Right Networks®

Murder Hornets?

Securing Your Firm Amidst the Next Wave of (Cyber) Attacks

Presented by Roman H. Kepczyk, CPA.CITP, CGMA

Director of Firm Technology Strategy, Right Networks

Roman H. Kepczyk, CPA.CITP

Director of Firm Technology Strategy- Right Networks

IT/Administrative Partner for Regional CPA Firm (10 Years)

Strategic IT/Production Partner to more than 400 CPA Firms (24 Years)

CPAFMA Public Accounting Firm Manager and Advisory Board Member

Lean Six Sigma Black Belt

Top 100 Most Influential People in Accounting (14 Years)

Top Thought Leader (10 Years)

Most Recommended Consultants (15 Years)

About Right Networks

Hosted/Technology:

CPA Practice Advisor
READERS' CHOICE
AWARDS 2020

Cloud Premier

- **100% accounting focused**
- Deep industry experience and knowledge required to provide **best-in-class cloud solutions**.
- Lead the market with **180,000 users.**
- **4,000+ accounting firms** trust us to deliver their applications in the cloud every day.
- Strategic partnerships with **Intuit, CCH-Wolters Kluwer, Thomson Reuters**, and others at the executive, technology, and support levels that are unmatched in the industry.
- Uniquely positioned to deliver the **best solution and service experience**.
- **Right Networks Cloud Premier** (formerly **Xcentric**)

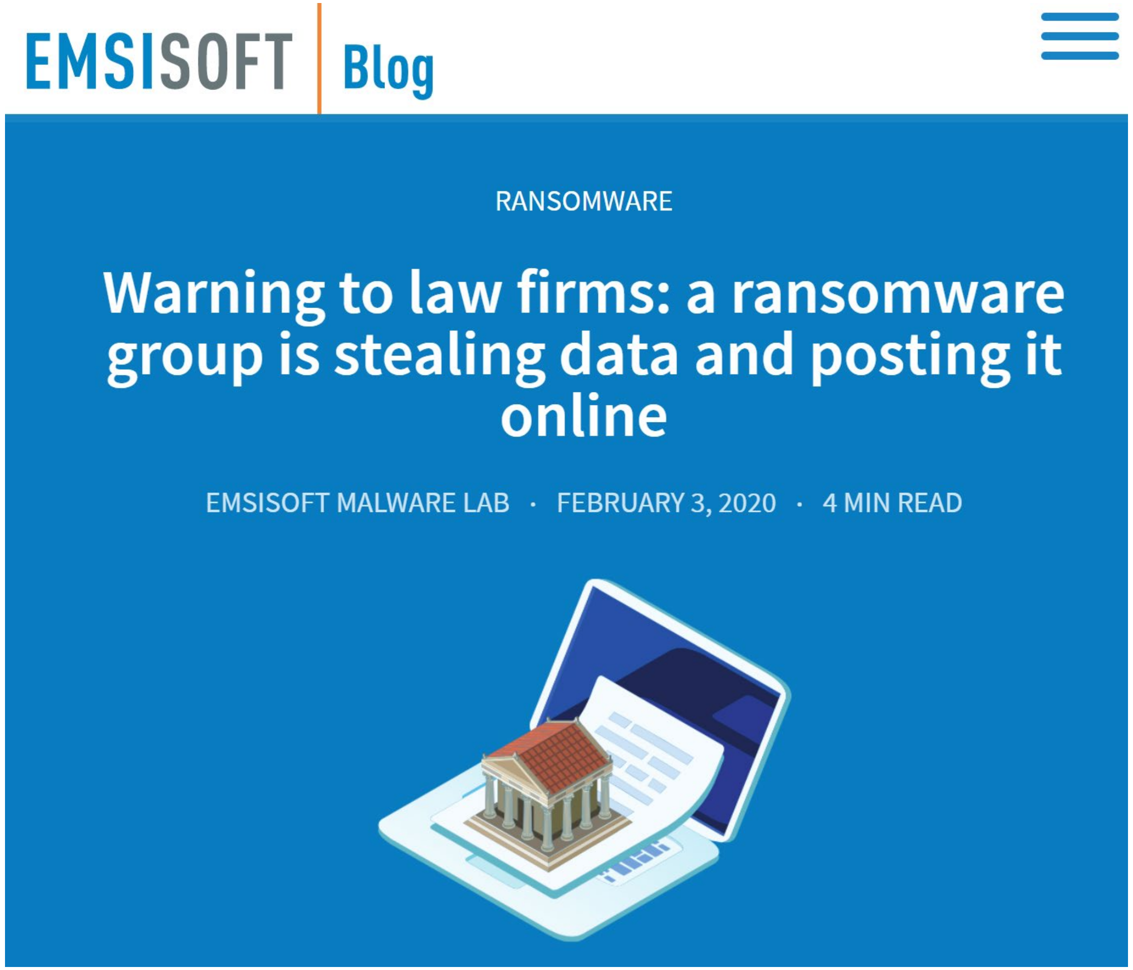
Agenda

Security Briefing for Accounting Professionals

- In the News: Security Headlines
- Advancing Cyber Threats
- Cybersecurity-It’s the Law!
- What to Do if You Suspect a Breach
- Cybersecurity Tips You Should Know
- Security Resources

…GOAL: provide you with updated threats and resolutions to protect your firm and educate your personnel!

In the News: Security Headlines

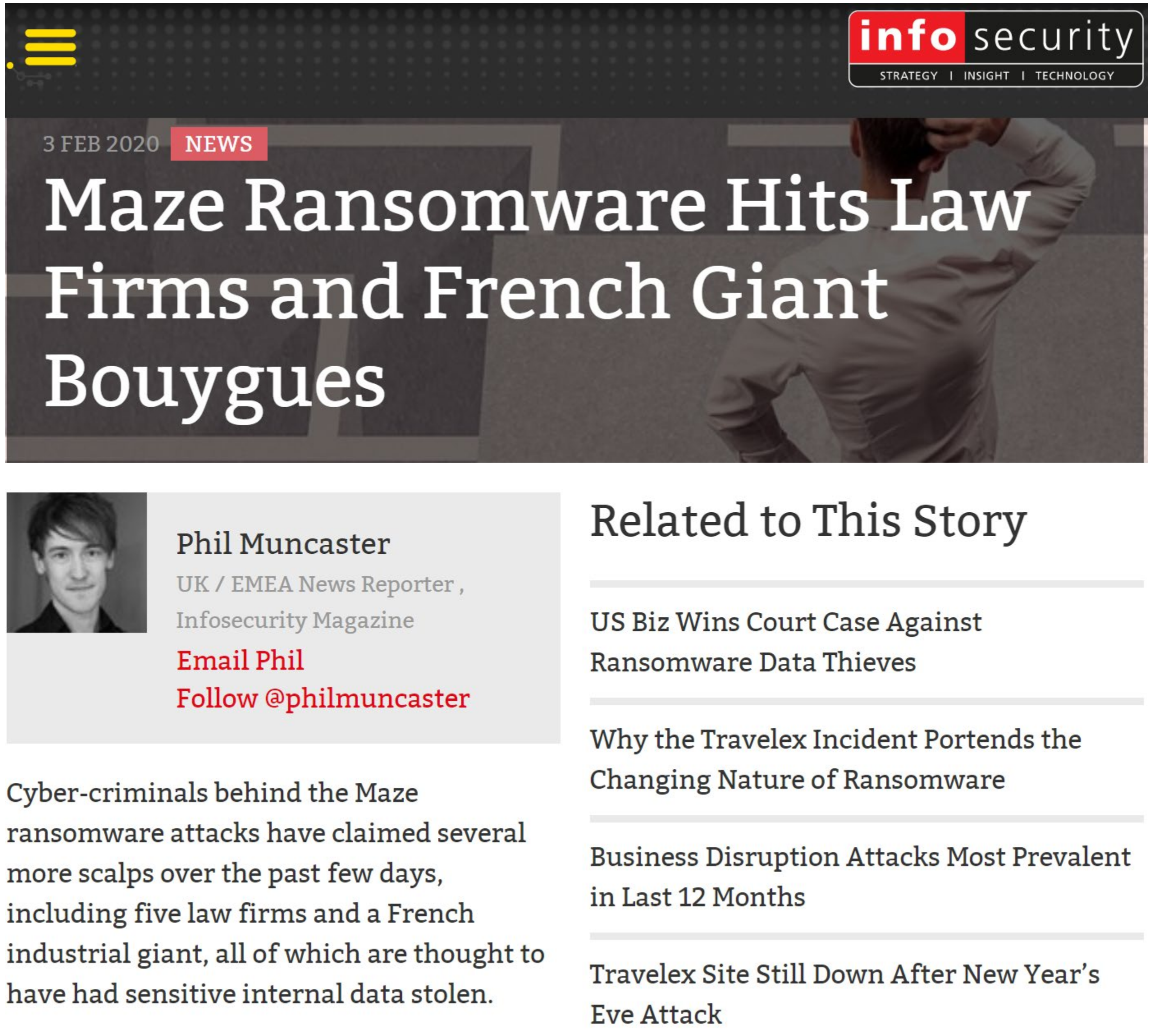


EMSISOFT | Blog

RANSOMWARE

Warning to law firms: a ransomware group is stealing data and posting it online

EMSISOFT MALWARE LAB · FEBRUARY 3, 2020 · 4 MIN READ



infosecurity STRATEGY | INSIGHT | TECHNOLOGY

3 FEB 2020 NEWS

Maze Ransomware Hits Law Firms and French Giant Bouygues

Phil Muncaster
UK / EMEA News Reporter , Infosecurity Magazine
Email Phil
Follow @philmuncaster

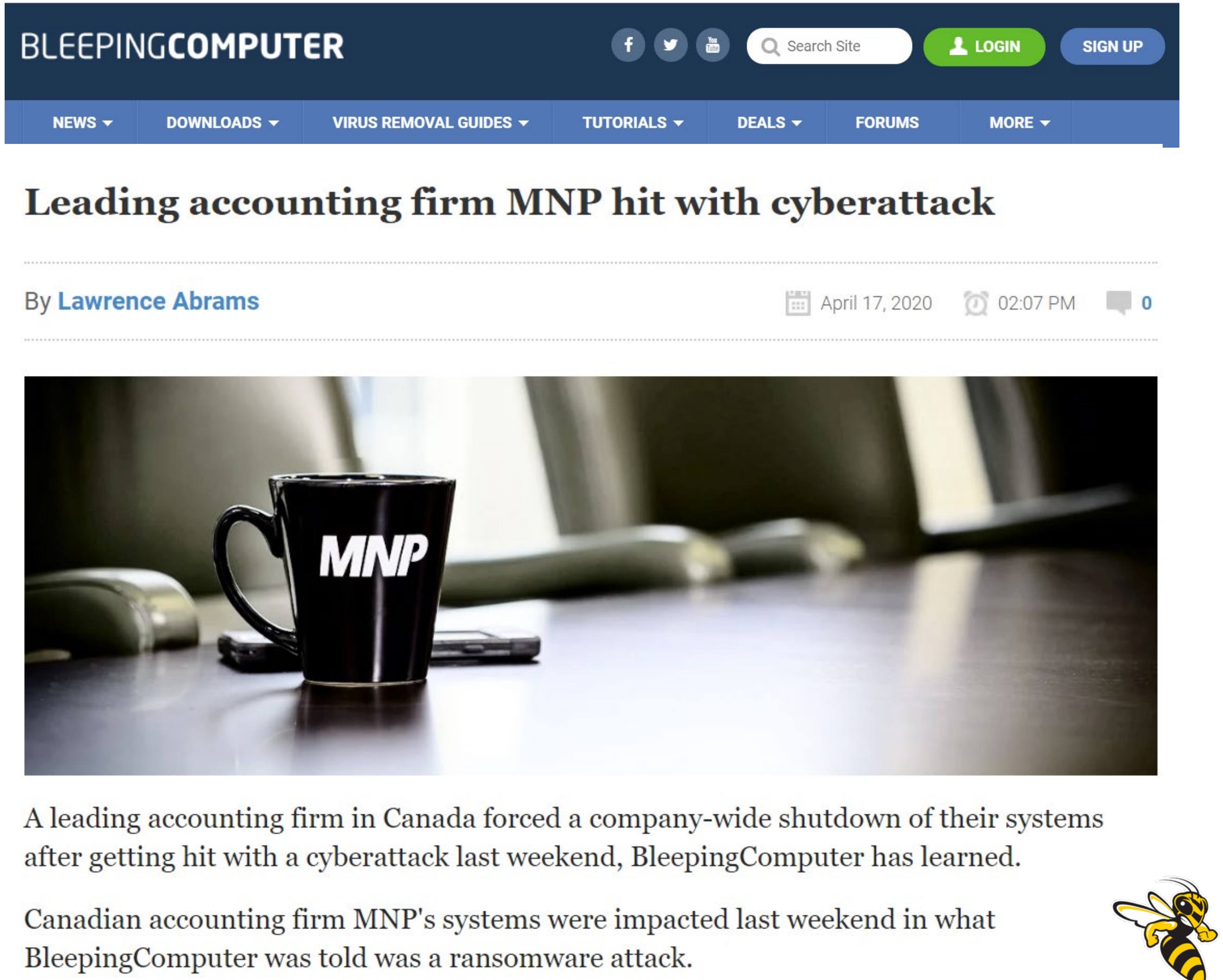
Cyber-criminals behind the Maze ransomware attacks have claimed several more scalps over the past few days, including five law firms and a French industrial giant, all of which are thought to have had sensitive internal data stolen.

Related to This Story

- US Biz Wins Court Case Against Ransomware Data Thieves
- Why the Travelex Incident Portends the Changing Nature of Ransomware
- Business Disruption Attacks Most Prevalent in Last 12 Months
- Travelex Site Still Down After New Year’s Eve Attack

Medical and Legal already being attacked ….will accounting firms be targeted next?

In the News: Security Headlines

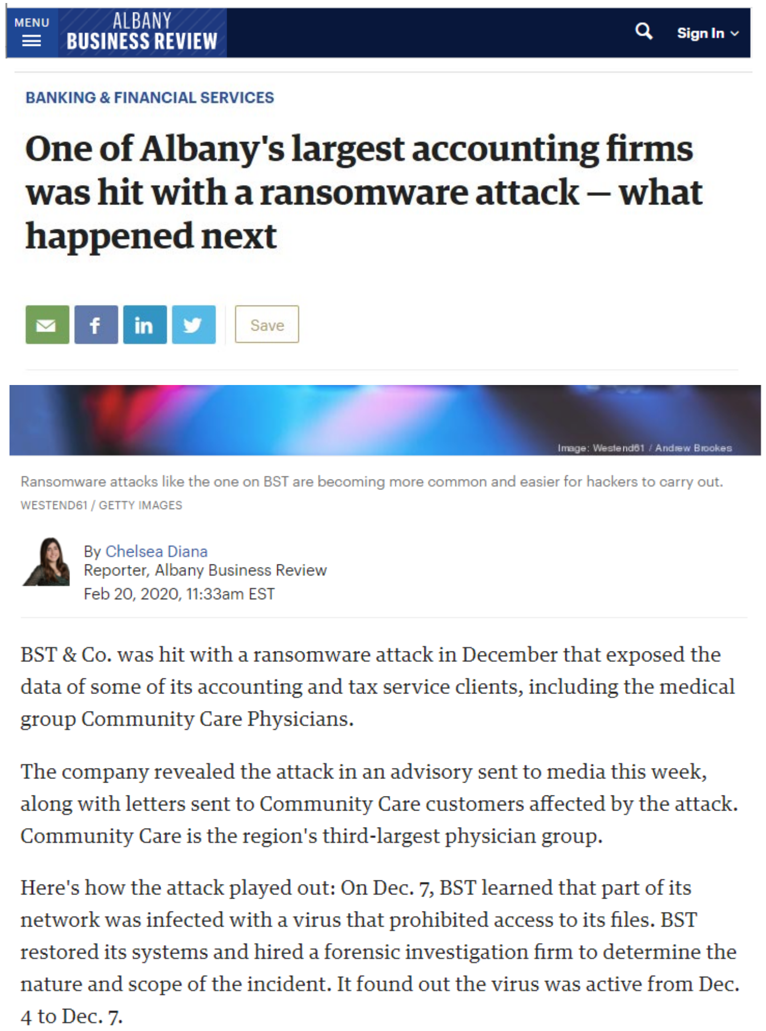


Leading accounting firm MNP hit with cyberattack

By Lawrence Abrams April 17, 2020 02:07 PM 0

A leading accounting firm in Canada forced a company-wide shutdown of their systems after getting hit with a cyberattack last weekend, BleepingComputer has learned.

Canadian accounting firm MNP's systems were impacted last weekend in what BleepingComputer was told was a ransomware attack.



BANKING & FINANCIAL SERVICES

One of Albany's largest accounting firms was hit with a ransomware attack – what happened next

Ransomware attacks like the one on BST are becoming more common and easier for hackers to carry out.
WESTEND61 / GETTY IMAGES

By Chelsea Diana
Reporter, Albany Business Review
Feb 20, 2020, 11:33am EST

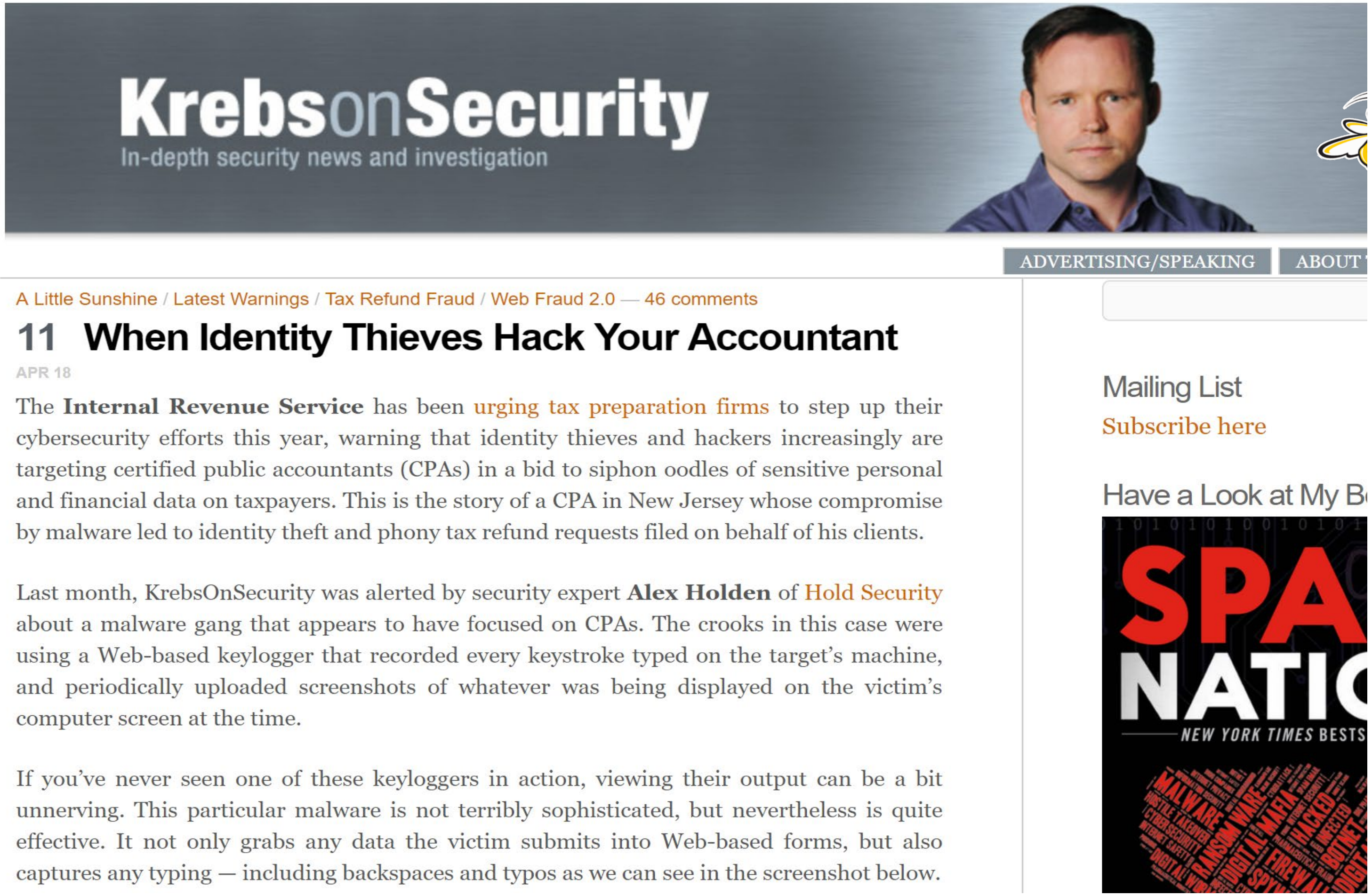
BST & Co. was hit with a ransomware attack in December that exposed the data of some of its accounting and tax service clients, including the medical group Community Care Physicians.

The company revealed the attack in an advisory sent to media this week, along with letters sent to Community Care customers affected by the attack. Community Care is the region's third-largest physician group.

Here's how the attack played out: On Dec. 7, BST learned that part of its network was infected with a virus that prohibited access to its files. BST restored its systems and hired a forensic investigation firm to determine the nature and scope of the incident. It found out the virus was active from Dec. 4 to Dec. 7.

Medical and Legal already being attacked
….will accounting firms be targeted next?

In the News: Security Headlines



KrebsonSecurity
In-depth security news and investigation

ADVERTISING/SPEAKING ABOUT

A Little Sunshine / Latest Warnings / Tax Refund Fraud / Web Fraud 2.0 — 46 comments

11 When Identity Thieves Hack Your Accountant

APR 18

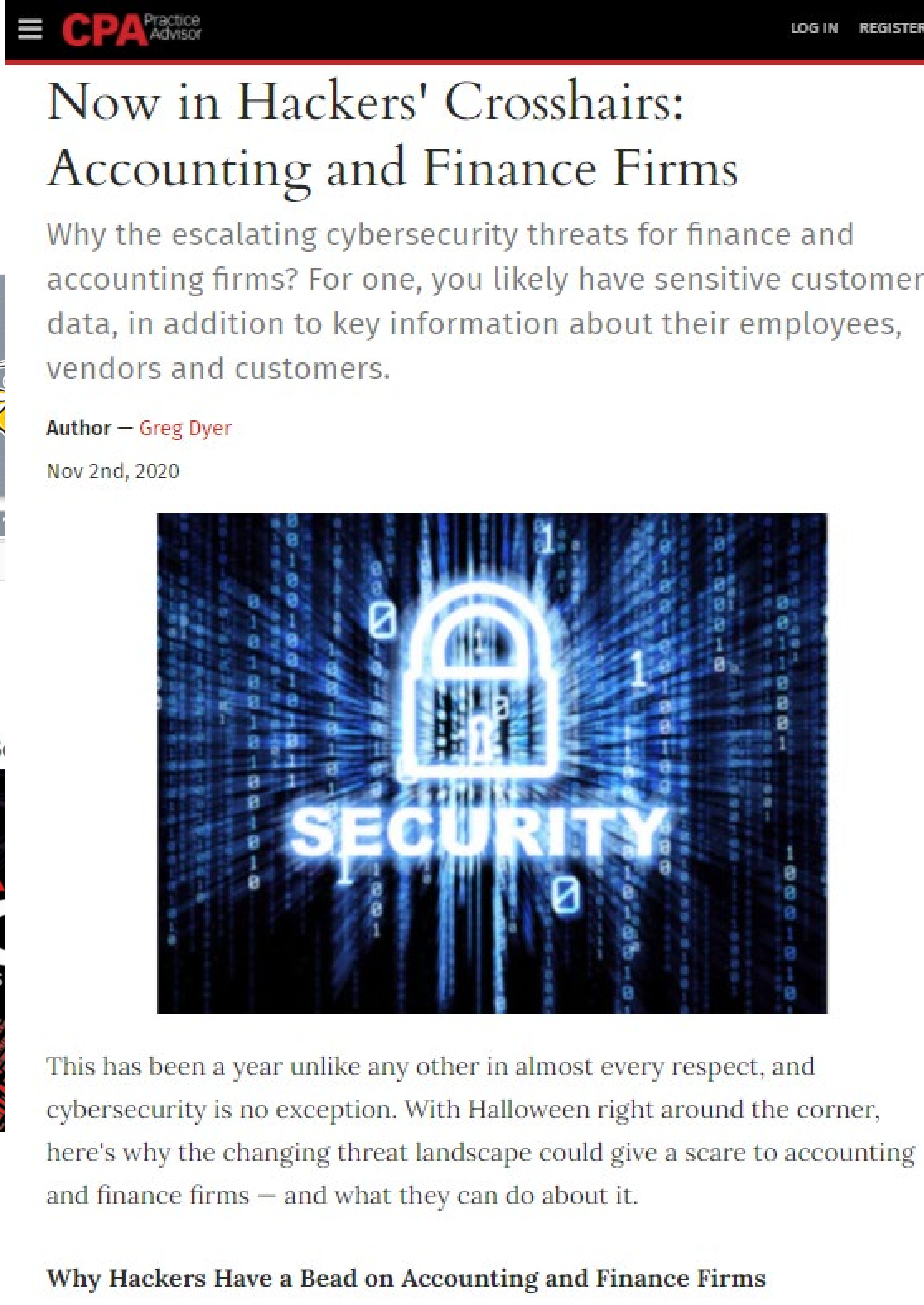
The **Internal Revenue Service** has been urging tax preparation firms to step up their cybersecurity efforts this year, warning that identity thieves and hackers increasingly are targeting certified public accountants (CPAs) in a bid to siphon oodles of sensitive personal and financial data on taxpayers. This is the story of a CPA in New Jersey whose compromise by malware led to identity theft and phony tax refund requests filed on behalf of his clients.

Last month, KrebsOnSecurity was alerted by security expert **Alex Holden** of Hold Security about a malware gang that appears to have focused on CPAs. The crooks in this case were using a Web-based keylogger that recorded every keystroke typed on the target's machine, and periodically uploaded screenshots of whatever was being displayed on the victim's computer screen at the time.

If you've never seen one of these keyloggers in action, viewing their output can be a bit unnerving. This particular malware is not terribly sophisticated, but nevertheless is quite effective. It not only grabs any data the victim submits into Web-based forms, but also captures any typing — including backspaces and typos as we can see in the screenshot below.

Mailing List
Subscribe here

Have a Look at My B



Now in Hackers' Crosshairs: Accounting and Finance Firms

Why the escalating cybersecurity threats for finance and accounting firms? For one, you likely have sensitive customer data, in addition to key information about their employees, vendors and customers.

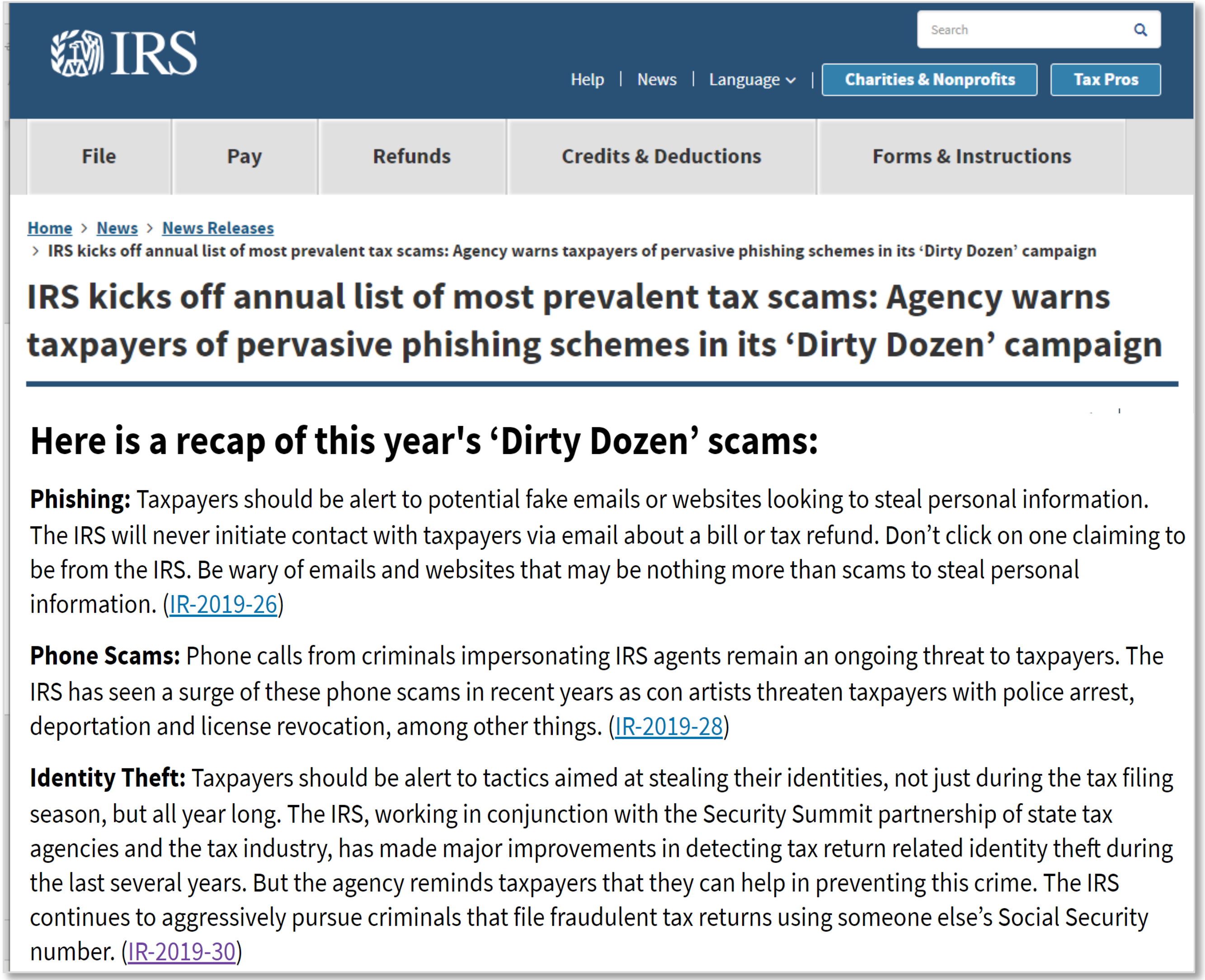
Author — Greg Dyer

Nov 2nd, 2020

This has been a year unlike any other in almost every respect, and cybersecurity is no exception. With Halloween right around the corner, here's why the changing threat landscape could give a scare to accounting and finance firms — and what they can do about it.

Why Hackers Have a Bead on Accounting and Finance Firms

In the News: Security Headlines


IRS
Search
Help | News | Language | Charities & Nonprofits | Tax Pros
File
Pay
Refunds
Credits & Deductions
Forms & Instructions
Home > News > News Releases
> IRS kicks off annual list of most prevalent tax scams: Agency warns taxpayers of pervasive phishing schemes in its ‘Dirty Dozen’ campaign

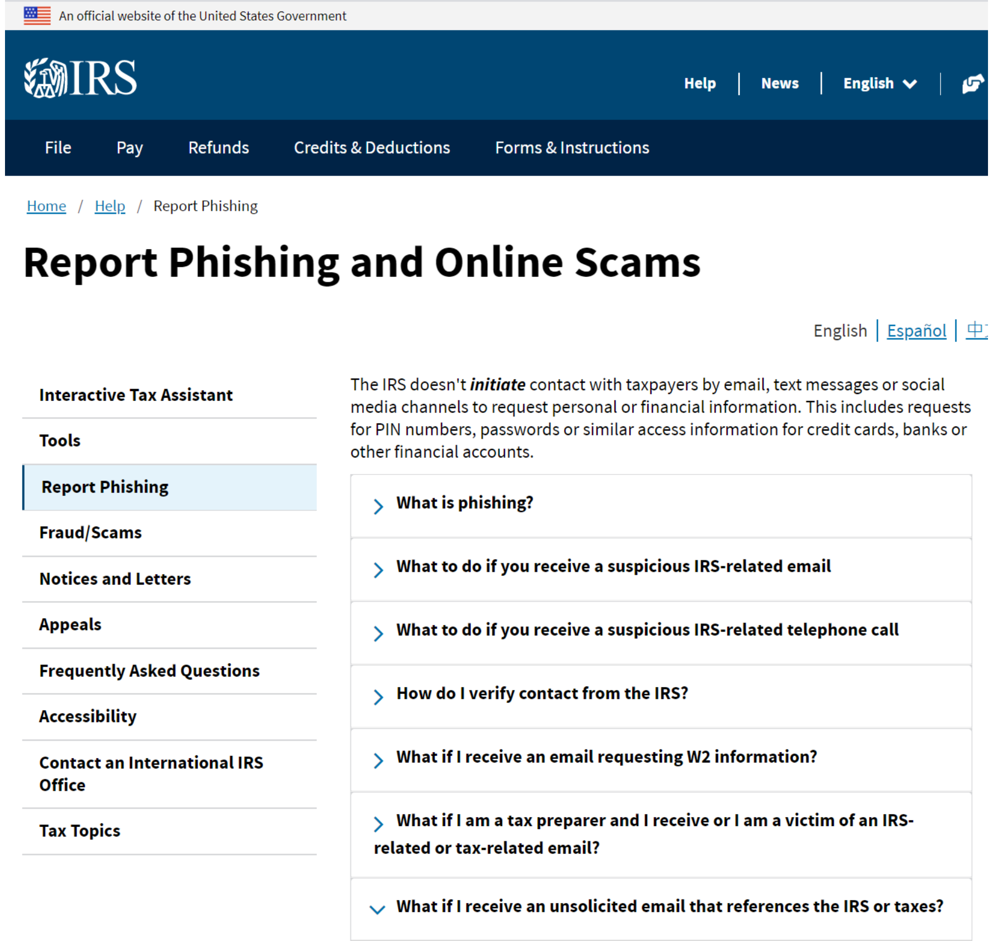
IRS kicks off annual list of most prevalent tax scams: Agency warns taxpayers of pervasive phishing schemes in its ‘Dirty Dozen’ campaign

Here is a recap of this year's ‘Dirty Dozen’ scams:

Phishing: Taxpayers should be alert to potential fake emails or websites looking to steal personal information. The IRS will never initiate contact with taxpayers via email about a bill or tax refund. Don’t click on one claiming to be from the IRS. Be wary of emails and websites that may be nothing more than scams to steal personal information. (IR-2019-26)

Phone Scams: Phone calls from criminals impersonating IRS agents remain an ongoing threat to taxpayers. The IRS has seen a surge of these phone scams in recent years as con artists threaten taxpayers with police arrest, deportation and license revocation, among other things. (IR-2019-28)

Identity Theft: Taxpayers should be alert to tactics aimed at stealing their identities, not just during the tax filing season, but all year long. The IRS, working in conjunction with the Security Summit partnership of state tax agencies and the tax industry, has made major improvements in detecting tax return related identity theft during the last several years. But the agency reminds taxpayers that they can help in preventing this crime. The IRS continues to aggressively pursue criminals that file fraudulent tax returns using someone else’s Social Security number. (IR-2019-30)



Report Phishing and Online Scams

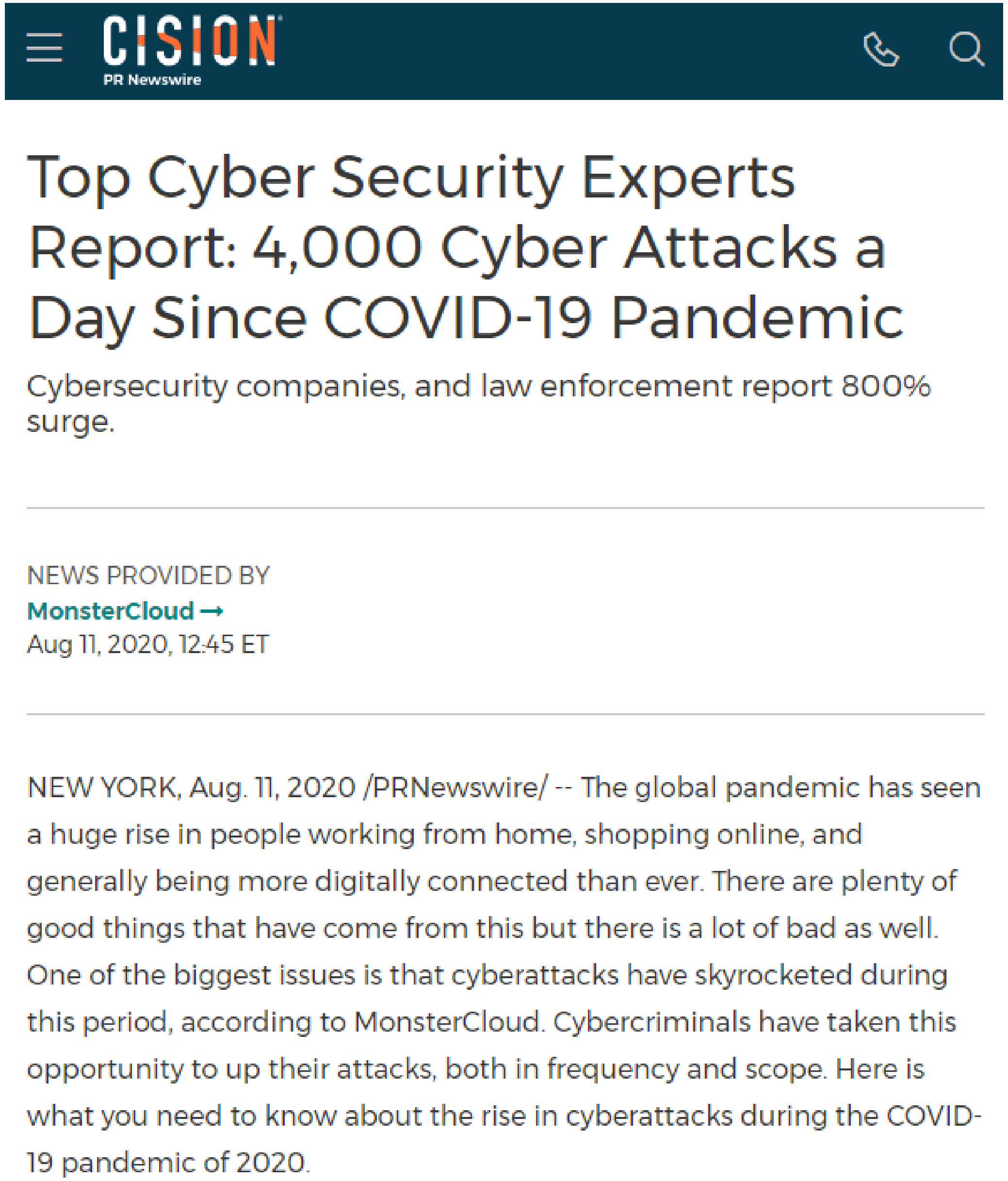
Interactive Tax Assistant
Tools
Report Phishing
Fraud/Scams
Notices and Letters
Appeals
Frequently Asked Questions
Accessibility
Contact an International IRS Office
Tax Topics

The IRS doesn't ***initiate*** contact with taxpayers by email, text messages or social media channels to request personal or financial information. This includes requests for PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

- What is phishing?
- What to do if you receive a suspicious IRS-related email
- What to do if you receive a suspicious IRS-related telephone call
- How do I verify contact from the IRS?
- What if I receive an email requesting W2 information?
- What if I am a tax preparer and I receive or I am a victim of an IRS-related or tax-related email?
- What if I receive an unsolicited email that references the IRS or taxes?

Report: phishing@irs.gov

In the News: Security Headlines



Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic

Cybersecurity companies, and law enforcement report 800% surge.

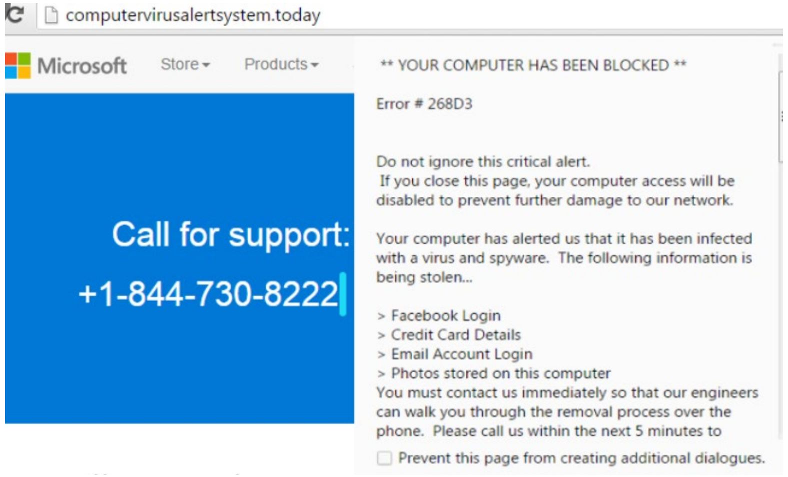
NEWS PROVIDED BY
MonsterCloud →
Aug 11, 2020, 12:45 ET

NEW YORK, Aug. 11, 2020 /PRNewswire/ -- The global pandemic has seen a huge rise in people working from home, shopping online, and generally being more digitally connected than ever. There are plenty of good things that have come from this but there is a lot of bad as well. One of the biggest issues is that cyberattacks have skyrocketed during this period, according to MonsterCloud. Cybercriminals have taken this opportunity to up their attacks, both in frequency and scope. Here is what you need to know about the rise in cyberattacks during the COVID-19 pandemic of 2020.

“Breach Fatigue”

Advancing Cyber Threats: Social Engineering

- Virtual Social Engineering (contact from unknown party)
  - Verify phone/email contacts
  - Security Pop Ups
    - Do not call listed number
    - Do not click link-contact sender to verify
    - Log into websites directly (verify HTTPS/SHTTPS)
    - Hover over any links to review properties
    - Do not access from another computer



Call for support:
+1-844-730-8222

** YOUR COMPUTER HAS BEEN BLOCKED **

Error # 268D3

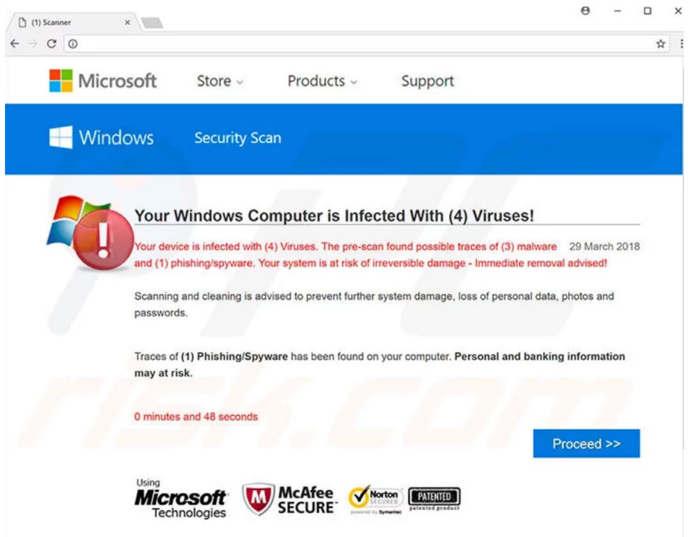
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

> Facebook Login
> Credit Card Details
> Email Account Login
> Photos stored on this computer

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to

□ Prevent this page from creating additional dialogues.



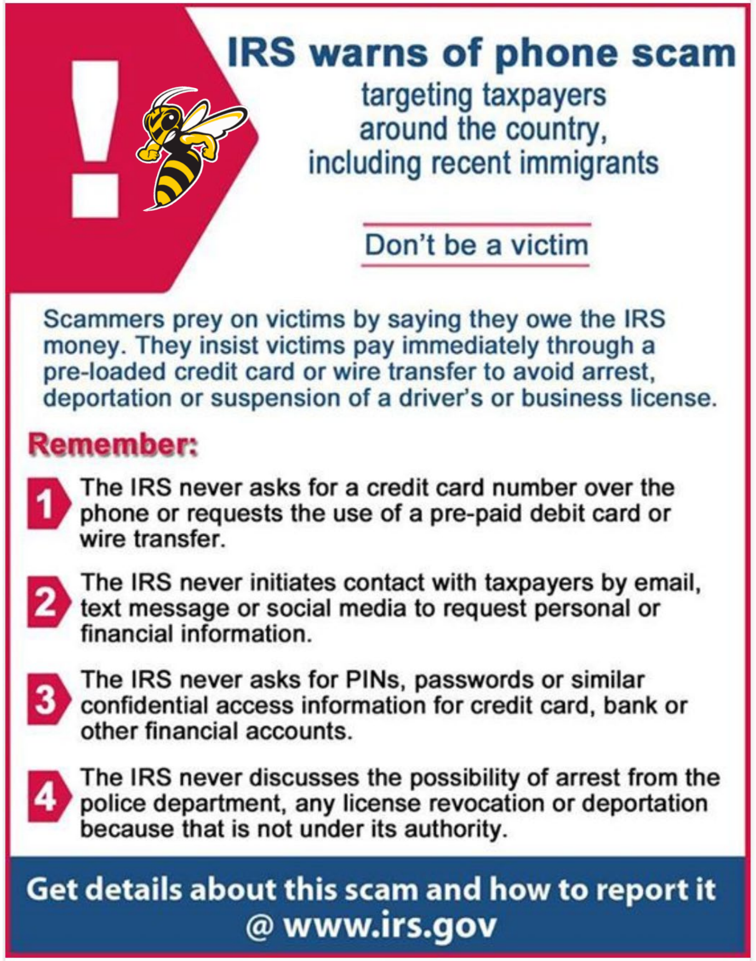
Your Windows Computer is Infected With (4) Viruses!

Your device is infected with (4) Viruses. The pre-scan found possible traces of (3) malware and (1) phishing/spyware. Your system is at risk of irreversible damage - Immediate removal advised! 29 March 2018

Scanning and cleaning is advised to prevent further system damage, loss of personal data, photos and passwords.

Traces of **(1) Phishing/Spyware** has been found on your computer. **Personal and banking information may at risk.**

0 minutes and 48 seconds



IRS warns of phone scam
targeting taxpayers
around the country,
including recent immigrants

Don't be a victim

Scammers prey on victims by saying they owe the IRS money. They insist victims pay immediately through a pre-loaded credit card or wire transfer to avoid arrest, deportation or suspension of a driver's or business license.

Remember:

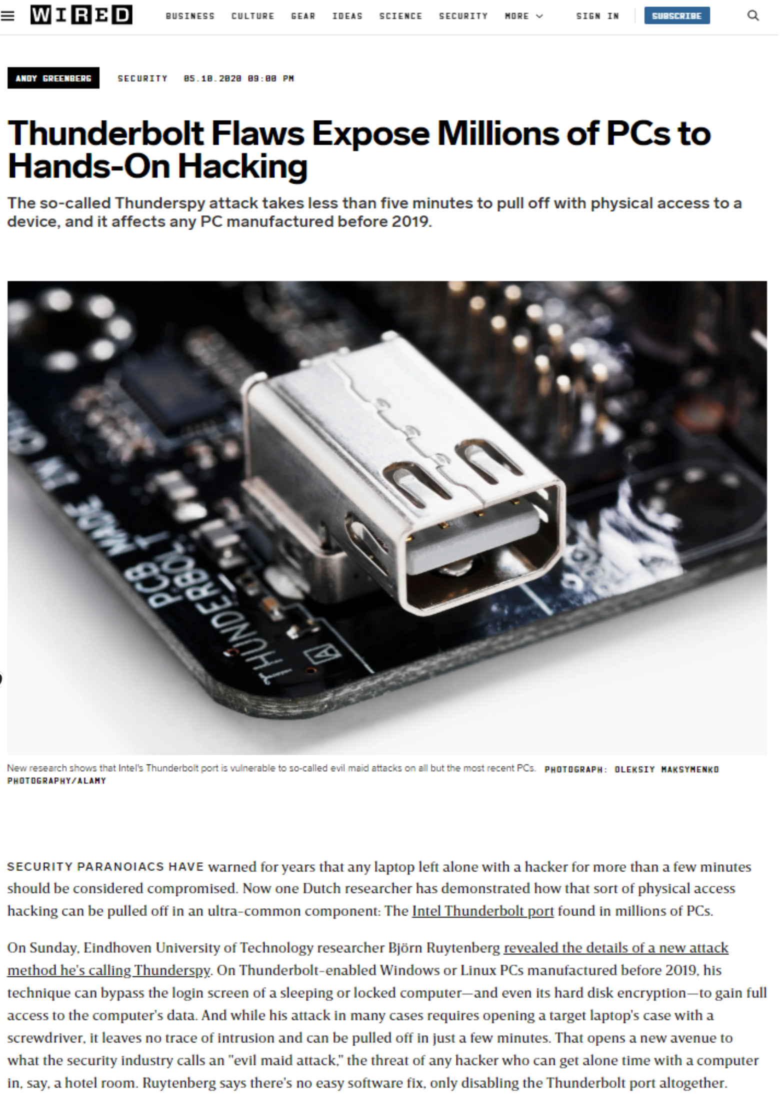
1. The IRS never asks for a credit card number over the phone or requests the use of a pre-paid debit card or wire transfer.
2. The IRS never initiates contact with taxpayers by email, text message or social media to request personal or financial information.
3. The IRS never asks for PINs, passwords or similar confidential access information for credit card, bank or other financial accounts.
4. The IRS never discusses the possibility of arrest from the police department, any license revocation or deportation because that is not under its authority.

Get details about this scam and how to report it @ www.irs.gov

Advancing Cyber Threats: Social Engineering

- Virtual Social Engineering (contact from unknown party)
    - Verify phone/email contacts
    - Security Pop Ups
        - Do not call listed number
        - Do not click link-contact sender to verify
        - Log into websites directly (verify HTTPS/SHTTPS)
        - Hover over any links to review properties
        - Do not access from another computer
- Social Engineering-Physical
    - Physically greet office visitors/accompany/monitor visit (8% physical)*
    - USB Warning (Malware/Data Theft)

…Evil Maid attacks



ANDY GREENBERG SECURITY 05.10.2020 09:00 PM

Thunderbolt Flaws Expose Millions of PCs to Hands-On Hacking

The so-called Thunderspy attack takes less than five minutes to pull off with physical access to a device, and it affects any PC manufactured before 2019.

New research shows that Intel's Thunderbolt port is vulnerable to so-called evil maid attacks on all but the most recent PCs. PHOTOGRAPH: OLEKSIY MAKSYMENKO PHOTOGRAPHY/ALAMY

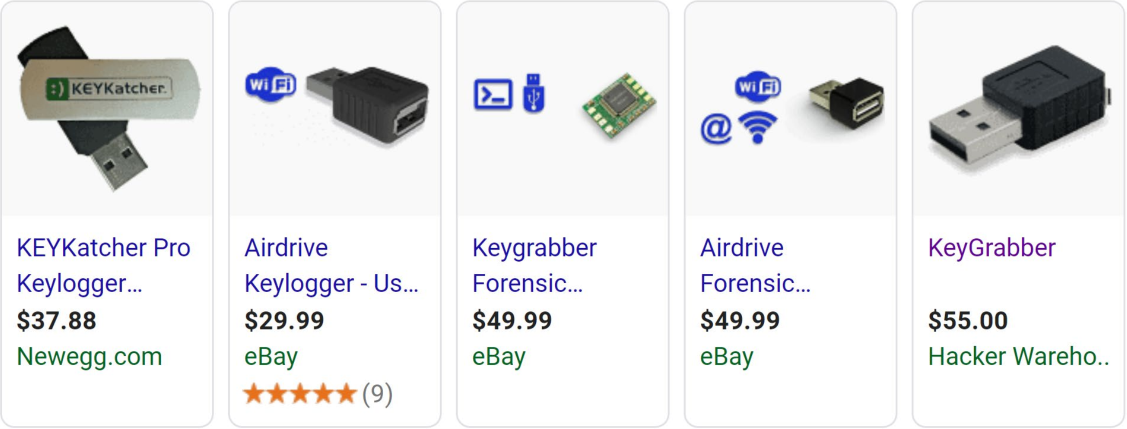
SECURITY PARANOIACS HAVE warned for years that any laptop left alone with a hacker for more than a few minutes should be considered compromised. Now one Dutch researcher has demonstrated how that sort of physical access hacking can be pulled off in an ultra-common component: The Intel Thunderbolt port found in millions of PCs.

On Sunday, Eindhoven University of Technology researcher Björn Ruytenberg revealed the details of a new attack method he's calling Thunderspy. On Thunderbolt-enabled Windows or Linux PCs manufactured before 2019, his technique can bypass the login screen of a sleeping or locked computer—and even its hard disk encryption—to gain full access to the computer's data. And while his attack in many cases requires opening a target laptop's case with a screwdriver, it leaves no trace of intrusion and can be pulled off in just a few minutes. That opens a new avenue to what the security industry calls an "evil maid attack," the threat of any hacker who can get alone time with a computer in, say, a hotel room. Ruytenberg says there's no easy software fix, only disabling the Thunderbolt port altogether.

*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Compromised Credentials

- Compromised Credentials/Password (81%)*
  - Re-used from other sites/seldom changed
  - Unsecure WiFi/Keyboard Logger
  - Accounting Specific Targets:
    - Client Tax Data (Document Management)
    - Electronic Filing (Tax Applications/Payroll)
    - Internal Finance (Banking/Payroll)
    - Internal/External Contacts (Outlook to spread malware)
  - Solutions:
    - Complex Passwords-Changed Frequently, Password Wallets
    - Utilize Multi-Factor Authentication (DUO/Okta)



KEYKatcher Pro Keylogger...
$37.88
Newegg.com

Airdrive Keylogger - Us...
$29.99
eBay
★★★★★ (9)

Keygrabber Forensic...
$49.99
eBay

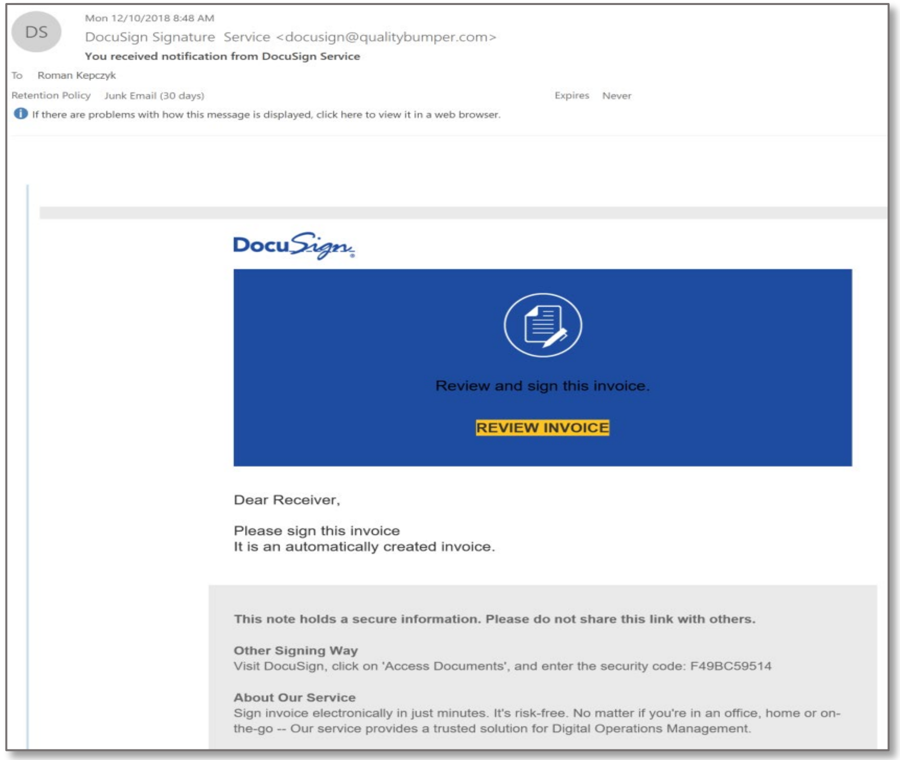
Airdrive Forensic...
$49.99
eBay

KeyGrabber
$55.00
Hacker Wareho..

*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Phishing-Spear Phishing

- Phishing Emails (66%)*
  - Attachments with Malware



Mon 12/10/2018 8:48 AM
DocuSign Signature Service <docusign@qualitybumper.com>
You received notification from DocuSign Service
To Roman Kepczyk
Retention Policy Junk Email (30 days) Expires Never
If there are problems with how this message is displayed, click here to view it in a web browser.

Review and sign this invoice.

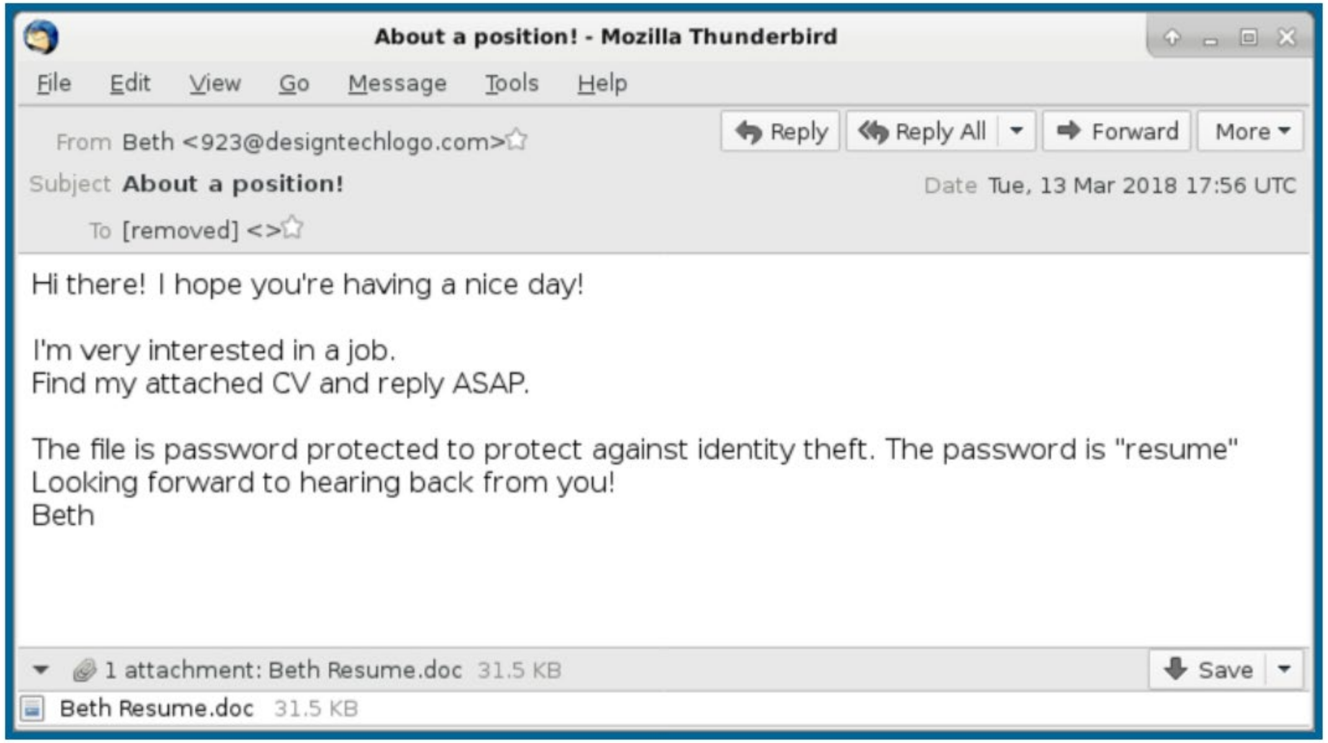
Dear Receiver,

Please sign this invoice
It is an automatically created invoice.

This note holds a secure information. Please do not share this link with others.

Other Signing Way
Visit DocuSign, click on 'Access Documents', and enter the security code: F49BC59514

About Our Service
Sign invoice electronically in just minutes. It's risk-free. No matter if you're in an office, home or on-the-go -- Our service provides a trusted solution for Digital Operations Management.



From Beth <923@designtechlogo.com>
Subject **About a position!**
Date Tue, 13 Mar 2018 17:56 UTC
To [removed] <>

Hi there! I hope you're having a nice day!

I'm very interested in a job.
Find my attached CV and reply ASAP.

The file is password protected to protect against identity theft. The password is "resume"
Looking forward to hearing back from you!
Beth

1 attachment: Beth Resume.doc 31.5 KB
Beth Resume.doc 31.5 KB

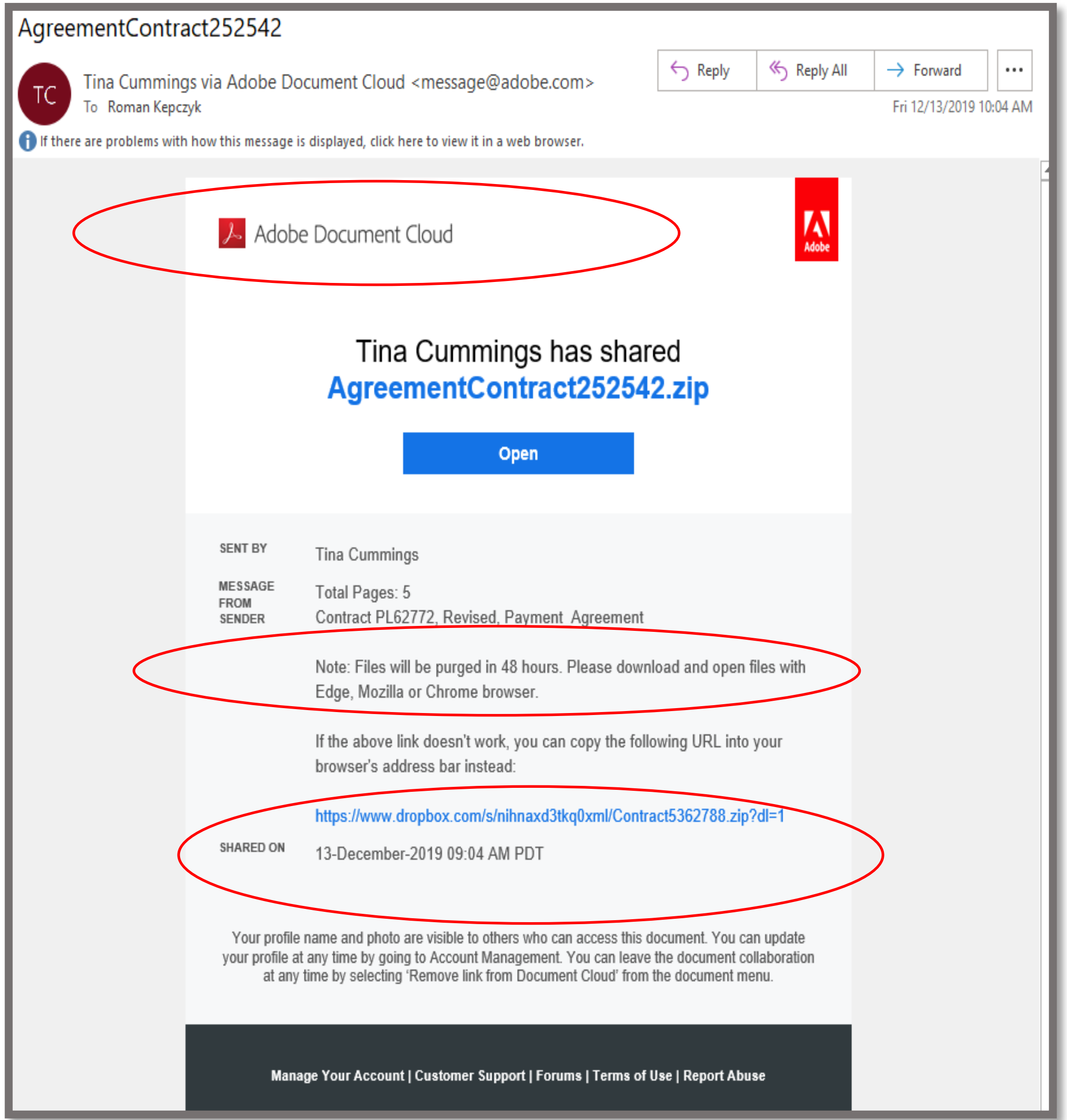
*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Phishing-Spear Phishing

- Phishing Emails (66%)*
  - Attachments with Malware
  - Links to websites
  - Accounting Firm Targets
    - DocuSign
    - Adobe Cloud

- Initial Warning Signs
  - Unexpected or Out of Character
  - Requires Immediate Response/Action
  - Requests click on Link, Credentials, Login, Financial

…take a minute to be sure.



AgreementContract252542

Tina Cummings via Adobe Document Cloud <message@adobe.com>
To Roman Kepczyk

Fri 12/13/2019 10:04 AM

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

Adobe Document Cloud

Tina Cummings has shared
AgreementContract252542.zip

Open

SENT BY Tina Cummings

MESSAGE FROM SENDER Total Pages: 5
Contract PL62772, Revised, Payment Agreement

Note: Files will be purged in 48 hours. Please download and open files with Edge, Mozilla or Chrome browser.

If the above link doesn't work, you can copy the following URL into your browser's address bar instead:

https://www.dropbox.com/s/nihnaxd3tkq0xml/Contract5362788.zip?dl=1

SHARED ON 13-December-2019 09:04 AM PDT

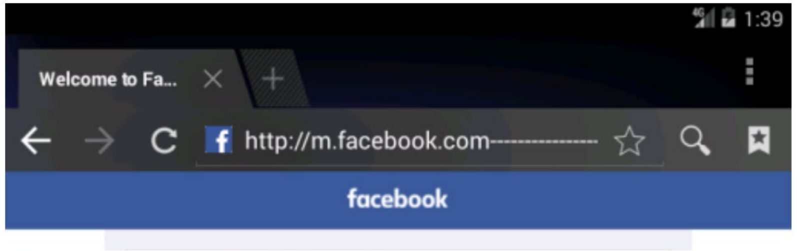
Your profile name and photo are visible to others who can access this document. You can update your profile at any time by going to Account Management. You can leave the document collaboration at any time by selecting 'Remove link from Document Cloud' from the document menu.

Manage Your Account | Customer Support | Forums | Terms of Use | Report Abuse

*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Phishing-Spear Phishing

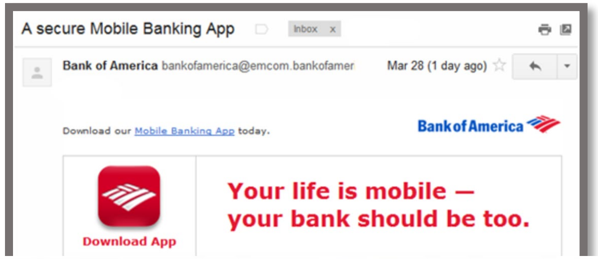
- Phishing Emails (66%)*
    - Attachments with Malware
    - Links to websites
    - Accounting Firm Targets
        - DocuSign,
        - Adobe Cloud
    - Initial Warning Signs
        - Unexpected or Out of Character
        - Requires Immediate Response/Action
        - Click on Link, Credentials, Login, Financ
    - Don’t forget about Mobile Phishing
        - URL Padding
        - SMS links (SMiShing)



1:39

Welcome to Fa...

http://m.facebook.com-------------



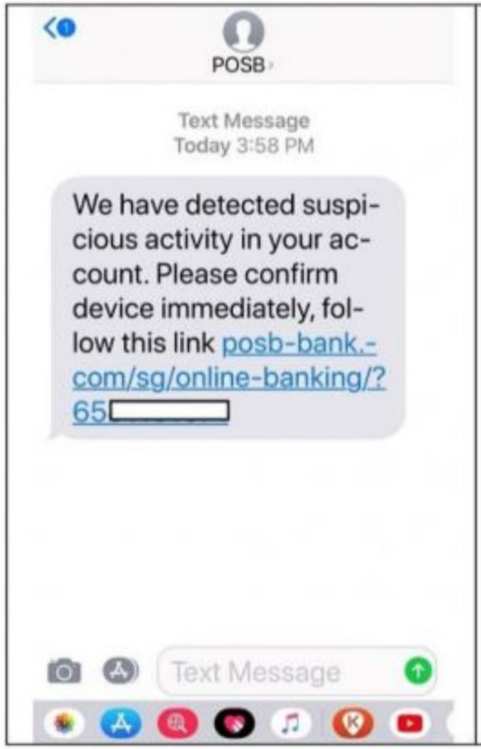
A secure Mobile Banking App

Inbox

Bank of America bankofamerica@emcom.bankofamer

Mar 28 (1 day ago)

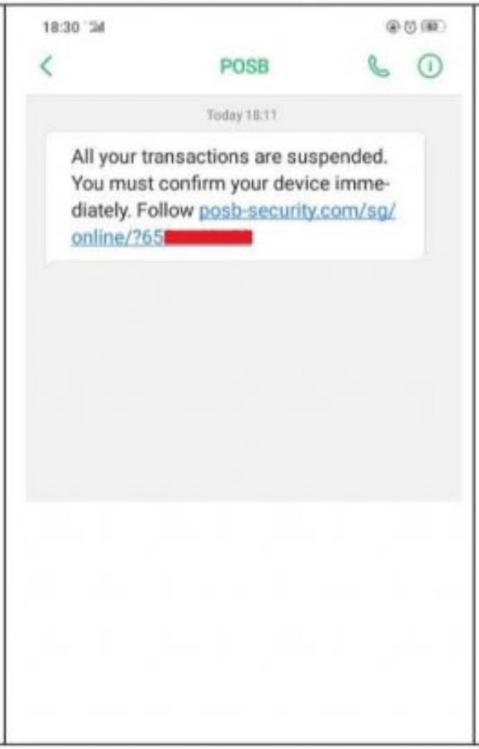
Download our Mobile Banking App today.



POSB

Text Message
Today 3:58 PM

We have detected suspicious activity in your account. Please confirm device immediately, follow this link posb-bank.com/sg/online-banking/?65[redacted]

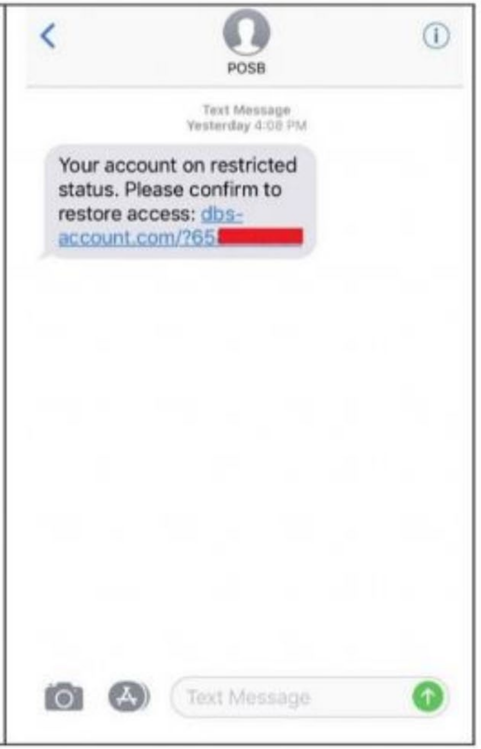


18:30

POSB

Today 18:11

All your transactions are suspended. You must confirm your device immediately. Follow posb-security.com/sg/online/?65[redacted]



POSB

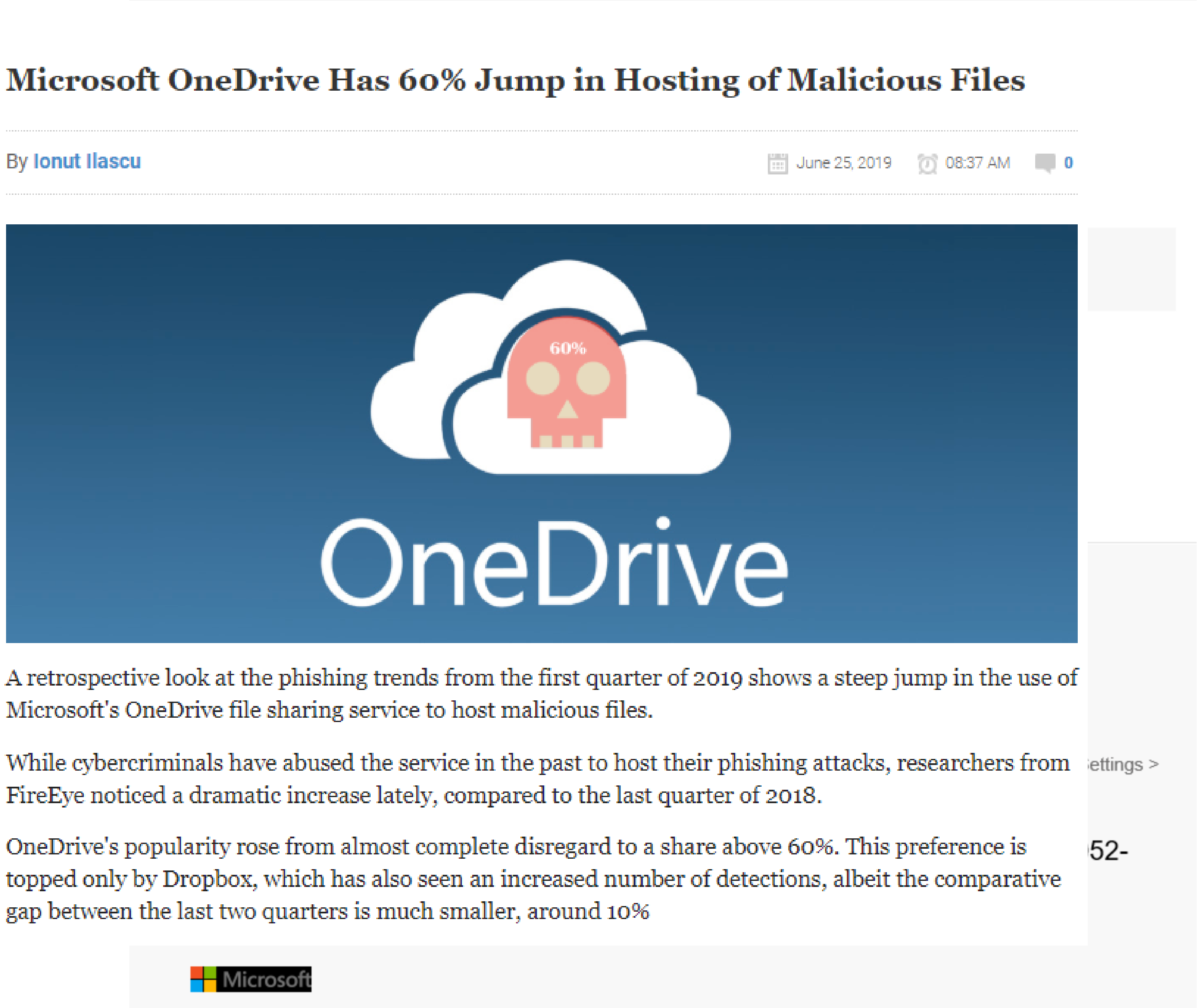
Text Message
Yesterday 4:08 PM

Your account on restricted status. Please confirm to restore access: dbs-account.com/?65[redacted]

*Verizon Data Breach Investigations Report /Phishlabs

Advancing Cyber Threats: Phishing-Spear Phishing

- Phishing Emails (66%)*
  - Attachments with Malware
  - Links to websites
  - Accounting Firm Targets
  - New Avenues of Attack: Application Upda
    - Meeting Notification Updates (WebEx)
    - Microsoft Office 365/TEAMS Alerts



Microsoft OneDrive Has 60% Jump in Hosting of Malicious Files

By Ionut Ilascu June 25, 2019 08:37 AM 0

A retrospective look at the phishing trends from the first quarter of 2019 shows a steep jump in the use of Microsoft's OneDrive file sharing service to host malicious files.

While cybercriminals have abused the service in the past to host their phishing attacks, researchers from FireEye noticed a dramatic increase lately, compared to the last quarter of 2018.

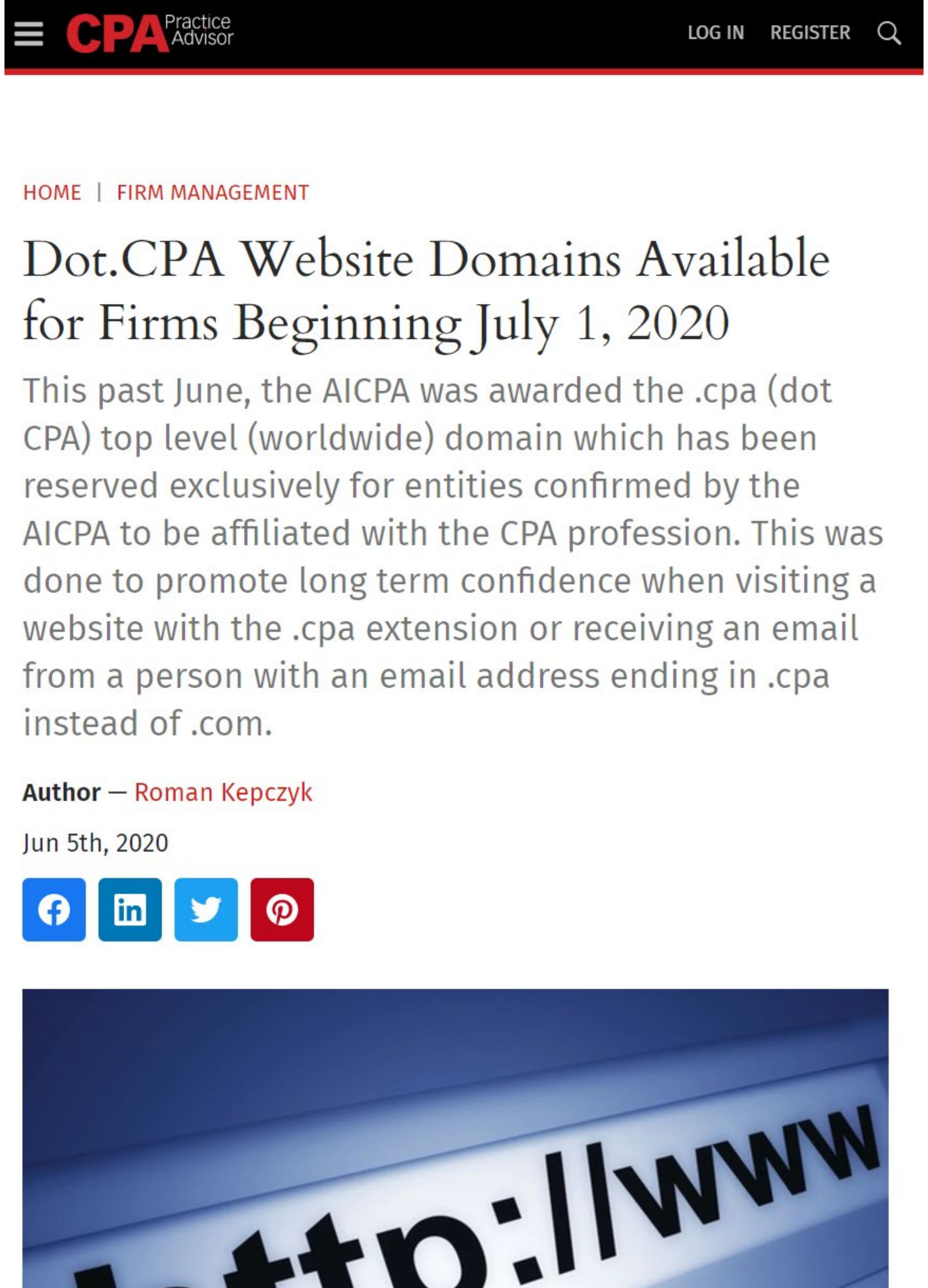
OneDrive's popularity rose from almost complete disregard to a share above 60%. This preference is topped only by Dropbox, which has also seen an increased number of detections, albeit the comparative gap between the last two quarters is much smaller, around 10%

*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Phishing

- Phishing Emails (66%)*
  - Attachments with Malware
  - Links to websites
  - Accounting Firm Targets
  - New Avenues of Attack: Application Updates
    - Meeting Notification Updates (WebEx)
    - Microsoft Office 365 /TEAMS Alerts
  - Phishing as a Service (PaaS)
  - Unrestricted .com vs. restricted .cpa domain

...rightnetworkx.com



HOME | FIRM MANAGEMENT

Dot.CPA Website Domains Available for Firms Beginning July 1, 2020

This past June, the AICPA was awarded the .cpa (dot CPA) top level (worldwide) domain which has been reserved exclusively for entities confirmed by the AICPA to be affiliated with the CPA profession. This was done to promote long term confidence when visiting a website with the .cpa extension or receiving an email from a person with an email address ending in .cpa instead of .com.

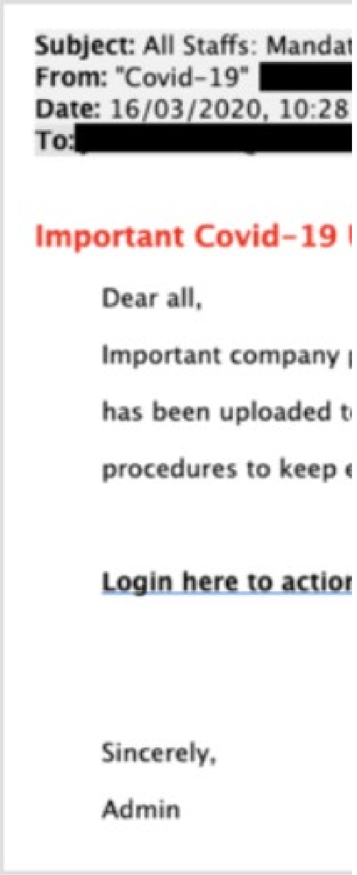
Author — Roman Kepczyk

Jun 5th, 2020

*Verizon Data Breach Investigations Report

Advancing Cyber Threats: Phishing

- Current scams and malware
  - Phishing/Pharming
    - Look-Alike Websites
    - Social Media Gift Exchange
    - Grandparent Scams
    - Temporary Holiday Jobs
    - Free Gift Cards
    - E-Cards
    - Fake Shipping Notifications
    - Phony Charities
    - Letters From Santa
    - Unusual Forms of Payments
    - Travel Scams



Subject: All Staffs: Mandat
From: "Covid-19" [redacted]
Date: 16/03/2020, 10:28
To: [redacted]

Important Covid-19

Dear all,

Important company

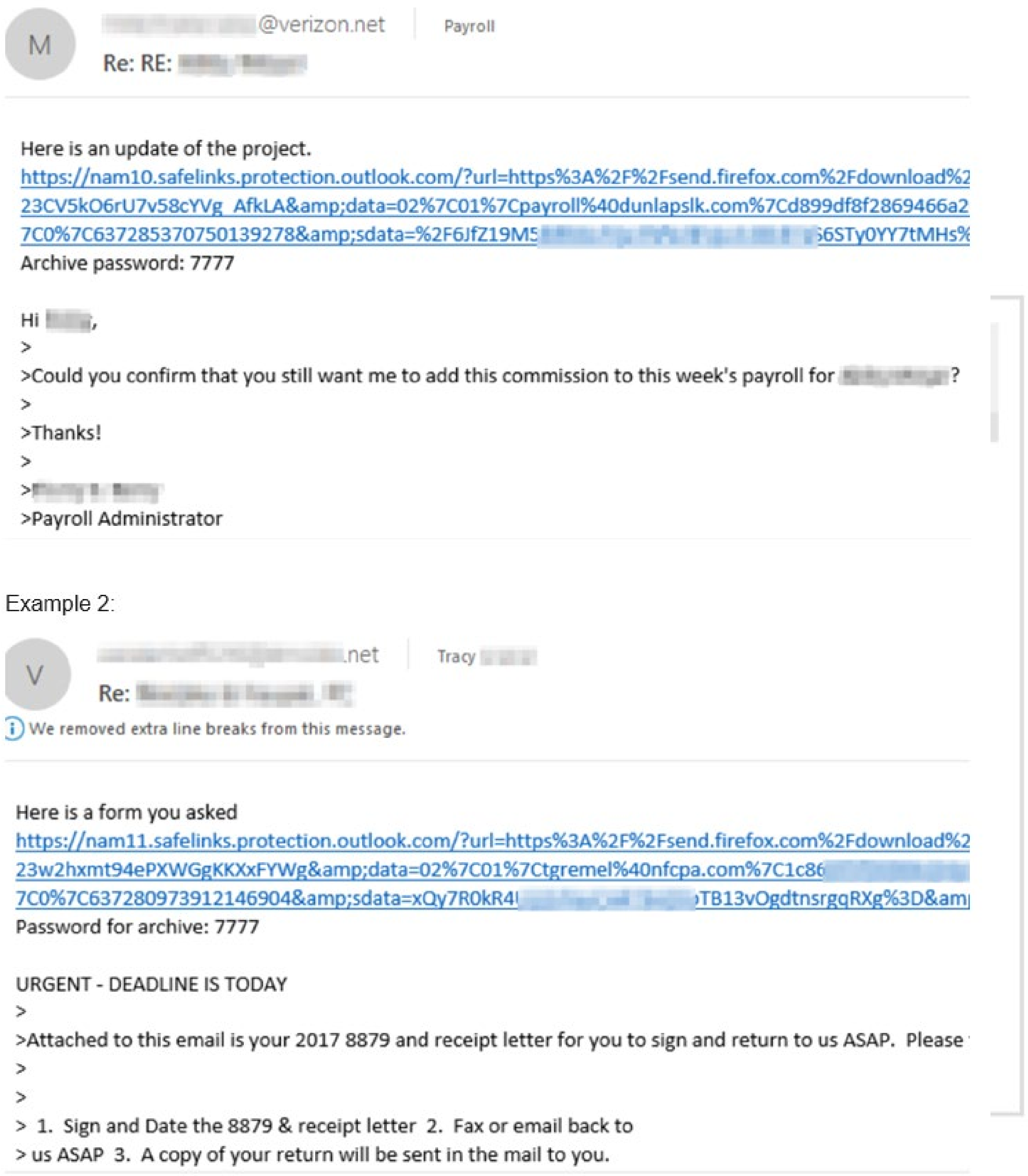
has been uploaded t

procedures to keep

Login here to actior

Sincerely,

Admin



M [redacted]@verizon.net | Payroll

Re: RE: [redacted]

Here is an update of the project.
https://nam10.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsend.firefox.com%2Fdownload%2
23CV5kO6rU7v58cYVg_AfkLA&amp;data=02%7C01%7Cpayroll%40dunlapslk.com%7Cd899df8f2869466a2
7C0%7C637285370750139278&amp;sdata=%2F6JfZ19M5[redacted]6STy0YY7tMHs%
Archive password: 7777

Hi [redacted],
>
>Could you confirm that you still want me to add this commission to this week's payroll for [redacted]?
>
>Thanks!
>
>[redacted]
>Payroll Administrator

Example 2:

V [redacted].net | Tracy [redacted]

Re: [redacted]

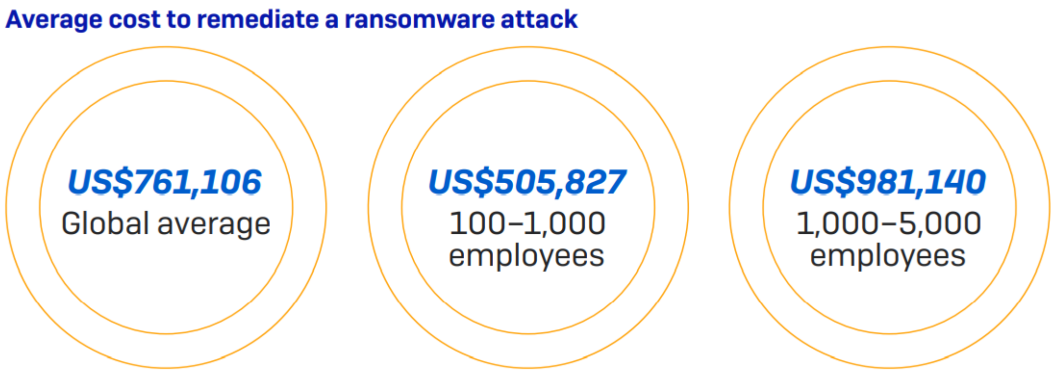
ⓘ We removed extra line breaks from this message.

Here is a form you asked
https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsend.firefox.com%2Fdownload%2
23w2hxmt94ePXWGgKKXxFYWg&amp;data=02%7C01%7Ctgremel%40nfcpa.com%7C1c86[redacted]
7C0%7C637280973912146904&amp;sdata=xQy7R0kR4[redacted]TB13vOgdtnsrgqRXg%3D&am
Password for archive: 7777

URGENT - DEADLINE IS TODAY
>
>Attached to this email is your 2017 8879 and receipt letter for you to sign and return to us ASAP. Please
>
>
> 1. Sign and Date the 8879 & receipt letter 2. Fax or email back to
> us ASAP 3. A copy of your return will be sent in the mail to you.

Advancing Cyber Threats

- 2020 State of Ransomware (Sophos)
  - 51% Hit with ransomware attack-73% encryption succeeded
  - 26% of encrypted companies got data back after paying (1% didn't)
  - 56% of encrypted companies got data back from backups
  - Paying the ransom effectively doubled the cost for remediation



Average cost to remediate a ransomware attack

US$761,106	US$505,827	US$981,140
Global average	100–1,000 employees	1,000–5,000 employees

THE STATE OF RANSOMWARE 2020

Results of an independent study of 5,000 IT managers across 26 countries

A Sophos white paper May 2020

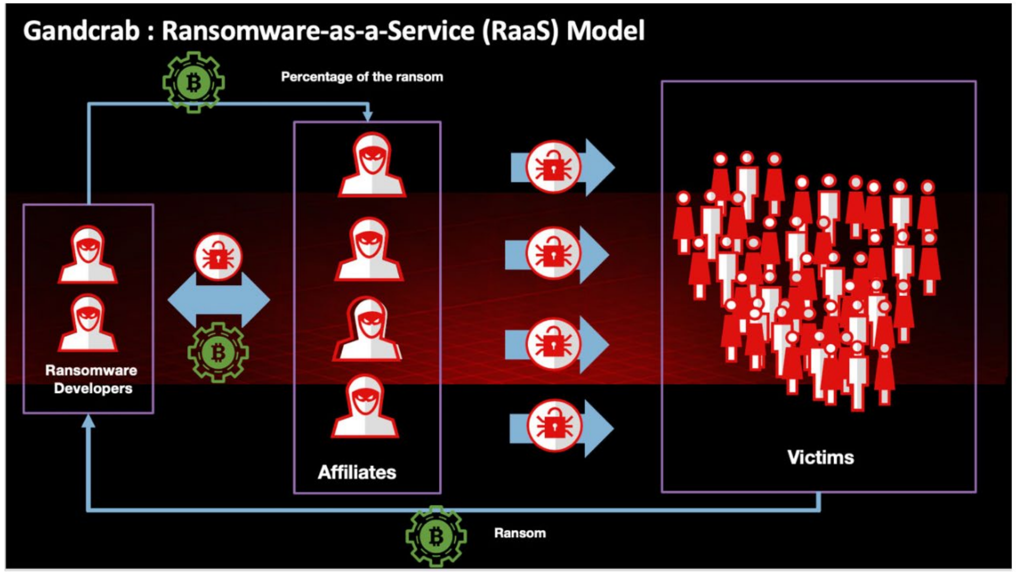
5,000 IT Managers in companies between 100-5,000 personnel (10% US

Advancing Cyber Threats

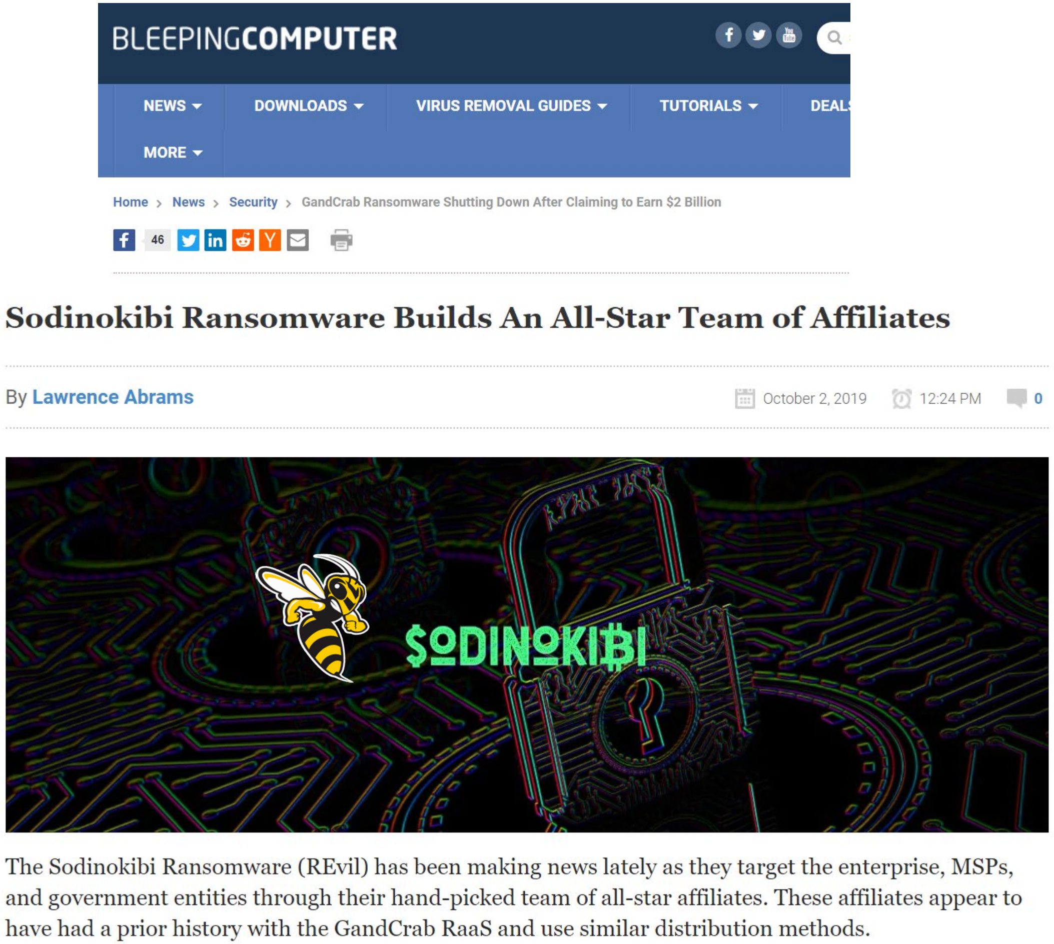
- 2020 State of Ransomware (Sophos)
- Current Ransomware Sequence (KnowBe4)
  - Criminal hackers infiltrate your network
  - Install Trojans and other malware
  - Delete your backups
  - Steal your data before encryption
  - Hold the data for ransom
  - Leak data and intellectual property, public shaming
  - Extortion of victim's clients, auction data troves

Advancing Cyber Threats

- 2020 State of Ransomware (Sophos)
- Current Ransomware Sequence (KnowBe4)
- Ransomware as a Service
  - Affiliate/Developer Split (Dot 50/50, Satan 70/30)
  - Tiered incentives



RaaS Explainer (Source: McAfee)


BLEEPINGCOMPUTER
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
MORE
Home › News › Security › GandCrab Ransomware Shutting Down After Claiming to Earn $2 Billion
46
$ODINOKIBI

Sodinokibi Ransomware Builds An All-Star Team of Affiliates

By Lawrence Abrams October 2, 2019 12:24 PM 0

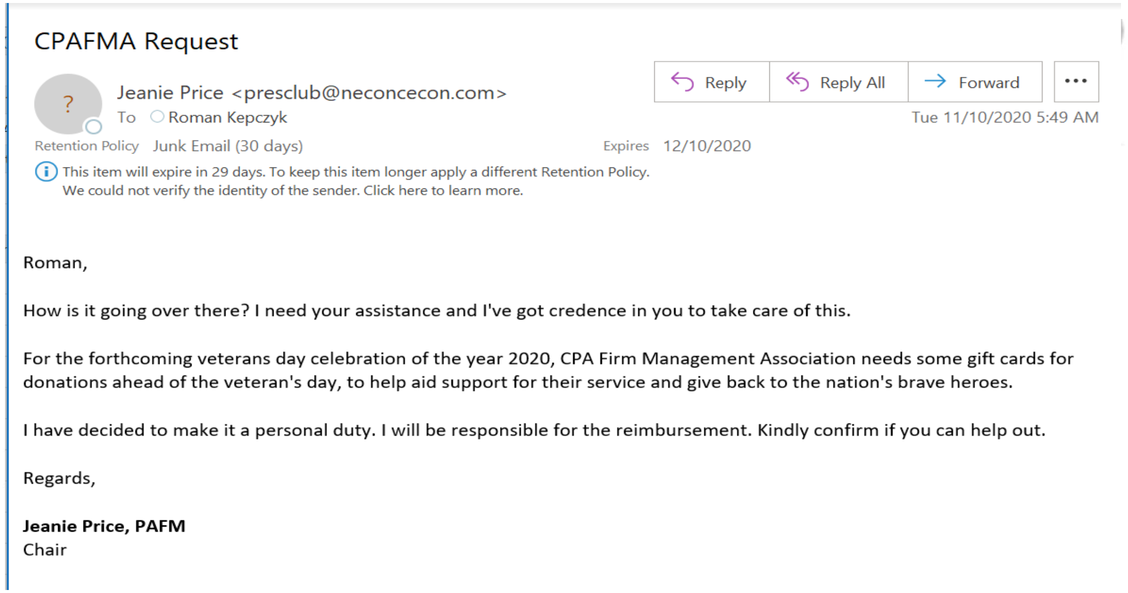
The Sodinokibi Ransomware (REvil) has been making news lately as they target the enterprise, MSPs, and government entities through their hand-picked team of all-star affiliates. These affiliates appear to have had a prior history with the GandCrab RaaS and use similar distribution methods.

Advancing Cyber Threats

- 2020 State of Ransomware (Sophos)
- Current Ransomware Sequence (KnowBe4)
- Ransomware as a Service
- Response if impacted?
  - Immediately validate backups and ability to recover
  - Know restoration time and critical file prioritization
  - Look for key missing files as email attachment
  - Erase, reformat, reinstall all workstations, servers

Advancing Cyber Threats: Whaling

- Hacker in the Middle
- Whaling (spoofed emails from known parties)
  roman@rightnetworkx.com
- Accounting Specific Targets: Payroll/Finance
  . ***...Gift Cards!!! Seriously????***



CPAFMA Request

Jeanie Price <presclub@neconcecon.com>
To ○ Roman Kepczyk
Tue 11/10/2020 5:49 AM

Retention Policy Junk Email (30 days) Expires 12/10/2020

ⓘ This item will expire in 29 days. To keep this item longer apply a different Retention Policy.
We could not verify the identity of the sender. Click here to learn more.

Roman,

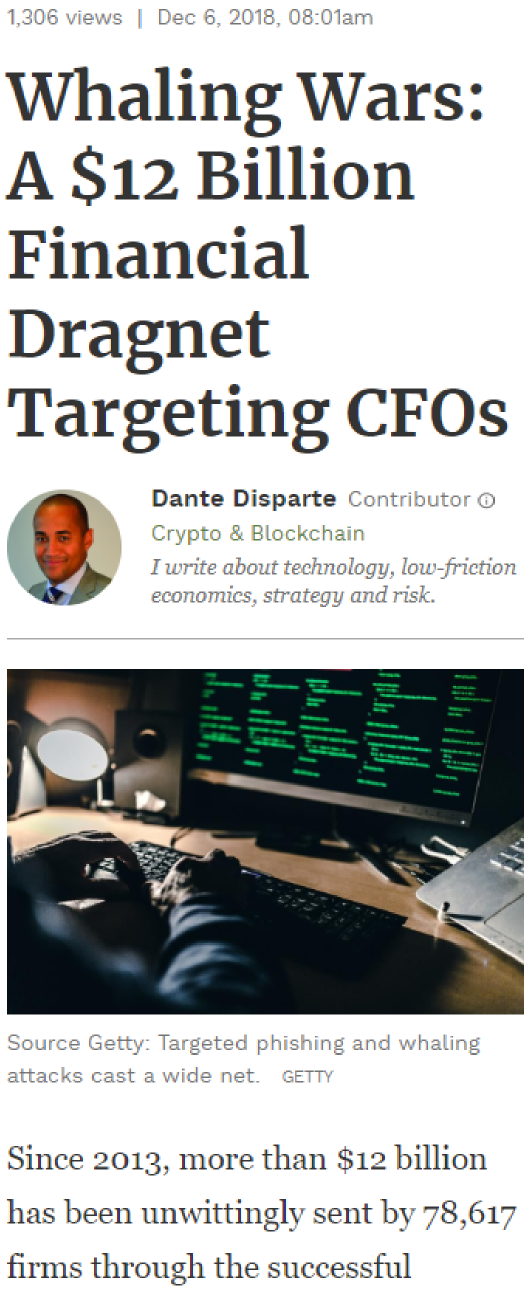
How is it going over there? I need your assistance and I've got credence in you to take care of this.

For the forthcoming veterans day celebration of the year 2020, CPA Firm Management Association needs some gift cards for donations ahead of the veteran's day, to help aid support for their service and give back to the nation's brave heroes.

I have decided to make it a personal duty. I will be responsible for the reimbursement. Kindly confirm if you can help out.

Regards,

Jeanie Price, PAFM
Chair



1,306 views | Dec 6, 2018, 08:01am

Whaling Wars: A $12 Billion Financial Dragnet Targeting CFOs

Dante Disparte Contributor ⓘ
Crypto & Blockchain
I write about technology, low-friction economics, strategy and risk.

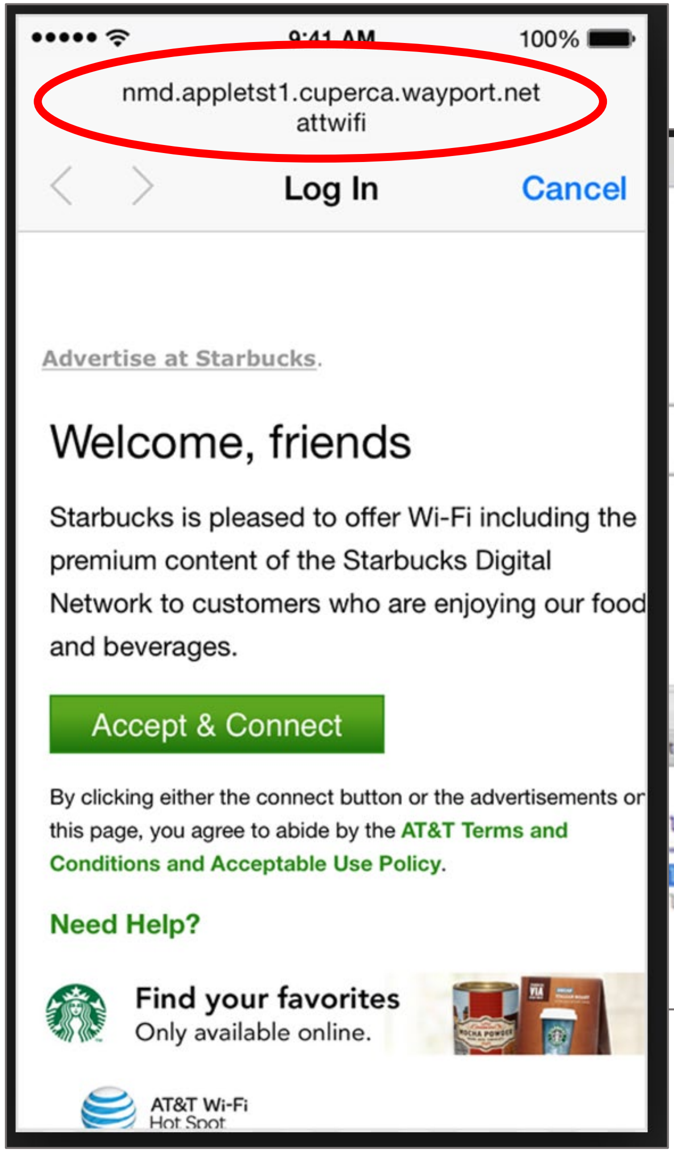
Source Getty: Targeted phishing and whaling attacks cast a wide net. GETTY

Since 2013, more than $12 billion has been unwittingly sent by 78,617 firms through the successful

Cyber Threat: Public/Client Wifi

- Verify WiFi before connecting
  - Identify client-provided WiFi SSID is valid before browsing

Wireless Access Point
(Target)
Wireless Client
(Victim)
StarbuckFreeWiFi
The MITM Attack Platform



nmd.appletst1.cuperca.wayport.net
attwifi

< > Log In Cancel

Advertise at Starbucks.

Welcome, friends

Starbucks is pleased to offer Wi-Fi including the premium content of the Starbucks Digital Network to customers who are enjoying our food and beverages.

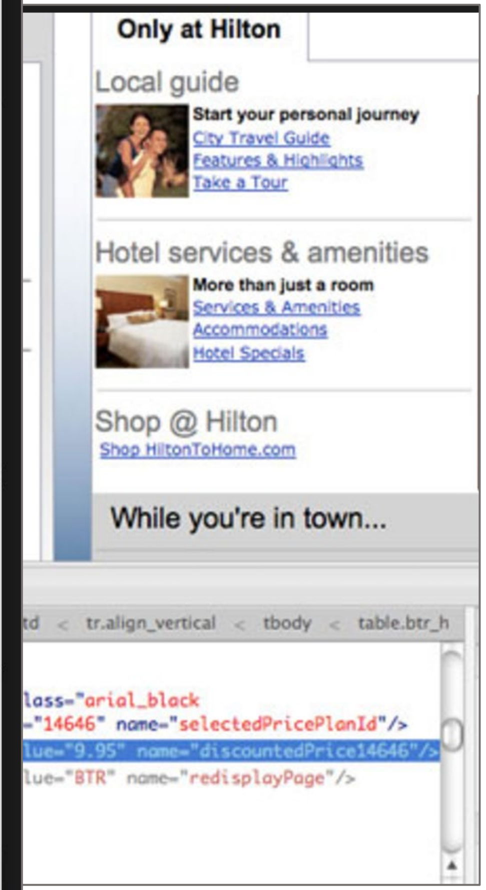
Accept & Connect

By clicking either the connect button or the advertisements on this page, you agree to abide by the AT&T Terms and Conditions and Acceptable Use Policy.

Need Help?

Find your favorites
Only available online.

AT&T Wi-Fi
Hot Spot


Only at Hilton

Local guide
Start your personal journey
City Travel Guide
Features & Highlights
Take a Tour

Hotel services & amenities
More than just a room
Services & Amenities
Accommodations
Hotel Specials

Shop @ Hilton
Shop HiltonToHome.com

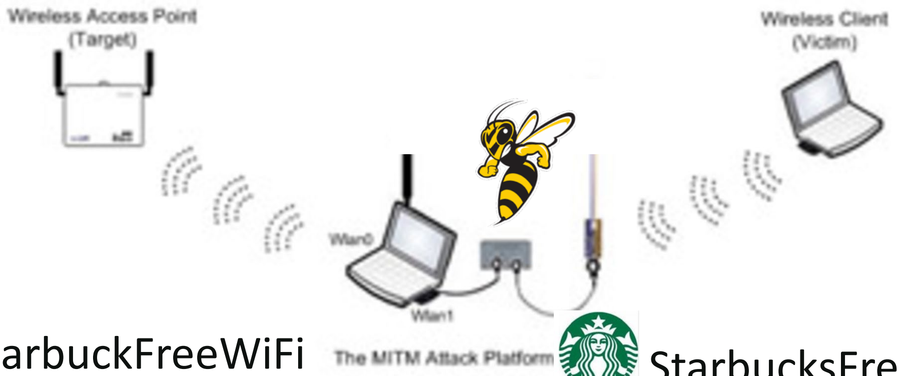
While you're in town...

td < tr.align_vertical < tbody < table.btr_h

```
lass="arial_black
="14646" name="selectedPricePlanId"/>
lue="9.95" name="discountedPrice14646"/>
lue="BTR" name="redisplayPage"/>
```

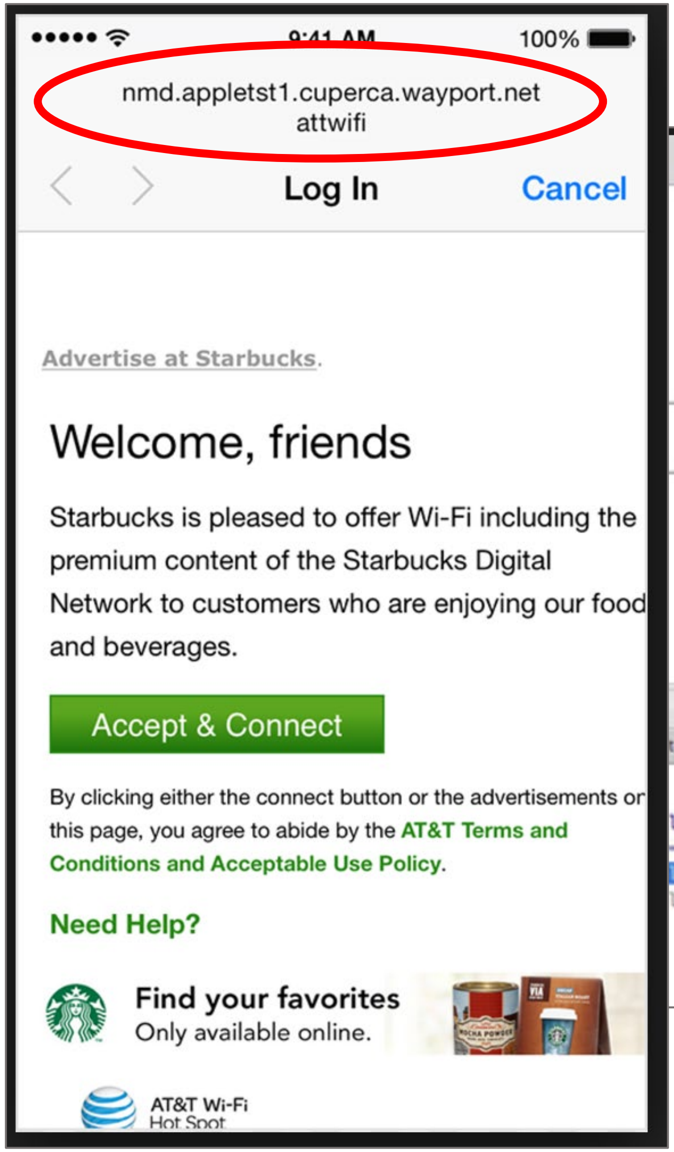
Cyber Threat: Public/Client Wifi

- Verify WiFi before connecting
  - Identify client-provided WiFi SSID is valid before browsing



StarbuckFreeWiFi

StarbucksFreeWiFi



Advertise at Starbucks.

Welcome, friends

Starbucks is pleased to offer Wi-Fi including the premium content of the Starbucks Digital Network to customers who are enjoying our food and beverages.

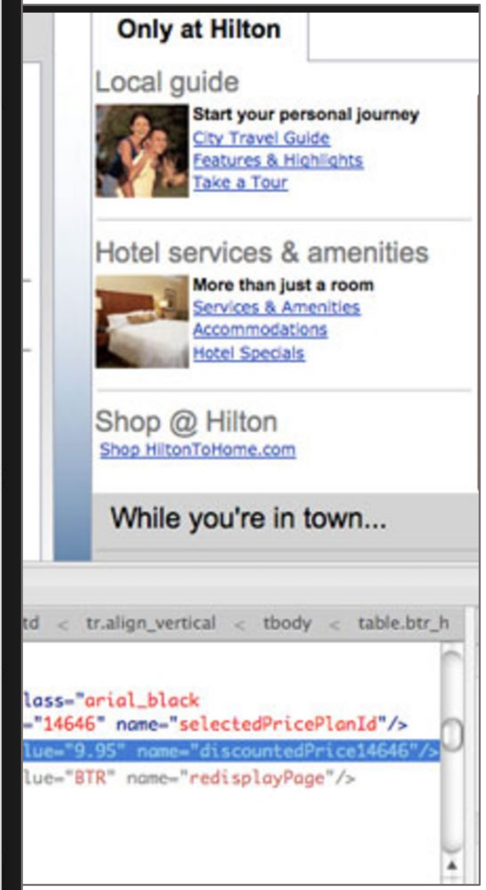
Accept & Connect

By clicking either the connect button or the advertisements on this page, you agree to abide by the AT&T Terms and Conditions and Acceptable Use Policy.

Need Help?

Find your favorites
Only available online.

AT&T Wi-Fi
Hot Spot



Only at Hilton

Local guide

Start your personal journey
City Travel Guide
Features & Highlights
Take a Tour

Hotel services & amenities

More than just a room
Services & Amenities
Accommodations
Hotel Specials

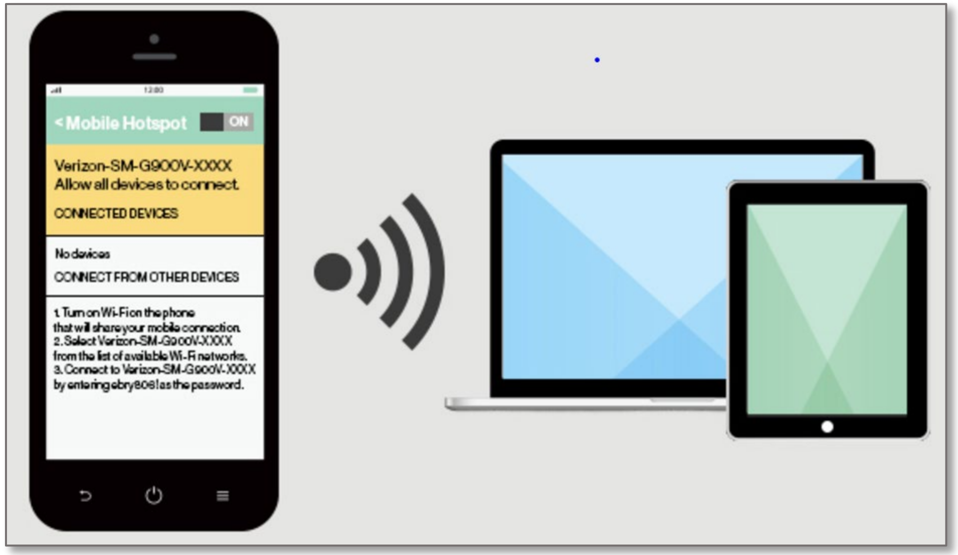
Shop @ Hilton
Shop HiltonToHome.com

While you're in town...

```
td < tr.align_vertical < tbody < table.btr_h
lass="arial_black
="14646" name="selectedPricePlanId"/>
lue="9.95" name="discountedPrice14646"/>
lue="BTR" name="redisplayPage"/>
```

Cyber Threat: Public/Client Wifi

- Verify WiFi before connecting
  - Identify client-provided WiFi SSID is valid before browsing
  - Do not recommend using public/hotel WiFi for any secure logins or browsing unless a VPN configured (i.e. Cisco AnyConnect/ NordVPN, IPVanish, ExpressVPN)
  - Solution: Utilize mobile hotspot/smartphone



Verizon-SM-G900V-XXXX
Allow all devices to connect.

CONNECTED DEVICES

No devices

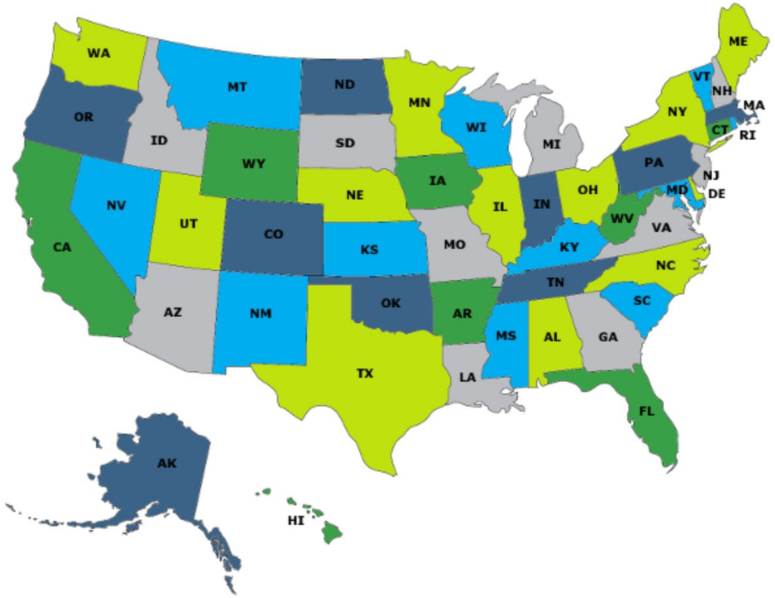
CONNECT FROM OTHER DEVICES

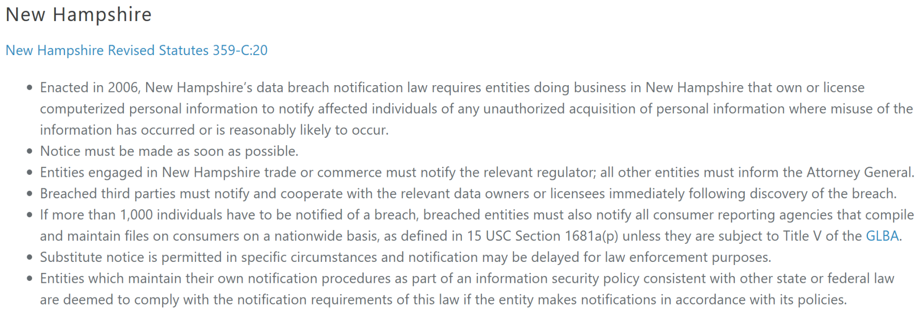
1. Turn on Wi-Fi on the phone that will share your mobile connection.
2. Select Verizon-SM-G900V-XXXX from the list of available Wi-Fi networks.
3. Connect to Verizon-SM-G900V-XXXX by entering ebry806! as the password.

Right Networks®

Advancing Cyber Threats: Reputation

- Impact of Breach on Reputation
- Legal Requirements to Notify





New Hampshire

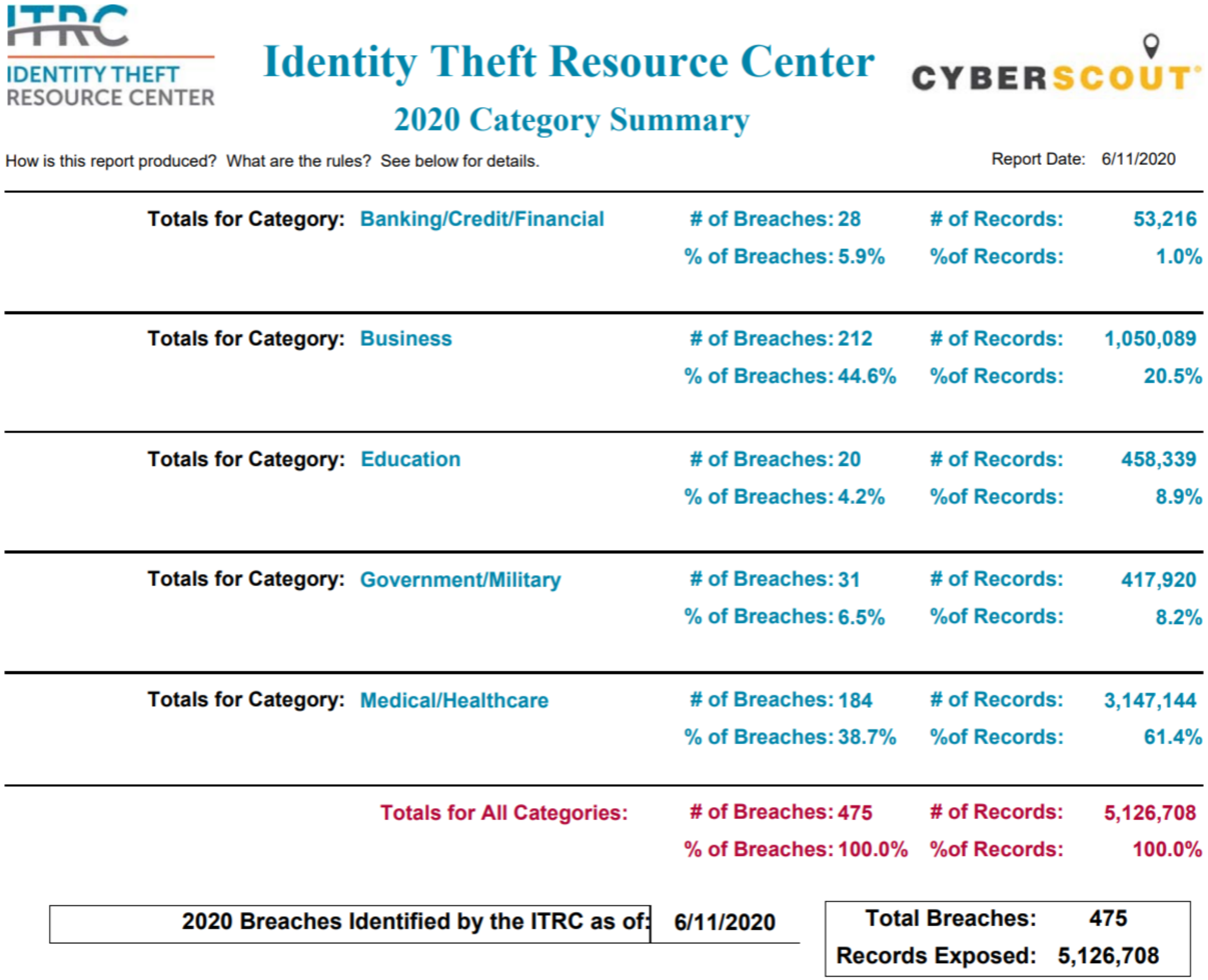
New Hampshire Revised Statutes 359-C:20

- Enacted in 2006, New Hampshire's data breach notification law requires entities doing business in New Hampshire that own or license computerized personal information to notify affected individuals of any unauthorized acquisition of personal information where misuse of the information has occurred or is reasonably likely to occur.
- Notice must be made as soon as possible.
- Entities engaged in New Hampshire trade or commerce must notify the relevant regulator; all other entities must inform the Attorney General.
- Breached third parties must notify and cooperate with the relevant data owners or licensees immediately following discovery of the breach.
- If more than 1,000 individuals have to be notified of a breach, breached entities must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC Section 1681a(p) unless they are subject to Title V of the GLBA.
- Substitute notice is permitted in specific circumstances and notification may be delayed for law enforcement purposes.
- Entities which maintain their own notification procedures as part of an information security policy consistent with other state or federal law are deemed to comply with the notification requirements of this law if the entity makes notifications in accordance with its policies.

- https://www.itgovernanceusa.com/data-breach-notification-laws

Advancing Cyber Threats: Reputation

- Impact of Breach on Reputation
- Legal Requirements to Notify
- Public Notification



ITRC IDENTITY THEFT RESOURCE CENTER

Identity Theft Resource Center

CYBERSCOUT

2020 Category Summary

How is this report produced? What are the rules? See below for details.

Report Date: 6/11/2020

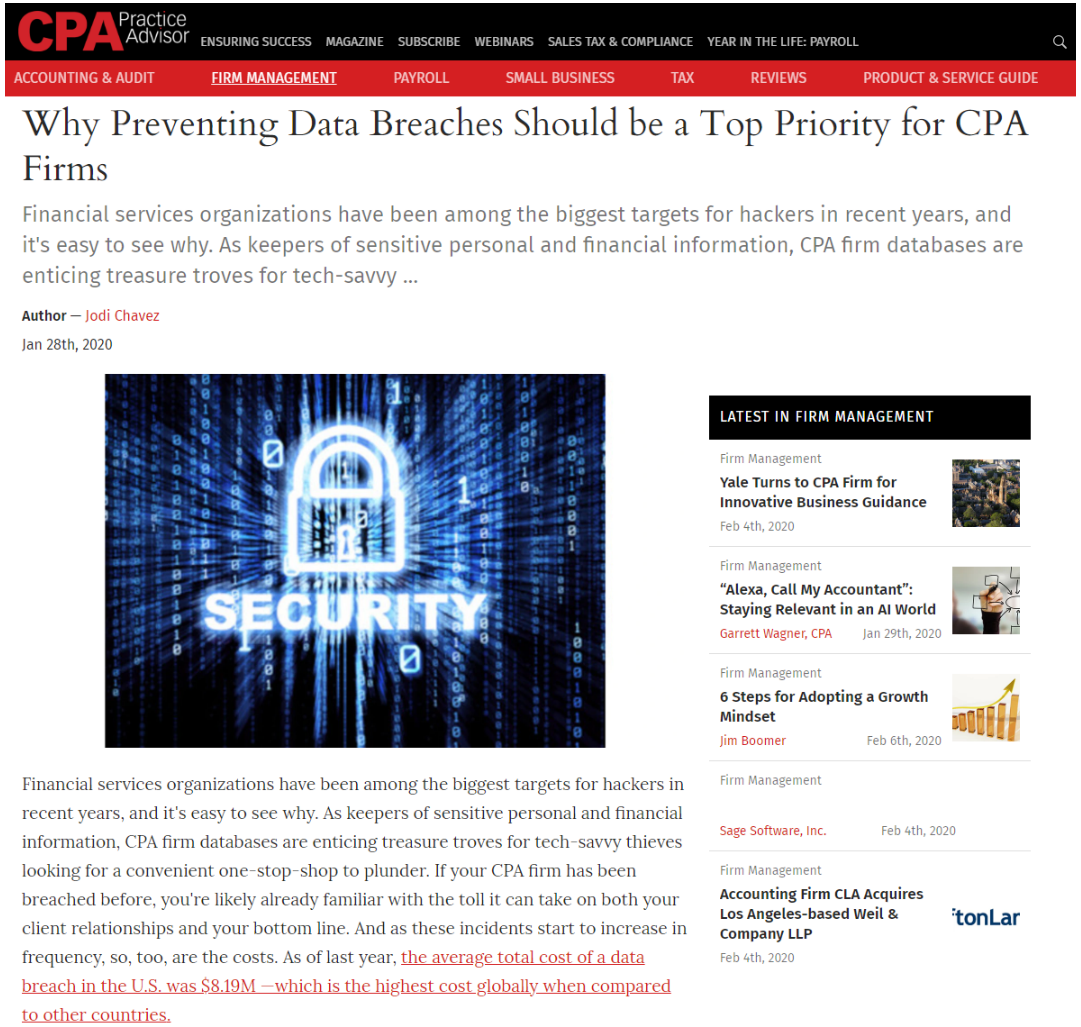
Totals for Category:	Banking/Credit/Financial	# of Breaches: 28	% of Breaches: 5.9%	# of Records: 53,216	%of Records: 1.0%
Totals for Category:	Business	# of Breaches: 212	% of Breaches: 44.6%	# of Records: 1,050,089	%of Records: 20.5%
Totals for Category:	Education	# of Breaches: 20	% of Breaches: 4.2%	# of Records: 458,339	%of Records: 8.9%
Totals for Category:	Government/Military	# of Breaches: 31	% of Breaches: 6.5%	# of Records: 417,920	%of Records: 8.2%
Totals for Category:	Medical/Healthcare	# of Breaches: 184	% of Breaches: 38.7%	# of Records: 3,147,144	%of Records: 61.4%
Totals for All Categories:		# of Breaches: 475	% of Breaches: 100.0%	# of Records: 5,126,708	%of Records: 100.0%

2020 Breaches Identified by the ITRC as of:	6/11/2020

Total Breaches:	475
Records Exposed:	5,126,708

Advancing Cyber Treats: Financial

- Finance/Business: Immediate 6% churn
- 64% would stop working with firm if PII breached
- 94% would pursue legal action
- Average breach cost-$8.19M
- IBM Ponemon $224/record



Why Preventing Data Breaches Should be a Top Priority for CPA Firms

Financial services organizations have been among the biggest targets for hackers in recent years, and it's easy to see why. As keepers of sensitive personal and financial information, CPA firm databases are enticing treasure troves for tech-savvy ...

Author — Jodi Chavez

Jan 28th, 2020

Financial services organizations have been among the biggest targets for hackers in recent years, and it's easy to see why. As keepers of sensitive personal and financial information, CPA firm databases are enticing treasure troves for tech-savvy thieves looking for a convenient one-stop-shop to plunder. If your CPA firm has been breached before, you're likely already familiar with the toll it can take on both your client relationships and your bottom line. And as these incidents start to increase in frequency, so, too, are the costs. As of last year, the average total cost of a data breach in the U.S. was $8.19M —which is the highest cost globally when compared to other countries.

LATEST IN FIRM MANAGEMENT

Firm Management
Yale Turns to CPA Firm for Innovative Business Guidance
Feb 4th, 2020

Firm Management
"Alexa, Call My Accountant": Staying Relevant in an AI World
Garrett Wagner, CPA Jan 29th, 2020

Firm Management
6 Steps for Adopting a Growth Mindset
Jim Boomer Feb 6th, 2020

Firm Management
Sage Software, Inc. Feb 4th, 2020

Firm Management
Accounting Firm CLA Acquires Los Angeles-based Weil & Company LLP
Feb 4th, 2020

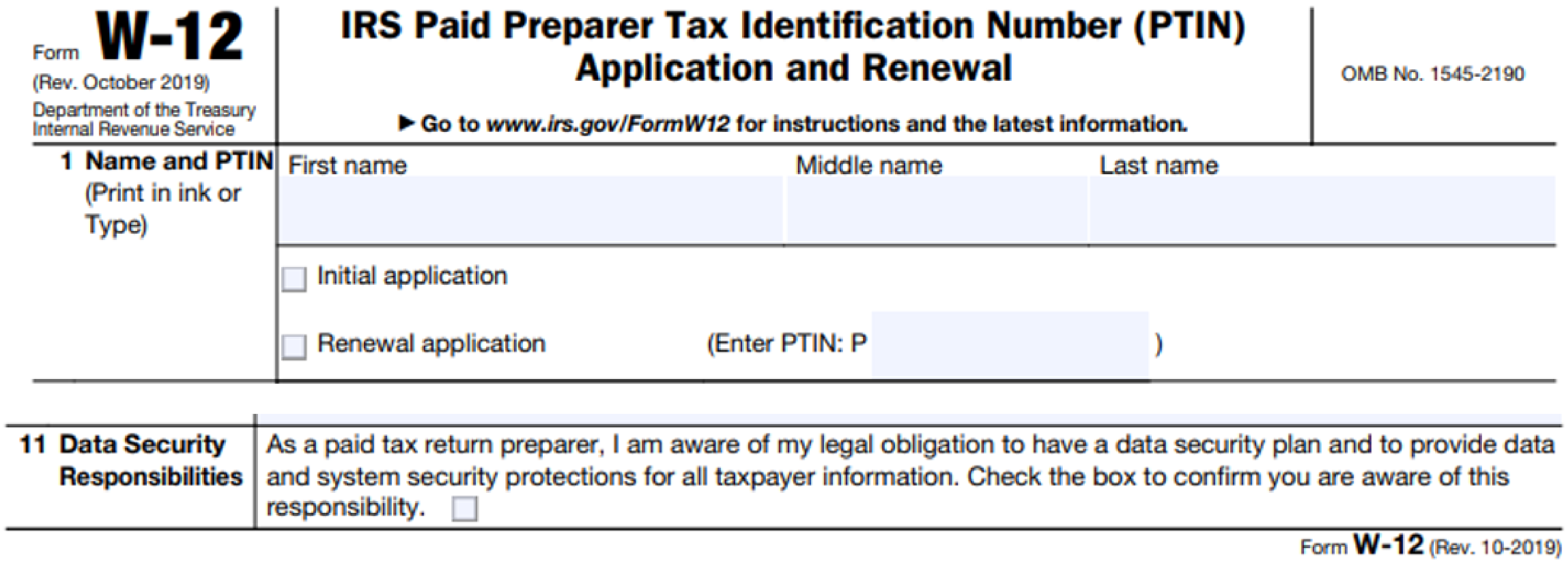
Right Networks

Cyber Security: It's the Law!

- Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley) gave Federal Trade Commission the authority to set safeguard regulations for paid tax preparers. The FTC Safeguard Rule states they must create and enact security plans to protect client data.
- Violation of the FTC Safeguards Rule is regarded as a violation of IRS Revenue Procedure 2007-40, which sets the rules for tax professionals participating as an Authorized IRS e-file Provider.
- During the 2018 filing season the IRS noted a 29% increase in the number of tax practices that reported they had been the victim of a data breach.
- IRS holds annual Security Summits to outline security requirements.

Cyber Security: It's the Law!

- 2019 PTIN Renewal



Form **W-12**
(Rev. October 2019)
Department of the Treasury
Internal Revenue Service

IRS Paid Preparer Tax Identification Number (PTIN)
Application and Renewal

▶ **Go to *www.irs.gov/FormW12* for instructions and the latest information.**

OMB No. 1545-2190

1 Name and PTIN (Print in ink or Type)

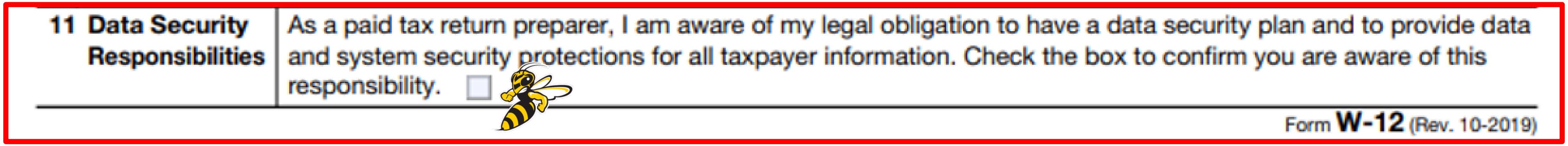
First name	Middle name	Last name

□ Initial application

□ Renewal application (Enter PTIN: P)

11 Data Security Responsibilities As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information. Check the box to confirm you are aware of this responsibility. □

Form **W-12** (Rev. 10-2019)



11 Data Security Responsibilities As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information. Check the box to confirm you are aware of this responsibility. □

Form **W-12** (Rev. 10-2019)

Cyber Security: It's the Law!

- IRS Security Summit Requirements
  - IRS Security Six:
    - Anti-virus/Malware Application
    - Firewalls
    - Multi-Factor Authentication
    - Backup Software
    - Drive Encryption
    - Virtual Private Network

Cyber Security: It’s the Law!

- IRS Security Summit Requirements
  - IRS Security Six
  - Phishing Training

Cyber Security: It’s the Law!

- IRS Security Summit Requirements
  - IRS Security Six
  - Phishing Training
  - Security Awareness Training

Cyber Security: It’s the Law!

- IRS Security Summit Requirements
  - IRS Security Six
  - Phishing Training
  - Security Awareness Training
  - Written Plan: “Appropriate to their own Circumstances”
    - Designate an employee to coordinate Security Plan development
    - Identify and assess risks to client information
    - Evaluate effectiveness of current safeguards and adjust as necessary
    - Design, implement and monitor a safeguards program
    - Select service providers than can maintain appropriate safeguards

Spot Something Phishy? (Warning Signs of a Breach)

- Increase in computer connecting to Internet when not working, browser pop-ups, new tool bars, or searches jumping to unexpected sites, mouse pointer moving, noticeable degradation
- New files/applications appearing on your computer
- Website/email notification of security/virus warning

Spot Something Phishy? (Warning Signs of a Breach)

- Notification of changed passwords or password not working
- Receiving notification of odd emails being received by peers
- Emails with your address being bounced back
- Tax returns being inexplicably filed or bank routing information changed
- Notification of ransomware

If You Suspect a breach

- Stop Work on the PC
- Disconnect the workstation from the internet immediately (unplug Ethernet cable or turn wireless connection off)
- Contact your IT/Support Team to Remediate Issue
  - Investigate data breach complaint
  - Document event sequence through incident response form
  - Preserve/review workstation/server logs as well as suspected files
  - Partner with forensic company and law enforcement if needed
  - Scan/rebuild or reassign a workstation so staff can get back to work

Cyber Security Checklist

- What Should YOU Know?

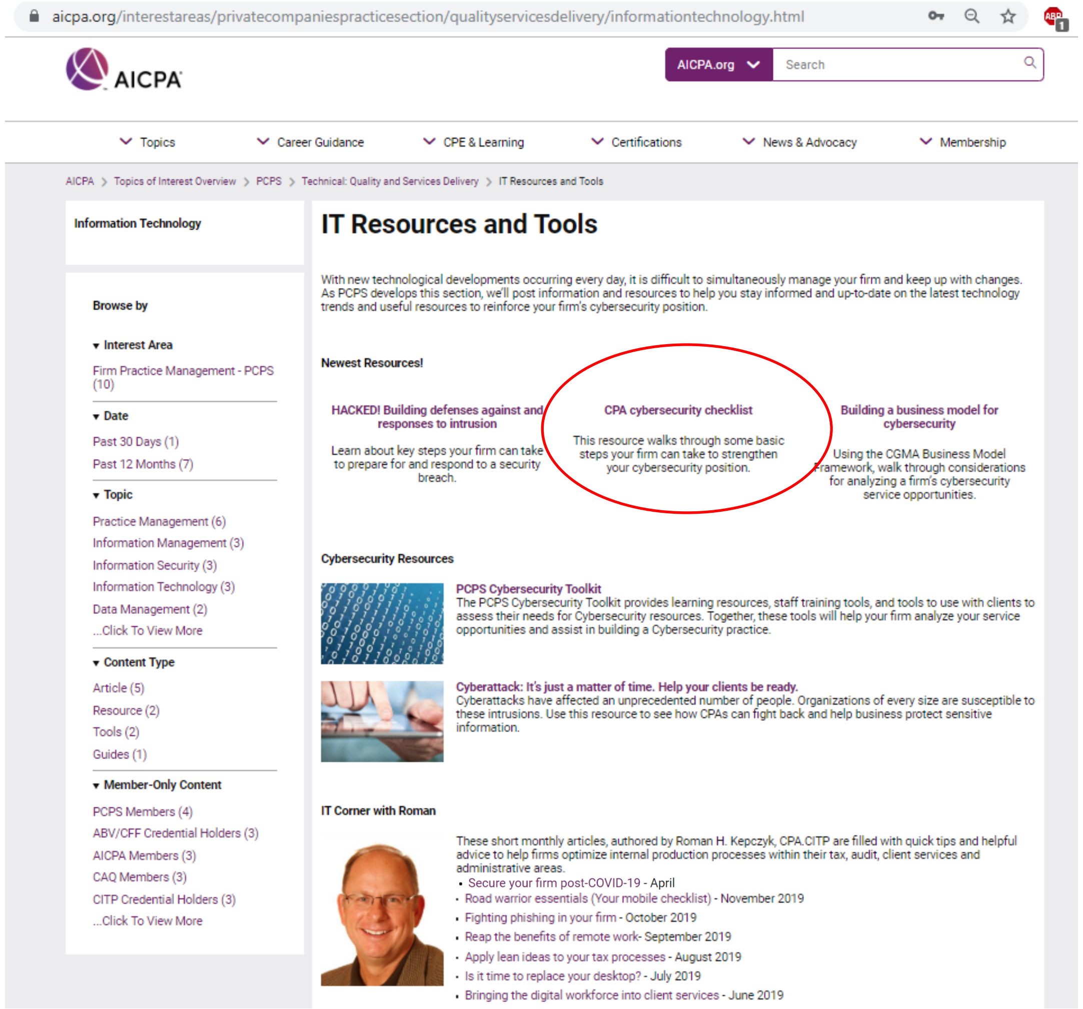
https://info.rightnetworks.com/cloud-premier/cpa-cybersecurity-checklist-2020

Right Networks

CPA Cybersecurity Checklist

2020 Edition

Checklist



aicpa.org/interestareas/privatecompaniespracticesection/qualityservicesdelivery/informationtechnology.html

AICPA
AICPA.org
Search
Topics
Career Guidance
CPE & Learning
Certifications
News & Advocacy
Membership
AICPA > Topics of Interest Overview > PCPS > Technical: Quality and Services Delivery > IT Resources and Tools

Information Technology

Browse by

▾ Interest Area

Firm Practice Management - PCPS (10)

▾ Date

Past 30 Days (1)

Past 12 Months (7)

▾ Topic

Practice Management (6)

Information Management (3)

Information Security (3)

Information Technology (3)

Data Management (2)

...Click To View More

▾ Content Type

Article (5)

Resource (2)

Tools (2)

Guides (1)

▾ Member-Only Content

PCPS Members (4)

ABV/CFF Credential Holders (3)

AICPA Members (3)

CAQ Members (3)

CITP Credential Holders (3)

...Click To View More

IT Resources and Tools

With new technological developments occurring every day, it is difficult to simultaneously manage your firm and keep up with changes. As PCPS develops this section, we'll post information and resources to help you stay informed and up-to-date on the latest technology trends and useful resources to reinforce your firm's cybersecurity position.

Newest Resources!

HACKED! Building defenses against and responses to intrusion

Learn about key steps your firm can take to prepare for and respond to a security breach.

CPA cybersecurity checklist

This resource walks through some basic steps your firm can take to strengthen your cybersecurity position.

Building a business model for cybersecurity

Using the CGMA Business Model Framework, walk through considerations for analyzing a firm's cybersecurity service opportunities.

Cybersecurity Resources

PCPS Cybersecurity Toolkit
The PCPS Cybersecurity Toolkit provides learning resources, staff training tools, and tools to use with clients to assess their needs for Cybersecurity resources. Together, these tools will help your firm analyze your service opportunities and assist in building a Cybersecurity practice.

Cyberattack: It's just a matter of time. Help your clients be ready.
Cyberattacks have affected an unprecedented number of people. Organizations of every size are susceptible to these intrusions. Use this resource to see how CPAs can fight back and help business protect sensitive information.

IT Corner with Roman

These short monthly articles, authored by Roman H. Kepczyk, CPA.CITP are filled with quick tips and helpful advice to help firms optimize internal production processes within their tax, audit, client services and administrative areas.

- Secure your firm post-COVID-19 - April
- Road warrior essentials (Your mobile checklist) - November 2019
- Fighting phishing in your firm - October 2019
- Reap the benefits of remote work- September 2019
- Apply lean ideas to your tax processes - August 2019
- Is it time to replace your desktop? - July 2019
- Bringing the digital workforce into client services - June 2019

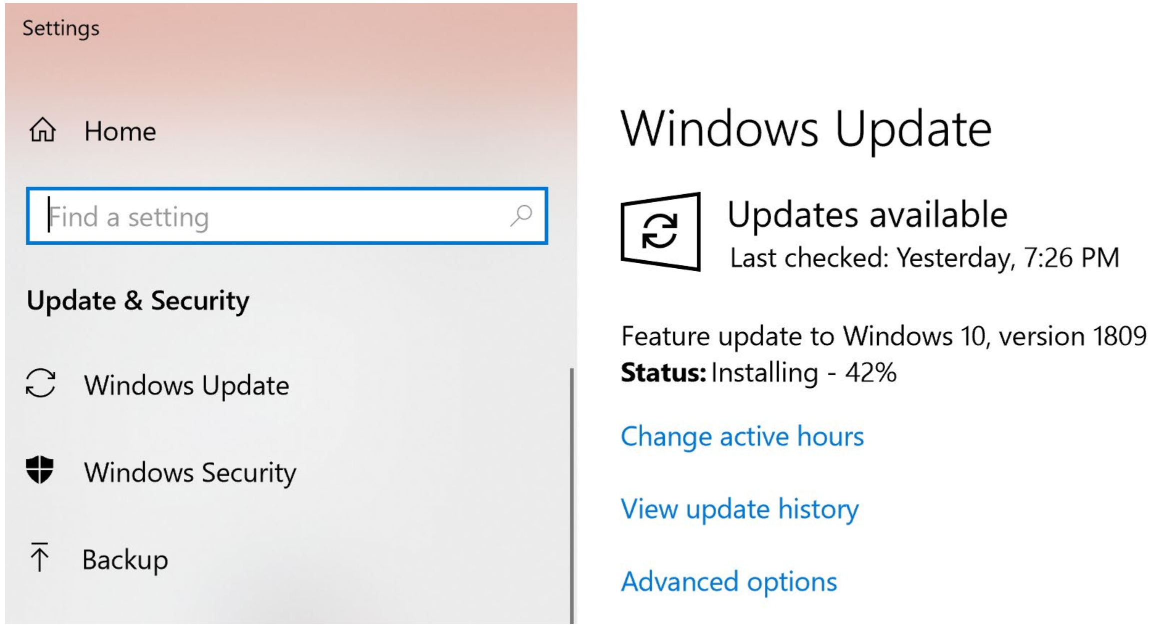
Secure Your Firm Post-COVID-19

- When working remotely: Secure Your Computer

  - Authorized Equipment
    - Firm designated computers, tablets, smartphones
    - Confidential (not shared/utilized by other family members)

Secure Your Firm Post-COVID-19

- When working remotely: Secure Your Computer
  - Authorized Equipment
  - Automatic Updates
    - Windows operating system



Windows Update

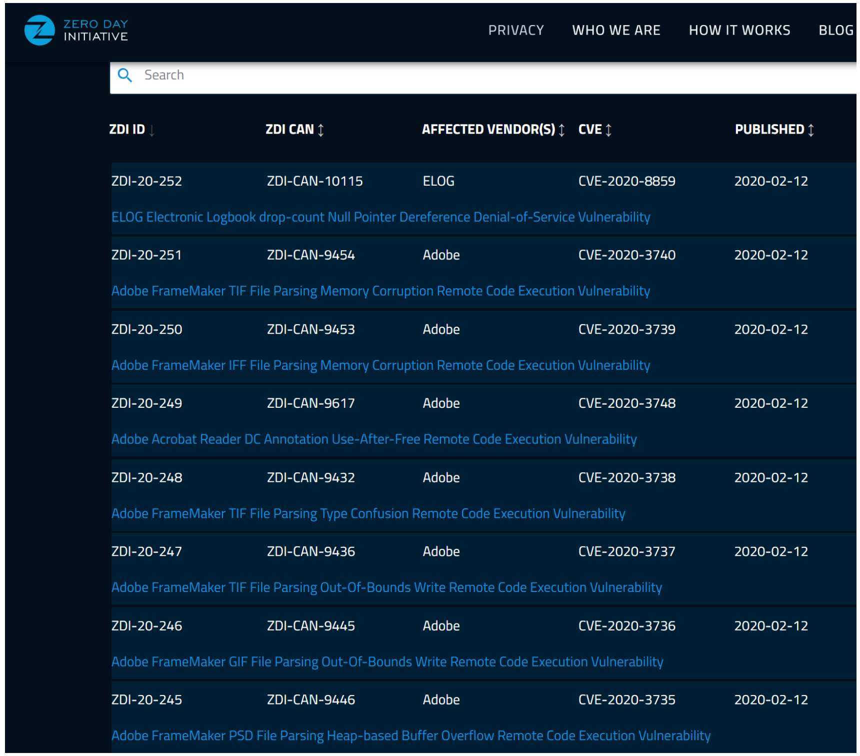
Updates available
Last checked: Yesterday, 7:26 PM

Feature update to Windows 10, version 1809
Status: Installing - 42%

Change active hours

View update history

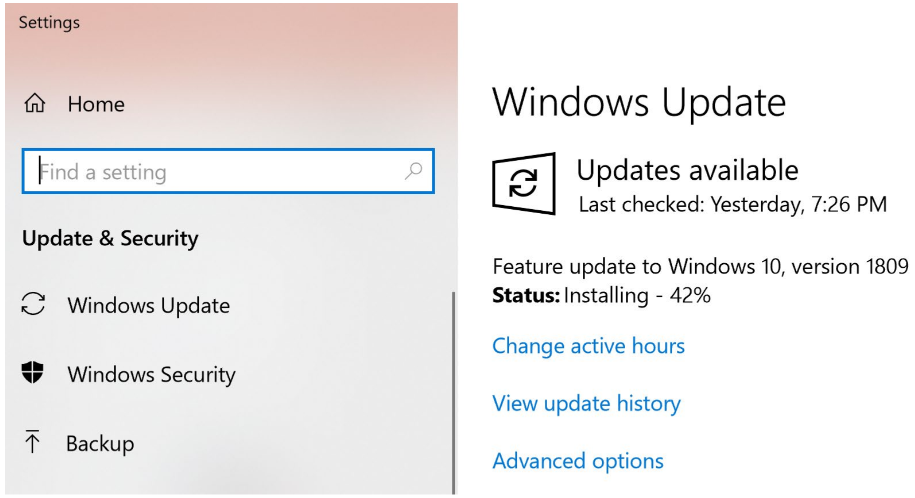
Advanced options



ZDI ID ↓	ZDI CAN ↕	AFFECTED VENDOR(S) ↕	CVE ↕	PUBLISHED ↕
ZDI-20-252	ZDI-CAN-10115	ELOG	CVE-2020-8859	2020-02-12
ELOG Electronic Logbook drop-count Null Pointer Dereference Denial-of-Service Vulnerability				
ZDI-20-251	ZDI-CAN-9454	Adobe	CVE-2020-3740	2020-02-12
Adobe FrameMaker TIF File Parsing Memory Corruption Remote Code Execution Vulnerability				
ZDI-20-250	ZDI-CAN-9453	Adobe	CVE-2020-3739	2020-02-12
Adobe FrameMaker IFF File Parsing Memory Corruption Remote Code Execution Vulnerability				
ZDI-20-249	ZDI-CAN-9617	Adobe	CVE-2020-3748	2020-02-12
Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability				
ZDI-20-248	ZDI-CAN-9432	Adobe	CVE-2020-3738	2020-02-12
Adobe FrameMaker TIF File Parsing Type Confusion Remote Code Execution Vulnerability				
ZDI-20-247	ZDI-CAN-9436	Adobe	CVE-2020-3737	2020-02-12
Adobe FrameMaker TIF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability				
ZDI-20-246	ZDI-CAN-9445	Adobe	CVE-2020-3736	2020-02-12
Adobe FrameMaker GIF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability				
ZDI-20-245	ZDI-CAN-9446	Adobe	CVE-2020-3735	2020-02-12
Adobe FrameMaker PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability				

Secure Your Firm Post-COVID-19

- When working remotely: Secure Your Computer
  - Authorized Equipment
  - Automatic Updates
    - Windows operating system (No Windows 7!)



Settings

Home

Find a setting

Update & Security

Windows Update

Windows Security

Backup

Windows Update

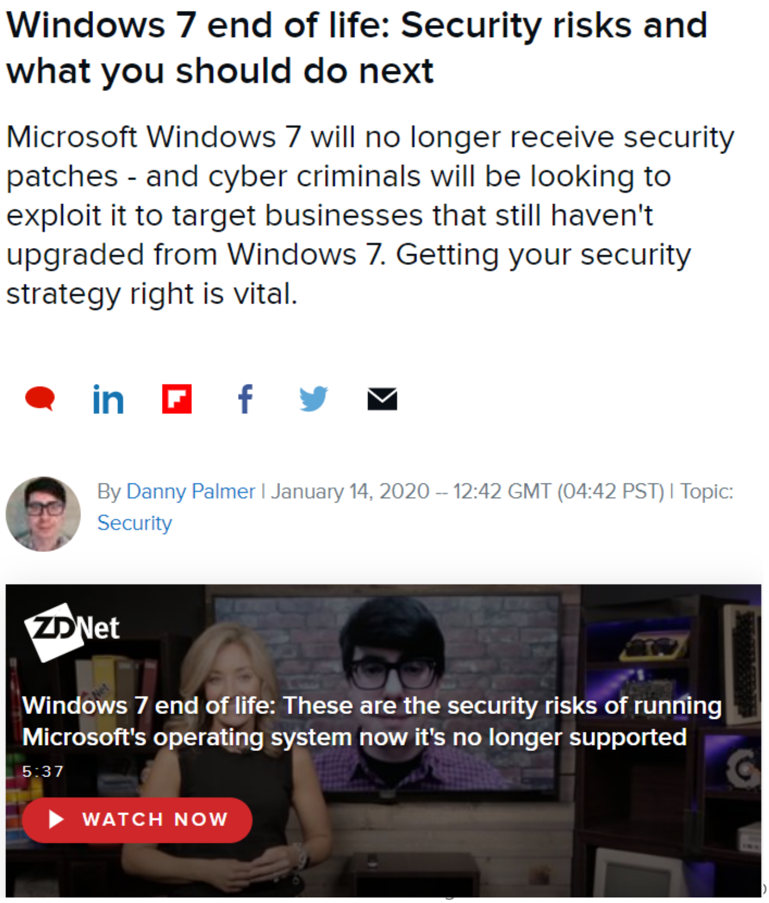
Updates available
Last checked: Yesterday, 7:26 PM

Feature update to Windows 10, version 1809
Status: Installing - 42%

Change active hours

View update history

Advanced options



Windows 7 end of life: Security risks and what you should do next

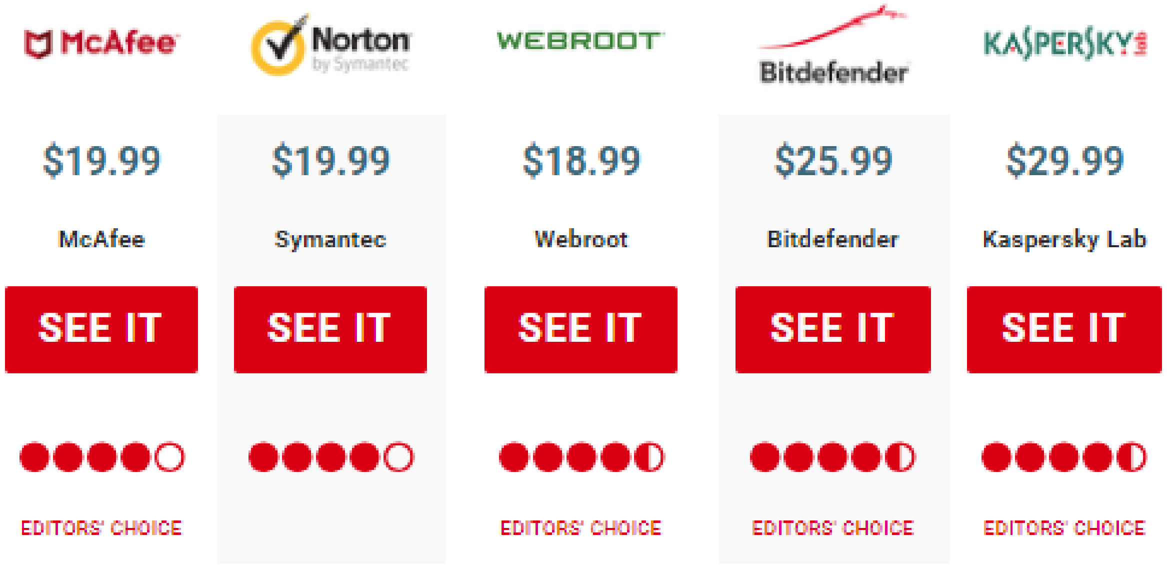
Microsoft Windows 7 will no longer receive security patches - and cyber criminals will be looking to exploit it to target businesses that still haven't upgraded from Windows 7. Getting your security strategy right is vital.

By Danny Palmer | January 14, 2020 -- 12:42 GMT (04:42 PST) | Topic: Security

ZDNet
Windows 7 end of life: These are the security risks of running Microsoft's operating system now it's no longer supported
5:37
WATCH NOW

Secure Your Firm Post-COVID-19

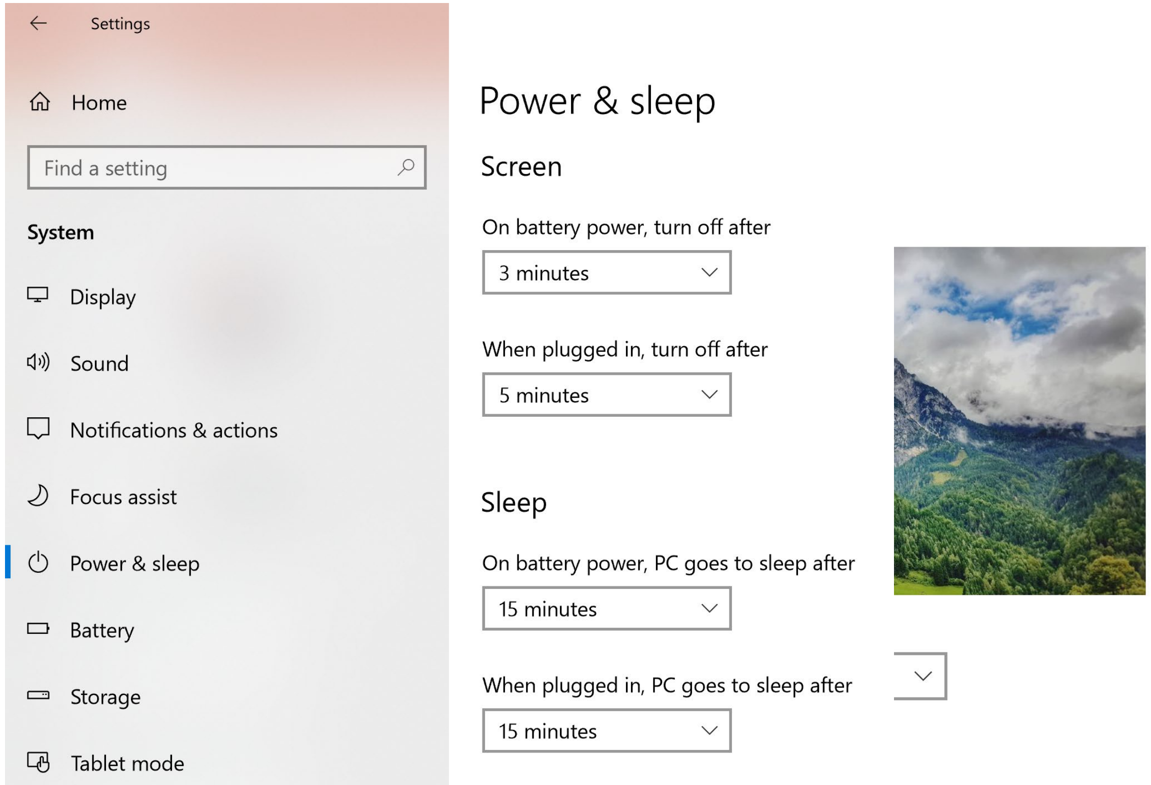
- When working remotely: Secure Your Computer
  - Authorized Equipment
  - Automatic Updates
    - Windows operating system (No Windows 7!)
    - Anti-virus/malware
    - Only load/disable with *verified* IT support person



McAfee	Norton by Symantec	WEBROOT	Bitdefender	KASPERSKY lab
$19.99	$19.99	$18.99	$25.99	$29.99
McAfee	Symantec	Webroot	Bitdefender	Kaspersky Lab
SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
●●●●○	●●●●○	●●●●◐	●●●●◐	●●●●◐
EDITORS' CHOICE		EDITORS' CHOICE	EDITORS' CHOICE	EDITORS' CHOICE

Secure Your Firm Post-COVID-19

- When working remotely: Secure Your Computer
  - Authorized Equipment
  - Automatic Updates
  - Automatic Screen Locking
    - <5 minutes
    - Sleep when walking away/guests
    - Reboot daily for system cleanup/updates



Power & sleep

Screen

On battery power, turn off after: 3 minutes

When plugged in, turn off after: 5 minutes

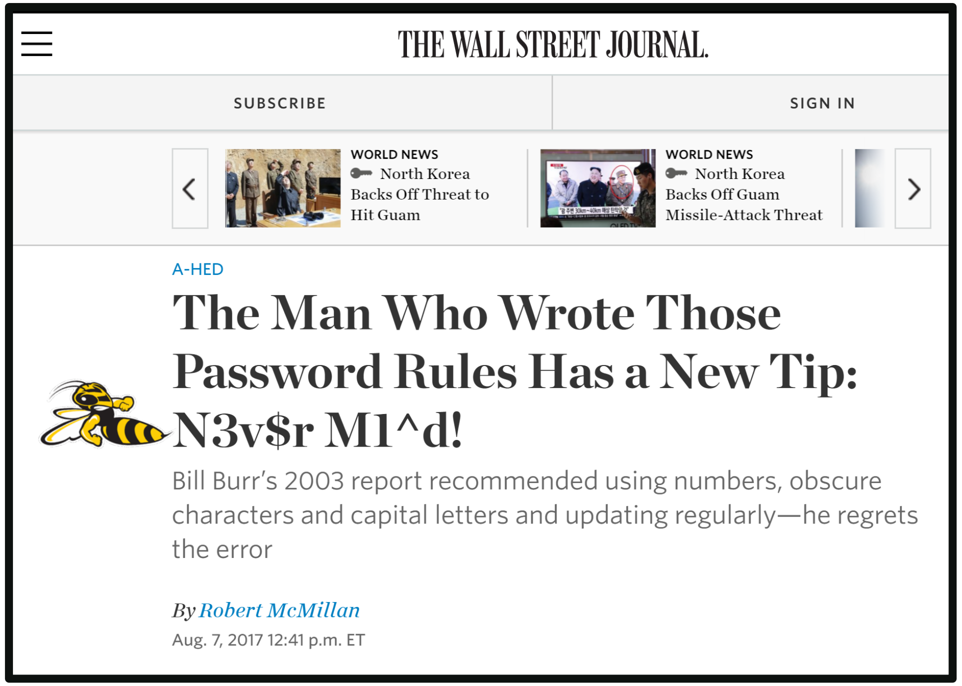
Sleep

On battery power, PC goes to sleep after: 15 minutes

When plugged in, PC goes to sleep after: 15 minutes

Secure Your Firm Post-COVID-19

- When working remotely: **Secure Connections**
  - Identity Verification
    - Passwords?
      - Hardened rules (8 character, upper/lower, number, special)
      - Change 90 days



WORLD NEWS
North Korea Backs Off Threat to Hit Guam

WORLD NEWS
North Korea Backs Off Guam Missile-Attack Threat

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

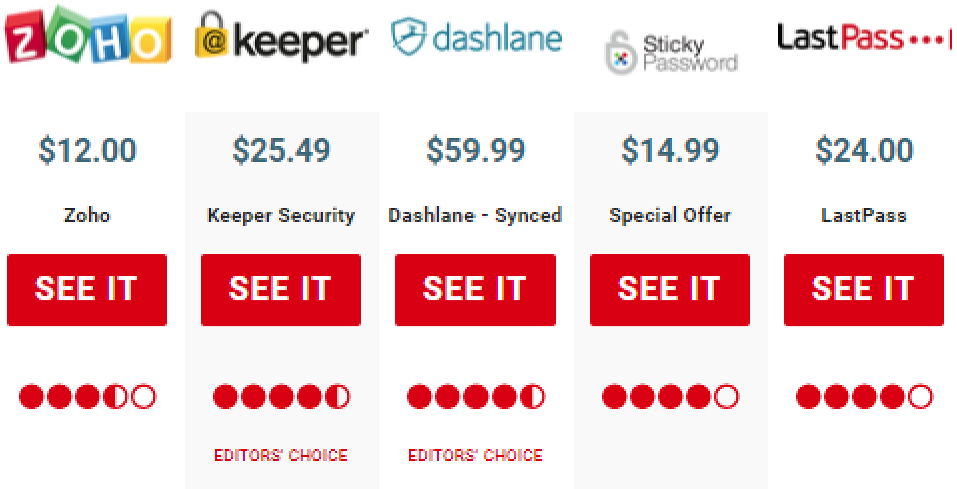
Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By Robert McMillan

Aug. 7, 2017 12:41 p.m. ET

Secure Your Firm Post-COVID-19

- When working remotely: Secure Connections
  - Identity Verification
    - Utilize Passphrases*
      - Disallow numerical derivatives~
      - Terminate with employee
      - Unique to each site
    - Password Managers



$12.00	$25.49	$59.99	$14.99	$24.00
Zoho	Keeper Security	Dashlane - Synced	Special Offer	LastPass
SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
●●●◐○	●●●●◐	●●●●◐	●●●●○	●●●●○
	EDITORS' CHOICE	EDITORS' CHOICE		

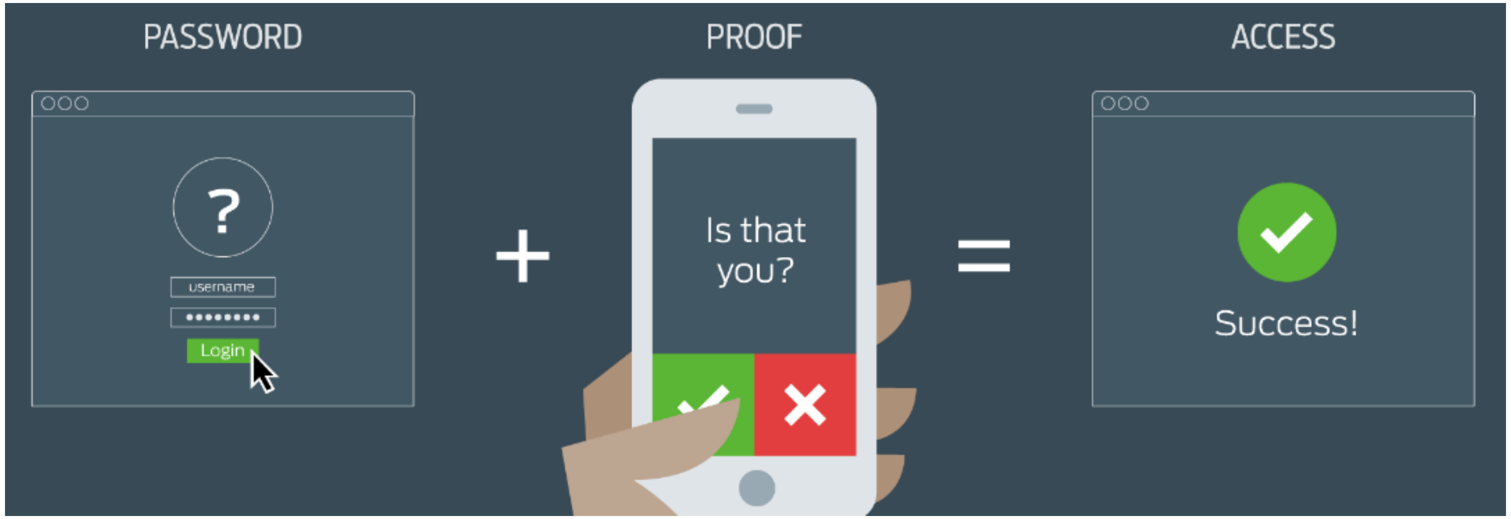
*Random words-at least 12 characters

Data Blue 1040 Sunday
NotHackedOnMyWatch
4Sc0re&7YEARSag0

~PhX!cc01, PhX!cc02, PhX!cc03…

Secure Your Firm Post-COVID-19

- When working remotely: Secure Connections
  - Identity Verification
    - Utilize Passphrases
    - Password Managers
    - Multi-factor authentication (Duo/Okta, USB, Biometric)



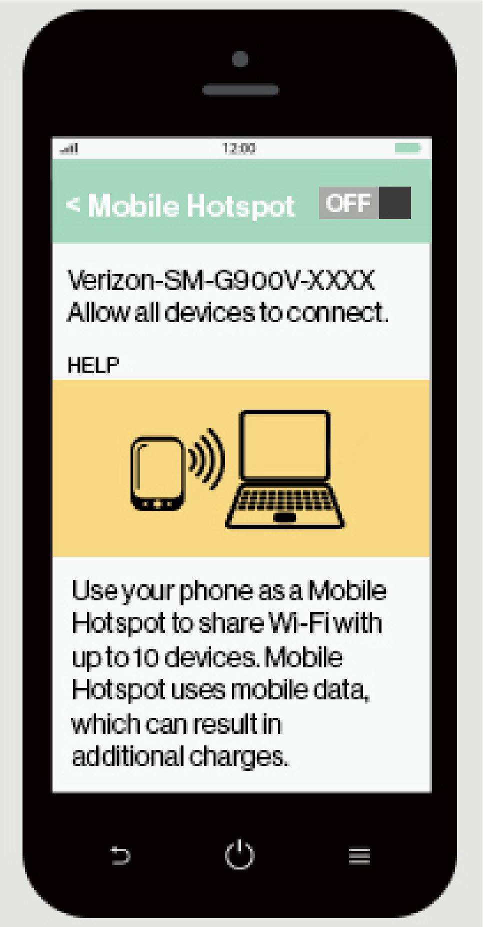
Secure Your Firm Post-COVID-19

- When working remotely: Secure Connections
  - Identity Verification
  - Home Internet
    - Direct ethernet connection
    - Secure your WiFi (update firmware/change password)
    - Segment work vs. guest/IoT* access
    - Utilize VPN (virtual private network)

*IoT=Internet of Things: Ring Doorbells, Smart TVs, Baby Monitors, Garage Doors, Security Systems-connected to **home** network.

Secure Your Firm Post-COVID-19

- When working remotely: Secure Connections
  - Identity Verification
  - Home Internet
    - Direct ethernet connection
    - Secure your WiFi (update firmware/change password)
    - Segment work vs. guest/IoT* access
    - Utilize VPN (virtual private network)
    - Mobile hotspot access



Verizon-SM-G900V-XXXX
Allow all devices to connect.

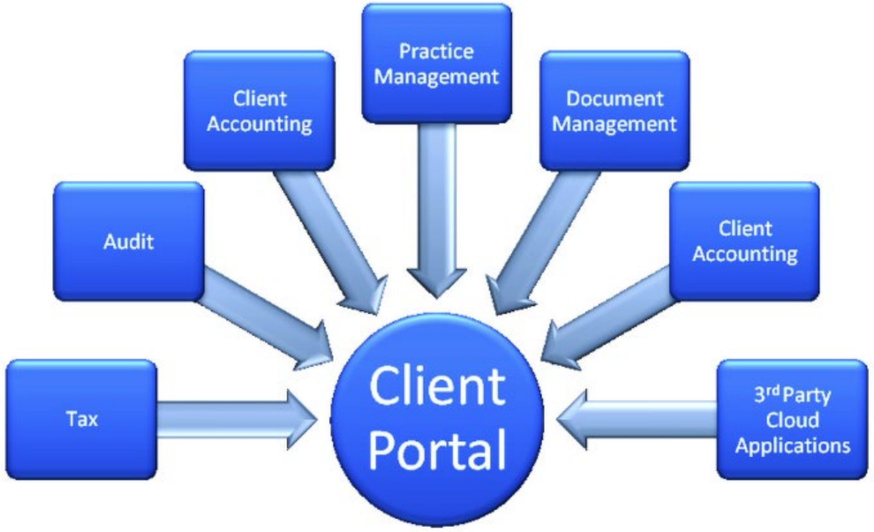
HELP

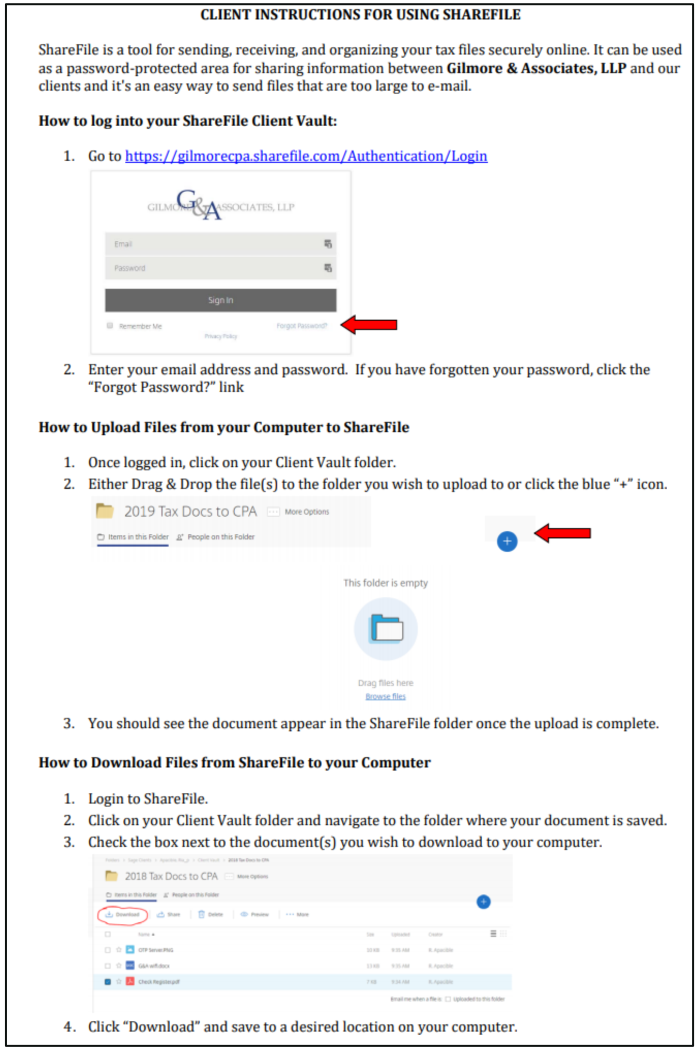
Use your phone as a Mobile Hotspot to share Wi-Fi with up to 10 devices. Mobile Hotspot uses mobile data, which can result in additional charges.

*IoT=Internet of Things: Ring Doorbells, Smart TVs, Baby Monitors, Garage Doors, Security Systems-connected to **home** network.

Secure Your Firm Post-COVID-19

- When working remotely: Secure Connections
  - Identity Verification
  - Home Internet
  - Encrypted File Transfer With Clients
    - Mandate portal/secure email
    - Disallow USB flash drives (7% of Ransomware Attack: Sophos)
    - Personnel should mentor clients/firm should make it easy





CLIENT INSTRUCTIONS FOR USING SHAREFILE

ShareFile is a tool for sending, receiving, and organizing your tax files securely online. It can be used as a password-protected area for sharing information between **Gilmore & Associates, LLP** and our clients and it's an easy way to send files that are too large to e-mail.

How to log into your ShareFile Client Vault:

1. Go to https://gilmorecpa.sharefile.com/Authentication/Login

2. Enter your email address and password. If you have forgotten your password, click the "Forgot Password?" link

How to Upload Files from your Computer to ShareFile

1. Once logged in, click on your Client Vault folder.
2. Either Drag & Drop the file(s) to the folder you wish to upload to or click the blue "+" icon.

3. You should see the document appear in the ShareFile folder once the upload is complete.

How to Download Files from ShareFile to your Computer

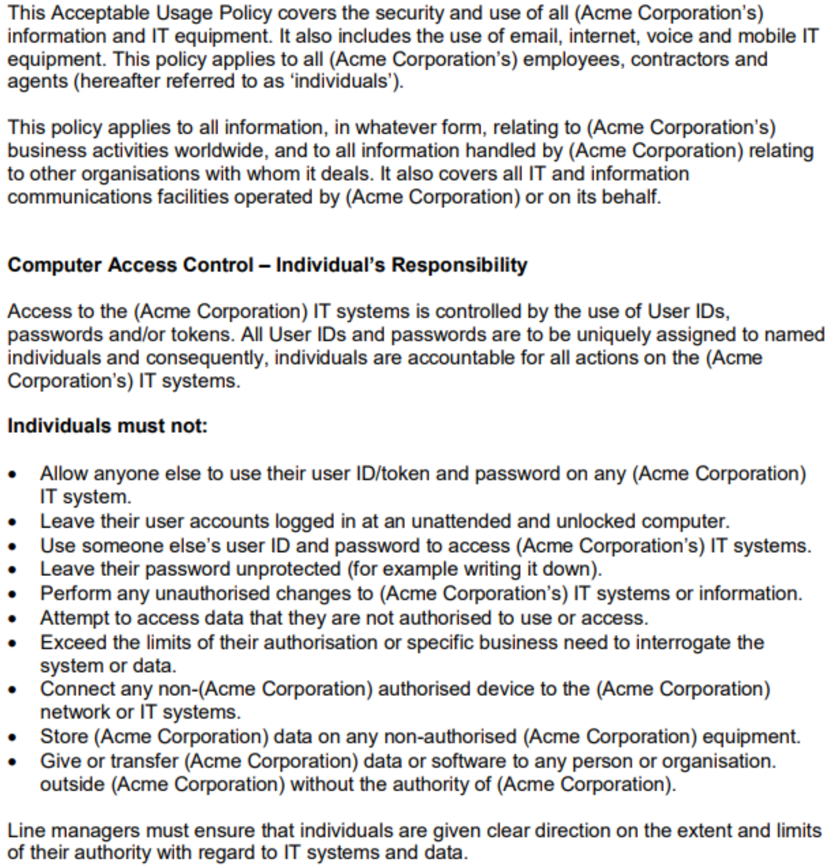
1. Login to ShareFile.
2. Click on your Client Vault folder and navigate to the folder where your document is saved.
3. Check the box next to the document(s) you wish to download to your computer.

4. Click "Download" and save to a desired location on your computer.

Right Networks®

Secure Your Firm Post-COVID-19

- Minimize Human Error
    - IT Policies
        - Update annually with human resources/external IT
            - IT Assets
            - Access Control
            - Password/MFA
            - Remote Access
            - Electronic Communication
            - Acceptable Use
            - Antivirus
            - Backup
            - Information Classification
            - Physical Security
            - Outsourcing
            - Client Confidentiality
        - Impact of new technologies/security threats (BYOD/Mobile Malware/Remote Flextime/Portals/COVID)



This Acceptable Usage Policy covers the security and use of all (Acme Corporation's) information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all (Acme Corporation's) employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to (Acme Corporation's) business activities worldwide, and to all information handled by (Acme Corporation) relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by (Acme Corporation) or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the (Acme Corporation) IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the (Acme Corporation's) IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any (Acme Corporation) IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access (Acme Corporation's) IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to (Acme Corporation's) IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-(Acme Corporation) authorised device to the (Acme Corporation) network or IT systems.
- Store (Acme Corporation) data on any non-authorised (Acme Corporation) equipment.
- Give or transfer (Acme Corporation) data or software to any person or organisation. outside (Acme Corporation) without the authority of (Acme Corporation).

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Secure Your Firm Post-COVID-19

- Minimize Human Error
  - IT Policies
  - Security Education
    - Latest threats (phishing/ransomware)
    - IRS security six requirements
      - Antivirus/malware
      - Firewalls
      - Multi-factor authentication
      - Backup software
      - Drive encryption
      - Virtual private network

KnowBe4 Human error. Conquered.

PHISHME

wombat security technologies

Stay Safe Online During Tax Time 2019: Prot against fraudster tricks with these "Take Action Tips"

StaySafeOnline
Powered by: National Cyber Security Alliance

CyberSecure My Business™

CyberSecure My Business™ is a national program helping small and medium-sized businesses (SMBs) learn to be safer and more secure online.

CyberSecure My Business™

Be a Part of Something Big

Secure Your Firm Post-COVID-19

- Minimize Human Error
  - IT Policies
  - Security Education
    - Latest threats (phishing/ransomware)
    - IRS security six requirements
    - How to respond if a breach is suspected

If You Suspect a breach

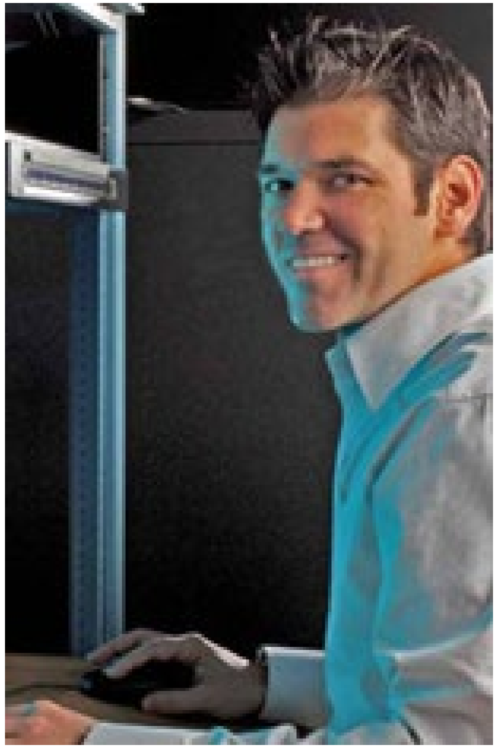
- Stop Work on the PC
- Disconnect the workstation from the internet immediately (unplug Ethernet cable or turn wireless connection off)
- Contact your IT/Support Team to Remediate Issue
  - Investigate data breach complaint
  - Document event sequence through incident response form
  - Preserve/review workstation/server logs as well as suspected files
  - Partner with forensic company and law enforcement if needed
  - Scan/Rebuild or reassign a workstation so staff can get back to work

Secure Your Firm Post-COVID-19

- Minimize Human Error
  - IT Policies
  - Security Education
  - Screen Potential Hires/Contractors
    - Background checks
    - Chaperone unrecognized personnel

Secure Your Firm Post-COVID-19

- Firm IT Support Security Considerations
  - Independent Security Review
    - Is your firm providing Security/SOC compliance services?
    - How much security training do internal IT members have?
    - How much time is allocated for internal IT security maintenance?



Secure Your Firm Post-COVID-19

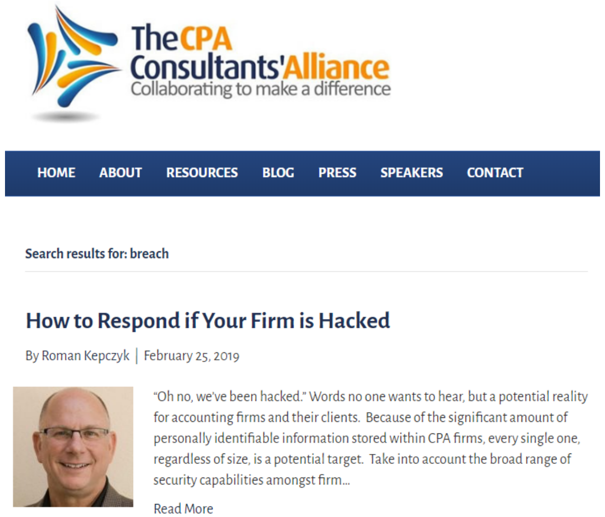
- Firm IT Support Security Considerations
  - Independent Security Review
  - Verified Backups
    - Hourly “shadow” copies
    - Disk to encrypted disk to offsite
    - Daily offsite with recovery scenario
    - Tested restore and recovery
    - Endgame: transition to cloud services

Secure Your Firm Post-COVID-19

- Firm IT Support Security Considerations
  - Independent Security Review
  - Verified Backups
  - Minimize Access Privileges
    - “Required for work”
    - Avoid “Administrator” default

Secure Your Firm Post-COVID-19

- Firm IT Support Security Considerations
  - Independent Security Review
  - Verified Backups
  - Minimize Access Privileges
  - **Breach Response Plan**
    - Identify team (Single lead/communicator, IT, Forensic, Legal, Insurance)
      - Respond timely
      - Be transparent
      - Control the message
      - Deliver concurrently
    - Explain remediation
    - Practice incident response (tabletop)


The CPA Consultants' Alliance
Collaborating to make a difference
HOME
ABOUT
RESOURCES
BLOG
PRESS
SPEAKERS
CONTACT

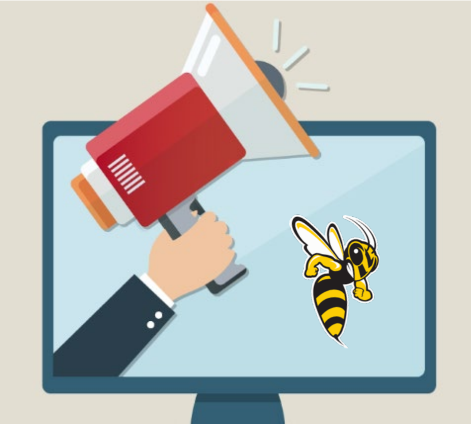
Search results for: breach

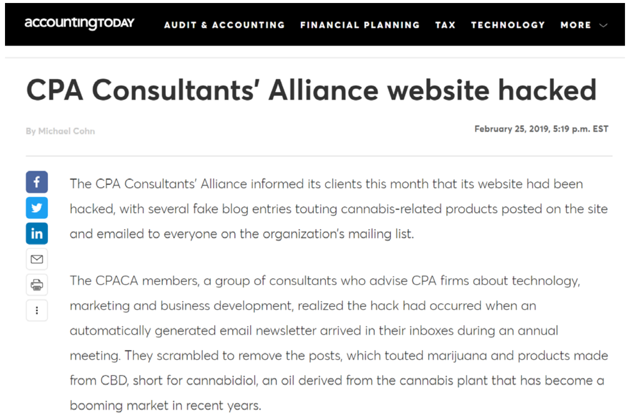
How to Respond if Your Firm is Hacked

By Roman Kepczyk | February 25, 2019

"Oh no, we've been hacked." Words no one wants to hear, but a potential reality for accounting firms and their clients. Because of the significant amount of personally identifiable information stored within CPA firms, every single one, regardless of size, is a potential target. Take into account the broad range of security capabilities amongst firm…

Read More





CPA Consultants' Alliance website hacked

By Michael Cohn

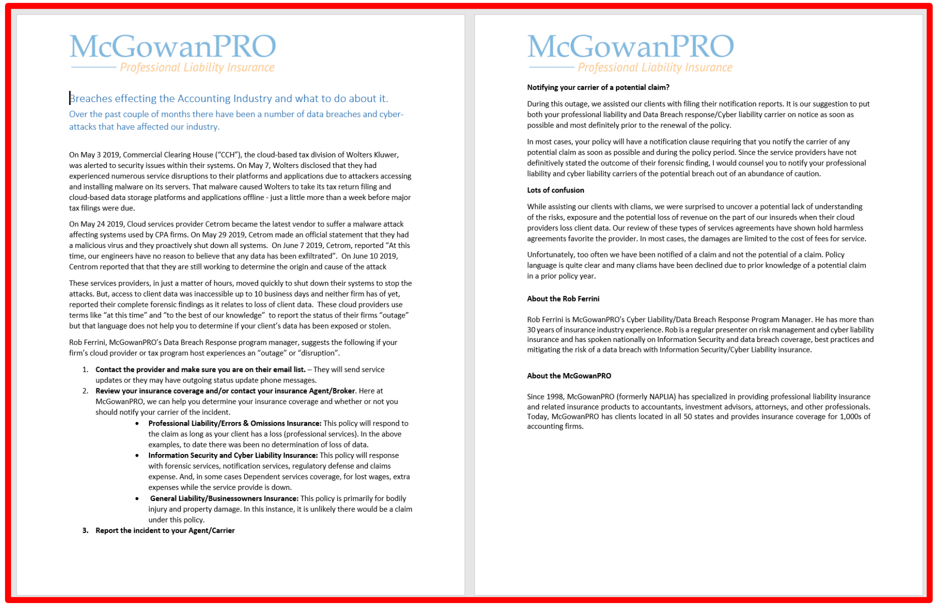
February 25, 2019, 5:19 p.m. EST

The CPA Consultants' Alliance informed its clients this month that its website had been hacked, with several fake blog entries touting cannabis-related products posted on the site and emailed to everyone on the organization's mailing list.

The CPACA members, a group of consultants who advise CPA firms about technology, marketing and business development, realized the hack had occurred when an automatically generated email newsletter arrived in their inboxes during an annual meeting. They scrambled to remove the posts, which touted marijuana and products made from CBD, short for cannabidiol, an oil derived from the cannabis plant that has become a booming market in recent years.

Secure Your Firm Post-COVID-19

- Firm IT Support Security Considerations
  - Independent Security Review
  - Verified Backups
  - Minimize Access Privileges
  - Breach Response Plan
  - Cybersecurity Insurance (entrusted with PII*)
    - First and third-party coverage
      - 84% have cyber insurance, only 64% cover ransomware
    - Re-evaluate/verify
    - Claim notification on outage



McGowanPRO
Professional Liability Insurance

Breaches effecting the Accounting Industry and what to do about it.

Over the past couple of months there have been a number of data breaches and cyber-attacks that have affected our industry.

On May 3 2019, Commercial Clearing House ("CCH"), the cloud-based tax division of Wolters Kluwer, was alerted to security issues within their systems. On May 7, Wolters disclosed that they had experienced numerous service disruptions to their platforms and applications due to attackers accessing and installing malware on its servers. That malware caused Wolters to take its tax return filing and cloud-based data storage platforms and applications offline - just a little more than a week before major tax filings were due.

On May 24 2019, Cloud services provider Cetrom became the latest vendor to suffer a malware attack affecting systems used by CPA firms. On May 29 2019, Cetrom made an official statement that they had a malicious virus and they proactively shut down all systems. On June 7 2019, Cetrom, reported "At this time, our engineers have no reason to believe that any data has been exfiltrated". On June 10 2019, Centrom reported that that they are still working to determine the origin and cause of the attack

These services providers, in just a matter of hours, moved quickly to shut down their systems to stop the attacks. But, access to client data was inaccessible up to 10 business days and neither firm has of yet, reported their complete forensic findings as it relates to loss of client data. These cloud providers use terms like "at this time" and "to the best of our knowledge" to report the status of their firms "outage" but that language does not help you to determine if your client's data has been exposed or stolen.

Rob Ferrini, McGowanPRO's Data Breach Response program manager, suggests the following if your firm's cloud provider or tax program host experiences an "outage" or "disruption".

1. **Contact the provider and make sure you are on their email list.** – They will send service updates or they may have outgoing status update phone messages.
2. **Review your insurance coverage and/or contact your insurance Agent/Broker**. Here at McGowanPRO, we can help you determine your insurance coverage and whether or not you should notify your carrier of the incident.
   - **Professional Liability/Errors & Omissions Insurance:** This policy will respond to the claim as long as your client has a loss (professional services). In the above examples, to date there was been no determination of loss of data.
   - **Information Security and Cyber Liability Insurance:** This policy will response with forensic services, notification services, regulatory defense and claims expense. And, in some cases Dependent services coverage, for lost wages, extra expenses while the service provide is down.
   - **General Liability/Businessowners Insurance:** This policy is primarily for bodily injury and property damage. In this instance, it is unlikely there would be a claim under this policy.
3. **Report the incident to your Agent/Carrier**

McGowanPRO
Professional Liability Insurance

Notifying your carrier of a potential claim?

During this outage, we assisted our clients with filing their notification reports. It is our suggestion to put both your professional liability and Data Breach response/Cyber liability carrier on notice as soon as possible and most definitely prior to the renewal of the policy.

In most cases, your policy will have a notification clause requiring that you notify the carrier of any potential claim as soon as possible and during the policy period. Since the service providers have not definitively stated the outcome of their forensic finding, I would counsel you to notify your professional liability and cyber liability carriers of the potential breach out of an abundance of caution.

Lots of confusion

While assisting our clients with cliams, we were surprised to uncover a potential lack of understanding of the risks, exposure and the potential loss of revenue on the part of our insureds when their cloud providers loss client data. Our review of these types of services agreements have shown hold harmless agreements favorite the provider. In most cases, the damages are limited to the cost of fees for service.

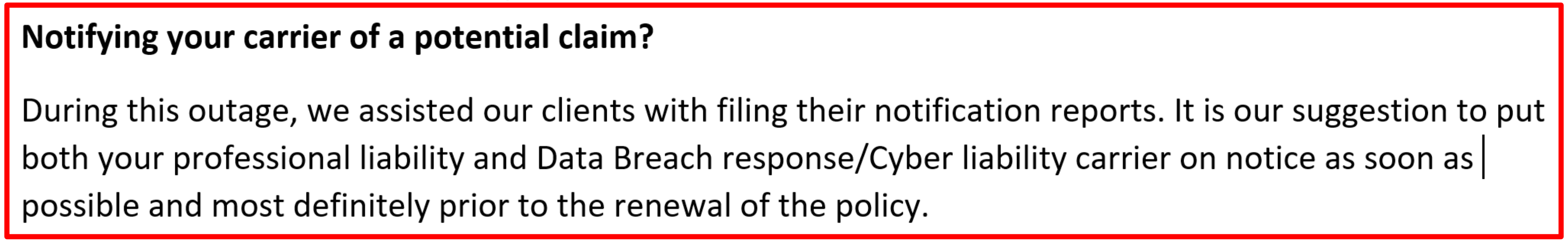
Unfortunately, too often we have been notified of a claim and not the potential of a claim. Policy language is quite clear and many cliams have been declined due to prior knowledge of a potential claim in a prior policy year.

About the Rob Ferrini

Rob Ferrini is McGowanPRO's Cyber Liability/Data Breach Response Program Manager. He has more than 30 years of insurance industry experience. Rob is a regular presenter on risk management and cyber liability insurance and has spoken nationally on Information Security and data breach coverage, best practices and mitigating the risk of a data breach with Information Security/Cyber Liability insurance.

About the McGowanPRO

Since 1998, McGowanPRO (formerly NAPLIA) has specialized in providing professional liability insurance and related insurance products to accountants, investment advisors, attorneys, and other professionals. Today, McGowanPRO has clients located in all 50 states and provides insurance coverage for 1,000s of accounting firms.



Notifying your carrier of a potential claim?

During this outage, we assisted our clients with filing their notification reports. It is our suggestion to put both your professional liability and Data Breach response/Cyber liability carrier on notice as soon as possible and most definitely prior to the renewal of the policy.

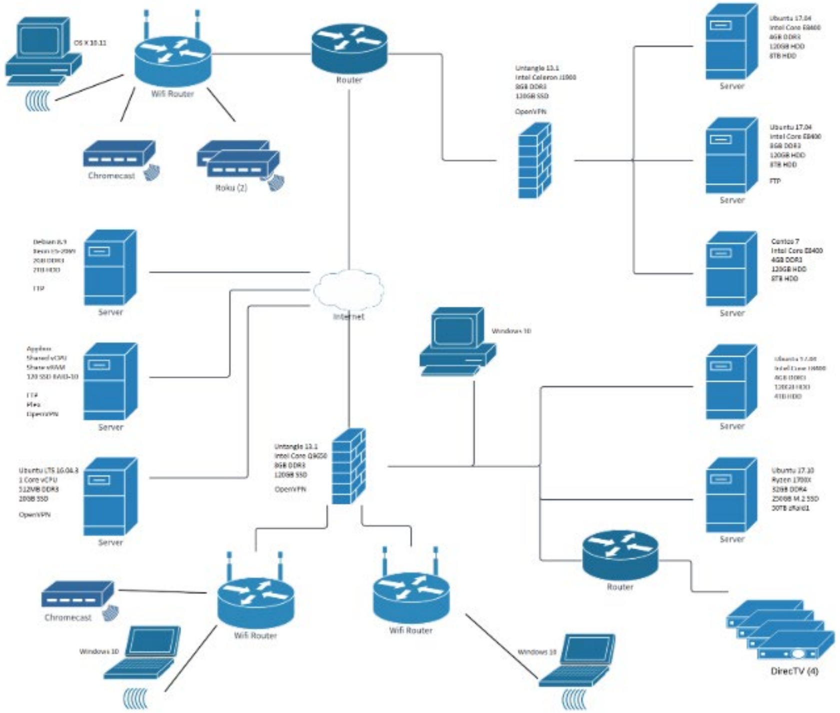
*Personally Identifiable Information

Secure Your Firm Post-COVID-19

- Firm IT Support Security Considerations
  - Independent Security Review
  - Verified Backups
  - Minimize Access Privileges
  - Breach Response Plan
  - Cybersecurity Insurance
  - Data/Equipment Tracking
    - Document where data resides
    - Inventory computer equipment
    - Destroy hard drives at termination

Secure Your Firm Post-COVID-19

- Additional Concerns for Non-Cloud Firms (maintain own servers)
  - Network Equipment System Updates
    - Monitored server operating system updates/patches
    - Update "connected" devices
    - Segment out IoT (Internet of Things)

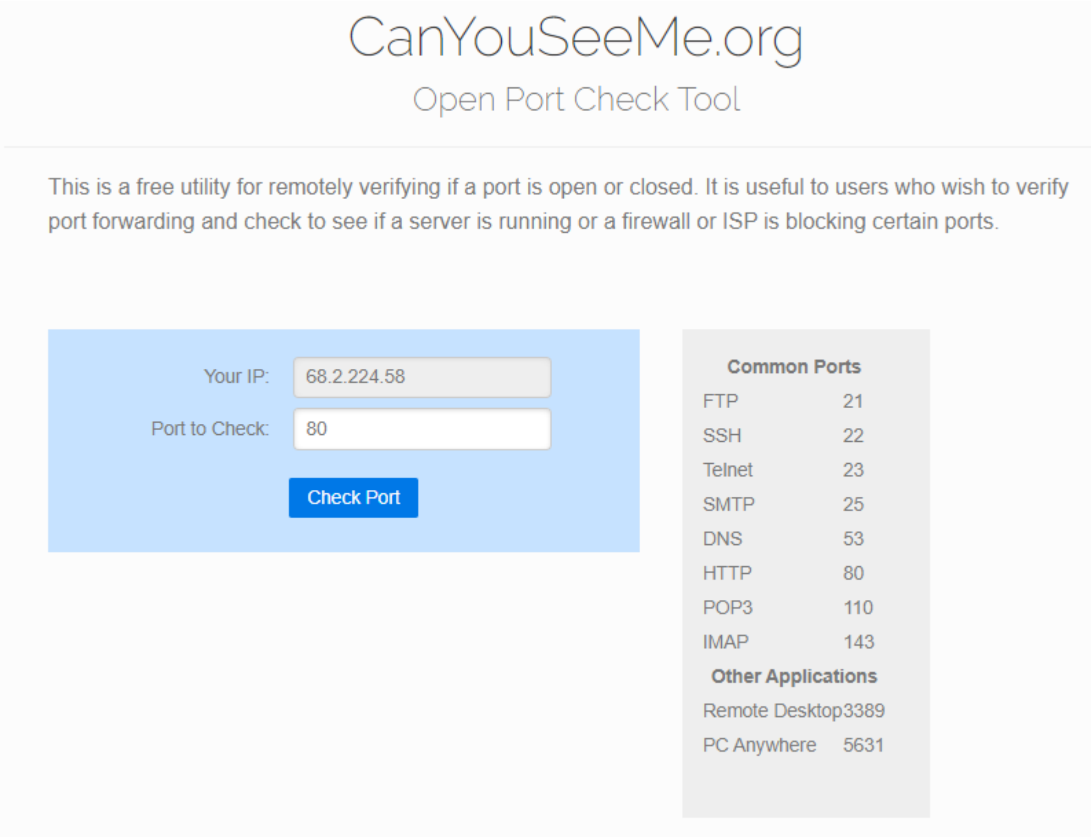


Secure Your Firm Post-COVID-19

- Additional Concerns for Non-Cloud Firms (maintain own servers)
  - Network Equipment System Updates
  - Secure On-Premise Equipment
    - Servers in unmarked/protected room
    - Physical and virtual locking of equipment
    - Building/suite alarm systems

Secure Your Firm Post-COVID-19

- Additional Concerns for Non-Cloud Firms (maintain own servers)
  - Network Equipment System Updates
  - Secure On-Premise Equipment
  - Firm Internet Performance
    - Monitor increased external activity
    - Verify security configuration after upgrades
    - Review “open” ports regularly



CanYouSeeMe.org

Open Port Check Tool

This is a free utility for remotely verifying if a port is open or closed. It is useful to users who wish to verify port forwarding and check to see if a server is running or a firewall or ISP is blocking certain ports.

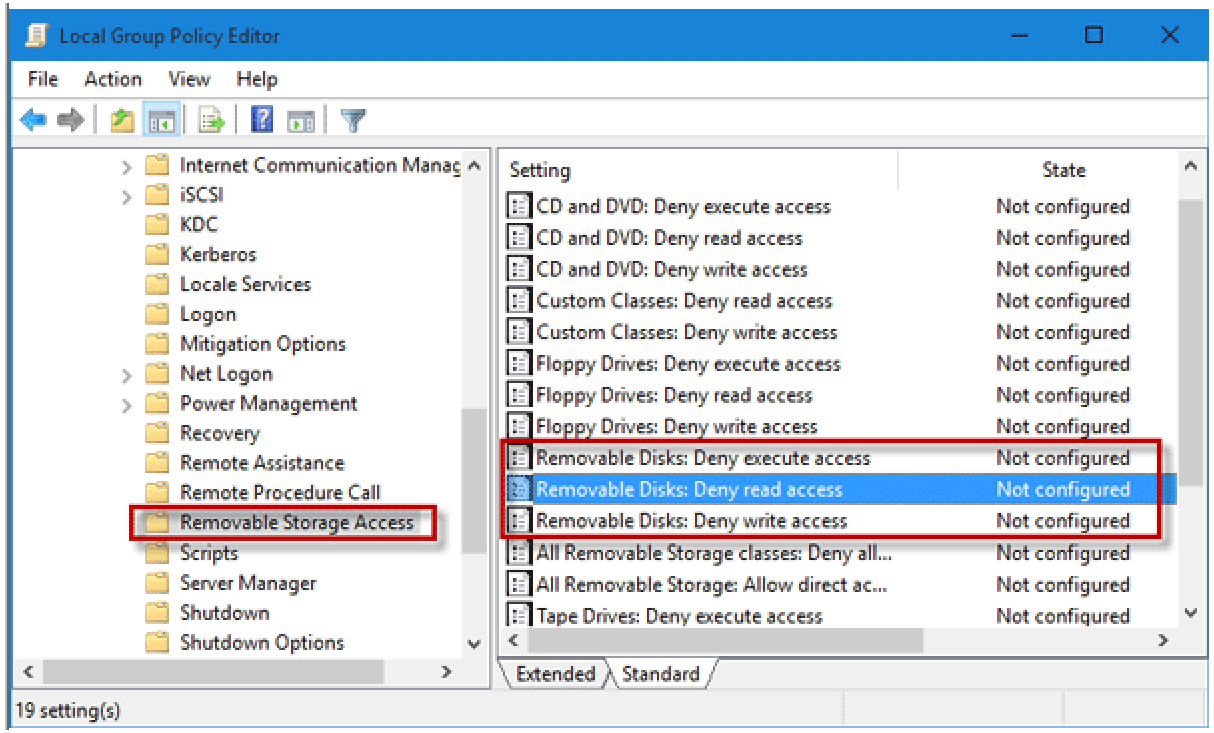
Your IP: 68.2.224.58

Port to Check: 80

Common Ports	
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
IMAP	143
Other Applications	
Remote Desktop	3389
PC Anywhere	5631

Secure Your Firm Post-COVID-19

- Additional Concerns for Non-Cloud Firms (maintain own servers)
  - Network Equipment System Updates
  - Secure On-Premise Equipment
  - Firm Internet Performance
  - Local Disk Storage (C: Drives)
    - Must be encrypted
    - Disable USB storage
    - Don’t keep anything local!



Setting	State
CD and DVD: Deny execute access	Not configured
CD and DVD: Deny read access	Not configured
CD and DVD: Deny write access	Not configured
Custom Classes: Deny read access	Not configured
Custom Classes: Deny write access	Not configured
Floppy Drives: Deny execute access	Not configured
Floppy Drives: Deny read access	Not configured
Floppy Drives: Deny write access	Not configured
Removable Disks: Deny execute access	Not configured
Removable Disks: Deny read access	Not configured
Removable Disks: Deny write access	Not configured
All Removable Storage classes: Deny all...	Not configured
All Removable Storage: Allow direct ac...	Not configured
Tape Drives: Deny execute access	Not configured

19 setting(s)

Resources

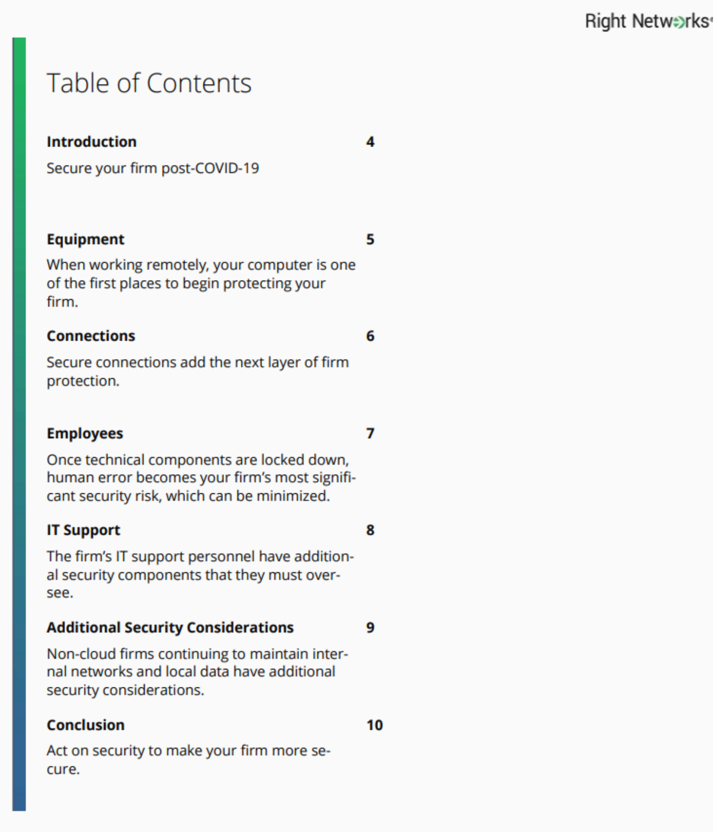
- Post COVID-19 Security Checklist

https://info.rightnetworks.com/webinar/cpa-cybersecurity-checklist

Right Networks

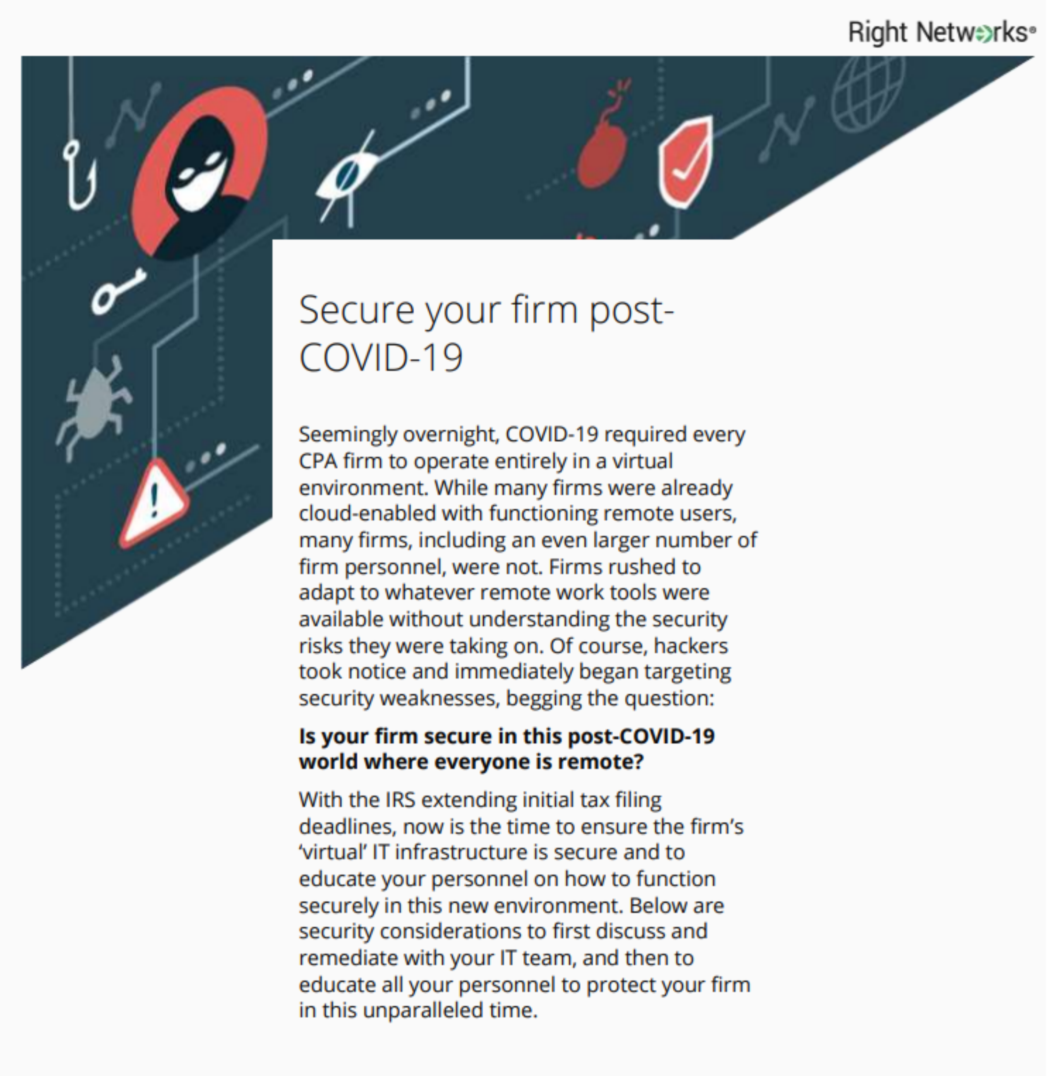
CPA Cybersecurity Checklist

2020 Edition



Right Networks

Table of Contents



Right Networks

Secure your firm post-COVID-19

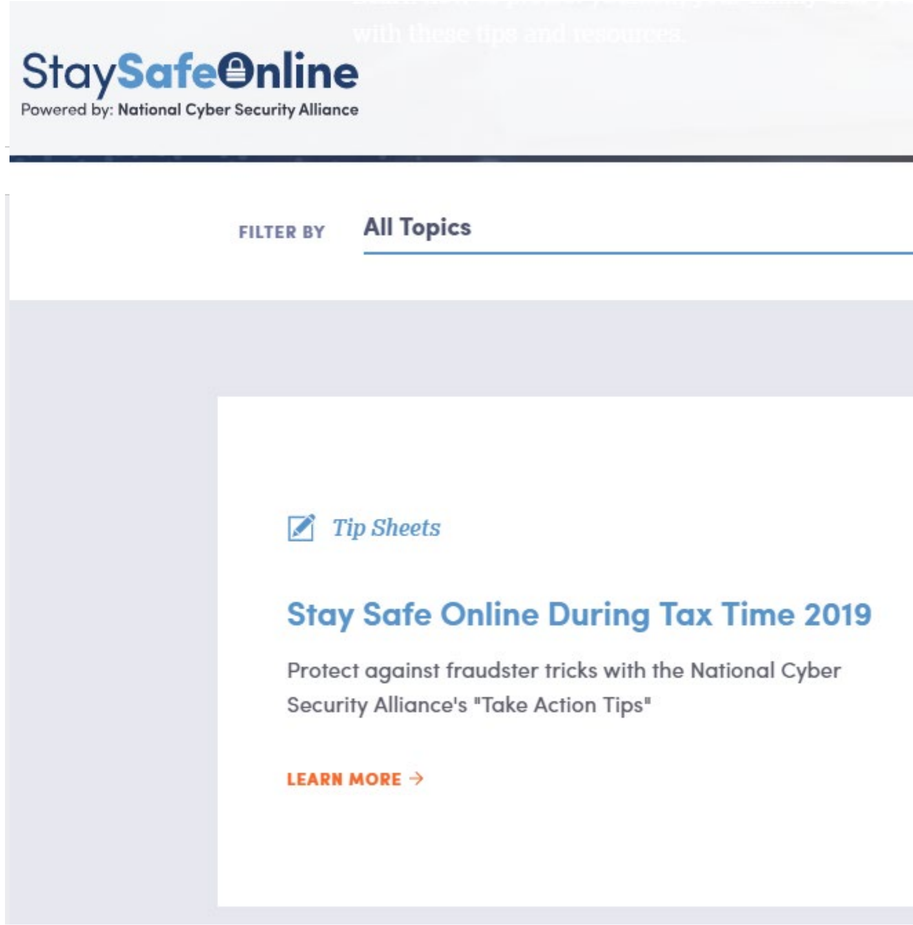
Seemingly overnight, COVID-19 required every CPA firm to operate entirely in a virtual environment. While many firms were already cloud-enabled with functioning remote users, many firms, including an even larger number of firm personnel, were not. Firms rushed to adapt to whatever remote work tools were available without understanding the security risks they were taking on. Of course, hackers took notice and immediately began targeting security weaknesses, begging the question:

Is your firm secure in this post-COVID-19 world where everyone is remote?

With the IRS extending initial tax filing deadlines, now is the time to ensure the firm's 'virtual' IT infrastructure is secure and to educate your personnel on how to function securely in this new environment. Below are security considerations to first discuss and remediate with your IT team, and then to educate all your personnel to protect your firm in this unparalleled time.

Resources

- Post COVID-19 Security Checklist
- AICPA Cyber Security Resource Center
- StaySafeOnline.org
- IDTheftCenter.org
- IRS Supporting Documents
  - Publication 5293, Data Security Resource Guide for Tax Professionals (PDF)
  - Publication 4557, Safeguarding Taxpayer Data (PDF)
  - Small Business Information Security: the Fundamentals (PDF) by NIST
- State Data Breach Reporting Requirements
  - https://www.itgovernanceusa.com/data-breach-notification-laws
- Response Considerations (CPAConsultantsAlliance.com)



with these tips and resources.

StaySafeOnline
Powered by: National Cyber Security Alliance

FILTER BY All Topics

Tip Sheets

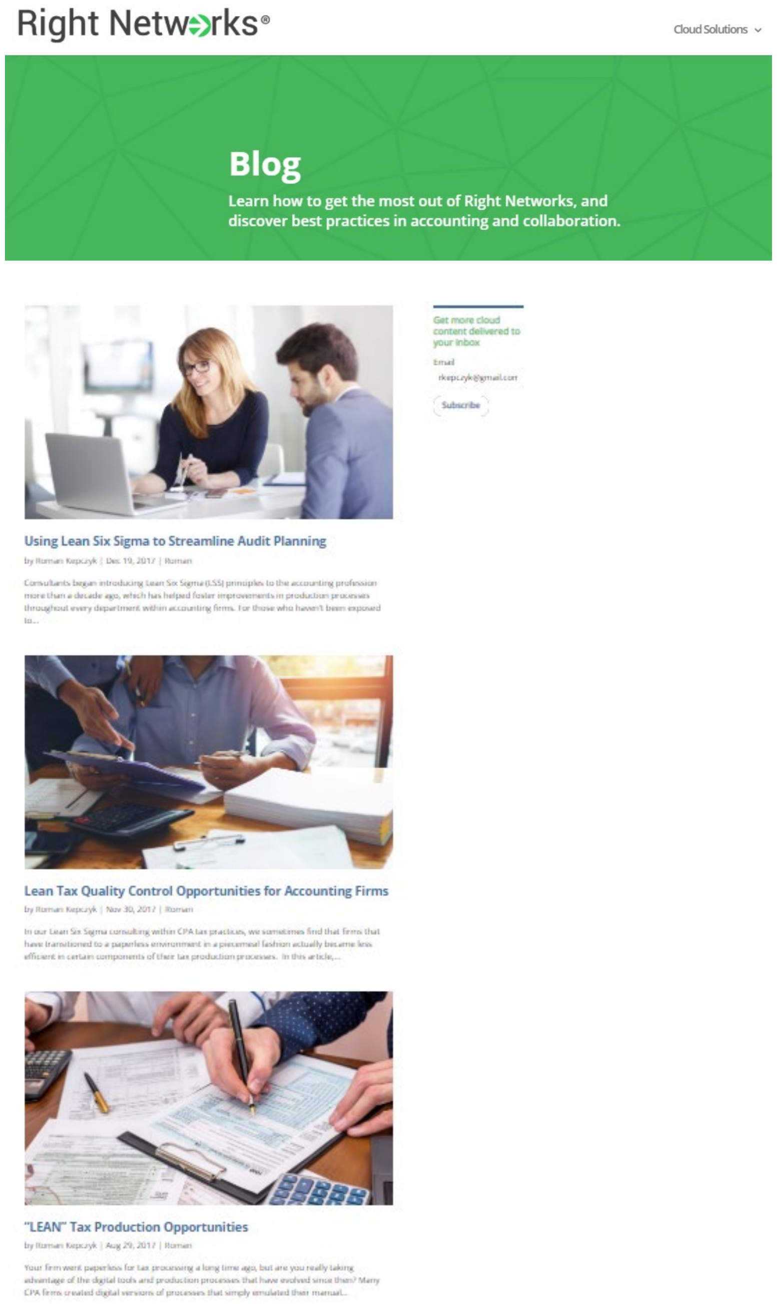
Stay Safe Online During Tax Time 2019

Protect against fraudster tricks with the National Cyber Security Alliance's "Take Action Tips"

LEARN MORE →

Resources

- Post COVID-19 Security Checklist
- AICPA Cyber Security Resource Center
- StaySafeOnline.org
- IDTheftCenter.org
- IRS Supporting Documents
  - Publication 5293, Data Security Resource Guide for Tax Professionals (PDF)
  - Publication 4557, Safeguarding Taxpayer Data (PDF)
  - Small Business Information Security: the Fundamentals (PDF) by NIST
- State Data Breach Reporting Requirements
  - https://www.itgovernanceusa.com/data-breach-notification-laws
- Response Considerations (CPAConsultantsAlliance.com)



Blog

Learn how to get the most out of Right Networks, and discover best practices in accounting and collaboration.

Get more cloud content delivered to your inbox

Email
rkepczyk@gmail.com

Subscribe

Using Lean Six Sigma to Streamline Audit Planning

by Roman Kepczyk | Dec 19, 2017 | Roman

Consultants began introducing Lean Six Sigma (LSS) principles to the accounting profession more than a decade ago, which has helped foster improvements in production processes throughout every department within accounting firms. For those who haven't been exposed to...

Lean Tax Quality Control Opportunities for Accounting Firms

by Roman Kepczyk | Nov 30, 2017 | Roman

In our Lean Six Sigma consulting within CPA tax practices, we sometimes find that firms that have transitioned to a paperless environment in a piecemeal fashion actually became less efficient in certain components of their tax production processes. In this article,...

"LEAN" Tax Production Opportunities

by Roman Kepczyk | Aug 29, 2017 | Roman

Your firm went paperless for tax processing a long time ago, but are you really taking advantage of the digital tools and production processes that have evolved since then? Many CPA firms created digital versions of processes that simply emulated their manual...

Right Networks®

◆◆◆

Right Networks®

CPA Cybersecurity Checklist

2020 Edition

https://info.rightnetworks.com/cloud-premier/cpa-cybersecurity-checklist-2020

THANK YOU!

Presented by Roman H. Kepczyk, CPA.CITP, CGMA

Director of Firm Technology Strategy

◆◆◆

www.rightnetworks.com