



***horseshmouth***®

# **Hacked! 5 Things Every Advisor Must Know About Cybersecurity**

**Presenter:**  
**Sean Bailey**  
**Editor in Chief**  
**Horseshmouth**

# Presentation Goals:

Overview: **The Growing Cyberthreat**

Survey: **Advisors and Cybersecurity**

Digital Life: **Anatomy of an Email Hack**

Action: **How to Make Clients Safer**

Introduction: **The Savvy Cybersecurity Program**

**Something Happened**

# CryptoWall

Decrypt service

https://kpai7ycr7jxqkulp.torexplorer.com/

**Your files are encrypted.**

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **12/05/14 - 21:37** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:


**103h 37m 58s**

Your system: Windows 7 (x64) First connect IP: [IP Address] Total encrypted 56 files.

Refresh Payment FAQ Decrypt 1 file for FREE Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

**How to buy CryptoWall decrypter?**

 **bitcoin**

- 1. You should register Bitcon wallet ([click here for more information with pictures](#))**
- 2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**  
**Here are our recommendations:**
  - [LocalBitcoins.com](#) - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
  - [How To Buy Bitcoins](#) - An international directory of bitcoin exchanges
  - [Cash Into Coins](#) - Recommended for fast, simple service.
  - [Coinbase](#) - Bitcoin exchange based in the United States. (Highly rated)
  - [BitStamp](#) - A multi currency bitcoin exchange based in Slovenia. (Highly rated)
  - [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
  - [anxpro.com](#)
  - [bitlycious.com](#)
  - [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

# Ransomware:

**“Malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key.”**

# The Growing Cyberthreat

# **144 Billion Spam Messages Sent Daily**

Source: Agari Phishing Study

**100,000 New Malware  
Samples Every Day**

Source: McAfee: State of Malware



**91.9 Million Records  
Exposed in 619 Data  
Breaches in 2013...**

Source: Identity Theft Resource Center

# **1.2 Billion Records Stolen by Russian Hackers**

# **1 in 3 Data Breach Victims Later Suffers From Identity Theft**

Source: Javelin Strategy and Research:  
2013 Identity Fraud Report

# **500,000 Children Are Affected by Identity Theft per Year**

Source: Child Identity Theft: What Every Parent  
Needs to Know by Robert Chappell Jr.

**Over \$1 Billion is  
Illegally Withdrawn From  
Skimming or Rigged  
ATMs Annually**

Source: US Secret Service

**50% of Passwords Are  
Considered Weak**

Source: Imperva's Report: Consumer  
Password Worst Practices

# **\$5 Billion Issued in Fraudulent Tax Returns in 2013**

Source: Audit by the Treasury Inspector  
General for Tax Administration)

**24% of PCs Are Not  
Protected by Up to Date  
Anti-Virus Software**

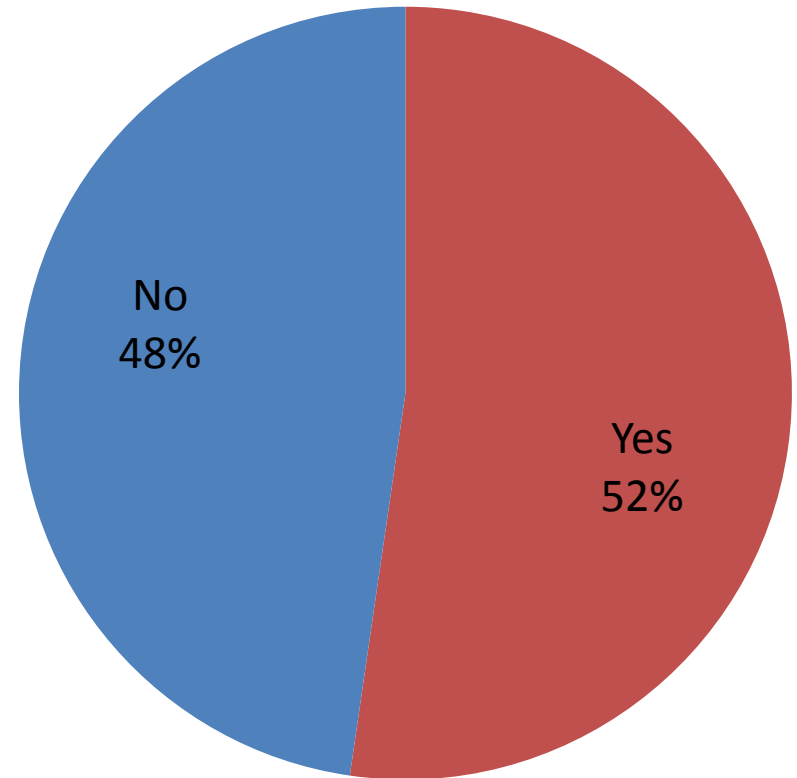
Source: Microsoft's Security Intelligence  
Report, Volume 14



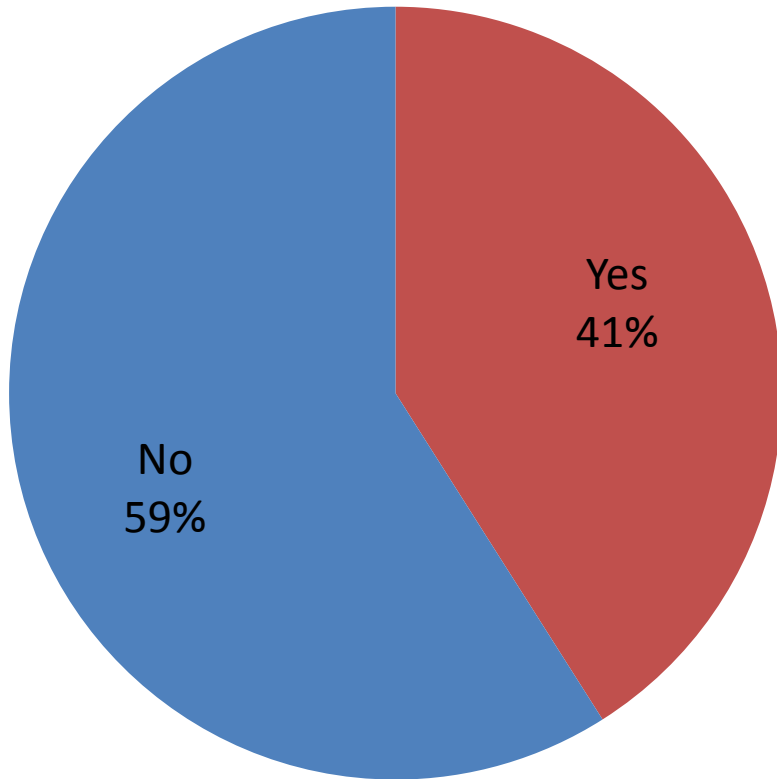
# Advisors and Cybersecurity

# Have any clients been fraud victims?

**More than half of advisors surveyed have had clients who suffered from fraud.**



# Have you suffered from fraud?

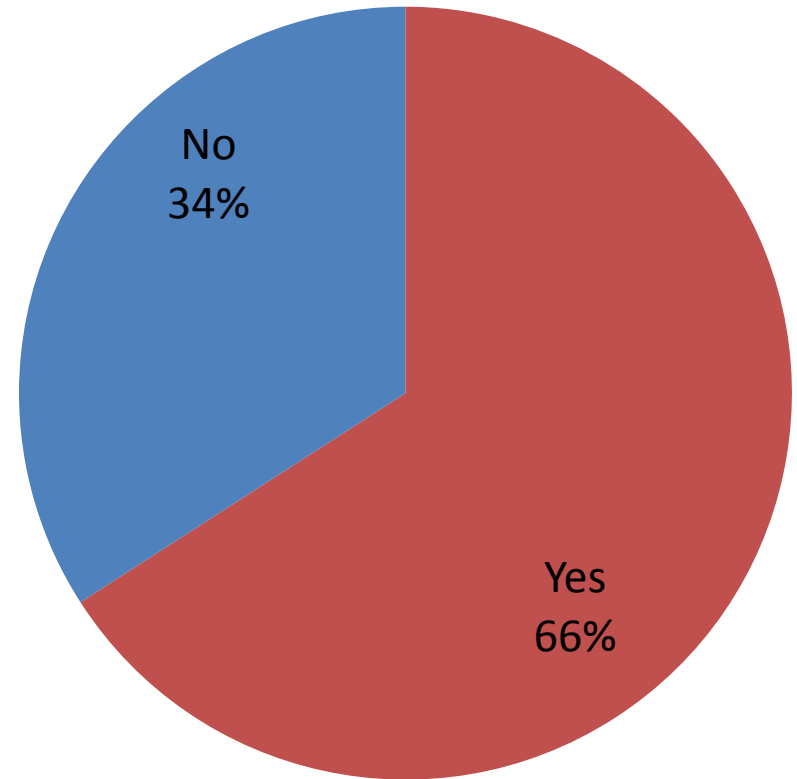


**However, the majority of advisors have not personally suffered from fraud.**



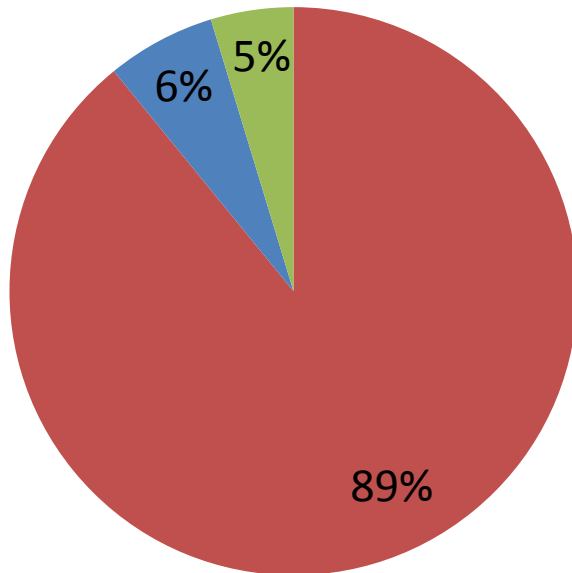
# Credit report checks

**Two-thirds of advisors encourage their clients to check their credit reports for fraud.**



# Advisors feelings about fraud

- I'm concerned for both myself and my clients.
- I'm concerned mostly for my clients.
- I'm not concerned about this issue.

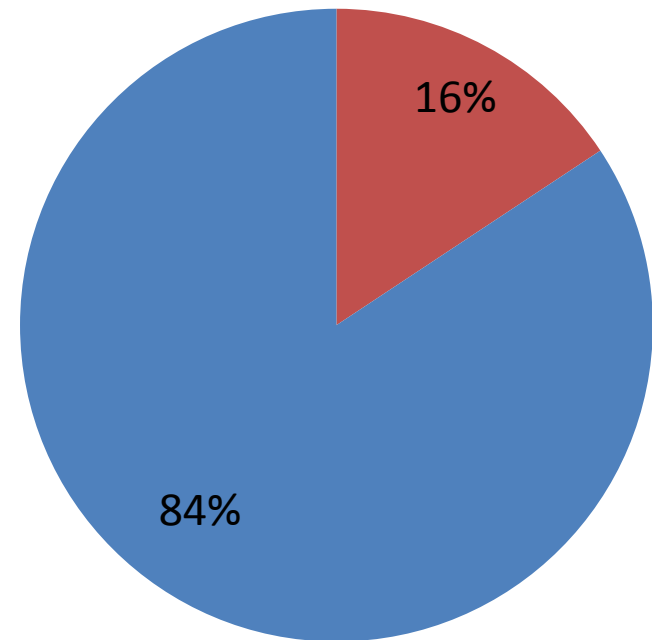


**The vast majority of advisors are worried about fraud for their clients, and also themselves.**

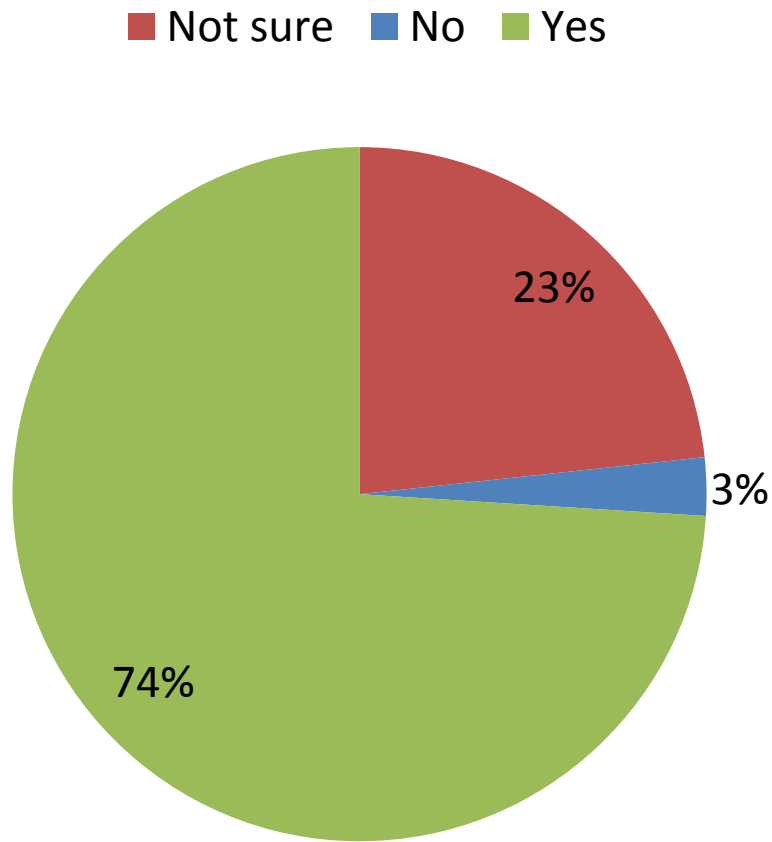
# Fraud presentations

**While the majority of advisors are concerned about fraud, 84% of advisors have not made a presentation about fraud to clients.**

- Have made fraud presentation
- Have not made fraud presentation



# Incorporating Fraud Education



**Three in four advisors believe that fraud protection and education should be an aspect of what they do.**

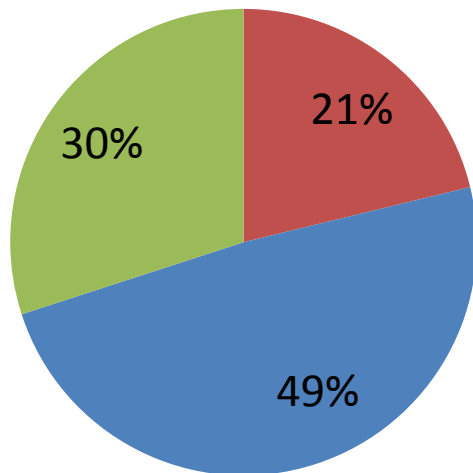


# Role Advisors Should Play



# Advisors' Level of Knowledge

- I know what to do to stay safe
- I feel safe but that feeling has been eroded in recent years
- I feel less safe and think I should do more to increase my security.

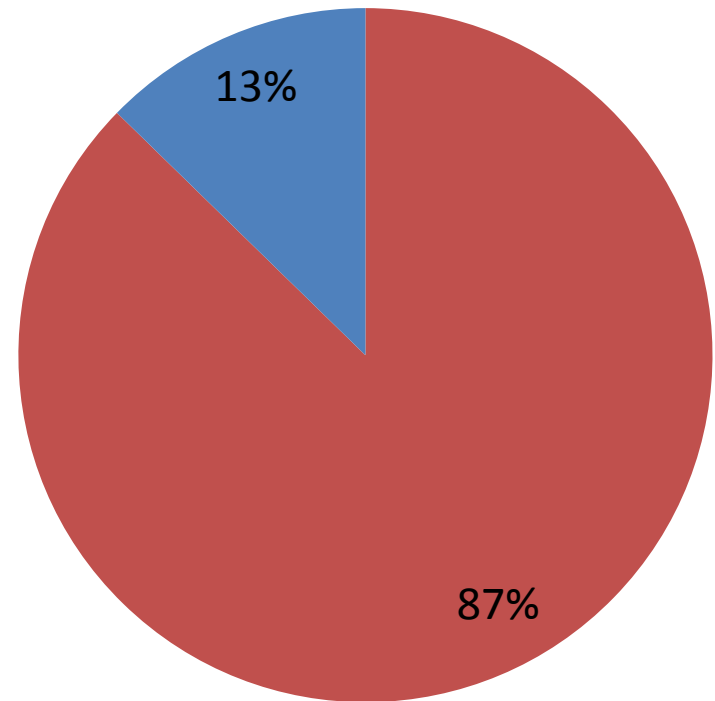


**About half of advisors surveyed feel safe but their confidence on the subject has decreased in recent years.**

# Protecting Clients' Data

**The majority of advisors surveyed do encrypt electronic files that contain clients' personal data.**

■ Encrypt files    ■ Do not encrypt files



# Advisors' Password Security

- 84% of advisors use one or more special characters in their key work passwords
- 21% use names of family members, city of birth, favorite team, or “password” as their password
- 17% of advisors use dictionary words as their work password
- 10% use consecutive numbers in their password

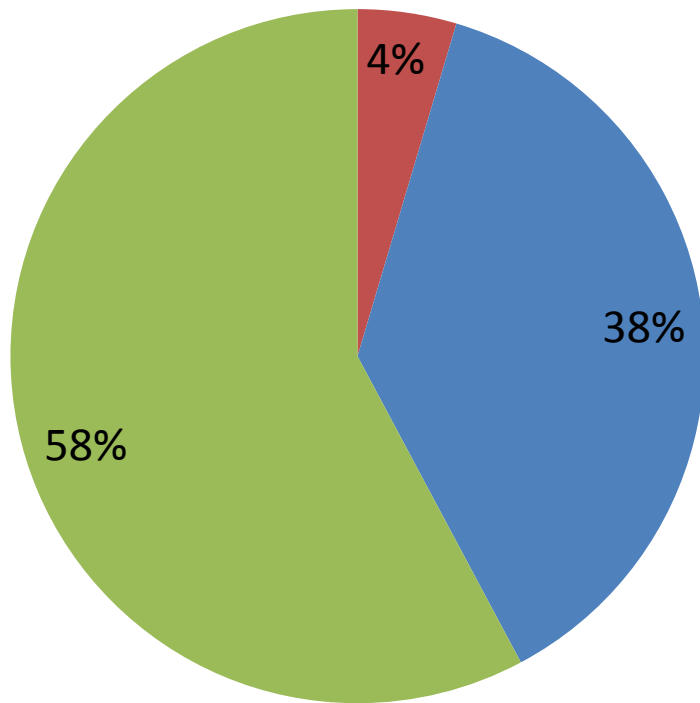
# Smartphone and Tablet Security

- About half of advisors store client contacts in their smartphone and 82% have a password on the opening screen of their phone.
- A quarter of advisors store client contacts on their tablet with 62% protected by a password on the opening screen.



# How Often Advisors Change Passwords

■ Never   ■ Occasionally   ■ Routinely



**More than half of advisors have a set pattern of when they change their passwords.**

# Personal Security Measures Taken by Advisors

- 86% use a shredder to discard personal financial statements
- 57% review their credit file once a year
- 13% use verbal passcodes for some or all bank/credit card accounts
- 12% have a locked credit file

# **Digital Life: Anatomy of an Email Hack**



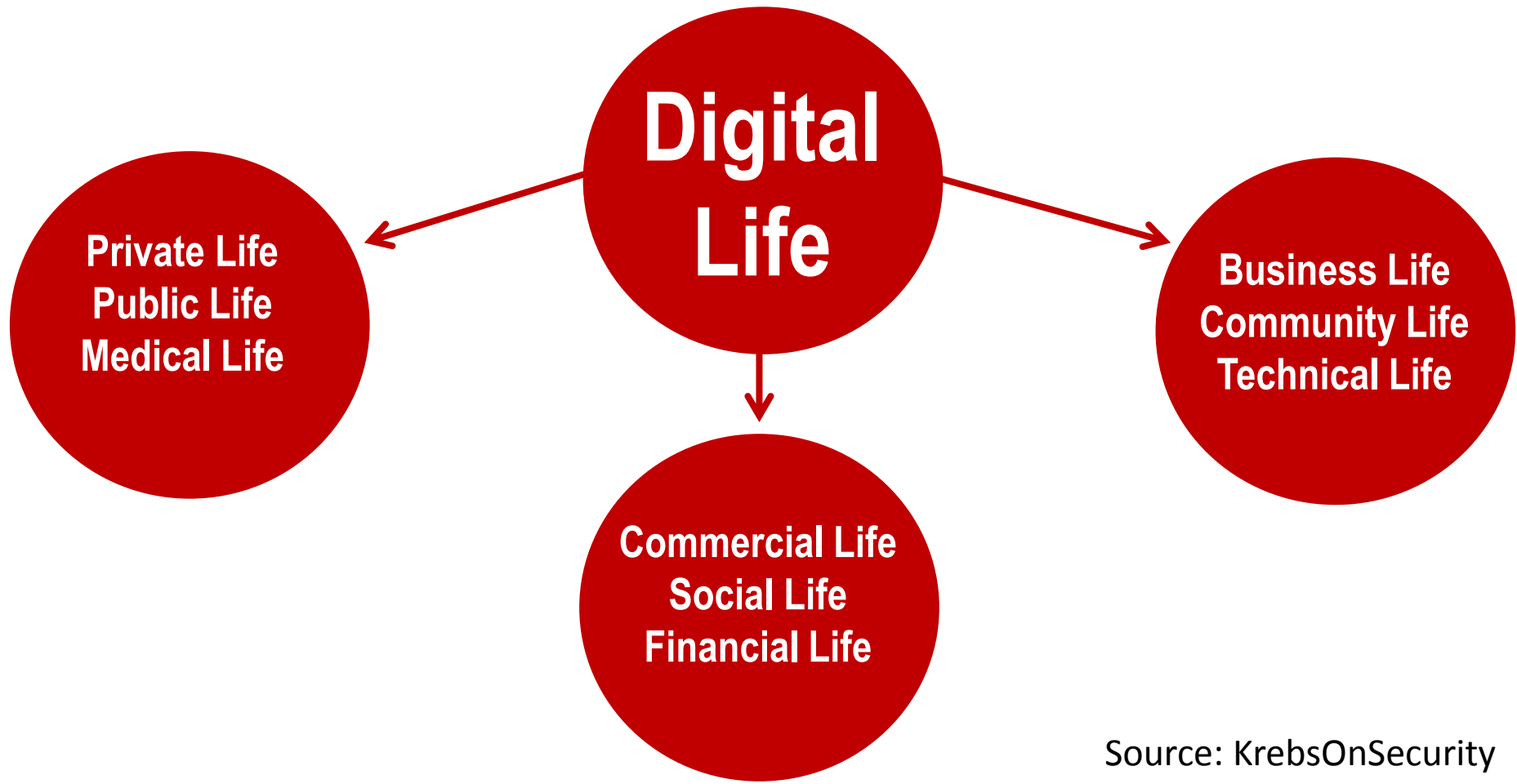
**“It has been said that if you own a person’s email, you own the person. This means that once your email is hacked, pretty much your entire digital life is up for grabs...”**

**- Robert Siciliano, CEO of [IdentityTheftSecurity.com](http://IdentityTheftSecurity.com)**

**“...So even if you’ve done your due diligence to have all your passwords be different, if your email is hacked and it is associated with your other online accounts, the hacker could simply use a reset password and get access to all your other accounts.”**

**- Robert Siciliano, CEO of [IdentityTheftSecurity.com](http://IdentityTheftSecurity.com)**

# Your Digital Life: More Than Just Money



# You've Been Hacked!



**Private  
Life**

- Correspondences
- Names
- Addresses
- Phone numbers
- Emails
- Birthdates
- Passwords
- Appointments
- Calendars
- Photos
- Recordings
- Videos

# You've Been Hacked!



**Public  
Life**

- Affiliations
- Support of causes/organizations
- Donations
- Petitions
- Discussion comments
- Posts and Likes
- Web history

# You've Been Hacked!



**Commercial  
Life**

- Amazon
- Airlines
- E-Bay
- UPS/Fed-Ex
- Walmart
- iTunes
- Netflix
- Skype
- Cellphone
- Google
- Dropbox
- Evernote
- LinkedIn
- Mileage & Points accounts

# You've Been Hacked!



**Social  
Media**

- Facebook
- Twitter
- Instagram
- Pinterest
- Flickr
- YouTube
- LinkedIn
- Monster
- Disqus

# You've Been Hacked!



**Financial  
Life**

- Checking
- Savings
- Debit
- Direct Deposit
- Credit Card
- PayPal
- Insurance
- Loans
- Mortgage



# You've Been Hacked!



**Medical  
Life**

- Doctors
- Medical tests
- Drugs/prescriptions/medications
- Health insurance
- Dental
- Appointments
- Health card numbers

# You've Been Hacked!



## Commercial Life

- Business contacts
- Emailed or forwarded company documents
- Meeting notes
- Customers/clients
- Competitors
- Competitive intelligence
- Credit
- CRM
- Expense reports
- Travel
- Purchases
- Employee reviews
- Salary records
- Secret/sensitive files
- Network access
- Contacts
- Business plans

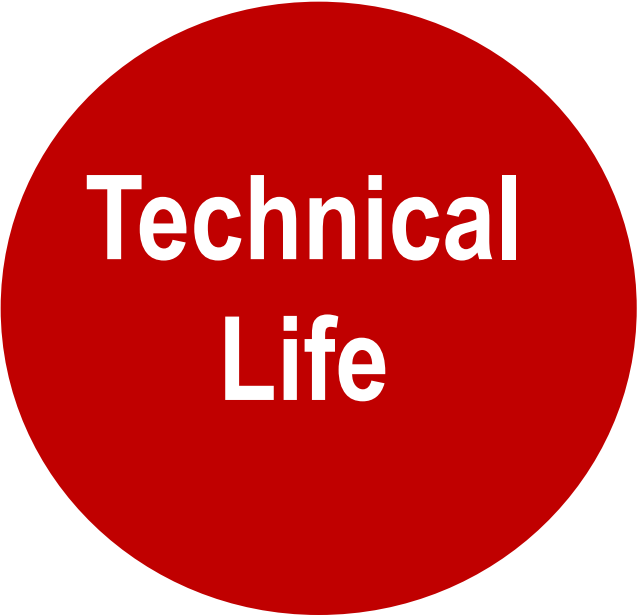
# You've Been Hacked!



**Community  
Life**

- Executive leadership
- Donations
- Contributors
- Meeting minutes
- Strategic documents
- Volunteers
- Capital plans
- Endowment
- Staff contacts
- Correspondence
- Financials

# You've Been Hacked!



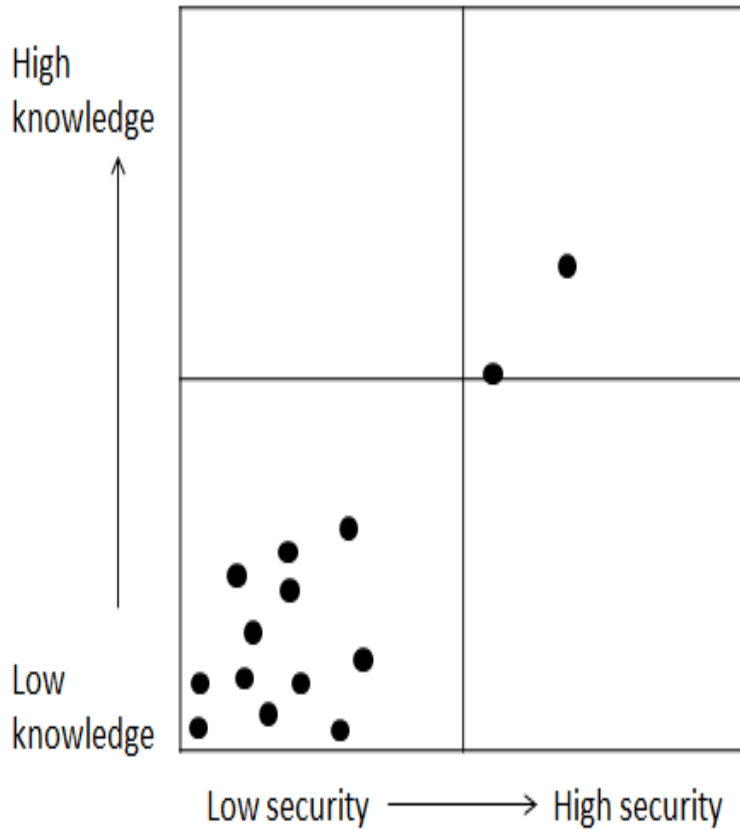
**Technical  
Life**

- Software keys
- File hosting
- Network info
- Wireless passwords
- Cloud accounts

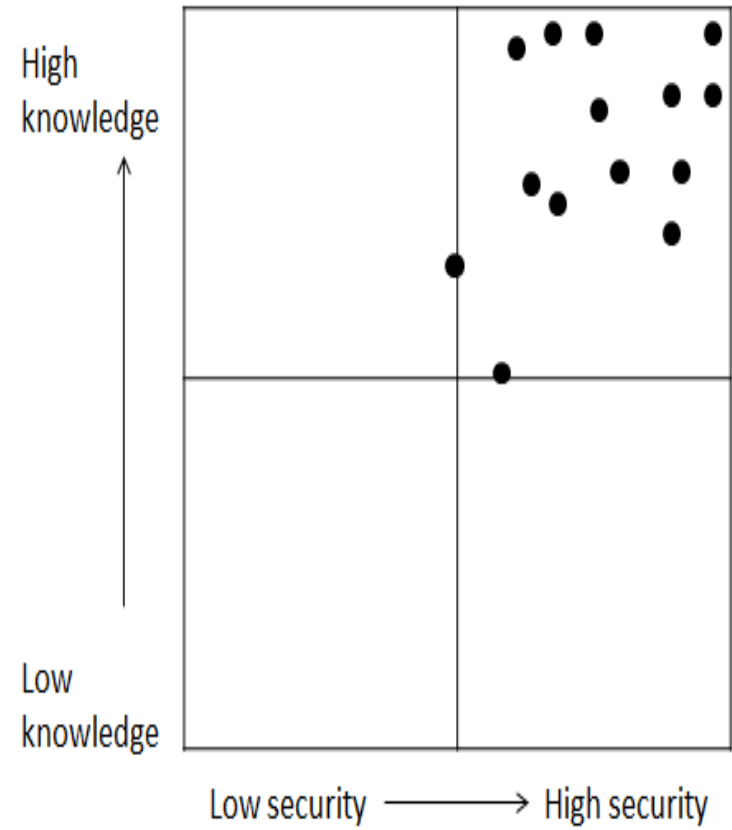
# How to Make Your Clients Safer

**This is the Challenge**

# Before



# After



**People Need Someone  
to Guide Them to Be  
More Secure**



**89% of Advisors  
Concerned About  
Themselves and Clients**

**84% of Advisors Have  
Never Made a Client  
Presentation on Fraud  
Dangers**

**74% of Advisors Believe  
Fraud Protection/  
Education Should Be a  
Part of What They Do for  
Clients**

**Challenge: How to  
Effectively Shift Clients  
from Low Security to  
High Security**

# **Strategy: Interactive Cybersecurity Presentation**

**1 Hour to Savvy Cybersecurity:  
10 Threats Every Person and  
Business Faces—and How to  
Fight Them**

# How It Works

**Clients Measure Their  
Own Cybersecurity  
Score...**



# Savvy Cybersecurity,<sup>TM</sup> Quick Reference Guide, 2015

Teresa S. Sampleton, CFP®, CLU ChFC, CLTC  
Vice President  
Sampleton Wealth Management Group

123 Main Street  
12th Floor  
New York, NY 10018

(212) 555-1111 ext. 10  
tsampleton@sampletonwealth.com

www.sampletonwealth.com



**SAMPLETON**  
Wealth Management  
Group

## A. Scorecard

Answer Yes or No to the following questions. When complete, follow the instructions at bottom to get your raw score.

Topic	Question	Yes	No	Score
<b>CREDIT REPORTS:</b>	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.			15 pts
<b>SOCIAL MEDIA:</b>	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.			5 pts
<b>COMPUTER/LAPTOP:</b>	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up to date versions of Java, Flash, and Adobe.			10 pts
<b>BUSINESS ID THEFT:</b>	My employer trains its staff on business or personal cybersecurity measures.			5 pts
<b>WI-FI:</b>	I know how to determine if FREE public Wi-Fi is safe to use.			10 pts
<b>HACKED DEVICES:</b>	My smartphone and/or tablet has a security passcode.			5 pts
<b>PASSWORDS:</b>	I have enabled two-factor authentication on my key accounts that allow it.			15 pts
<b>SKIMMING:</b>	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.			5 pts
<b>DATA BREACH:</b>	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction			15 pts
<b>PHISHING:</b>	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.			15 pts
Circle 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

>100-85	GOOD
84-60	OKAY
59-0	DANGER
Consult the Checklist in Section C. to identify key items to include in your Action Plan now.	

## C. Checklist

Action	Time	Points
<b>Principle #1: Devices</b>		
<input type="checkbox"/> Create a passcode for smartphone and tablet.	2 min	4 pts
<input type="checkbox"/> Install "Locate My Device" or "Find My Phone" app in case device is lost or stolen.	1 min	1 pt
<b>Principle #2: Software</b>		
<input type="checkbox"/> Update all software on your home laptop/computer.	5 min	10 pts
<b>Principle #3: Wi-Fi</b>		
<input type="checkbox"/> Secure home Wi-Fi network by changing default password and name.	20 min	10 pts
<b>Principle #4: Passwords</b>		
<input type="checkbox"/> Change weak passwords to strong and secure passwords.	5 min	4 pts
<input type="checkbox"/> Passwords don't include names, birthdates, pets' names, etc.	Always	1 pt
<input type="checkbox"/> Passwords include nonconsecutive numbers and symbols.	Always	1 pt
<input type="checkbox"/> Change passwords every six months.	Always	1 pt
<input type="checkbox"/> Use a mnemonic device to create password.	5 min	5 pts
<input type="checkbox"/> Consider password storage system.	Always	2 pts
<b>Principle #5: Transactions</b>		
<input type="checkbox"/> Sign up for text/email alerts for debit/credit card.	2 min	10 pts
<b>Principle #6: Credit</b>		
<input type="checkbox"/> Sign up for credit freeze.	20 min	15 pts
<b>Principle #7: E.M.A.I.L.</b>		
<input type="checkbox"/> Examine emails carefully before clicking, sharing, or visiting links.	Always	15 pts
<b>Additional Cybersecurity Actions</b>		
<b>Document Safe</b>		
<input type="checkbox"/> Put personal documents in a safe place.	2 min	1 pt
<input type="checkbox"/> Shred documents with personal information before throwing them out.	1 min	2 pts
<input type="checkbox"/> Give out Social Security number when necessary. Question why needed.	Always	2 pts
<b>Social Media Safe</b>		
<input type="checkbox"/> Strengthen Facebook and other social media privacy settings.	5 min	2 pts

## A. Scorecard

Answer Yes or No to the following questions. When complete, follow directions at bottom to get your raw score.

Topic	Question	Yes/No	Score
<b>CREDIT REPORTS:</b>	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.		15 pts
<b>SOCIAL MEDIA:</b>	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.		5 pts
<b>COMPUTER/ LAPTOP:</b>	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up to date versions of Java, Flash, and Adobe.		10 pts
<b>BUSINESS ID THEFT:</b>	My employer trains its staff on business or personal cybersecurity measures.		5 pts
<b>WI-FI:</b>	I know how to determine if FREE public Wi-Fi is safe to use.		10 pts
<b>HACKED DEVICES:</b>	My smartphone and/or tablet has a security passcode.		5 pts
<b>PASSWORDS:</b>	I have enabled two-factor authentication on my key accounts that allow it.		15 pts
<b>SKIMMING:</b>	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.		5 pts
<b>DATA BREACH:</b>	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction		15 pts
<b>PHISHING:</b>	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.		15 pts
<b>Circle points for each question answered with a Yes. Add points to get score. Consult section B to get your cybersecurity rating.</b>		<b>Raw Score:</b>	

# Cybersecurity Scorecard

Y/N

**Credit:** I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.

## A. Scorecard

Answer Yes or No to the following questions. When complete, follow directions at bottom to get your raw score.

Topic	Question	Yes/No	Score
<b>CREDIT REPORTS:</b>	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.	N	15 pts
<b>SOCIAL MEDIA:</b>	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.		5 pts
<b>COMPUTER/ LAPTOP:</b>	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up to date versions of Java, Flash, and Adobe.		10 pts
<b>BUSINESS ID THEFT:</b>	My employer trains its staff on business or personal cybersecurity measures.		5 pts
<b>WI-FI:</b>	I know how to determine if FREE public Wi-Fi is safe to use.		10 pts
<b>HACKED DEVICES:</b>	My smartphone and/or tablet has a security passcode.		5 pts
<b>PASSWORDS:</b>	I have enabled two-factor authentication on my key accounts that allow it.		15 pts
<b>SKIMMING:</b>	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.		5 pts
<b>DATA BREACH:</b>	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction		15 pts
<b>PHISHING:</b>	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.		15 pts
Circle points for each question answered with a Yes. Add points to get score. Consult section B to get your cybersecurity rating.		<b>Raw Score:</b>	

# **Demonstration of Threat #4**

## Threat #4:

# Your Passwords Are Weak, Easily Hacked

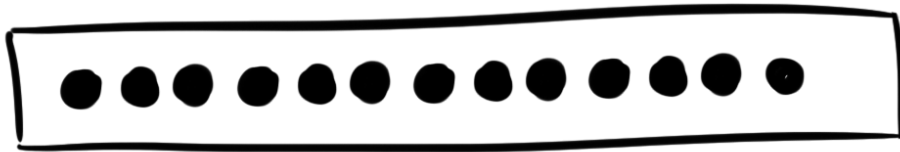
- 50 percent of all passwords considered weak
- Common, weak passwords: “123456” or “password”
- Others: birthdates, names, pet names, team names



# Response:

# Use Strong Passwords and Change Frequently

Password



- Include letters, numbers and symbols/characters
- Change passwords every six months
- Add two-factor authentication
- Password managers

# Password-Safe Tip: Use a Mnemonic Phrase



- Create strong password with 1 letter per word
- Ex: prayer, poem, lyric or phrase
- Knock out letters, replace with symbols
- Ex: “Jack and Jill went up the hill to fetch a pail of water.” becomes: J&Jw^thtf@p0w



# Goal-Setting Passwords

Run everyday → Run3v3ryd@y

Eat more fruit → 3@t>fru1t

No more soda → N0m0r3s0d@

Save for house → \$@v34h0u\$3

Get outside → G3t@0ut\$!d3



# Savvy Cybersecurity Action: Passwords

- **Estimated Time:** 5 minutes
- **Estimated Cost:** Free

Login

Username:

Password:

# Savvy Cybersecurity Alert



**SAVVY CYBERSECURITY**

21 West 38th Street, 14th Fl. New York, NY 10018 phone: (888) 336-6884 ext.1 [www.horsemouth.com](http://www.horsemouth.com)

**Russian Hack 17 Times Bigger Than Target Data Breach—All Must Change Passwords Now.**

**New Ways to Think About Passwords: Mnemonic and Goal-Setting—Try Them Out!**

Dear Devin,

This is your first Savvy Cybersecurity Alert. When you joined, we promised we'd send you occasional "alert" emails when something really big happens. Now it has.

As you may have seen in the headlines today, an unknown group of Russian hackers has compromised the security of more than 420,000 websites and has collected more than 1.2 billion unique records of people's usernames and passwords. That number is 17 times larger than the Target breach last fall which covered 70 million records.

**In our judgment, you and your clients are at serious risk.**

Here's what we recommend: Immediately reset passwords on your email, financial, e-commerce accounts (Amazon, Netflix, iTunes, etc.), and any other accounts that would give hackers insights into your life, such as social media accounts, etc.

# SAVVY CYBERSECURITY



## Mnemonic device

Use a mnemonic device to create your password. Here's how to do it step-by-step.

1. Pick a phrase you're fond of and can easily recall such as a prayer, poem, pledge, song, or quote.
2. Start your new password by taking the first letter of each word of your phrase. So, the phrase "The harder you work, the luckier you get" becomes: thywtlyg.
3. Now swap some letters and punctuation with some symbols and two upper case letters: Thyw@Tlyg.
4. Then supercharge it by bracketing the phrase with a meaningful number in your life that is not your birthday or Social Security number. So the date April 13, 2003 is added this way and then you get: 04Thyw@Tlyg2003 as the very strong password.
5. The numbers, uppercases, and symbols elevate the strength of the password.

# SAVVY CYBERSECURITY



## Goal Setting Password

Here's a password type that is actually fun to type over and over. Turn your password into a goal you are trying to achieve. Try this:

- Pick a goal you want to achieve. Remember, it could be anything: lose weight, eat better, find a new job, save for a new purchase—anything. For example, if you want to start running every day, you'd start with this goal: I will run every day.
- Turn your goal into one word: "iwillruneveryday."
- Now add an uppercase letter and swap out the letters E and A with the number 3 and the symbol @. It becomes: "Iwillrun3v3ryd@y"
- Make it even stronger by inserting a meaningful number that is not your Social or birth date.

# SAVVY CYBERSECURITY

SAVVY  
CYBERSECURITY  
Marketing Toolkit

Cybersecurity and  
Identity Theft:  
15 Threats You Must  
Against Now

horsesmouth

04Thyw@Tlyg2003

Partial Date    Upper-Case    Comma    Upper-Case    Partial Date

A diagram showing the email address '04Thyw@Tlyg2003' with lines connecting it to labels for its parts: '04' is labeled 'Partial Date', 'Thyw' is labeled 'Upper-Case', '@' is labeled 'Comma', 'Tlyg' is labeled 'Upper-Case', and '2003' is labeled 'Partial Date'.

# SAVVY CYBERSECURITY



## Password Symbol Conversion Chart

Password Symbol Conversion Chart	
Change this...	To this.
At	@
For	4
To, Too, Two	2
S	\$
I	1 or !
E	3
A	4 or @
O	0
And	&
Example phrases made into passwords	
Run everyday	Run3v3ryd@y
Eat more fruit	3@t>fru1t
Sleep at 11	\$l33p@11pm
Bring own lunch	BrIng0wnlunch!
No more soda	N0m0r3s0d@
Save for house	\$@v34h0u\$3
Get outside	G3t@0ut\$lD3

# **Back to the Demonstration**



# 1 Hour to Savvy Cybersecurity:

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

Advisor Name

Advisor Practice Name

DISCLAIMERS

**Have You  
Ever Worried  
About  
Being Hacked?**



# The Unseen Cyber Attack You Face Each Day



- 52 trillion emails sent each year
- 144 billion each day
- 90% of all email is spam

# Evolving Cybersecurity Attacks

<b>Early 2000s</b>	<b>Today</b>
<ul style="list-style-type: none"><li>• Mostly malicious</li></ul>	<ul style="list-style-type: none"><li>• Malicious, criminal, espionage, warfare, terrorism</li></ul>
<ul style="list-style-type: none"><li>• Done for sport and notoriety</li></ul>	<ul style="list-style-type: none"><li>• Done for variety of motives</li></ul>
<ul style="list-style-type: none"><li>• Amateurs</li></ul>	<ul style="list-style-type: none"><li>• Amateurs, professionals, governments</li></ul>

Source: Craig Mundie, Microsoft

# Mind-Boggling Array of Terms

*HEARTBLEED*

PHISHING

*Malware*

Attack

GAMEOVER ZEUS

Juicing

*Zero Day*

*SPEAR  
PHISHING*

CRYPTOWALL

*Virus*

“We Should Be  
Super-Worried.”

*--Craig Mundie, Microsoft*



# U.S. Cyber Command Formed as Part of U.S. Strategic Command



“The cyberthreat is one of the most serious economic and national security challenges we face as a nation.”

-Obama in 2009

# Banks Dreading Computer Hacks Call for Cyber War Council

—Bloomberg News, July 2014



- Account balances *converted to zeros*
- Fear of bank runs
- No plan or protection in place



# Cybercrime and Business

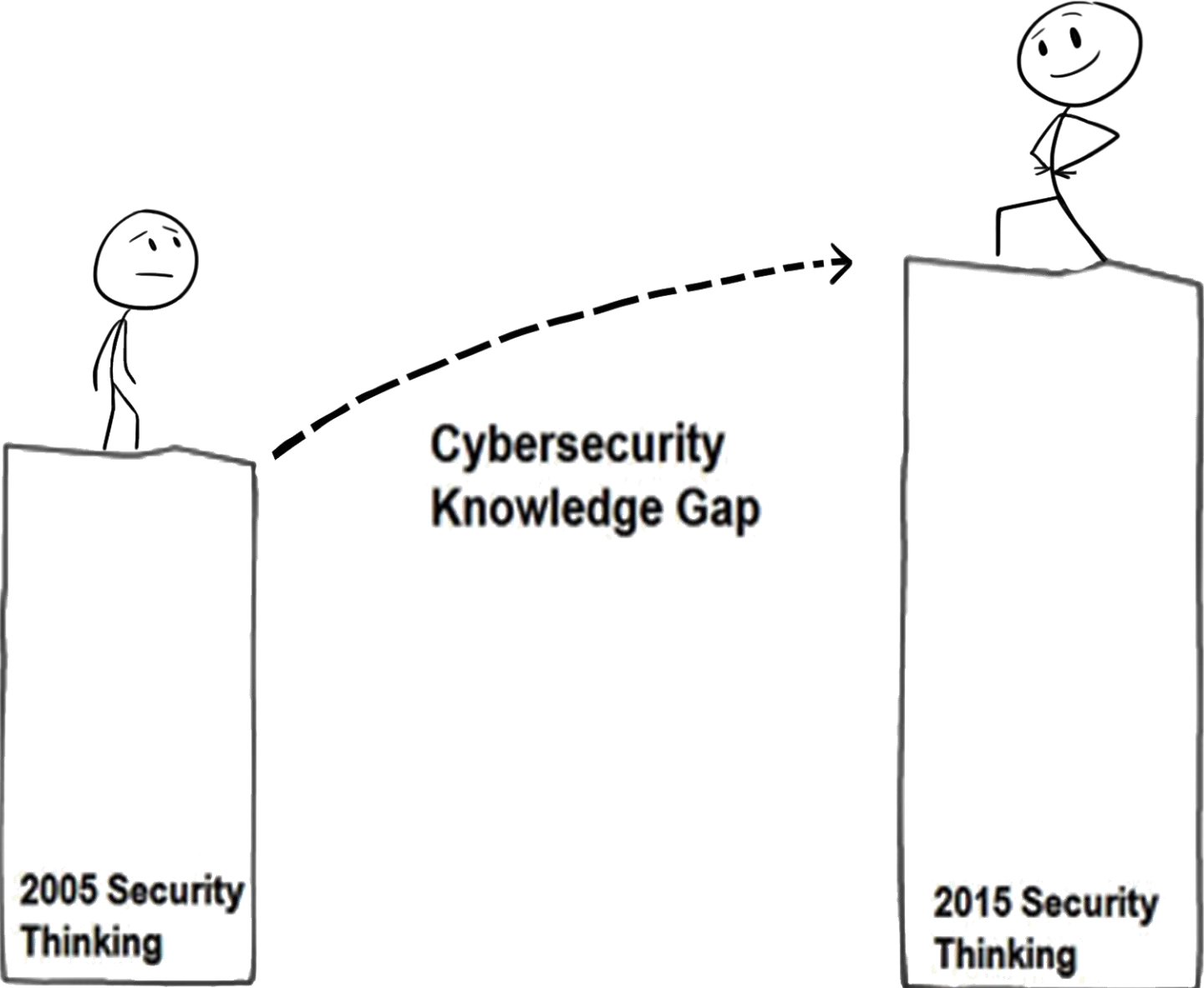
**NC Bank Sues Cyberheist Victim to Recover Funds**

**Wash. Hospital Hit By \$1.03 Million Cyberheist**

***Missouri Court Rules Against \$440,000 Cyberheist Victim***

**Attack on Bank Hid \$900,000 Cyberheist**

# Cybersecurity Knowledge Gap



# **Another Presentation Excerpt**

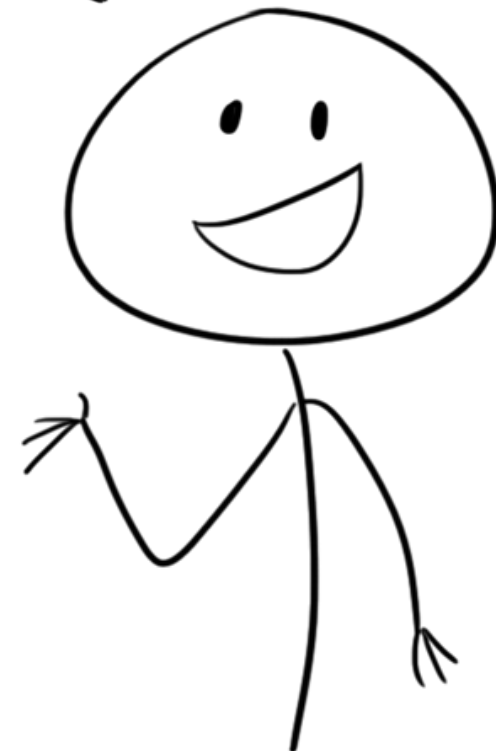
# How to Boost Your Cybersecurity



# This Is the Challenge



**How It Works**



# Sample Savvy Cybersecurity Reference Guide

## Savvy Cybersecurity,<sup>SM</sup> Quick Reference Guide, 2015

Teresa S. Sampleton, CFP®, CLU, ChFC, CLTC  
Vice President  
Sampleton Wealth Management Group  
123 Main Street  
12th Floor  
New York, NY 10018  
(212) 555-1111 ext. 10  
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 rating.		
Topic	Question	Points
CREDIT REPORTS	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.	10 pts
SOCIAL MEDIA	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.	5 pts
COMPUTER/LAPTOP	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up to date versions of Java, Flash, and Adobe.	10 pts
BUSINESS ID THEFT	My employer trains its staff on business or personal cybersecurity measures.	5 pts
WI-FI	I know how to determine if FREE public Wi-Fi is safe to use.	10 pts
HACKED DEVICES	My smartphone and/or tablet has a security password.	5 pts
PASSWORDS	I have enabled two-factor authentication on my key accounts that allow it.	10 pts
SKIMMING	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.	5 pts
TEXT BREACH	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction.	15 pts
PHISHING	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.	15 pts
Circle points for each question answered with a Yes. Add points to get score. Consult Section B to get your cybersecurity rating.		
B. Rating		
>100-85	GOOD	
84-60	OKAY	
59-0	DANGER	
Consult the Checklist in Section C, to identify key items to include in your Action Plan now.		

C. Checklist		
Action	Time	Points
<b>Principle #1: Devices</b>		
<input type="checkbox"/> Create a password for smartphone and tablet.	2 min	4 pts
<input type="checkbox"/> Install "Locate My Device" or "Find My Phone" app in case device is lost or stolen.	1 min	1 pt
<b>Principle #2: Software</b>		
<input type="checkbox"/> Update all software on your home laptop/computer.	5 min	10 pts
<b>Principle #3: Wi-Fi</b>		
<input type="checkbox"/> Secure home Wi-Fi network by changing default password and name.	20 min	10 pts
<b>Principle #4: Passwords</b>		
<input type="checkbox"/> Change weak passwords to strong and secure passwords.	5 min	4 pts
<input type="checkbox"/> Passwords don't include names, birthdates, pets' names, etc.	Always	1 pt
<input type="checkbox"/> Passwords include nonconsecutive numbers and symbols.	Always	1 pt
<input type="checkbox"/> Change passwords every six months.	Always	1 pt
<input type="checkbox"/> Use a mnemonic device to create password.	5 min	5 pts
<input type="checkbox"/> Consider password storage system.	Always	2 pts
<b>Principle #5: Transactions</b>		
<input type="checkbox"/> Sign up for text/email alerts for debit/credit card.	2 min	10 pts
<b>Principle #6: Credit</b>		
<input type="checkbox"/> Sign up for credit freezes.	20 min	15 pts
<b>Principle #7: E.M.A.I.L.</b>		
<input type="checkbox"/> Examine emails carefully before clicking, sharing, or visiting links.	Always	15 pts
<b>Additional Cybersecurity Actions</b>		
<b>Document Safe</b>		
<input type="checkbox"/> Put personal documents in a safe place.	2 min	1 pt
<input type="checkbox"/> Shred documents with personal information before throwing them out.	1 min	2 pts
<input type="checkbox"/> Give out Social Security number when necessary. Question why needed.	Always	2 pts
<b>Social Media Safe</b>		
<input type="checkbox"/> Strengthen Facebook and other social media privacy settings.	5 min	2 pts

Copyright © 2014 HomeSouth, LLC. All Rights Reserved.

HomeSouth is an independent organization providing unique, unbiased insight into the critical issues facing financial advisors and their clients. HomeSouth, LLC is not affiliated with the reprint licensee or any of its affiliates.

Check with your financial advisor for updates.

# Partial Savvy Cybersecurity Scorecard

<b>HACKED DEVICES:</b>	My smartphone and/or tablet has a security passcode.	<i>Y</i>	5 pts
<b>PASSWORDS:</b>	I have enabled two-factor authentication on my key accounts that allow it.	<i>N</i>	15 pts
<b>SKIMMING:</b>	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.	<i>N</i>	5 pts
<b>DATA BREACH:</b>	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction	<i>N</i>	15 pts
<b>PHISHING:</b>	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.	<i>N</i>	15 pts
<b>Circle points for each question answered with a Yes. Add points to get score. Consult section B to get your cybersecurity rating.</b>			<b>Raw Score:</b> 25



# Your Cybersecurity Rating

## B. Rating

>100-85

GOOD

84-60

OKAY

59-0

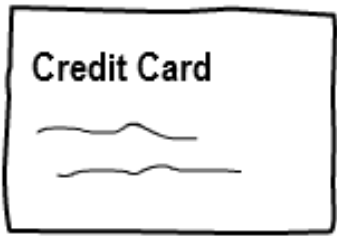
DANGER

Consult the Checklist in Section C. to identify key items to include in your Action Plan now.

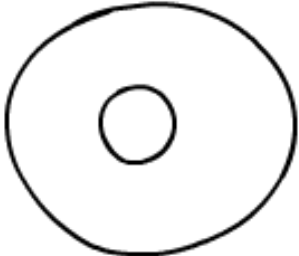
# Principles of Savvy Cybersecurity



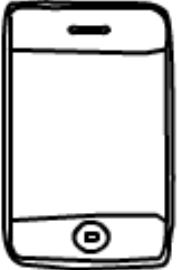
**TRANSACTIONS**



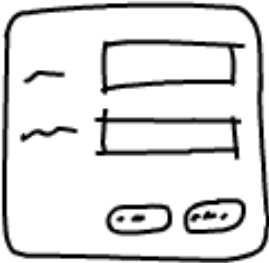
**CREDIT**



**SOFTWARE**



**DEVICES**



**PASSWORDS**



**Wi-Fi**



**E.M.A.I.L.**

# Partial Cybersecurity Checklist

<b>C. Checklist</b>			
	<b>Action</b>	<b>Time</b>	<b>Points</b>
<b>Principle #1: Devices</b>			
<input type="checkbox"/>	Create a passcode for smartphone and tablet.	2 min	4 pts
<input type="checkbox"/>	Install "Locate My Device" or "Find My Phone" app in case device is lost or stolen.	1 min	1 pt
<b>Principle #2: Software</b>			
<input type="checkbox"/>	Update all software on your home laptop/computer.	5 min	10 pts
<b>Principle #3: Wi-Fi</b>			
	Secure home Wi-Fi network by changing default password and name.	20 min	10 pts
<b>Principle #4: Passwords</b>			
<input type="checkbox"/>	Change weak passwords to strong and secure passwords.	5 min	4 pts
<input type="checkbox"/>	Passwords don't include names, birthdates, pets' names, etc.	Always	1 pt
<input type="checkbox"/>	Passwords include nonconsecutive numbers and symbols.	Always	1 pt
<input type="checkbox"/>	Change passwords every six months.	Always	1 pt
<input type="checkbox"/>	Use a mnemonic device to create password.	5 min	5 pts
<input type="checkbox"/>	Consider password storage system.	Always	2 pts
<b>Principle #5: Transactions</b>			
<input type="checkbox"/>	Sign up for text/email alerts for debit/credit card.	2 min	10 pts
<b>Principle #6: Credit</b>			
<input type="checkbox"/>	Sign up for credit freeze.	20 min	15 pts
<b>Principle #7: E.M.A.I.L.</b>			
<input type="checkbox"/>	Examine emails carefully before clicking, sharing, or visiting links.	Always	15 pts

# Your Action Plan

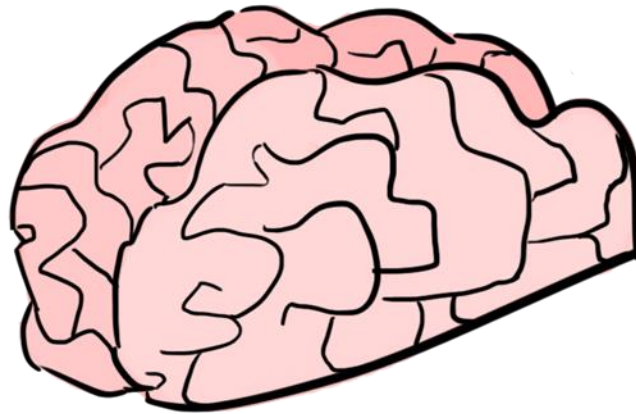
D. Action Plan	
I commit to taking the following steps to boost my cybersecurity by this date: 8/3/14	
①	<i>Update all software on computer/laptop.</i>
②	<i>Set up text alerts for debit card.</i>
③	<i>Request and review copy of credit report.</i>
Signature:	<i>Joe Smith</i>

**Sign and date your Action Plan commitment for best results.**

# Savvy Cybersecurity Countdown: Top 10 Threats



# Your Brain and Cybersecurity



# The Two Sides of Security

“Security is both a feeling and a reality. **And they’re not the same.**”

- Bruce Scheiner

- 1.: Feelings
- 2,: Reality



# Problem:

## You can **FEEL SECURE** even though **YOU ARE NOT**.

“Our feeling of security diverges from the reality of security, and **we get things wrong.**”

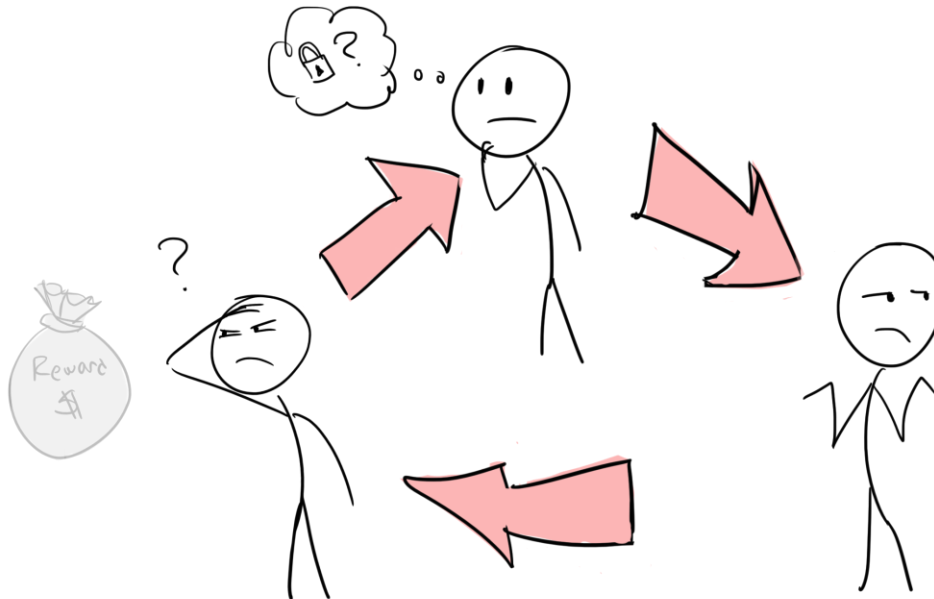
- Bruce Schneier





# Psychology of Security Disconnect

1. People don't think they're at risk (Optimism Bias).
2. People are unmotivated.
3. Security is invisible and unrewarded.



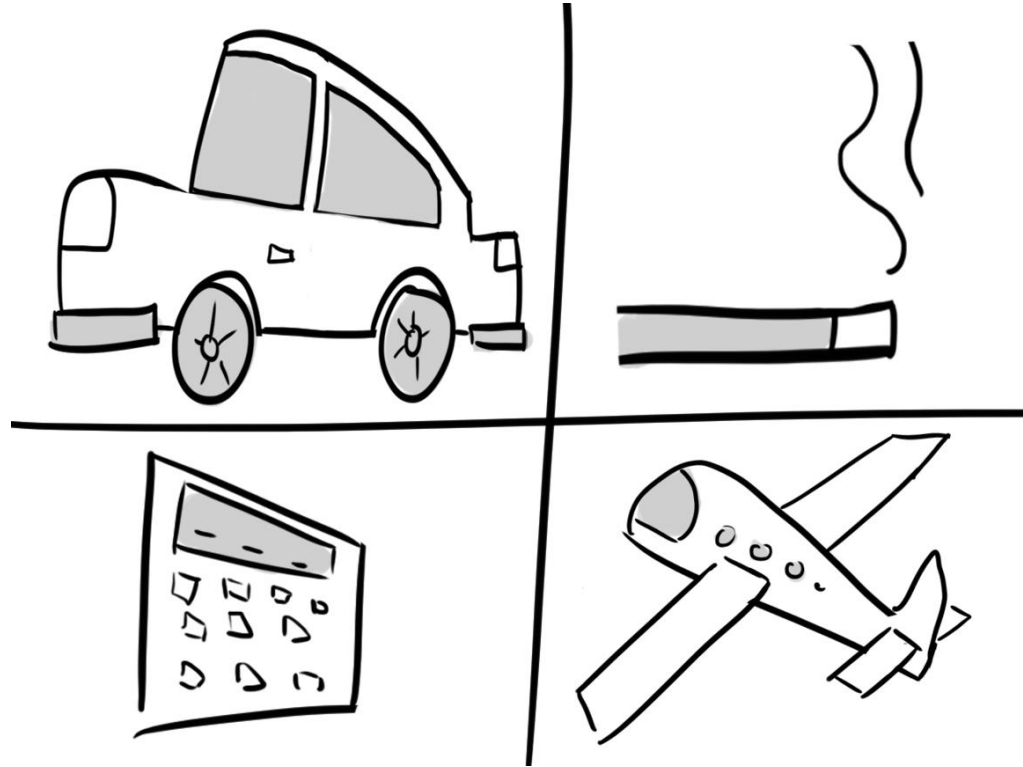
# Judging Risk: What's the Trade-off?

- How severe is it?
- How likely is it?
- How big is the possible damage?
- How effective are the countermeasures?
- How much can I risk?

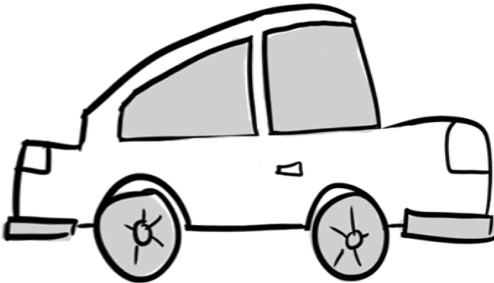


# Security Trade-offs of the Past

- **Smoking:** filters, warnings, bans
- **Homes:** locks, alarms, webcams
- **Cars:** seat belts, air bags, driverless?

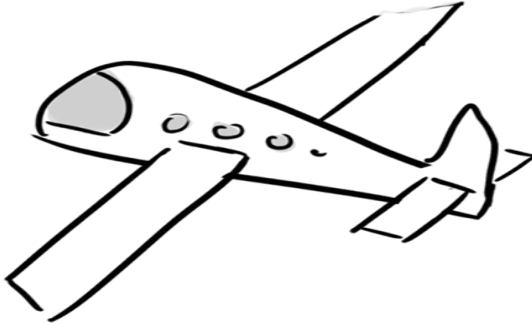


# Irrational Security Tradeoffs



Driving: 40,000 killed

VS



Flying: hundreds killed

VS



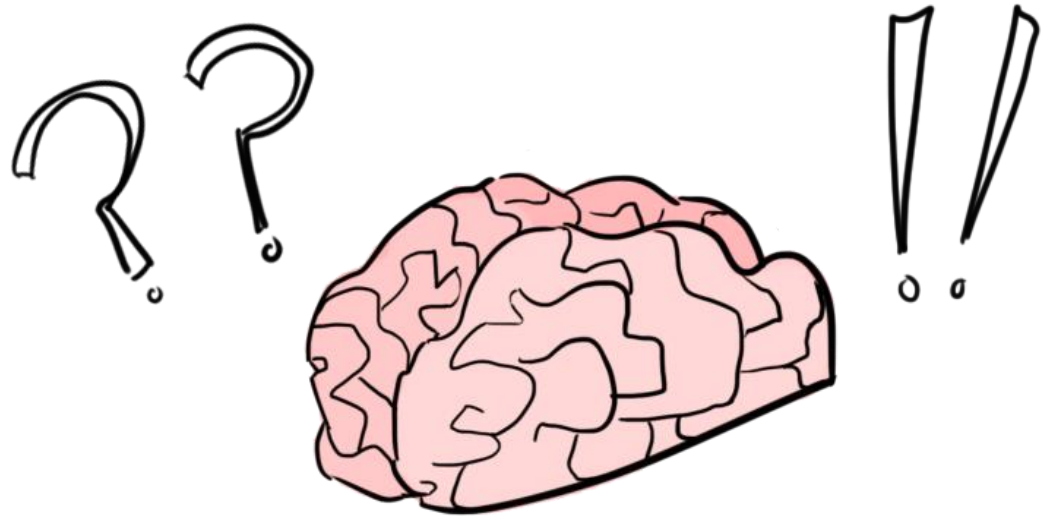
Al Queda terrorist



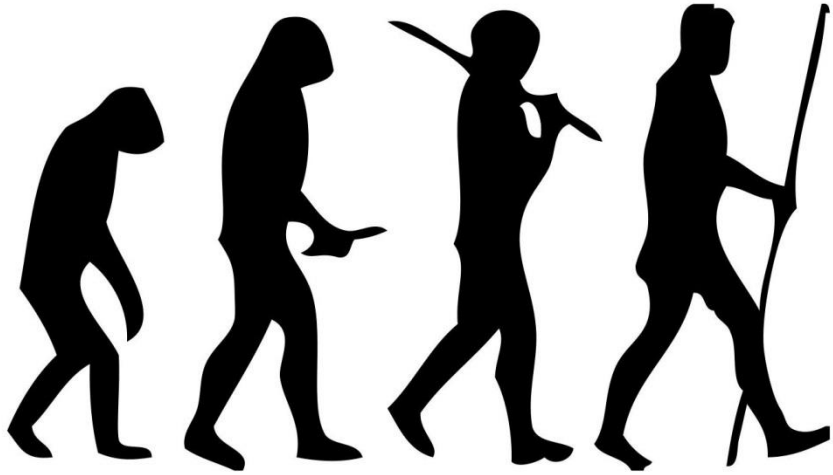
Burgular

# 2 Brain Systems for Reacting to Risk

- Primitive, intuitive system (amygdala)
- Advanced analytic system (neocortex)



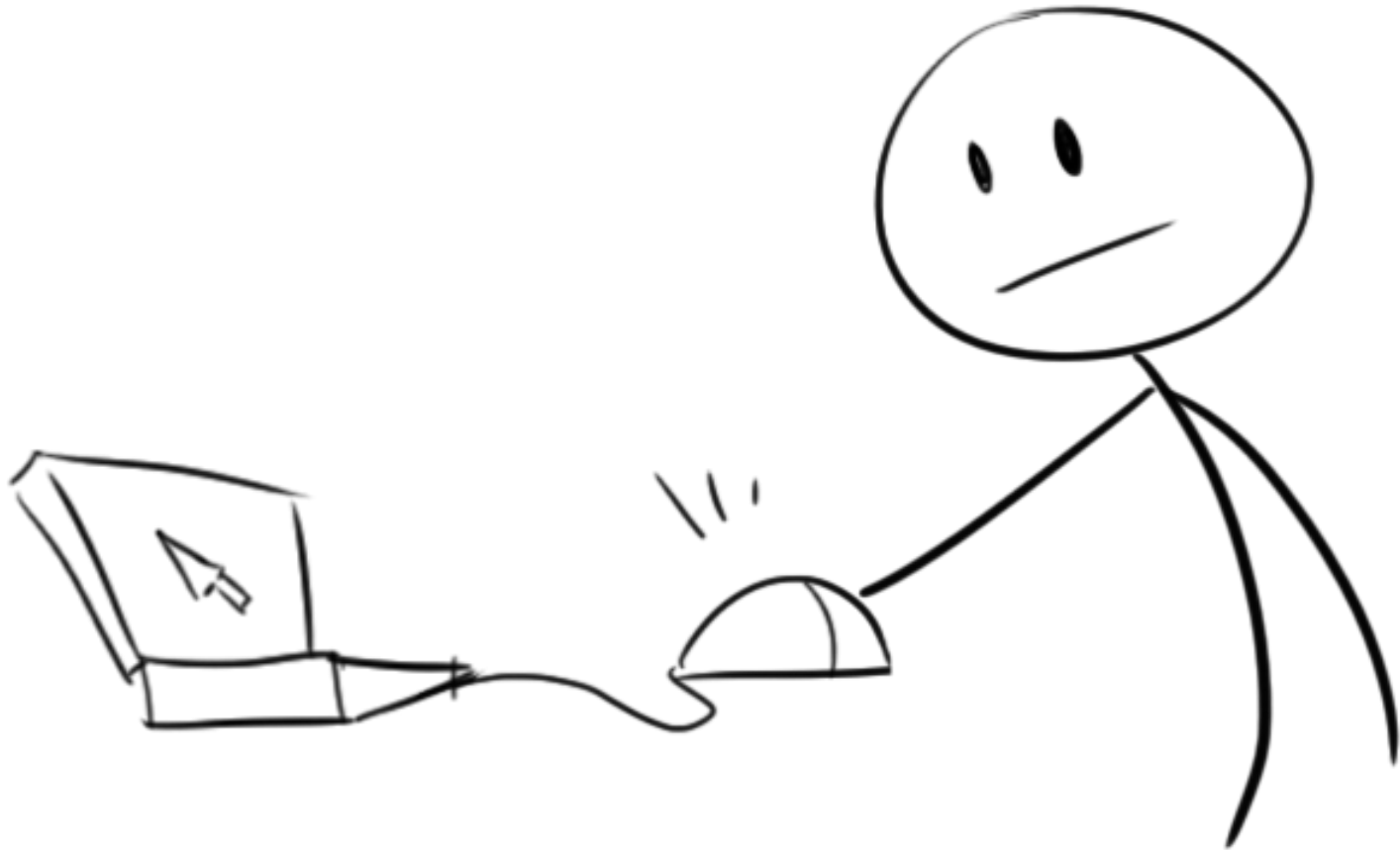
# Failure of Our Perception of Risk



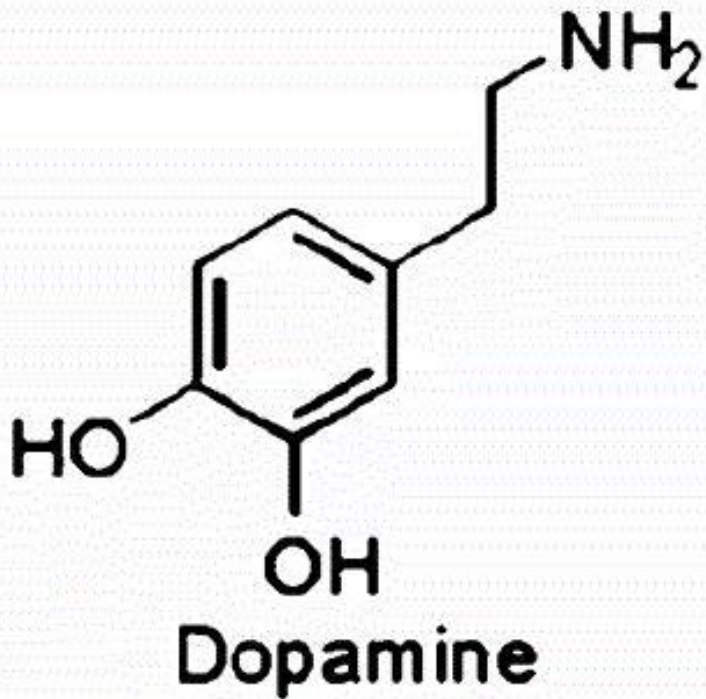
New problems have occurred at a faster rate than evolution...

We face situations today that didn't exist in the world of 10,000 BC.

# Cybersecurity and the Click



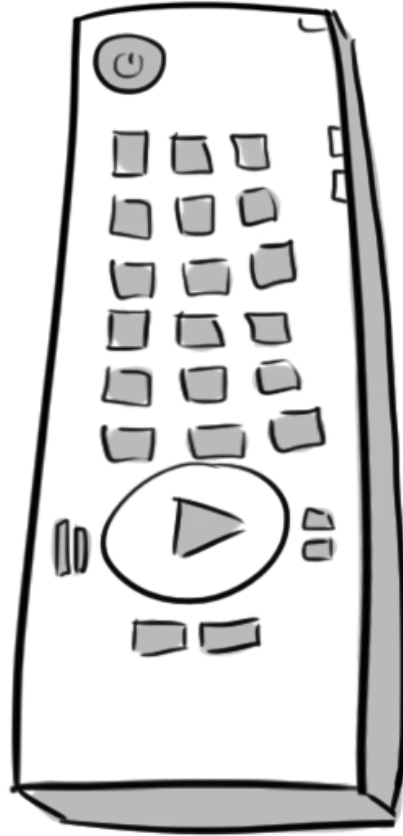
# Your Brain and Dopamine



- Critical to brain function
- Causes us to want, desire, seek out, and search
- Makes us curious about ideas and fuels our searching for information

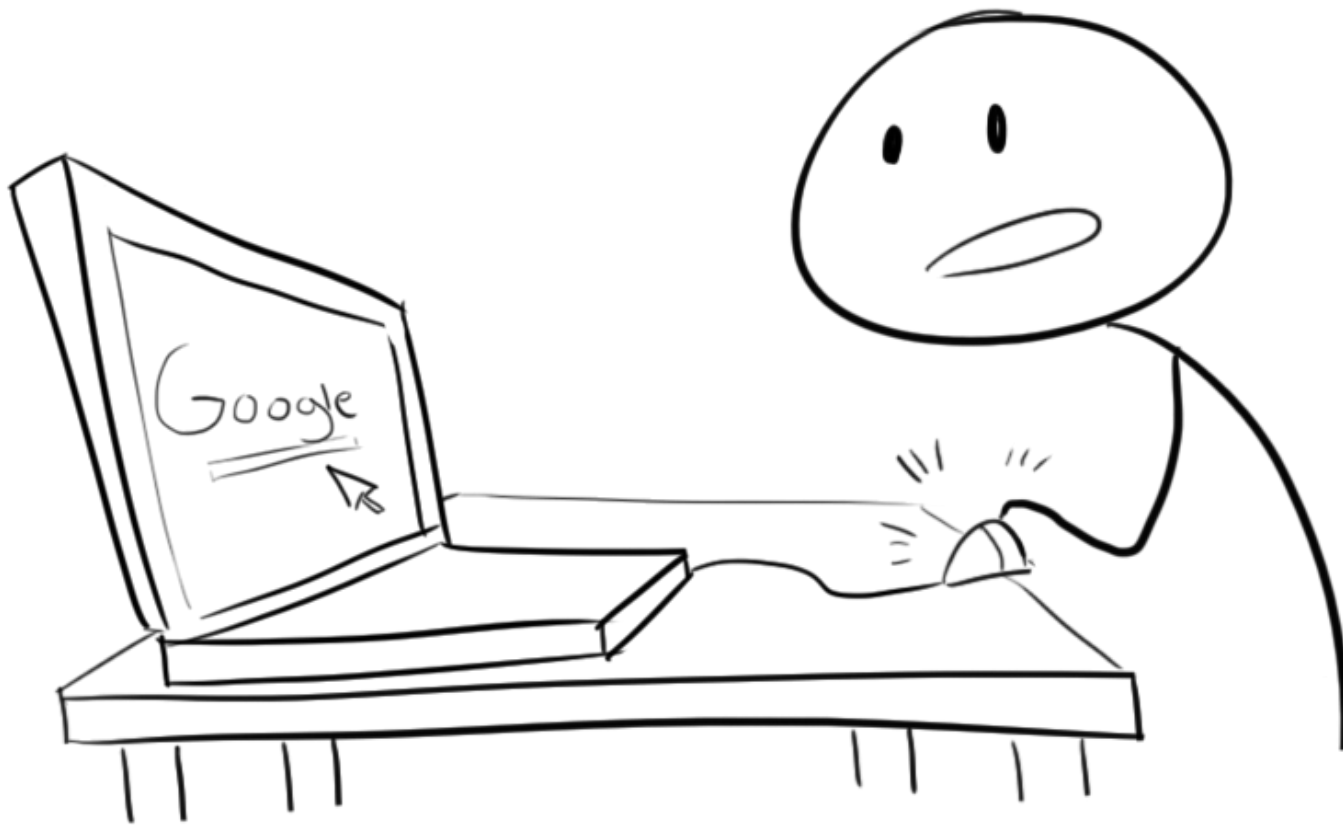


# The Age of Clicking



The TV remote: Technology's first dopamine delivery device .

# The Computer and the Click



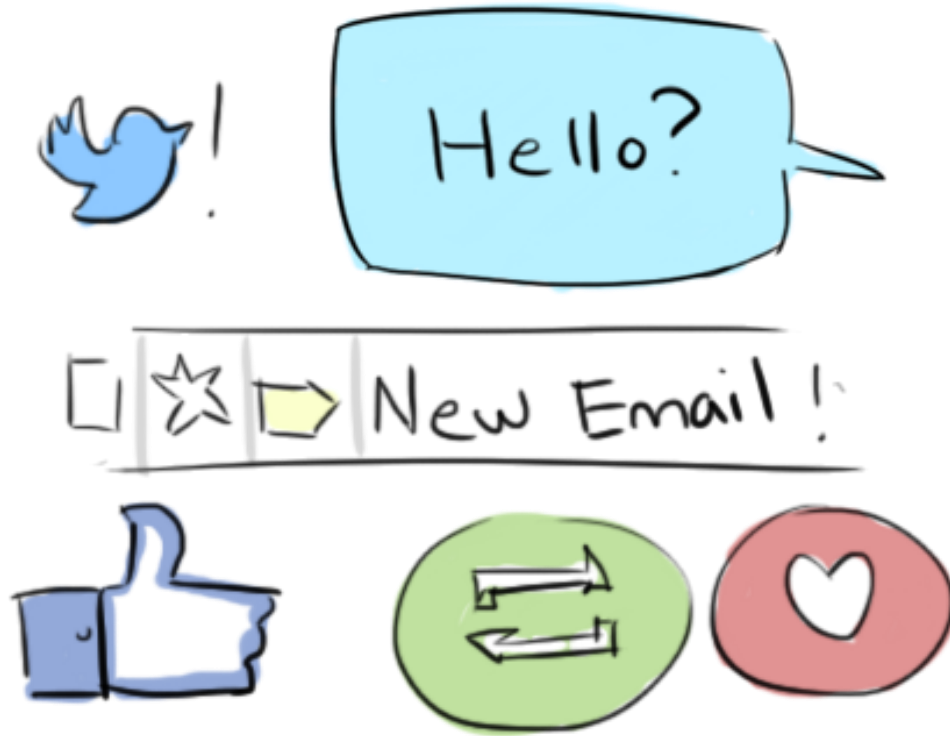
# On Dopamine and Google Searches

“The dopamine system does not have satiety built into it...It can lead us to irrational wants, excessive wants we'd be better off without.

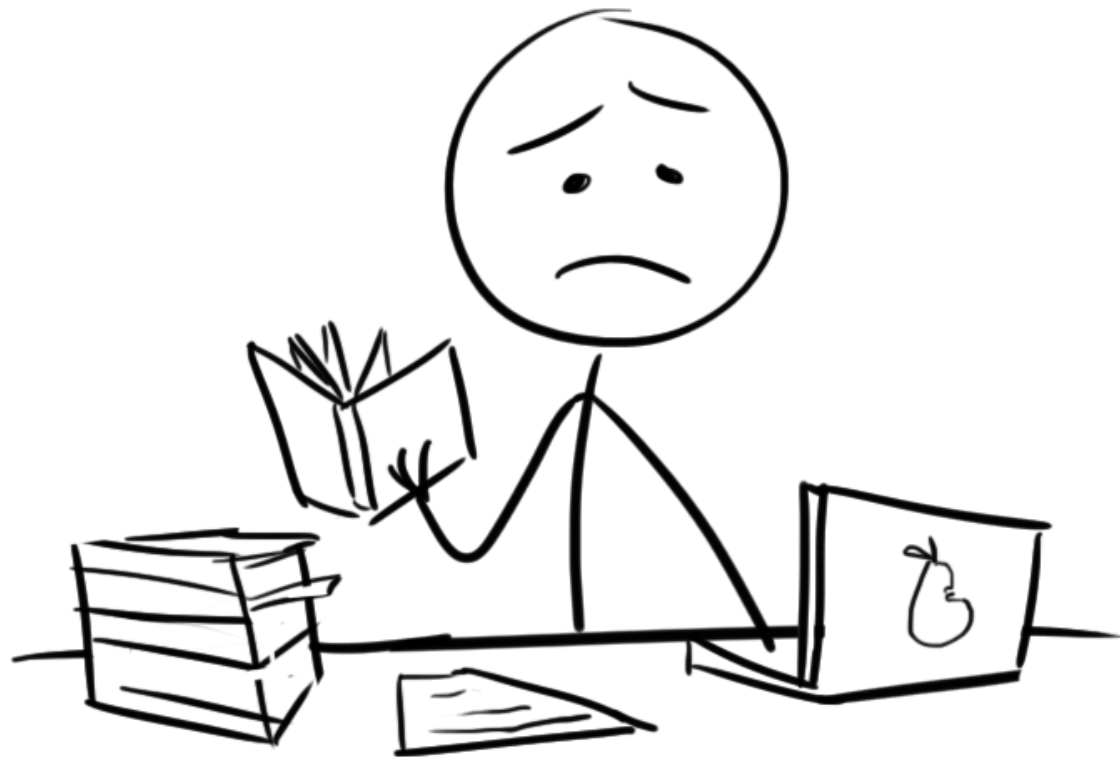
“So we find ourselves letting one Google search lead to another...As long as you sit there, the consumption renews the appetite.”

- Kent Berridge, professor of psychology, University of Michigan

# Gadgets: the New Dopamine Delivery Device

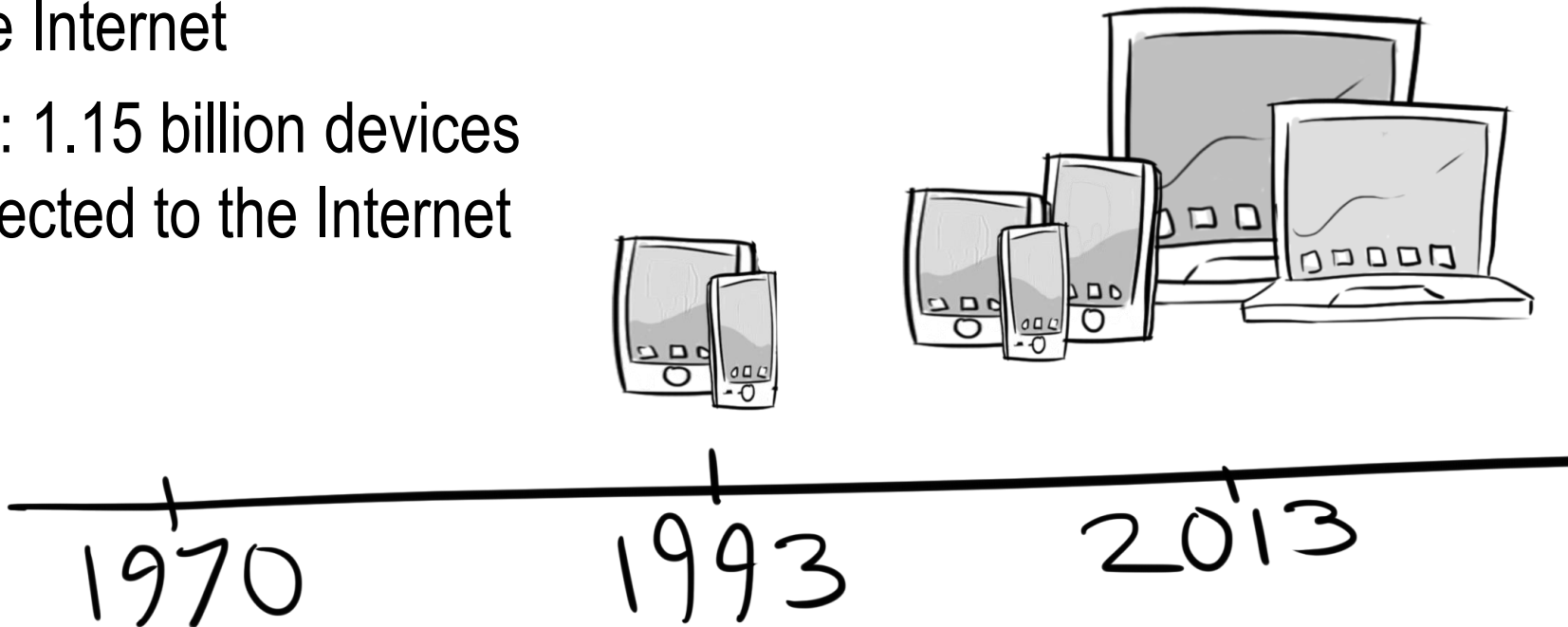


# Clicking and the Fatigue Factor



# More Devices, More Clicking, More Points of Entry for Cybercriminals

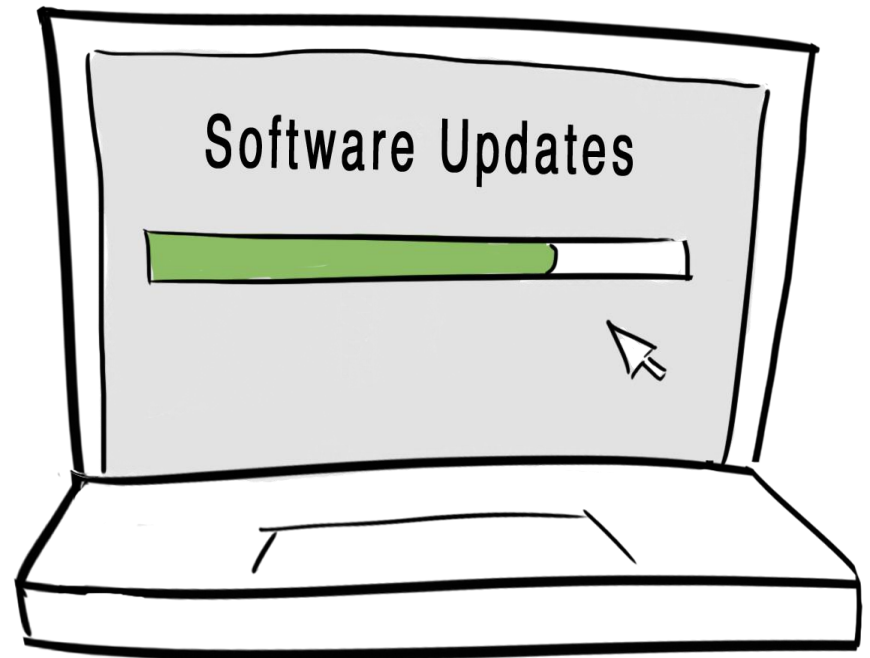
- **1970s:** Zero
- **1993:** 2 million connected to the Internet
- **2013:** 1.15 billion devices connected to the Internet



# **First Step to Security**

# Clean and Update Your Computer First...

- Before taking steps to increase your security on your computers/devices you must:
  - Run anti-virus and anti-malware scans
  - Update all software and programs

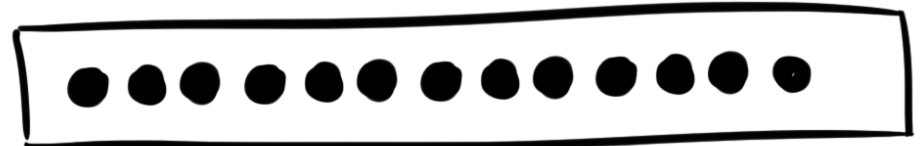




# Then Tackle Passwords

- Ensure there is no malware running in the background of your device
- Then, change your passwords and add other security measures such as 2-factor authentication

Password



**LIFELock**

# Lifelock vs. Savvy Cybersecurity

- Lifelock costs \$100-\$329/year
- You can do everything they offer yourself for a much smaller fee
- Lifelock's \$1 million guarantee— doesn't account for time, stress, and emotional damage



# Lifelock vs. Savvy Cybersecurity

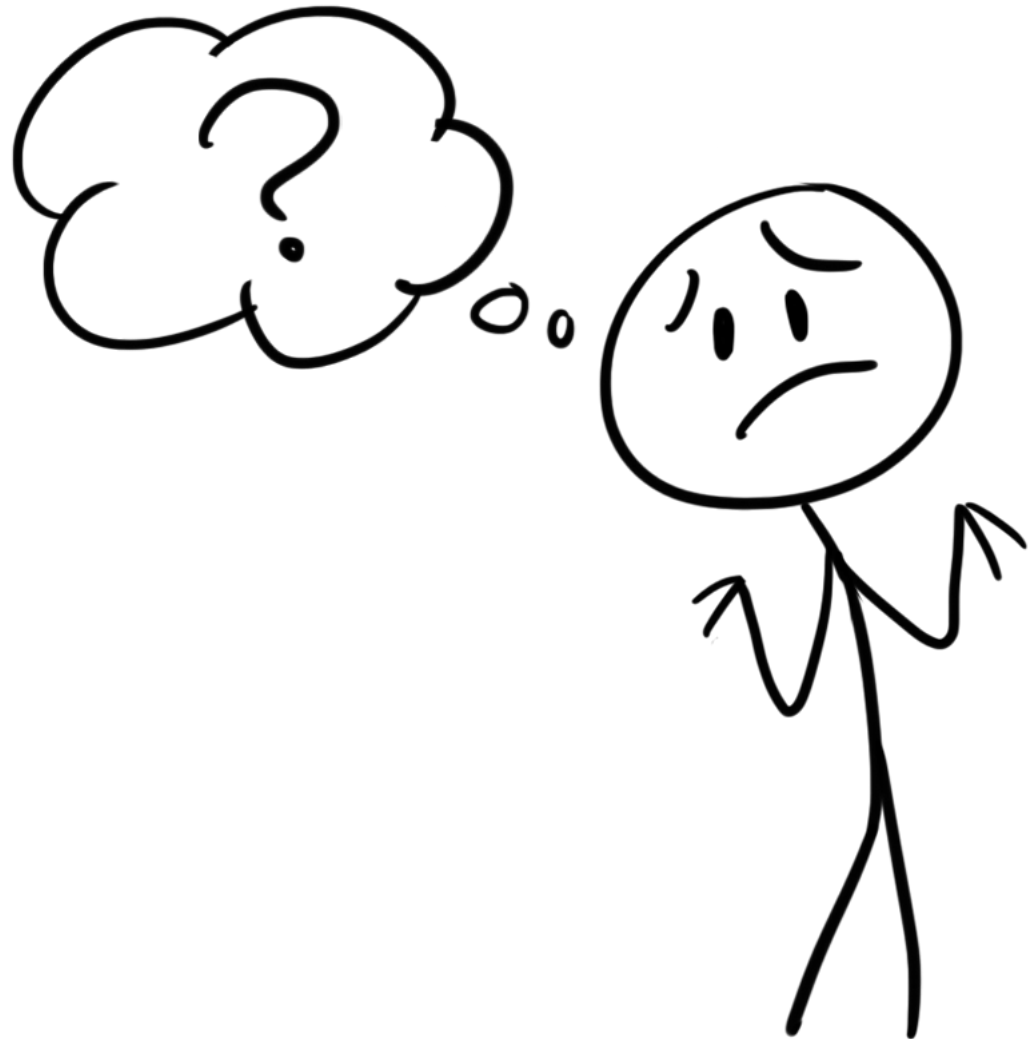
LIFELOCK	SAVVY CYBERSECURITY
1. Credit monitoring	Credit freeze
2. Credit card, checking and savings account activity alerts	Sign up for text/email alerts
3. Lost or stolen wallet- Cancel affected cards.	Call bank and credit card companies and cancel cards
4. Reduced pre-approved credit card offers	Sign up for Do Not Mail list ( <a href="http://www.dmachoice.com">www.dmachoice.com</a> ) and opt out of prescreened credit card offers ( <a href="http://www.optoutprescreen.com">www.optoutprescreen.com</a> )
5. Fictitious identity monitoring	Credit freeze

# Lifelock vs. Savvy Cybersecurity

LIFELOCK	SAVVY CYBERSECURITY
6. Online annual credit report	Order free credit report from the credit bureaus
7. Bank account takeover alerts	Sign up for text/email alerts
8. Credit inquiry activity	Credit freeze

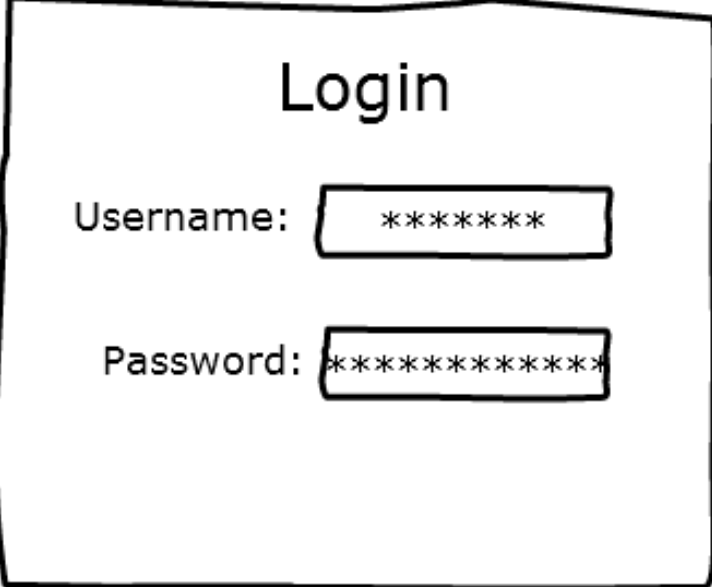
# Cybersecurity Myth

# Why Worry?



# Example: Choice Escrow and Land Title, LLC

- 2009 cyberheist at Missouri, Choice Escrow and Land Title
- Hacker was able to log in to company's Bancorp South's online banking
- Wired \$440,000 out of account



Login

Username:

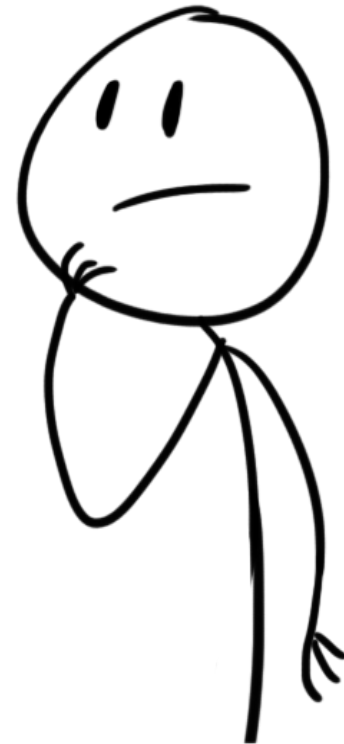
Password:

A hand-drawn diagram of a login form. The form is enclosed in a rectangular border. At the top center, the word "Login" is written. Below it, there are two input fields. The first field is labeled "Username:" and contains seven asterisks. The second field is labeled "Password:" and contains ten asterisks.



# Choice Escrow vs. Bancorp South

- Choice Escrow argued that the bank did not have strong enough security features
- Bank argued that the Escrow firm had turned down “dual control” which would have required two separate user IDs and passwords to approve wire
- Bank won the case. Choice Escrow was responsible for the missing \$440,000 from their account



# Introducing Savvy Cybersecurity

# SAVVY CYBERSECURITY

**1 Hour to Savy Cybersecurity:**  
10 Threats Every Person and Business Faces—and How to Fight Them



## 1 Hour to Savy Cybersecurity

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

#### Savvy Cybersecurity, Quick Reference Guide, 2015

Terese S. Samplenton, CPPM, CLU, CMC, CLTC  
Vice President  
Samplenton Wealth Management Group  
423 Main Street  
12th Floor  
New York, NY 10018  
212.556.1111 ext. 10  
tsamplenton@samplentonwealth.com  
www.samplentonwealth.com



Topic	Question	Answer	Score
1. CREDIT REPORTS	How often should I check my credit report?	At least once a year.	10 pts
2. SOCIAL MEDIA	How often should I update my social media profiles?	At least once a month.	10 pts
3. CRYPTOCURRENCY	How often should I update my cryptocurrency wallets?	At least once a month.	10 pts
4. MOBILE DEVICES	How often should I update my mobile device software?	At least once a month.	10 pts
5. PHISHING	How often should I update my email filters?	At least once a month.	10 pts
6. SPAMMING	How often should I update my spam filters?	At least once a month.	10 pts

Principle #1: Awareness	Score	Points
1. Create a password for your smartphone and email.	10 pts	10 pts
2. Update your smartphone and email software.	10 pts	10 pts
3. Create a password for your home laptop/desktop.	10 pts	10 pts
4. Update your home network to changing default password and name.	10 pts	10 pts
5. Change your passwords to strong and secure passwords.	10 pts	10 pts
6. Create a password for your social media profiles.	10 pts	10 pts
7. Change your mobile device software.	10 pts	10 pts
8. Change your mobile device software.	10 pts	10 pts
9. Use a password manager to create passwords.	10 pts	10 pts
10. Update your mobile device software.	10 pts	10 pts

### SAVVY CYBERSECURITY

Thursday, July 10, 2014  
www.savvycybersecurity.net

**IN THIS ISSUE**

- Protecting Sensitive Information: What Small Business Owners Need to Know
- Cybersecurity news worth reading
- Software updates
- FAQ

**Protecting Sensitive Information: What Small Business Owners Need to Know**

Dear Cybersecurity Advisor,

Do your small business owner clients know how to protect their customer information? With data breaches on the rise, make sure they know these tips:

Many businesses must store their customers' financial and personal information for legal purposes. This becomes an issue if the company has been security compromised and is hacked by hackers who are then able to obtain the records of their customers. Social Security numbers, credit card numbers, passwords, bills of lading, addresses, and names can all be used by thieves to steal the identities of past customers. And this can be costly for businesses. A recent survey done by the Financial Institute found that an average data breach costs a company \$100 per compromised record. Another study by the CISO Council discovered that a company's stock value drops significantly when a data breach is reported.

It is important for your business owner clients to protect this information very carefully and know the right ways to keep their customers safe. Educating your clients on these prevention methods can help them handle personal data responsibly and safely.

1. Store it. When you no longer need a document with consumer information on it, shred the document with a cross shredder before discarding.
2. Limit what you know. Only collect the information that you absolutely need from your customers. The less information you have, the harder it is for thieves to piece together a full stolen identity that they can use.
3. Store safe. Keep any documents with customer information in safe, secure places. If you can avoid storing customer information on a computer with Internet connectivity, do so.

## SAVVY CYBERSECURITY

Marketing Toolkit

Cyber fraud

horsesmouth

### Child ID Theft: 8 Steps to Keep Your Kids Safe

Terese S. Samplenton, CPPM, CLU, CMC, CLTC  
Vice President  
Samplenton Wealth Management Group  
423 Main Street  
12th Floor  
New York, NY 10018  
212.556.1111 ext. 10  
tsamplenton@samplentonwealth.com  
www.samplentonwealth.com

While you're being careful about guarding and monitoring your own personal data from theft, remember to keep your child's identity. What happens next is not pretty, but here's what you can do to guard against it!

**Child ID Theft**

The following are 8 steps to keep your child's identity safe from theft:

1. Don't give out your child's name and address to anyone who asks for it.
2. Don't give out your child's name and address to anyone who asks for it.
3. Don't give out your child's name and address to anyone who asks for it.
4. Don't give out your child's name and address to anyone who asks for it.
5. Don't give out your child's name and address to anyone who asks for it.
6. Don't give out your child's name and address to anyone who asks for it.
7. Don't give out your child's name and address to anyone who asks for it.
8. Don't give out your child's name and address to anyone who asks for it.

# Interactive Seminar Presentation: “1 Hour to Savvy Cybersecurity: 10 Threats Every Person and Business Faces—and How to Fight Them Now”



- A customizable Powerpoint presentation and speakers notes (70 + slides; speaker notes page)
- (\$497 value)


# SAVVY CYBERSECURITY



# Savvy Cybersecurity Quick Reference Guide, 2015

**Savvy Cybersecurity,  
Quick Reference Guide,  
2015**

Teresa S. Sampleton, CFP®, CLU ChFC, CLTC  
Vice President  
Sampleton Wealth Management Group  
123 Main Street  
12th Floor  
New York, NY 10018  
(212) 555-1111 ext. 10  
tsampleton@sampletonwealth.com  
www.sampletonwealth.com



**SAMPLETON**  
Wealth Management  
Group

A. Scorecard			
Answer Yes or No to the following questions. When complete, follow directions at bottom to get your raw score.			
Topic	Question	Yes/No	Score
CREDIT REPORTS:	I know the difference between putting my credit files on monitor, alert, or freeze AND I've had my minor children's names searched at the credit bureaus.		15 pts
SOCIAL MEDIA:	I have reviewed my "privacy settings" that control who sees and reads what I do on Facebook and other social media sites.		5 pts
COMPUTER/LAPTOP:	My personal computers have the most updated operating systems, browsers, virus/malware/firewall software, and up to date versions of Java, Flash, and Adobe.		10 pts
BUSINESS ID THEFT:	My employer trains its staff on business or personal cybersecurity measures.		5 pts
WI-FI:	I know how to determine if FREE public Wi-Fi is safe to use.		10 pts
HACKED DEVICES:	My smartphone and/or tablet has a security passcode.		5 pts
PASSWORDS:	I have enabled two-factor authentication on my key accounts that allow it.		15 pts
SKIMMING:	When using an ATM card, or self-paying for things such as gas, tickets, parking, I know what to look for to ensure that my transaction is safe from being fraudulently recorded.		5 pts
DATA BREACH:	I have a text and email alerts set up on my credit cards and bank accounts to receive a notification each time there is a transaction.		15 pts
PHISHING:	I know the tactics used by phishers to try to trick me into clicking on links or sharing personal information.		15 pts
Circle 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	
>100-85	GOOD
84-60	OKAY
59-0	DANGER

Consult the Checklist in Section C, to identify key items to include in your Action Plan now.

C. Checklist		
Action	Time	Points
<b>Principle #1: Devices</b>		
<input type="checkbox"/> Create a passcode for smartphone and tablet.	2 min	4 pts
<input type="checkbox"/> Install "Locate My Device" or "Find My Phone" app in case device is lost or stolen.	1 min	1 pt
<b>Principle #2: Software</b>		
<input type="checkbox"/> Update all software on your home laptop/computer.	5 min	10 pts
<b>Principle #3: Wi-Fi</b>		
<input type="checkbox"/> Secure home Wi-Fi network by changing default password and name.	20 min	10 pts
<b>Principle #4: Passwords</b>		
<input type="checkbox"/> Change weak passwords to strong and secure passwords.	5 min	4 pts
<input type="checkbox"/> Passwords don't include names, birthdates, pets' names, etc.	Always	1 pt
<input type="checkbox"/> Passwords include nonconsecutive numbers and symbols.	Always	1 pt
<input type="checkbox"/> Change passwords every six months.	Always	1 pt
<input type="checkbox"/> Use a mnemonic device to create password.	5 min	5 pts
<input type="checkbox"/> Consider password storage system.	Always	2 pts
<b>Principle #5: Transactions</b>		
<input type="checkbox"/> Sign up for text/email alerts for debit/credit card.	2 min	10 pts
<b>Principle #6: Credit</b>		
<input type="checkbox"/> Sign up for credit freeze.	20 min	15 pts
<b>Principle #7: E.M.A.I.L.</b>		
<input type="checkbox"/> Examine emails carefully before clicking, sharing, or visiting links.	Always	15 pts
<b>Additional Cybersecurity Actions</b>		
<b>Document Safe</b>		
<input type="checkbox"/> Put personal documents in a safe place.	2 min	1 pt
<input type="checkbox"/> Shred documents with personal information before throwing them out.	1 min	2 pts
<input type="checkbox"/> Give out Social Security number when necessary. Question why needed.	Always	2 pts
<b>Social Media Safe</b>		
<input type="checkbox"/> Strengthen Facebook and other social media privacy settings.	5 min	2 pts

Copyright © 2014 Horsmouth, LLC. All Rights Reserved. Check with your financial advisor for updates.

Horsmouth is an independent organization providing unique, unbiased insight into the critical issues facing financial advisors and their clients. Horsmouth, LLC is not affiliated with the reprint licensee or any of its affiliates.

- This two-sided reference includes: a personal Savvy Cybersecurity Scorecard; a Cybersecurity Checklist; and a "My Action Plan"
- 50 hard copies
- (\$197 value)

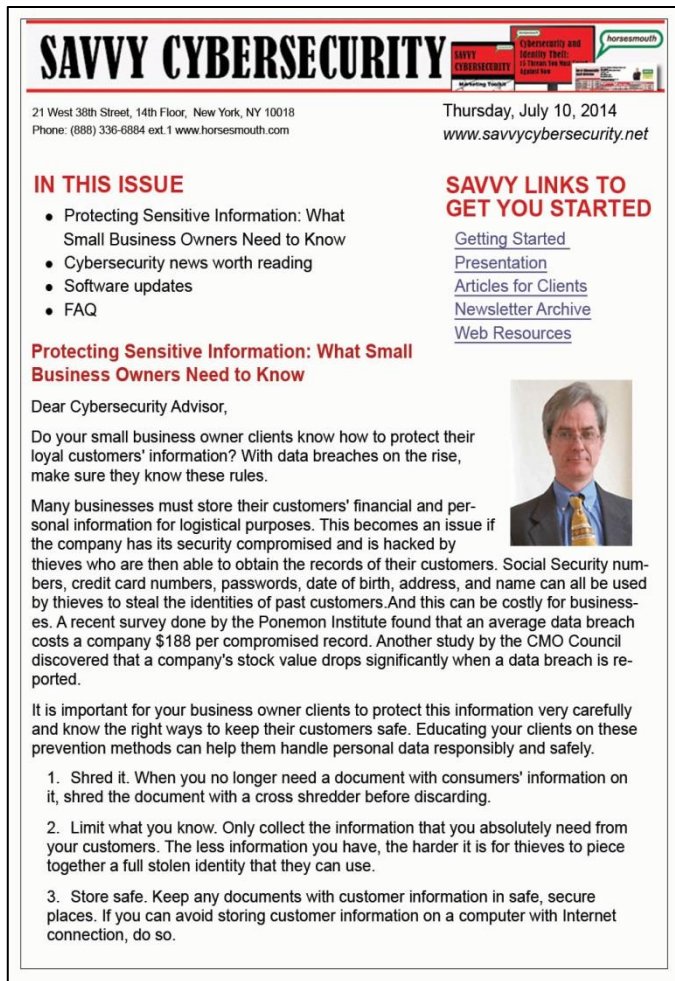
# SAVVY CYBERSECURITY







# Savvy Cybersecurity E-Newsletters



**SAVVY CYBERSECURITY** SAVVY CYBERSECURITY Cybersecurity and Identity Theft: 12 Steps You Can Control Now horsesmouth

21 West 38th Street, 14th Floor, New York, NY 10018  
Phone: (888) 336-6884 ext.1 www.horsesmouth.com

Thursday, July 10, 2014  
www.savvycybersecurity.net


**IN THIS ISSUE**

- Protecting Sensitive Information: What Small Business Owners Need to Know
- Cybersecurity news worth reading
- Software updates
- FAQ

**Protecting Sensitive Information: What Small Business Owners Need to Know**

Dear Cybersecurity Advisor,

Do your small business owner clients know how to protect their loyal customers' information? With data breaches on the rise, make sure they know these rules.



Many businesses must store their customers' financial and personal information for logistical purposes. This becomes an issue if the company has its security compromised and is hacked by thieves who are then able to obtain the records of their customers. Social Security numbers, credit card numbers, passwords, date of birth, address, and name can all be used by thieves to steal the identities of past customers. And this can be costly for businesses. A recent survey done by the Ponemon Institute found that an average data breach costs a company \$188 per compromised record. Another study by the CMO Council discovered that a company's stock value drops significantly when a data breach is reported.

It is important for your business owner clients to protect this information very carefully and know the right ways to keep their customers safe. Educating your clients on these prevention methods can help them handle personal data responsibly and safely.

1. Shred it. When you no longer need a document with consumers' information on it, shred the document with a cross shredder before discarding.
2. Limit what you know. Only collect the information that you absolutely need from your customers. The less information you have, the harder it is for thieves to piece together a full stolen identity that they can use.
3. Store safe. Keep any documents with customer information in safe, secure places. If you can avoid storing customer information on a computer with Internet connection, do so.

- Savvy Cybersecurity Watch: Get the latest, best informed newsletter on new scams and frauds, and what to do to prevent them, with links to resources you can share with clients (monthly)
- **Savvy Cybersecurity Alert:** When word of serious, widespread new scams hit, we'll send you an email alert with the latest details so you can share immediately with your clients and other people in your network
- (\$197 value)

# SAVVY CYBERSECURITY



**SAVVY CYBERSECURITY** Marketing Toolkit

**1 Hour to Savvy Cybersecurity:**  
10 Threats Every Person and Business Faces—  
and How to Fight Them Now

horsesmouth

# Article Reprints (PDF)

## Child ID Theft: 8 Steps to Keep Your Kids Safe

Teresa S. Sampleton, CFP®, CLU, ChFC, CLTC

Vice President

Sampleton Wealth Management Group

123 Main Street  
12th Floor  
New York, NY 10018  
(212) 555-1111 ext. 10

tsampleton@sampletonwealth.com  
www.sampletonwealth.com

By Devin Kropp

While you're being careful about guarding and monitoring your own personal data from theft, miscreants may assume your child's identity. What happens next is not pretty. But here's what you can do guard against child

The latest targets of identity thieves are not millionaires, but rather children with little to no financial history. According to the 2012 Child Identity Fraud Survey, conducted by Javelin Strategy and Research, one in 40 households had one child who has suffered from identity theft. In fact, children are affected by identity theft and fraud 35 more times than adults.

What makes a nine-year olds' identity so attractive? This theft is likely to go unnoticed for years.

The majority of parents and guardians do not request copies of their child's credit report, therefore not noticing fraudulent activity. This can affect the rest of your child's life.

### A nightmare

Take Gabriel Jimenez who shared his story with The NY Times. Jimenez's identity was stolen when he was a child. His mother discovered this issue when she went to file taxes for the work he did as a child model at age 11. The IRS notified her that taxes had already been filed under Gabriel's

Social Security number.

That's where Jimenez's nightmare began. His Social Security number had been stolen by an illegal immigrant and had been used for years. Now, as an adult, he has had issues setting up bank accounts, getting approved for car insurance and with his credit report. Jimenez was also denied when he tried to set up phone, gas, and electricity in his first apartment because his identity theft had already created accounts.

To this day, he can only rent apartments with utilities included and has problems with his credit rating due to the action of an identity thief. Jimenez and his mother were able to identify the thief years ago, but that did not clear Jimenez from having to prove his own identity time after time.

And he is not alone. It is estimated that 500,000 children are affected by identity theft each year. Children who have their identities stolen spend the rest of their lives dealing with complications regarding their personal information and

Copyright © 2014 by Horsmouth, LLC. All Rights Reserved.  
License #: 4004207-84309. Reprint License. Advisor Name  
PLEASE SEE NEXT PAGE FOR IMPORTANT RESTRICTIONS ON USE

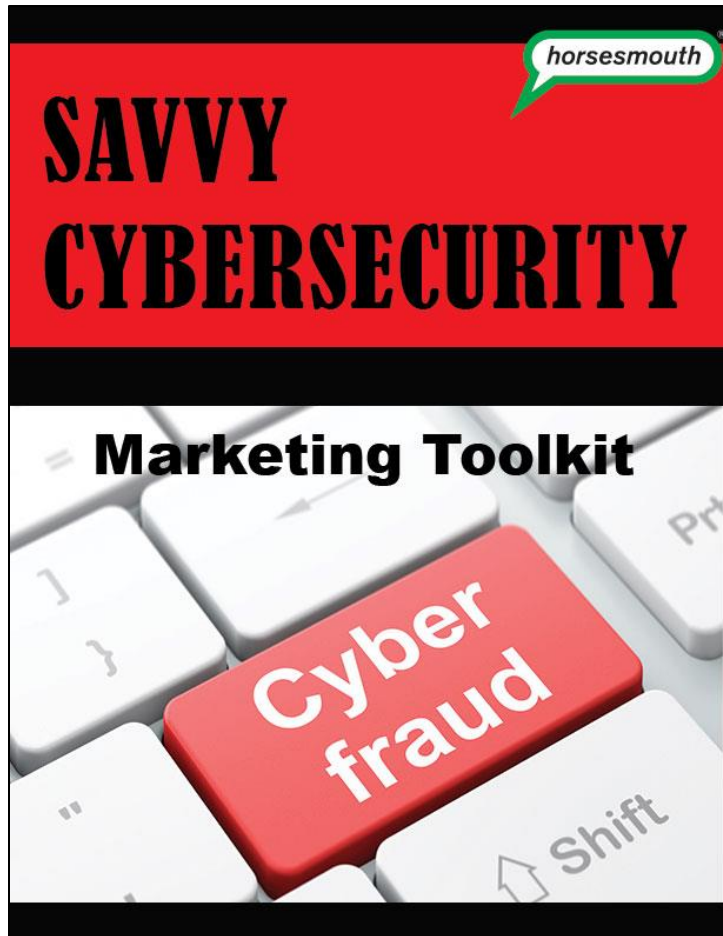
11

- Finra-reviewed article reprints you can personalize and use as part of your marketing and client communications.
- Each article focuses on important security measures clients should consider in order to maintain the best safety measures possible.
- (\$588 value)

# SAVVY CYBERSECURITY



# Marketing Toolkit



- Everything you need to promote your Savvy Cybersecurity presentation in your community:
- Flyer, Email, Press Release
- FINRA reviewed
- (\$375 value)

# SAVVY CYBERSECURITY





**Special Offer**

**Get Savvy Cybersecurity  
for \$497**

**Deadline: \$597 after Dec. 5th**