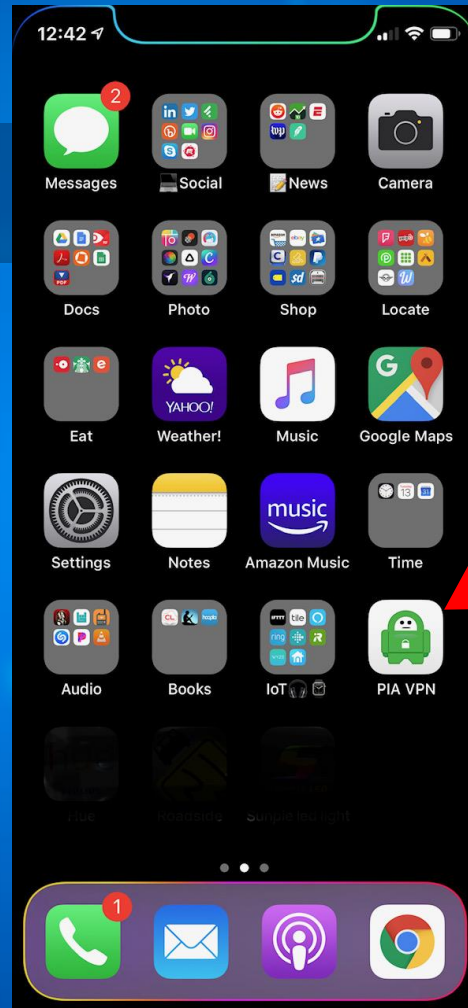


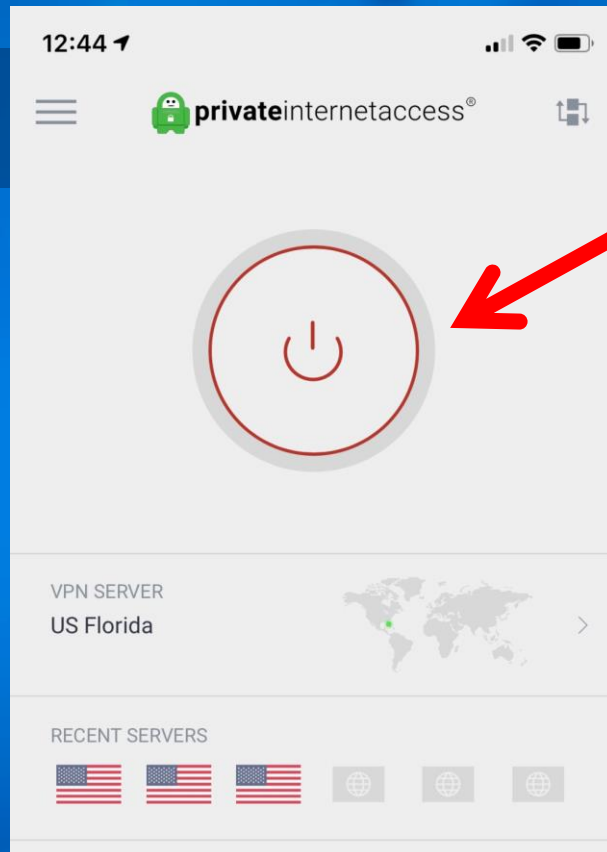
Cellular

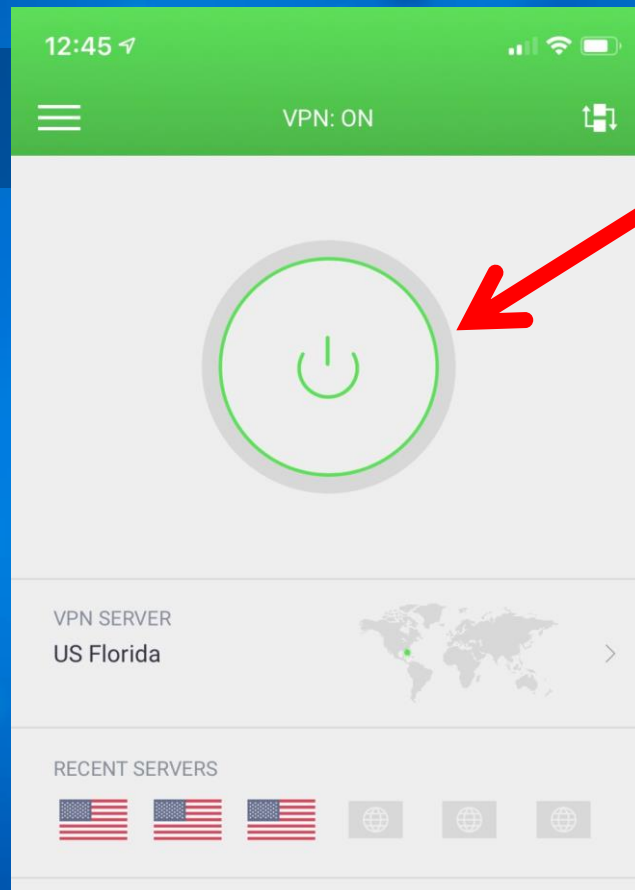


VPN



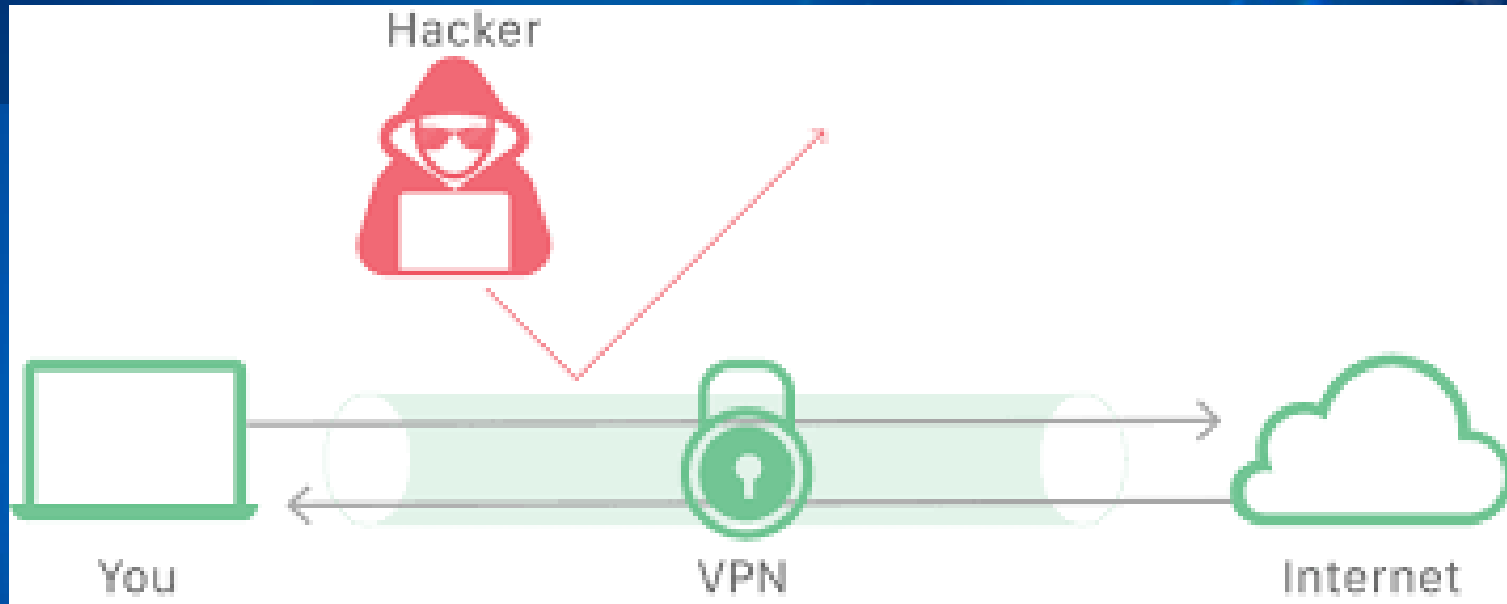






[PIA & image credit](#)

[CNET – Best VPN for 2020](#)





# 5. Steps You Can Use Now

Work Remotely Like a Pro

# DON'T BE A "COVIDIOT"

(we say this fondly and with humor)



The mailed packages sometimes include items like teddy bears or gift cards to employees of target companies

The enclosed USB device is a commercially available tool known as a "BadUSB" or "Bad Beetle USB" device. After the USB device is plugged into a target system, the device automatically injects a series of keystrokes in order to download and execute a unique malware payload

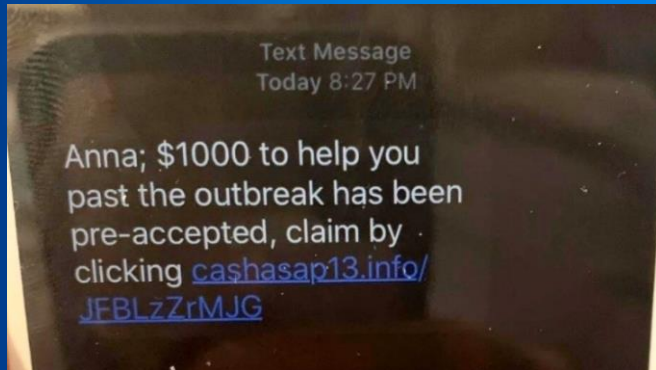
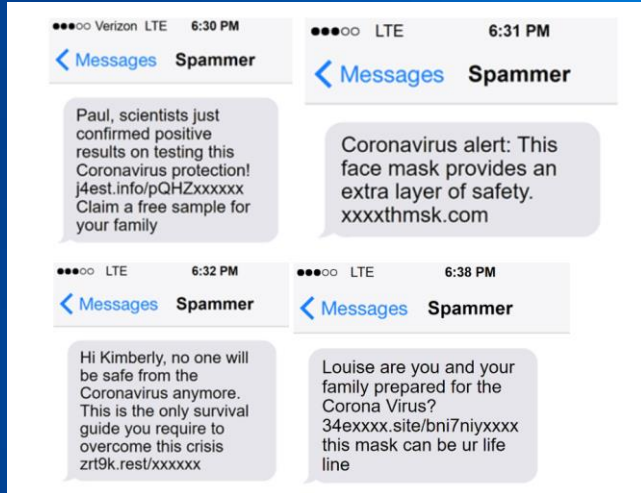
3/26/20 FBI Flash

[Bleeping Computer article](#)



# DON'T BE A "COVIDIOT"

(we say this fondly and with humor)



Kenneth Copeland healed viewers of the coronavirus through their televisions last night.



23.3K 10:30 AM - Mar 12, 2020



# POLICY CONSIDERATIONS

- Does your engagement letter give notice of client data use, your storage practices, and what cloud and third parties your Firm uses?
- Do your employees connect via VPN?
- Do you have a data map?
- Ask IT: do we have firewalls, end-to-end encryption, data separation?
- Do not save Firm and client information locally
- What's happening with paper printed at home?
- Stop using free USBs
- Have a policy (find one on internet, ask a colleague, call me)





## Lexis Practice Advisor<sup>®</sup> Coronavirus Resource Kit

FREE CORONAVIRUS RESOURCE KIT



- Forms to extend deadlines due to COVID-19
- Coronavirus and Force Majeure Checklist
- Force Majeure Clause Drafting & Proposed Clauses
- Excuses for Non-Performance
- Anticipatory Repudiation & Adequate Assurance of Future Performance
- Termination and Cancellation Rights & Notices
- Releases, Change Orders, Letters
- L&E Content – e.g., Telecommuting Policy

# \*Securely\* Use ZOOM Like a Pro

- Require a password (zoom-bombing)
- Mute audio/camera as you enter meeting  
(under Settings/Audio/Mute... and Settings/Video/Turn off...)
- Spacebar & Alt-A for mute
- Use a Virtual Background
- Limit Screensharing:  
(hit “...” / Meetings Settings / turn off Allow Participants to Share)
- Lock Meetings
- Kick Out! (Manage Participants / “More” next to person / Remove)
- Alternatives: FaceTime, Skype, Teams (365), WhatsApp, FB, HouseParty



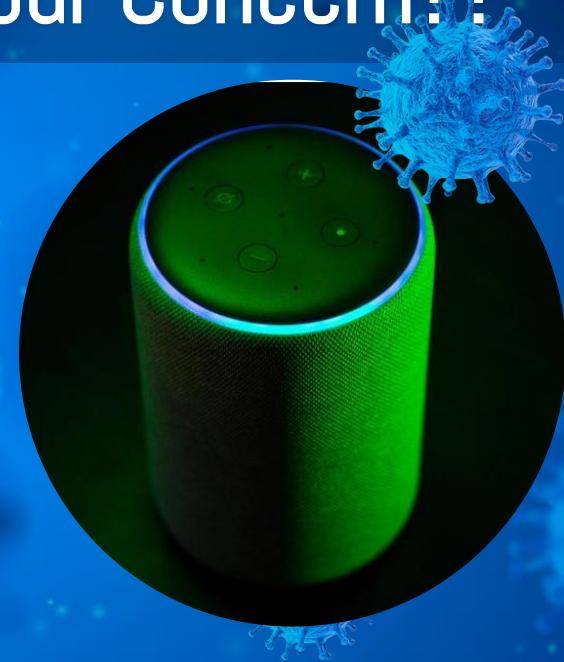
[Zoom's advice for party crashers](#)

[Tricks article](#)   [Password Steps](#)

[Christopher's Article on Zoom Privacy](#)

# Of All Your Devices... Alexa is Your Concern??

- Set Up Delete By Voice (in App, 3 lines / Settings / Alexa Privacy / Review Voice History / Enable Deletion by Voice – tell her what to delete)
- What Did She Hear? (“Alexa , tell me what you heard?” “Alexa, why did you do that?”)
- Delete Old Recordings (in App, 3 lines / Settings / Alexa Privacy / Manage Your Alexa Data / Auto Delete 3 or 18 months)
- Unplug or Cover it
- Where’s your phone, PC mic, tablet, etc?



*Love Zoom but fear Alexa? Up until March 27, 2020, Zoom was sending your data to Facebook!*

[CNET article & image credit](#)

[Christopher’s Article on Alexa Privacy](#)



## TECHNOLOGY CORNER



CHRISTOPHER B. HOPKINS

### Protect The Privacy of Your iOS 13 Device

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

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

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

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

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

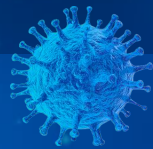
**I See You Are Not in Your Office:** Why broadcast that you are out of the office? Turn off "sent from my iPhone" under Settings / Mail / Signatures (leave it blank). There is still another trick. When sending a reply, your email will be entitled "Re:" when you reply on a mobile device whereas it will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

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

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

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

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



## TECHNOLOGY Corner



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.



# Finally... Stay Healthy!

## Free workouts from Peloton, Nike and others to help you stay active during your quarantine

Published: March 28, 2020 at 12:57 p.m. ET

By [Nicole Lyn Pesce](#)

14 fitness apps and streaming services that you can try at home for free



[Click for Full Article](#)

# Credits / Sources

Special thanks to all the people who made and released these awesome resources for free:

- ▶ Presentation template by [SlidesCarnival](#)
- ▶ Fonts & Emojis by [FontAwesome](#)
- ▶ This PPT is at [InternetLawCommentary.com](#)
- ▶ Articles too!



# Thanks!

[Chopkins@McDonaldHopkins.com](mailto:Chopkins@McDonaldHopkins.com)

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

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