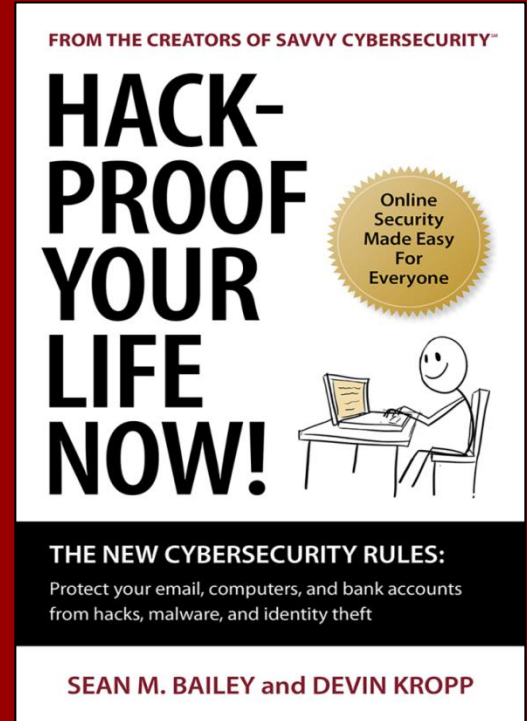


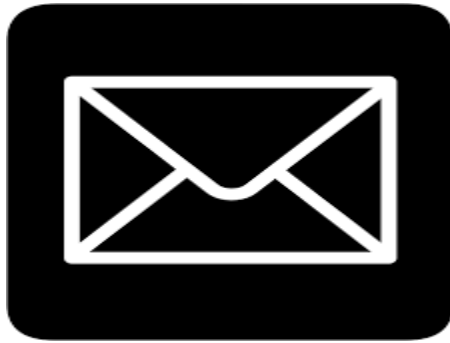
# The Case for Advisors Becoming Cybersecurity Guides

Sean Bailey and Devin Kropp

Authors of *Hack-Proof Your Life Now!* and creators of Savvy Cybersecurity



**One day in May of 2014,  
a Minnesota CEO sent an email to his  
accounts payable coordinator...**



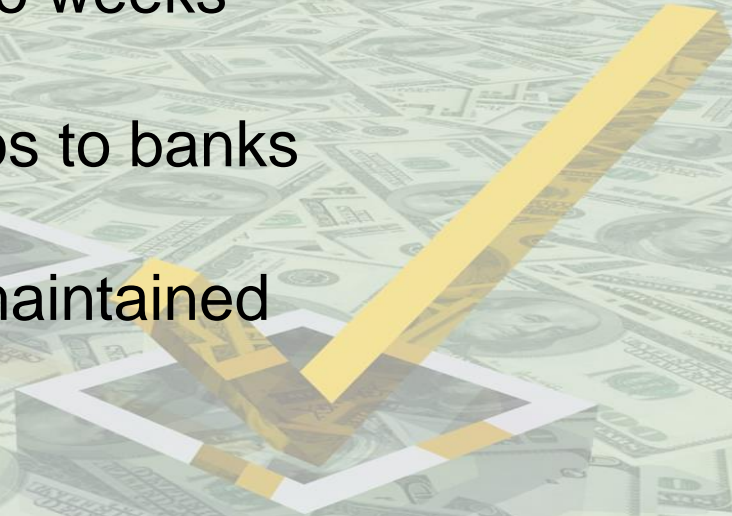
# Subject Line: Confidential Matter

**“Attorney David Madison is going to contact you. We are currently acquiring a company and so we will be needing your direct attention concerning accounting documents to finalize this acquisition. I inform you that I gave all the power to our Attorney that will be handling this operation. So please send the information and execute everything he needs.”**

**“This is of the utmost (sic) importance, we need to file this asap and conclude with the first deposit. Attorney Madison will inform me of the evolution of this operation. For reason of confidentiality and to follow the strict guidelines of an Acquisition we will only be in contact by email. Any questions you may have, please address them directly to Mr. Madison. You are the only one that is aware as of now, so I would need you to keep this reserved for yourself until the public announcement.”**

# A Smooth acquisition completed:

- Nine transactions in two weeks totaling \$40 million US
- Transfers made in euros to banks in Slovakia and China
- Payment coordinator maintained confidentiality

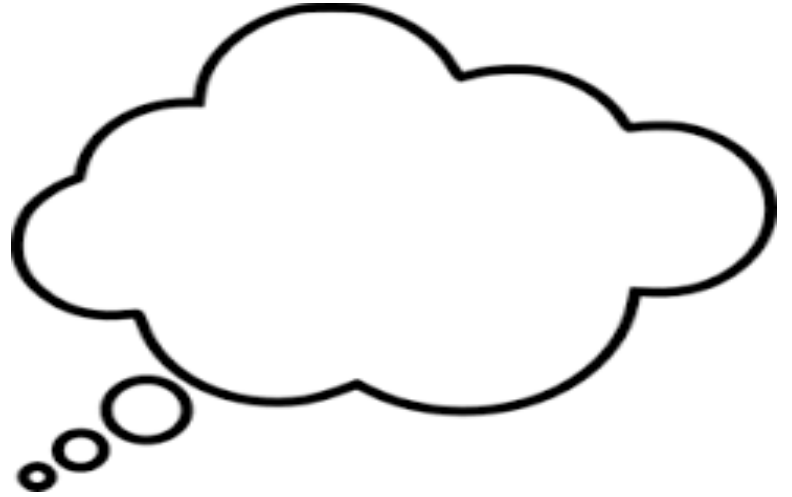


# CEO SCAM!

- Discovered day after last transfer
- Only \$12.7 million recovered
- CEO and payment coordinator: **Shocked!**

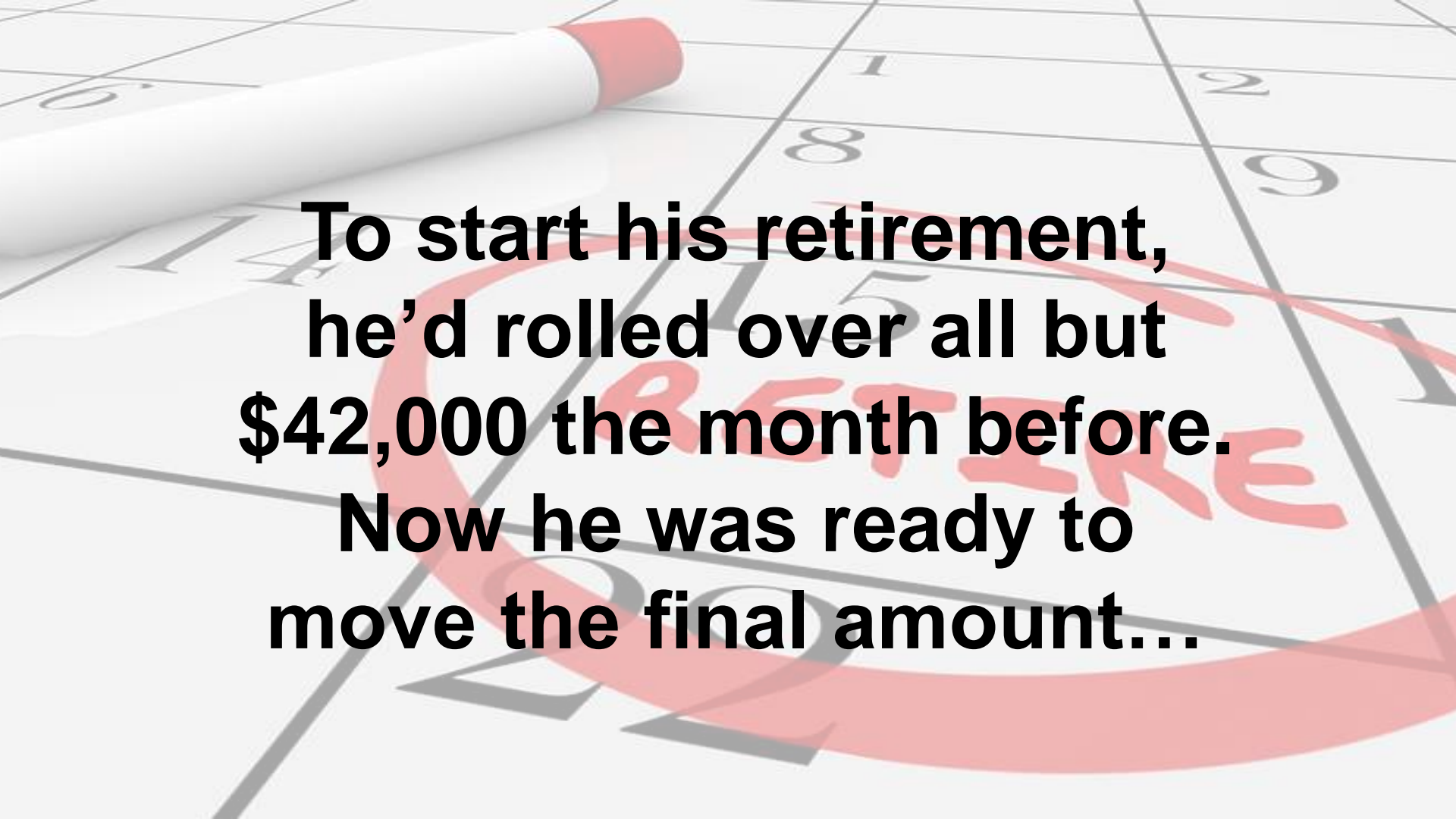


*Imagine if that CEO  
was a prospect  
you were cultivating...*



**One day in the fall of 2017, Utah-based CSX engineer Steve Voss pulled up his 401(k) account...**





**To start his retirement,  
he'd rolled over all but  
\$42,000 the month before.  
Now he was ready to  
move the final amount...**





**But his Prudential Financial  
account was empty! Zero!**

***“It’s an awful feeling.”***

**-Steve Voss**

# 401(k) SCAM!



- Thieves ransacking retirement accounts
- New, growing threat to everyone
- FBI is investigating at least five similar cases at Prudential Financial



*Imagine if Steve Voss  
was your client...*

**One day in the fall of 2015, Wells Fargo advisor Kathleen Kincade received an email from a client...**



**The client requested a series of wire transfers, which Kincade pushed through.**

**Two transfers totaled \$349,947.53**

# FRAUD!

- The wire transfer requests were from a hacker
- The client had been hacked and didn't know
- Kincade falsely checked a Wells Fargo security box that said she'd verbally confirmed the transfer with her client



# Fired!



- Wells Fargo fired Kincaid
- Kincaid fined \$5,000 by FINRA and suspended for 30 days
- Kincaid largely disappears from view on the Internet, except...

# Except for lawyers looking to sue Kincade...



WHITE LAW GROUP  
ATTORNEYS AT LAW

SECURITIES LITIGATION • ATTORNEYS PUBLICATIONS BLOG • PODCASTS

October 7, 2016 Comments (0) Current Investigations, Securities Fraud

## Investigation of Kathleen Kincade

*(Last Updated On: October 7, 2016)*

According to FINRA, Kathleen Kincade (CRD # 2634321, Irvine, CA) submitted an AWC in which she was fined \$5,000 and suspended for 30 days from the securities industry.

In October 2015, while registered with FINRA-regulated Firm Wells Fargo, Kincade allegedly caused two domestic wire disbursements totaling \$349,947.53 to be effected from the account of a customer to bank accounts held by third parties.

Purportedly, Kincade processed the wires based on e-mailed instructions that she received from an impostor who had hacked the customer's email account. In each instance, Kincade falsely represented in the firm's internal systems that she had verbally confirmed the wire disbursement instructions with her customer, which was not true, according to the settlement document.

Apparently, Kincade fell prey to a type of phishing scam that hackers use when targeting financial advisers; the fraudster hacks into a client's email, poses as the client in email exchanges with the adviser and then requests an electronic transfer of cash to an outside account.

Firms typically have rules that require the adviser speak to the client and verify the request before making the transfer. And that's where Ms. Kincade fell short, according to the Finra settlement.

A series of three wire transfers were made in the matter; after it learned they were fraudulent, Wells Fargo was able to reverse one transfer. It then reimbursed the client for the other withdrawals.

For FINRA's full findings see FINRA Case # 2016048659801

According to FINRA BrokerCheck, Kincade was registered with Wells Fargo Advisors Financial Network in Irvine, CA from 05/2007 – 01/2016. Kincade was discharged from Wells Fargo in January 2016.

If you suffered losses investing with Kathleen Kincade, the attorneys at The White Law Group may be able to help. For a free consultation, please call (888) 637-5510.



*Imagine if you were  
Kathleen Kincade...*



# PROBLEM ANALYSIS

# You've been hacked! (Your clients, too)

- Equifax, 2017: 145.5 million people
- Anthem Health Care, 2015: 78 million people
- JP Morgan, 2013: 83 million people



Source: Savvy Cybersecurity



# In the next 24 hours...

- 94 billion spam emails
- 35,000 identity theft victims
- 88,000 ransomed computers

Source: *Hack-Proof Your Life Now!*

# Identity theft hits record level

- 16.7 million victims in 2017
- 8% increase over 2016
- \$16.8 billion in theft

Source: Javelin Research, 2018



# What your clients fear most

How often do you, yourself, worry about the following things?

% “Frequently” or “occasionally”

	2017
Having your personal credit card or financial information stolen by computer hackers	67%
Being the victim of identity theft	66%
Having your car stolen or broken into	38%
Your home being burglarized when you are not there	36%
Being the victim of terrorism	30%
Having a school-aged child physically harmed attending school	26%
Getting mugged	25%
Your home being burglarized when you are there	23%
Being the victim of a hate crime	22%
Getting murdered	18%

Source: Gallup, Oct. 5-11, 2017

***Question:*** *What's a top challenge facing financial professionals in the age of Robo-advisors?*

**Answer:** Continuing to deliver meaningful value to clients that makes them feel your guidance and expertise are money well spent.

# FPA-LinkedIn survey

“How important is it that your adviser provides you with education related to the market, investments or another financial topic?”





# FPA-LinkedIn survey results

**76%**

of clients want advisors to deliver financial education

“Your clients want to tell you, if you let them...what it is that they want, what it is that they fear. When you do that, you will increase their well-being immensely. You will increase yours, **because you will get their gratitude, and you will get also to keep them as clients.**”

—Meir Statman, finance professor, Santa Clara University

**TWO PROBLEMS...**

# Problem #1

- Business leaders and private individuals face an ever-growing barrage of scary cybersecurity and identity theft threats.
- But there's **no one in their lives consistently helping them to learn to protect their identities and financial accounts**

# Problem #2

- Advisors need to deliver value in the form financial education AND **differentiate themselves from competitors**

# Key #1

**Individual's cybersecurity can be vastly improved by just taking a handful of actions in key areas of their lives.**

# Action 1: Set up instant text/email notifications for credit cards and bank accounts

---

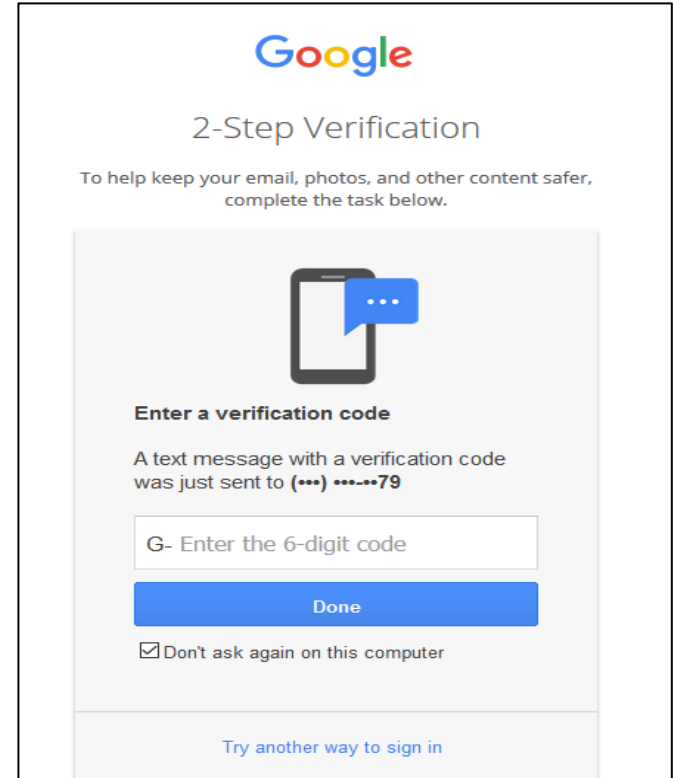
- Get notified for every charge or withdrawal from your account
- Can be done online
- Builds financial omniscience



# Action 2: Enable 2-step verification on accounts

---

- Requires additional code when you login
- Crucial for email and financial accounts
- Authenticator apps
- Builds secrecy





## Action 3: Freeze your credit

---

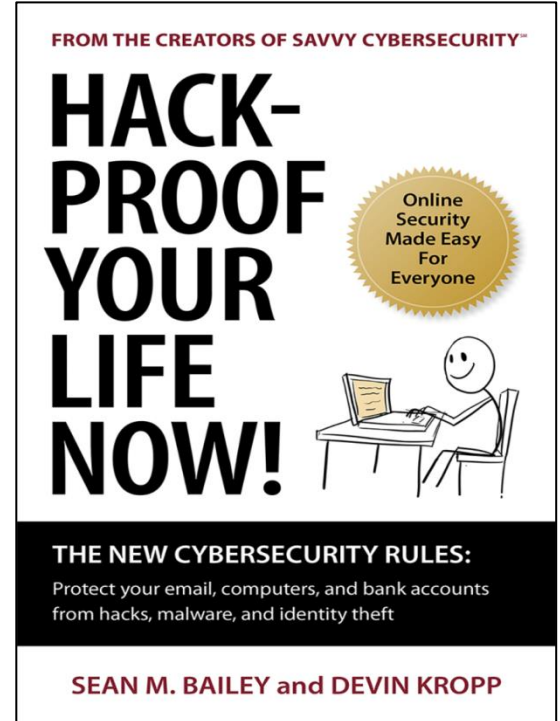


- Sign up for a credit freeze at all three of the credit bureaus
- Locks your credit with a PIN
- Free in all states
- No LifeLock!

## Other steps:

Complete 15 other actions to boost your cybersecurity score.

Then teach your clients the new cybersecurity rules



*“But what about the  
business threats you  
mentioned earlier?”*



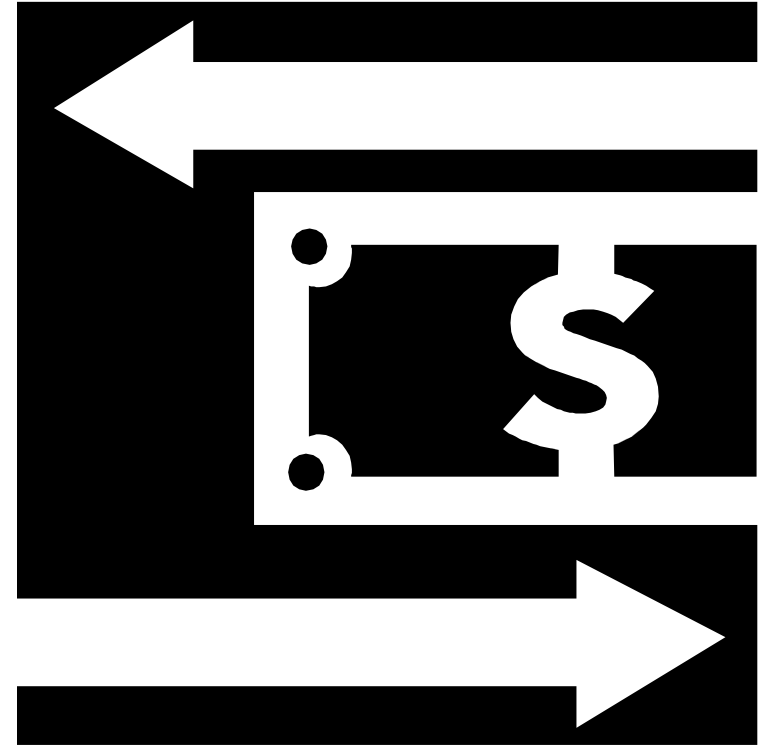
## Key #2

**Business leaders can shut down many high-dollar scam vulnerabilities with some easy security boosts and policy changes for all people who handle money.**

# Action 1: Add tighter wire transfer controls

---

- Require extra security:
  - Multiple sign-offs
  - Two-step confirmation (ex. Email and phone)
- Stipulate a lapsed time period between request and transfer



## Action 2: Boost mobile-phone security

---

- Require financial staff and senior level employees have PINS on mobile accounts
- Requires passcode before any changes can be made to account



# Action 3: Encrypt website, files, network connections

---

- Encrypt:
  - Most important, sensitive files
  - Customer data
- Outside employees' connections to company networks VPN (Virtual Private Network)
- Websites
- Wireless routers



**Other steps:**  
 Learn to Hack-Proof your  
 business and team.  
 Complete the Business  
 Protection Checklist.

**Then take it to  
 local CEOs**

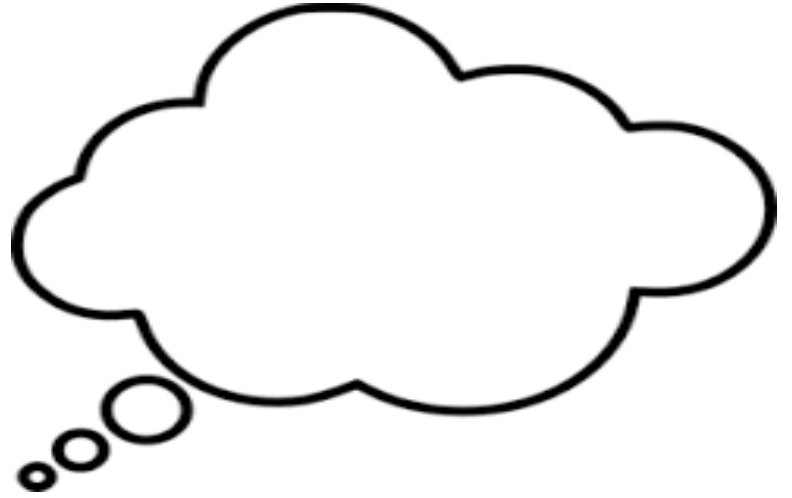


	<p><b>Teresa A. Sampleton, CFP®, CPA</b>  <b>Vice President</b>  <b>Sampleton Wealth Management</b>        123 Main Street        12th Floor        New York, NY 10018        888-336-6884        tsampleton@sampletonwealth.com        www.sampletonwealth.com</p>		
<p>Use the following topics and questions to guide a cybersecurity discussion with your security professionals and management team. The goal is to share information, identify problems and strengths, and take action.</p>			
<p><b>Ask your IT or Security Professional:</b></p>			
<p><b>CYBERSECURITY PLANS</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have a written information security policy?</li> <li><input type="checkbox"/> Do we conduct periodic reviews to identify security threats and vulnerabilities to our system?</li> <li><input type="checkbox"/> Do we have a written plan of action if we do suffer a cybersecurity attack?</li> <li><input type="checkbox"/> How do we protect ourselves from ransomware?</li> <li><input type="checkbox"/> What do you think is the most serious cybersecurity threat our business faces?</li> </ul>	<p><b>DATA PROTECTION</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have a regular backup system in place?</li> <li><input type="checkbox"/> Where is our customer data housed on the network and how is it protected versus other locations?</li> <li><input type="checkbox"/> How do we control the transfer of customer data?</li> <li><input type="checkbox"/> Who has access to download customer data?</li> <li><input type="checkbox"/> Is our data encrypted?</li> <li><input type="checkbox"/> How is our communication encrypted?</li> <li><input type="checkbox"/> How do we protect customer information?</li> <li><input type="checkbox"/> What is our policy for aging out old data?</li> <li><input type="checkbox"/> How do we track computers and devices and the data they hold?</li> <li><input type="checkbox"/> How is mission critical data warehoused offsite?</li> </ul>	<p><b>NETWORK/CONNECTION</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Who connects to our networks from the outside and how do we manage?</li> <li><input type="checkbox"/> How do we monitor for unauthorized users or devices on the network?</li> <li><input type="checkbox"/> How restrictive is our firewall for inbound communication and access?</li> <li><input type="checkbox"/> Does our firewall have proxying services, antivirus gateway services, and intrusion detection and prevention services?</li> <li><input type="checkbox"/> What endpoint security do we have in place?</li> <li><input type="checkbox"/> Do we conduct vulnerability scans of the network?</li> <li><input type="checkbox"/> Do we have the ability to know we have an active attacker in our network?</li> </ul>	
<p><b>DEVICES</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have an inventory of all physical devices and systems within the company?</li> <li><input type="checkbox"/> Are all devices used in the company running antivirus software?</li> <li><input type="checkbox"/> How do we ensure all devices are running up-to-date software?</li> <li><input type="checkbox"/> Are our routers secure and are they running the most up-to-date firmware?</li> </ul>	<p><b>EMPLOYEE POLICIES</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we limit employee access to only networks, systems, files, and programs that they need for their job?</li> <li><input type="checkbox"/> What kind of employee cybersecurity training do we have?</li> <li><input type="checkbox"/> What is our policy for employees working or accessing work data on their personal devices?</li> <li><input type="checkbox"/> Do we offer employees a VPN for working remotely?</li> <li><input type="checkbox"/> What is our password policy?</li> </ul>	<p><b>THIRD PARTY POLICIES</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do any third parties have access to our data?</li> <li><input type="checkbox"/> How do we vet the security of third party companies we use?</li> <li><input type="checkbox"/> Do we discuss cybersecurity risks and responsibilities when going into contract with other companies?</li> </ul>	
<p><small>Copyright © 2018 Horseshoath, LLC. All Rights Reserved.        License #: 4622288 Regulated Licensee: Teresa A. Sampleton        Horseshoath is an independent organization providing unique, unbiased insight into the critical issues facing financial advisors and their clients.        Horseshoath, LLC is not affiliated with the report licensee or any of its affiliates.</small></p>			

Click with your financial advisor for updates.



*“Ok, so how do I actually position myself as a cybersecurity guide?”*



## Key #3

**Financial advisors can differentiate themselves by making improving the public's cybersecurity a key aspect of their financial education programs in 2019 and beyond.**

# Case study:

## Jeanne Mraz

- SVA Plumb Financial
- Madison, Wisconsin
- 20+ years in business
- Started presenting Savvy Cybersecurity to clients and prospects





## **Clients were suffering**

- Clients were hacked
- Needed to be proactive and be able to help them

## First, presented to clients...



- 2 presentations at client appreciation events
- 40-50 attendees at each

# Then invited to present in the community

- Contacted by groups in Madison to come present to their clients
- Source of referrals





## Audience feedback

- Mostly: Generation X, Pre-Retirees, Retirees
- Certain threats resonate with certain groups
- People always walk away with tips

# Advisor success: Tony LaJeunesse

- TL Financial Group
- Southgate, Michigan
- Cybersecurity  
workshops are the best  
attended of all topics





## Advisor success: Donald Morgan



*"We LOVE the Cybersecurity Workshop!! We have already done 2 lunch/learn workshops with 10 at the first and 14 at the second (which is a full house for our office).*

*"The response has been overwhelming and we have an in-house tech that has been doing follow up appointments with anyone wanting them.*

*"We have had 70% non-clients at our events too which has been great!!"*

Independent Wealth Connections, Spokane Valley, WA

# Advisor success: Mike Makonnen

- Makonnen Financial Group
- Alexandria, VA
- Gifted 300 copies of *Hack-Proof Your Life Now!*
- Client asked him to send copy to friend
- Friend came to office and opened \$3 million account



# We have a two-prong problem

1. Client and businesses, including all of us, face an ever-growing cybersecurity onslaught. No one in their lives guiding them to boost their security
2. Advisors need to deliver value in the form of Financial Education AND they need to differentiate themselves from competitors

## One solution

Become a “hero” to your clients and your community by positioning yourself as a cybersecurity guide (not a tech expert) in your financial education activities.

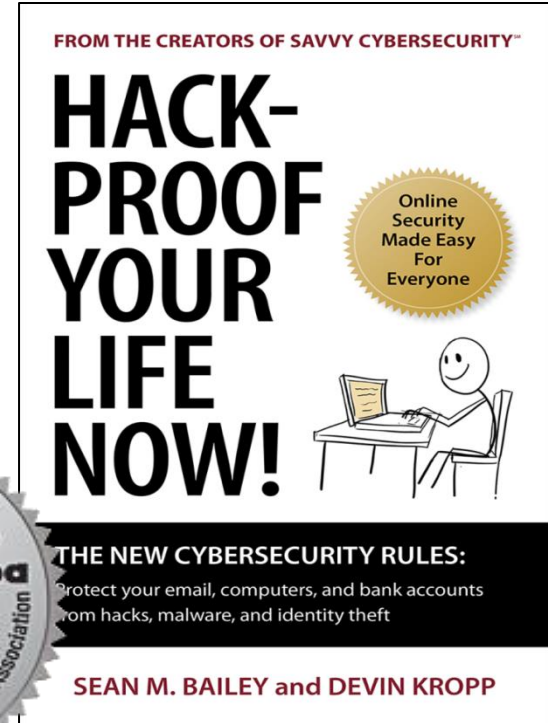


*“How do I get started?”*

Read:

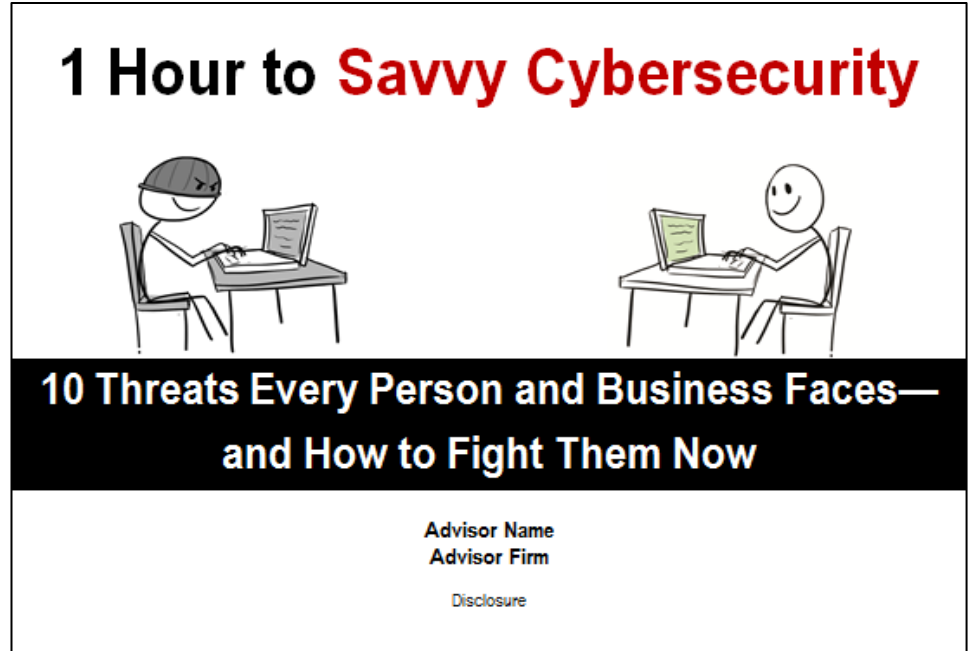
# *Hack-Proof Your Life Now! The New Cybersecurity Rules*

- Amazon best seller
- IBPA silver medal winner:  
Best New Voice Non-Fiction  
and Reference




# Present “1 Hour to Savvy Cybersecurity” to clients and prospects

- 25+ slides  
and speaker  
notes
- Finra  
reviewed



**1 Hour to Savvy Cybersecurity**



**10 Threats Every Person and Business Faces—and  
How to Fight Them Now**

Advisor Name  
Advisor Firm  
Disclosure

# Send the Savvy Cybersecurity Quick Reference Guide

## Savvy Cybersecurity

### Quick Reference Guide, 2018

**Teresa A. Sampleton, CFP®, CPA**  
**Vice President**  
**Sampleton Wealth Management**  
 123 Main Street  
 12th Floor  
 New York, NY 10018  
 888-336-6884  
 tsampleton@sampletonwealth.com  
 www.sampletonwealth.com



#### A. Scorecard

Answer Yes or No to the following questions. When complete, follow directions at bottom to get your raw score and rating. Then review checklist and complete action plan.

Question	Yes/No
I have one email address that I use exclusively for my online financial accounts (banking, credit cards, payment services, brokerage, etc.) and nothing else.	
I have two-step verification (two-factor authentication) turned on for my email and online financial accounts.	
I can spot the difference between dangerous free public Wi-Fi and useful, secure free public Wi-Fi.	
I understand how to tell if my home Wi-Fi network is vulnerable to hackers and how to boost the network's security.	
Whenever any money leaves my bank accounts or my credit cards are charged, I'm alerted to the transaction.	
I have complete control over my credit files at the big-three bureaus (Equifax, Experian, and TransUnion), because I have placed them on the highest security level.	
I have confirmed with the credit bureaus that my minor children have not been the victims of identity theft.	
I run an updated antivirus software program on my computers and devices.	
I always make sure that my computer and devices have the most up-to-date software programs, including operating system, browsers, Microsoft Office, iTunes player, virus protection, wireless router, and Adobe programs.	
I have a system for ensuring that I can recover from a ransomware phishing attack without paying an extortion fee to a criminal.	
Give yourself five points for each question answered with a Yes. Add points to get score. Consult section B to get your cybersecurity rating.	Raw Score:

B. Rating	
50-40	GOOD
35-25	OKAY
20-0	DANGER

Consult the Checklist in section C to identify key items to include in your Action Plan in section D.

#### C. Checklist

Action	Time
<b>Email</b>	
<input type="checkbox"/> Create a secret email address for your financial accounts and set it up with the strongest possible security settings.	5 min
<b>Passwords</b>	
<input type="checkbox"/> Create stronger passwords using mnemonic, goal-setting, Diceware, or poetic password approaches.	5 min
<input type="checkbox"/> Enable two-step verification on all your key accounts that allow it—financial accounts and personal email.	5 min
<input type="checkbox"/> Download a password manager and put it on all your computers and devices. Pick a strong master password using the mnemonic or Diceware approach.	15 min
<b>Wi-Fi</b>	
<input type="checkbox"/> Install a VPN program on your laptop and mobile devices for safe use of free Wi-Fi.	10 min
<input type="checkbox"/> Change your router's default username and password—don't keep the factory settings.	15 min
<input type="checkbox"/> Select the WPA or WPA2 encryption setting.	5 min
<input type="checkbox"/> Disable the WPS setting on your router.	5 min
<input type="checkbox"/> Update your router's firmware.	20 min
<b>Transactions</b>	
<input type="checkbox"/> Create text or email alerts for your bank accounts and credit cards.	2 min
<b>Credit</b>	
<input type="checkbox"/> Place a credit freeze on your credit files at all three reporting agencies: Equifax, Experian, and TransUnion.	20 min
<input type="checkbox"/> Request a search on your children's Social Security numbers at all three credit bureaus.	30 min
<input type="checkbox"/> Review your state's laws to determine the best way to protect your children from identity theft.	15 min
<b>Software</b>	
<input type="checkbox"/> Update all software on all devices.	10 min
<input type="checkbox"/> Set auto-update for programs that allow it.	5 min
<input type="checkbox"/> Run an antivirus software.	5 min
<b>Back-Up</b>	
<input type="checkbox"/> Back up your data on ALL your devices to at least two locations—the cloud and a physical device.	20 min

Copyright © 2018 Horseshoof, LLC. All Rights Reserved.  
 License #: 4692213 Reprint License: Teresa A. Sampleton  
 Horseshoof is an independent organization providing unique, unbiased insight into the critical issues facing financial advisors and their clients.  
 Horseshoof, LLC is not affiliated with the reprint licensee or any of its affiliates.

Check with your financial advisor for updates.

Advisory Services offered through Sampleton Wealth Management LLC, a Registered Investment Advisor.

Copyright © 2018 Horseshoof, LLC. All Rights Reserved.

Check with your financial advisor for updates.

#### Inversion Chart

Example phrases made into passwords	
Run everyday	Run3v3ryd@y
Eat more fruit	3@t>frui1t
Sleep at 11	5133p@11pm
Bring own lunch	B@rn@ownlunch!
No more soda	N0m0r3s0d@
Save for house	5@v@34th0u53
Get outside	G3t@Out5id3

Canada
<b>Credit Reporting Agencies</b> Equifax Canada: 800-465-7166 TransUnion Canada: 800-663-9980 French correspondence: 877-713-3393
<b>Canadian Anti-Fraud Centre:</b> 1-888-495-8501

#### TAKE CHARGE TODAY

Learn the New Cybersecurity Rules and regain control of your online security. *Hack-Proof Your Life Now!* is the cybersecurity survival guide for everyone.

This book will guide you through all the actions included in the above checklist with detailed instructions.

It also includes recommendations for products such as password managers and antivirus software.

Get your copy today and start building your personal cybersecurity plan.

Visit [www.hackproofyourlifeforlife.com](http://www.hackproofyourlifeforlife.com) for more details.



# Present “Will Hackers Scam Your Business? 5 Threats Every Company Faces and What Executives Should Do to Boost Cybersecurity at Work”

- 70+ slides and speaker notes
- Finra reviewed



# Share the Savvy Cybersecurity Business Protection Checklist



## Business Protection Checklist

Teresa A. Sampleton, CFP®, CPA  
 Vice President  
 Sampleton Wealth Management  
 123 Main Street  
 12th Floor  
 New York, NY 10018  
 888-336-6884  
 tsampleton@sampletonwealth.com  
 www.sampletonwealth.com



Use the following topics and questions to guide a cybersecurity discussion with your security professionals and management team. The goal is to share information, identify problems and strengths, and take action.

### Ask your IT or Security Professional:

<b>CYBERSECURITY PLANS</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have a written information security policy?</li> <li><input type="checkbox"/> Do we conduct periodic reviews to identify security threats and vulnerabilities to our system?</li> <li><input type="checkbox"/> Do we have a written plan of action if we do suffer a cybersecurity attack?</li> <li><input type="checkbox"/> How do we protect ourselves from ransomware?</li> <li><input type="checkbox"/> What do you think is the most serious cybersecurity threat our business faces?</li> </ul>	<b>DATA PROTECTION</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have a regular backup system in place?</li> <li><input type="checkbox"/> Where is our customer data housed on the network and how is it protected versus other locations?</li> <li><input type="checkbox"/> How do we control the transfer of customer data?</li> <li><input type="checkbox"/> Who has access to download customer data?</li> <li><input type="checkbox"/> Is our data encrypted?</li> <li><input type="checkbox"/> How is our communication encrypted?</li> <li><input type="checkbox"/> How do we protect customer information?</li> <li><input type="checkbox"/> What is our policy for aging out old data?</li> <li><input type="checkbox"/> How do we track computers and devices and the data they hold?</li> <li><input type="checkbox"/> How is mission critical data warehoused offsite?</li> </ul>	<b>NETWORK/CONNECTION</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Who connects to our networks from the outside and how do we manage?</li> <li><input type="checkbox"/> How do we monitor for unauthorized users or devices on the network?</li> <li><input type="checkbox"/> How restrictive is our firewall for inbound communication and access?</li> <li><input type="checkbox"/> Does our firewall have proxying services, antivirus gateway services, and intrusion detection and prevention services?</li> <li><input type="checkbox"/> What endpoint security do we have in place?</li> <li><input type="checkbox"/> Do we conduct vulnerability scans of the network?</li> <li><input type="checkbox"/> Do we have the ability to know we have an active attacker in our network?</li> </ul>
<b>DEVICES</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we have an inventory of all physical devices and systems within the company?</li> <li><input type="checkbox"/> Are all devices used in the company running antivirus software?</li> <li><input type="checkbox"/> How do we ensure all devices are running up-to-date software?</li> <li><input type="checkbox"/> Are our routers secure and are they running the most up-to-date firmware?</li> </ul>	<b>EMPLOYEE POLICIES</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do we limit employee access to only networks, systems, files, and programs that they need for their job?</li> <li><input type="checkbox"/> What kind of employee cybersecurity training do we have?</li> <li><input type="checkbox"/> What is our policy for employees working or accessing work data on their personal devices?</li> <li><input type="checkbox"/> Do we offer employees a VPN for working remotely?</li> <li><input type="checkbox"/> What is our password policy?</li> </ul>	<b>THIRD PARTY POLICIES</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Do any third parties have access to our data?</li> <li><input type="checkbox"/> How do we vet the security of third party companies we use?</li> <li><input type="checkbox"/> Do we discuss cybersecurity risks and responsibilities when going into contract with other companies?</li> </ul>

Copyright © 2018 Horseshoemouth, LLC. All Rights Reserved.  
 License #: 4692238 Reprint Licensee: Teresa A. Sampleton  
 Horseshoemouth is an independent organization providing unique, unbiased insight into the critical issues facing financial advisors and their clients.  
 Horseshoemouth, LLC is not affiliated with the reprint licensee or any of its affiliates.

Check with your financial advisor for updates.

...count to commit a fraud. Example: Your mobile phone  
 ...ed on a specific person or institution. Over time, a hacker  
 or security holes.  
 ...es compromised devices to push traffic to a single website  
 wn.  
 ...n so only others with permission can read them.  
 o travel through.  
 k accessed by remote wireless devices. The system secures  
 ...ned to monitor inbound and outbound communication  
 to a device, such as a wireless router.  
 connected to the Internet.  
 fs the keys that you hit on the keyboard. This is used to gain  
 ...uses—designed to interfere with a computer's normal  
 ...pped into revealing personal, confidential, or monetary  
 us link or attachment. Spear phishing is when these  
 ...pects data between an external network (the Internet) and  
 s from directly accessing internal information.  
 ts the victim's data and demands payment for the  
 ...giving up confidential information or breaking security  
 ...tity when trying to access an online account. It requires  
 ...ates a private encrypted Internet tunnel using a public

# Present “Hack-Proof Your Smartphone”


- 15+ slides and speaker notes
- Lunch and learn
- Finra reviewed



# Connect with CPAs and COIs


- “1 Hour to Savvy Cybersecurity” approved for CPE credit when presenting to CPAs
- CPE credit guide
- Finra reviewed

## 1 Hour to Savvy Cybersecurity




10 Threats Every Person and Business Faces—  
How to Fight Them Now

Advisor Name  
Advisor Firm  
Disclosure




## CPE Credits Guide

What you need to do to award  
Continuing Education  
to CPAs



Horseshmouth, LLC  
of Accountancy (NAC) is  
the national register  
authority on the act  
regarding registrars  
CPE Sponsors



Horseshmouth, 21 West 38th Street, New York, NY 10018, 888-336-6884

### CERTIFICATE OF COMPLETION

This certificate is presented to:  
[Participant Name]  
For successful completion of:  
**1 Hour to Savvy Cybersecurity: 10 Threats Every  
Person and Business Faces – and How to Fight Them  
Now**

Presenter:  
[Advisor's name & firm]  
[Date]  
[Location]

- ◆ National Registry of CPE Sponsors Number: 130453
- ◆ Instructional delivery method: Group-Live
- ◆ Information technology: 1 CPE credit

*William T. Nicklin*  
William T. Nicklin, CEO, Horseshmouth

In accordance with the standards of the National Registry of CPE Sponsors, CPE credits have been granted based on a 50-minute hour.

# Send a monthly or quarterly newsletter

- Monthly newsletter comes with template
- Write your own



The image shows a screenshot of a newsletter header for 'Savvy Cybersecurity'. At the top left is the logo with 'horsesmouth' in a green speech bubble and 'Savvy Cybersecurity™' in black and red text with a padlock icon. To the right, the date 'December 29, 2017' and the website 'www.savvycybersecurity.com' are displayed. Below this is a large image of a person's hands holding a glowing crystal ball that reflects a globe. Underneath the image is the section 'In this issue' with a bulleted list of topics. At the bottom of the header is a salutation 'Dear Savvy Advisor,' followed by a paragraph of introductory text.

horsesmouth  
**Savvy Cybersecurity™**

December 29, 2017  
[www.savvycybersecurity.com](http://www.savvycybersecurity.com)



**In this issue**

- 3 cybersecurity predictions for 2018
- Emerging threats: New scams to look for
- Savvy Cybersecurity quick links
- Cybersecurity shorts: Cybersecurity legislation, an UberEATS hack, Android malware, and much more
- Software updates

Dear Savvy Advisor,

It's certainly been another wild year for cybersecurity. We saw the world-record-breaking Yahoo breach, a massive Google Doc phishing attack, a worldwide ransomware exploit, the Equifax hack—and that's just the biggest events. Of

tion, an UberEATS hack, Android

saw the world-record-breaking Yahoo breach, malware exploit, the Equifax hack—and that's 18 to bring us even more cybersecurity

months. In the cybersecurity world, there's a 2017—3 billion accounts exposed via Yahoo, payout at Uber to cover a breach affecting

over 1,250 breaches in 2017—nearly 200 that cyberattacks will continue to grow in

2018.

But what exactly will cybersecurity look like in 2018? Here are some predictions we've been reading about.

#### 1. Start saying goodbye to passwords


The sheer number of data breaches exposing usernames and passwords has highlighted the dangers in depending on this insecure login method. More often than not, users repeat passwords on multiple sites

# Join Savvy Cybersecurity for \$497 — \$100 discount

FROM THE CREATORS OF SAVVY CYBERSECURITY

## HACK-PROOF YOUR LIFE NOW!

Online Security Made Easy For Everyone



THE NEW CYBERSECURITY RULES:

### Will Hackers Scam Your Business?

#### 5 Threats Every Company Faces and What Executives Should Do to Boost Cybersecurity at Work

horsmouth

## Savvy Cybersecurity

### Marketing Toolkit

Savvy Cybersecurity

## Hack-Proof Your Smartphone



## 1 Hour to Savvy Cybersecurity

### 10 Threats Every Person and Business Faces — and How to Fight Them Now

Savvy Cybersecurity

### Business Protection Checklist

#### Quick Reference Guide, 2017

Ask your IT or Security Professional:

**CYBERSECURITY PLANS**

- Do we have a written information security policy?
- Do we conduct periodic reviews to identify security and privacy vulnerabilities in our systems?
- Do we have a written plan of action if we do suffer a cybersecurity attack?
- How do we protect ourselves from ransomware?
- What are your risks for the most serious cybersecurity threats to our business face?

**DATA PROTECTION**

- Do we have a regular backup system in place?
- Where is our customer data housed on the network and how do we monitor for unauthorized users on devices on our network?
- How do we control the transfer of customer data?
- What are our policies for handling customer data?
- Is our data encrypted?
- How do we protect customer information?
- How is our policy for aging out old data?
- How do we back up computers and devices and the data they hold?
- How do we ensure critical data is backed-up offsite?

**DEVICES**

- Do we have an inventory of all physical devices and systems that the company?
- Are all devices used by the company running antivirus software?
- Are our routers secure and are they running up-to-date software?
- Are our routers secure and are they running the most up-to-date firmware?

**EMPLOYEE POLICIES**

- Do we limit employee access to only network systems, files, and programs that they need for their job?
- What kind of employee cybersecurity training do we have?
- What is our policy for employees working or accessing work data on their personal devices?
- Do we offer employees a 24/7 help working remotely?
- What is our password policy?

**NETWORK/CONNECTION**

- Who connects to our network from the outside and from the internet?
- How do we monitor for unauthorized users on devices on our network?
- Do we use Remote help services, antivirus software, firewalls, and intrusion detection and prevention services?
- What endpoint security do we have in place?
- Do we conduct vulnerability scans of the network?
- Do we have the ability to know we have an active attacker in our network?

**THIRD PARTY POLICIES**

- Do any third parties have access to our data?
- How do we vet the security of third party companies we use?
- Do we discuss cybersecurity risks and company policies when going into contact with other companies?

Copyright © 2017 Horsmouth, LLC. All Rights Reserved. Savvy Cybersecurity is a registered trademark of Horsmouth, LLC. All other trademarks are the property of their respective owners. Contact with your financial advisor for updates.

Teresa A. Samperton, CFP®, CPA  
Vice President  
Samperton Wealth Management  
123 Main Street  
12th Floor  
New York, NY 10010  
(212) 555-1111 x102  
sampsert@sampletonwealth.com  
www.sampletonwealth.com



**SAMPLETON**  
Wealth Management Group

Use the following topics and questions to guide a cybersecurity discussion with your security professionals and management team. The goal is to share information, identify systems and threats, and take action.

Copyright © 2017 Horsmouth, LLC. All Rights Reserved. Savvy Cybersecurity is a registered trademark of Horsmouth, LLC. All other trademarks are the property of their respective owners. Contact with your financial advisor for updates.

# Become a cybersecurity hero for your community like Jeanne, Tony, and Mike



# Take your first step:

- ✓ **Read** *Hack-Proof Your Life Now!*  
*The New Cybersecurity Rules*
- ✓ Then **join Savvy Cybersecurity**
- ✓ We're making advisors heroes every day!

**Learn more. Go to: [www.horsemouth.com/cyber](http://www.horsemouth.com/cyber)**