“I am convinced that there are only two types of companies – those that have been hacked and those that will be... and even they are converging into one category – companies that have been hacked and will be hacked again.”


The words of the former FBI director are alarming, yet accurate. Cybercrime is an epidemic that is targeting the attorneys of North Carolina. Collectively, as a profession, we need to protect ourselves and our clients. Investors Title Insurance Company, Lawyers Mutual Insurance Company, the North Carolina State Bar, and the Federal Bureau of Investigation have teamed up to present the CYBER SECURITY SUMMIT.

False Sense of Cyber Security
It Could Not Happen to Me?
Jonathan W. Biggs, Vice President Risk Management & Education

Cyber Security Summit - January 2017
False Sense of Cyber Security – It Cannot Happen To Me!

Jonathan W. Biggs, J.D.
Vice President of Risk Management & Education
121 North Columbia Street | Chapel Hill, NC 27514
P.O. Drawer 2687 | Chapel Hill, NC 27515
Main: 919.968.2200 | Direct: 919.945.2597 | Fax 919.968.0728
JBiggs@InvTitle.com | www.InvTitle.com

1) Introduction
2) Cyber-Fraud Generally
3) Myths About Cyber-Fraud
4) Realities About Cyber-Fraud & You
5) Who Are the Criminals Today?
6) How Do Criminals Gain Access?
7) Actual Stories About Types of Cyber-Fraud
8) So What Do I Do
9) Cyber-Fraud Insurance
What is Fraud?

• A **false representation** of a material of fact—whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed—
  • is **intended to deceive** another
  • so that the individual **will act** in reliance upon it
  • that, in fact, **deceives** and
  • to her or his **legal injury** (**DAMAGE**)
False Sense of Cyber Security – It Cannot Happen To Me!

Introduction

What is Fraud Prevention?

- Fraud deterrence is the proactive identification and removal of the causal and enabling factors of fraud.
- Fraud deterrence is based on the premise that fraud is not a random occurrence; fraud occurs where the conditions are right for it to occur.
- Fraud deterrence attacks the root causes and enablers of fraud.
- This analysis could reveal potential fraud opportunities in the process, but is performed on the premise that improving organizational procedures to reduce or eliminate the causal factors of fraud is the single best defense against fraud.

What is Fraud Deterrence?

Fraud deterrence involves both short term (procedural) and long term (cultural) initiatives.

What Are We Really Talking About?

- Professional & Ethical Representation
- Protecting Clients
- Avoiding Liability
- Avoiding Damage To Reputation

Investors Title
What is CYBER - Fraud?

Cyber-Fraud is an all-encompassing term that includes a wide variety of types of fraud. It is often confused and identified with each of the subclasses of Cyber-Fraud and used interchangeably.

Cyber - Fraud Generally

• Same as Fraud Generally
  • A **false representation** of a material of fact
  • is **intended to deceive** another
  • so that the individual **will act** in reliance upon it
  • that, in fact, **deceives** and
  • to her or his **legal injury** (DAMAGE)
• **ADDITIONAL ELEMENT**
• **Uses phone, computer or digital network to perpetrate the fraud**

Investors Title
False Sense of Cyber Security – It Cannot Happen To Me!

Cyber - Fraud Generally

What is Cyber - Fraud?

• When DATA or INFORMATION is stolen, the type of liability you have and the type of insurance that you need is referred to as CYBER LIABILITY/ DATA BREACH insurance coverage.

• When MONEY is stolen, the type of liability you have and the type of insurance you need is referred to as CRIME INSURANCE or CYBER THEFT INSURANCE coverage.

Cyber-Breach - INFORMATION STOLEN

The cyber-breach fraud can be perpetrated many ways, including the following:

• Gaining credentials (login and password) for access to a computer network that contains NPI;
• Intercepting un-encrypted or improperly encrypted communication containing NPI;
• Improper disposal of NPI;
• Sharing NPI with a source that is believed to be trusted (but is not); and
• Many more.
False Sense of Cyber Security – It Cannot Happen To Me!

Cyber - Fraud Generally

Cyber-Theft or Cyber-Crime - **MONEY STOLEN**

- Cyber-Theft is what people generally think of when they think of Cyber-Fraud - someone stole **MONEY** from the trust account using the internet.
- A separate flavor of cyber-fraud.
- Needs to be explicitly covered by the insurance policy.
- Crime Insurance or Cyber-Theft Insurance Policy.
- Involves a computer and/or a computer network in order to steal or misappropriate money.
- Log into your online banking and transfer funds to themselves.
- Many banks will not reimburse a business for money lost if the transfer is made with the correct account number, login, and password.

Not Really

**NO!**

But Try Anyway!
Myths About Cyber-Fraud

Popular Myths

1. Birds will die if they eat the uncooked rice flung at newlyweds. **NOPE**

2. If you eat Mentos and drink Diet Coke simultaneously your stomach will explode. **Wrong Again. I Tried it!**

3. Carolina is a “Better Value” than Duke

---

Popular Myths About Cyber-Fraud

**False**

Myth #1 – Nobody Can Read My Emails

- Email Is Like a Post Card
- No Envelope
False Sense of Cyber Security – It Cannot Happen To Me!

Popular Myths About Cyber-Fraud

Myth #2 - Software Will Protect You

- Software alone is not going to stop cyber-crime. It is essential, but not the only thing you need.

- There is no more harmful notion than the one that leads people into doing whatever they want on their computers or smartphones because they have all of the latest software protections.

- Training is an absolute necessity.
The only thing worse than training your employees and having them leave, is not training them and having them stay.

- Henry Ford

Myth #3 – Using Encrypted Email Is All I Need to Protect Me from Cyber-Fraud

• The Encrypted Email May Come From or Go To The Wrong Address or Individual

• Check the Address on the Email Every Time.
Myths About Cyber-Fraud

Myth #3 – Using Encrypted Email Is All I Need to Protect Me from Cyber-Fraud

- The Encrypted Email May Come From or Go To The Wrong Address or Individual
- Check the Address on the Email Every Time.

FALSE

Myth #4 – Once an Email is Encrypted, It Is Encrypted Forever

- Initiating an Email With Encryption Does Not Mean that Forwards or Replies Are Also Encrypted

FALSE
Popular Myths About Cyber-Fraud

Myth #5 – Wiring Instructions Can Be Trusted If They Are Received By Encrypted Email or Fax

- Cyber Criminals Can Buy Fax Machines
- Cyber Criminals Can Send Encrypted Emails
- **Always** Verify Wiring Instructions With a Call Back to a Trusted Source
  1. Proper Identification
  2. Verbal Confirmation
  3. Delivery Verification

Myth #6 – Changes In Wiring Instructions Is The Only Time That Warrants Call Back Procedures and Additional Caution

- A Change in Wiring Instructions Is Definitely a “Red Flag”
- **Always** Verify Wiring Instructions With a Call Back to a Trusted Source
  1. Proper Identification
  2. Verbal Confirmation
  3. Delivery Verification
Popular Myths About Cyber-Fraud

Red Flags

“Red Flags” are not absolute rules, but rather an indication that there may be something out of order with the wiring instructions. There may be reasons for the “Red Flag” that, upon proper investigation, may be very legitimate. However, you should look out for the following and investigate each instance of a “Red Flag” when they are discovered. Below is not an “all inclusive” list, but rather some of the more prevalent “Red Flags.”

- Wires to be sent outside of the United States
- Changes in Wiring Instructions
  - Very few individuals or corporations change their bank accounts in the middle of a transaction. Be very suspicious of change wiring instructions.
  - Similar But Slightly Different Email Addresses
    - Many cyber criminals will attempt to defraud you by communicating with a very similar (but slightly different email address)
- Wire to a different geographic location than Recipient
- Wire to account which is not in the name of the Recipient
Popular Myths About Cyber-Fraud

**Red Flags**

**RED FLAGS CONTINUED**

- Individual Wire Sent to Corporate Account
- Corporate Wire Sent to Individual Account
- Broken English
  - Many cyber criminals are outside of the United States and English may not be their first language
  - Not an absolute, but worth checking out
- Unnecessary Speed Requirements or Demands
  - Everyone understands the desire to receive their money from a third party, but extraordinary pressure for the speed of the wire is generally a sign that they do not want you to investigate this “Red Flag.”

---

**Myth #7 - Cyber-Crime Is Mostly About Credit Card Fraud**

- The idea that cyber-crime is just about credit card fraud is a misconception that, ironically, can lead to credit card fraud and other forms of credit-related crimes.

- The majority of the cyber attacks are focused on grabbing personal identifying information from organizations that do business with a lot of people.
Popular Myths About Cyber-Fraud

Myth #8 - Cyber-Crime Is Only About Making a Buck

- If cyber-crime were only about making money, we would all be a lot safer than we are right now.
- Large numbers of hackers are driven by ideology.
- Many are far less interested in making money than in making money disappear are just reeking havoc by destroying information.

Myth #9 - Cyber-Criminals Don’t Target Small Businesses

- Target was not really hacked
- The criminals hacked Target’s HVAC vendor
- Looking for vulnerabilities on the Internet
- Do not be low hanging fruit
Popular Myths About Cyber-Fraud [FALSE]

Myth #10 – My Errors & Omissions Insurance Will Cover Me for Cyber-Fraud

• General Liability and Errors & Omissions Policies generally have exclusions for Cyber-Fraud
• Confer with Your Insurance Agent About Cyber-Fraud Coverages
• There are Multiple Types of Cyber-Fraud Coverage

Myth #11 – All Cyber-Fraud Insurance Is the Same

• Not All Cyber-Fraud insurance Coverage is the Same
• Ask Your Insurance Agent About
  • Cyber-Liability Fraud Insurance (Loss of Data)
  • Cyber-Crime Fraud Insurance (Loss of Money)
  • Social Engineering Fraud Insurance
Myths About Cyber-Fraud

Popular Myths About Cyber-Fraud

Biggest Myth of All - It Cannot Happen To Me!

"There are only two types of companies: those that have been hacked, and those that will be."
Robert Mueller, FBI Director, 2012
Realities About Cyber-Fraud

Truth #1 – Cyber-Fraud is Rampant

- 12 Per Second
- 720 Per Minute
- 43,200 Per Hour
- 345,600 During the Seminar
- 518,400 Before Lunch
- 1,036,800 Today
False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

OVER 70% of organizations report having been compromised by a successful cyberattack in the past 12 months.

Realities About Cyber-Fraud & You

Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report

INVESTORS TITLE
False Sense of Cyber Security – It Cannot Happen To Me!

Realities About Cyber-Fraud & You

Realities About Cyber-Fraud

Truth #2 – You Are A Target

- Wrong Direction
- Only Road
- People Trying To Hit You
- Not Nimble Enough To Avoid Getting Hit
- No One Is!
Realities About Cyber-Fraud

Truth #3 – Social Media – a Hackers’ Favorite Target

• 1.6 +/- Billion Social Network Users Worldwide
• 64% of Internet Users Access Social Media Online
• More than 600,000 Facebook accounts are compromised

EVERY SINGLE DAY

• Like-Jacking & Link-Jacking – Involuntary Redirects
Realities About Cyber-Fraud

Truth #4 – 99% of Computers are Vulnerable to Exploit Kits

- One or More of Oracle Java, Adobe Reader or Adobe Flash Resides on 99% of Computers.
- These Computers are Vulnerable to Exploit Kits
- Exploit Kits = Software Vulnerabilities
- Generally Due To Failure To Update
  - Software
  - Operating Systems
  - Anti-Malware Software
Realities About Cyber-Fraud

Truth #5 – Insiders Biggest Cause of Cyber-Fraud
• Terminated Insiders - 59% of Employees Steal Proprietary Corporate Data when they quit or are fired
• Malicious Insiders are the least frequent, but have the potential to cause significant damage due to their level of access. Administrators with privileged identities are especially risky.
• Exploited Insiders may be “tricked” by external parties into providing data or passwords.

Truth #6 – Funds Lost Are Tough To Recover
• 68% of Funds Lost as a Result of a Cyber Attack Are Declared Unrecoverable
• Must Act Quickly to Contact Bank and Authorities
Realities About Cyber-Fraud

Truth #6 – Funds Lost Are Tough To Recover

• You Must Act **F.A.S.T.**
• You Need:
  • A Cyber-Fraud Response Team
  • A Cyber-Fraud Response Plan
  • To Keep Calm And Follow the Plan

**Fast Action Stops Theft**

Truth #7 – Your Old Cyber-Fraud Response Plan

1. Discover Breach or Loss
2. Panic, Curse & Throw Things
3. Cry
4. Call The Bank
5. Cry Again
6. Deny
7. Write a Big Check
8. Curse Again
9. Lose Sleep
10. Go To Dental School

You Need A New Plan!
**FAST. Fast Action Stops Theft.**

**RESPONSE PLAN DOCUMENTATION**

**STEP #1 - DO NOT PANIC**

**STEP #2 - Alert Internal Cyber Crime Response Team**
- Name
- Phone
- Email
- Date
- Time

**STEP #3 - Contact Bank(s)**
- Name
- Address
- Phone
- Email
- Date
- Time

**STEP #4 - File Report with FTC.gov - Internet Crime Complaint Center - FBI**
- Complete the Attached Document Prior to Filing Report
- Print and Keep Copy of Complaint Filed
- Date
- Time

**STEP #5 - Secure Your Office and Your Network**
- Secure the Physical Premises
- Secure Digital Devices
- Preserve Evidence
- Stop Additional Loss
- Date
- Time

**STEP #6 - Document Specifics of Breach/Loss**
- Complete the Attached Document
- Include FTC: KBB: Checklist, if a fraud involves a
- Date
- Time

**KEEP CALM AND FOLLOW THE PLAN**

*Follow All Steps Thoroughly!*

**January 2017**

False Sense of Cyber Security – It Cannot Happen To Me!

Jonathan W. Biggs, VP Risk Management & Education
Realities About Cyber-Fraud

Truth #9 – No Protection is Too Strong or Bulletproof

- Your protections must be appropriate to:
  - Your **size** and **complexity**
  - The **nature** and **scope** of your activities; and
  - The **sensitivity** of the **customer/client information** you handle.

- You must evaluate and adjust your protections in light of relevant circumstances, including changes in your business or operations, or the results of security testing and monitoring.

- Cost Will Always Be a Consideration and a Factor

---

Realities About Cyber-Fraud

Truth #10 – Cyber-Fraud Is Here To Stay

<table>
<thead>
<tr>
<th>Stone Age</th>
<th>19th Century</th>
<th>20th Century</th>
<th>21st Century</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>Wood Stove</td>
<td>Electric Stove</td>
<td>Microwave</td>
</tr>
<tr>
<td>Wheel</td>
<td>Horse Carriage</td>
<td>Car</td>
<td>Hover board</td>
</tr>
<tr>
<td>Tablet</td>
<td>Electricity</td>
<td>Carbon Paper</td>
<td>Email</td>
</tr>
<tr>
<td>Chisel</td>
<td>Gold &amp; Silver</td>
<td>Certified Checks</td>
<td>Wires</td>
</tr>
<tr>
<td>No Money</td>
<td>Stamps</td>
<td>Overnight Delivery</td>
<td>Video Chat</td>
</tr>
<tr>
<td>No Secrets</td>
<td>Radio</td>
<td>Landline Phones</td>
<td>OnLine Banking</td>
</tr>
<tr>
<td>Thief</td>
<td>Horse Thief</td>
<td>Organized Crime</td>
<td>Cyber-Criminals</td>
</tr>
<tr>
<td>Criminals!</td>
<td>Criminals!</td>
<td>Criminals!</td>
<td>Criminals!</td>
</tr>
</tbody>
</table>

If You Use 21st Century Technology, You Must Protect Yourself Against Criminals with 21st Century Safeguards!
Realities About Cyber-Fraud

Biggest Truth of All – Do You Need Cyber-Fraud Insurance?

Two Part Test:

1) Do I Have a Computer?
2) Do I Have a Cellular Phone?

If You Answered “YES” to either, then you NEED Cyber-Fraud Insurance.

Who Are The Cyber-Criminals Today?

Hacker Type #1 – “Script Kiddies”

- Novice or “Wannabe Hacker”
- Maybe Mathew Broderick type character
- Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise.
- They are usually only able to attack very weakly secured systems.
- There is enough “Low Hanging Fruit” to keep them in business
False Sense of Cyber Security – It Cannot Happen To Me!

Who Are the Cyber-Criminals Today?

Hacker Type #2 – “Scammers”

- Your Email Inbox is probably full of their work.
- Discount Pharmaceuticals
- Time-Shares
- Personal Ads from Available Women in Foreign Lands
- Weight Loss Programs
- Viagra etc.
- Desire to Secure Your Representation

...sound familiar?

Who Are The Cyber-Criminals Today?

Hacker Type #3 – “Hacker Groups”

- Work anonymously
- Create tools for hacking.
- They often hack computers for no financial reason (e.g. for fun)
- Sometimes even hired by companies wanting to test their security.
Who Are the Cyber-Criminals Today?

Hacker Type #4 – “Political/Religious/Commercial Groups”
- Advancing a Political Agenda
- Not Interested in Money
- Many times Designed to Destroy
- Russians Accused of Hacking the Democratic National Committee just before convention
- New Form of Militant Terrorism

Hacker Type #5 – “Advanced Persistent Threat Agents” - (APT)
- A network attack
- An unauthorized person gains access to a network and stays there undetected for a long period of time.
- The intention of an APT attack is to steal data rather than to cause damage to the network or organization.
- APT attacks target organizations in sectors with high-value information, such as national defense, banks, and anyone with a lot of consumer data.
Who Are The Cyber-Criminals Today?

Hacker Type #6 – “Phishers”

• An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money)

• Often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Hacker Type #7 – “Insiders”

• Represent 20% of the Cyber-Fraud threat

• Responsible for 80% of the damage.

• These attackers are considered to be the highest risk.

• Often employees of the organization
We Invite Them In!

Access #1 – Casual Use of Passwords

- Should use complex passwords
- ALTA Best Practices Require
  - At least 8 characters
  - Uppercase and Lowercase
  - Letters and Numbers
  - Special Character
- Should change complex passwords regularly
  (Every 3 Months Minimum)
- Should change factory installed passwords

Often Multi-Factor Verifications Are Used.

Question 1:

What was your high school mascot?
What was your favorite pet's name?
What is your favorite movie?
What was your favorite teacher's name?
What is your favorite sports team?
What is your favorite meal?
What is your favorite ice cream flavor?
What is the first and last name of your first boyfriend or girlfriend?
Which phone number do you remember most from your childhood?
What was your favorite place to visit as a child?
Who is your favorite actor, musician, or artist?

Question 3:
False Sense of Cyber Security - It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!

Access #1 – Casual Use of Passwords

Spouse’s Name
Kids’ Names
Parents’ Names
Relationship
Favorite Food
Vacation Spots
Hometown
Your Birthday
Family Birthdays
Employment
Pets’ Names
Your Schools
Kids’ Schools
Hospital Visits
Dentist & Doctor
Success Stories
Life’s Tragedies
& Rest of Your Life

REMEMBER THIS!

CONFIDENTIALITY NOTICE: This electronic mail transmission has been sent by a lawyer. It may contain information that is confidential, privileged, proprietary, or otherwise legally exempt from disclosure. If you are not the intended recipient, you are hereby notified that you are not authorized to read, print, retain, copy or disseminate this message, any part of it, or any attachments. If you have received this message in error, please delete this message and any attachments from your system without reading the content and notify the sender immediately of the inadvertent transmission at XXX-XXX-XXXX or me@lawfirm.com. There is no intent on the part of the sender to waive any privilege, including the attorney-client privilege, that may attach to this communication. Thank you for your cooperation.
False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In!
Access #3 – Inadequate Protections on Trust Accounts

- ATLA Best Practice #2
- Escrow Funds Held in Federally Insured Bank
- Escrow Accounts and Operating Accounts Separate
- Access Limited To Authorized Personnel Only
- Monthly Three Way Reconciliation of Escrow Accounts
- Separation of Duties
  - Separate Reconciliation From Disbursement Authority (Required)
  - Others - Writing Checks / Signing Checks (Suggested)
    - Initiating Wires / Approval of Wires (Suggested)
- Block ACH Access To Escrow Accounts
- Block International Access To Escrow Accounts
- Utilize Positive Pay or Reverse Positive Pay

Access #4 – Improper Disposal of NPI
False Sense of Cyber Security – It Cannot Happen To Me!

How Do Criminals Gain Access?

We Invite Them In! Access #4 – Improper Disposal of NPI

• Disposal and Decommission of Devices Containing NPI
  • Computers
  • Copiers
  • Hard Drives
  • Portable Media
  • Phones
False Sense of Cyber Security – It Cannot Happen To Me!

We Invite Them In!

Access #5 – Internet of Things (aka IoT)

How Do Criminals Gain Access?

How Many Internet Connected Devices Do You Have?

- Computers
- Copiers
- Television
- Cable Box
- Phone
- Cell Phone
- Tablet
- Car
- Watch
- Refrigerator
- Coffee Maker
- Toaster
- Washer and Dryer
- Dishwasher
- House Lights
- Water Heater
- Garage Doors
- Dog Collar ETC.

7,470,753,701
People In the World
12/12/16 6:15 PM EST

2016 - Already Over 3 Devices Per Person
# False Sense of Cyber Security – It Cannot Happen To Me!

## How Do Criminals Gain Access?

**We Invite Them In!**

### Access #5 – Social Media

**How Many Internet Accounts Devices Do You Have**

- Facebook
- Google Plus
- YouTube
- Twitter
- Instagram
- SnapChat
- TeamSnap
- MySpace
- Skype
- LinkedIn
- Dating Sites
- Search Engines
- AOL
- Yahoo
- Ebay
- Marketplace Platforms
- Yelp
- IHaveNoLife.com ETC.

## How Many Internet Accounts Devices Do You Have

<table>
<thead>
<tr>
<th>Spouse’s Name</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kids’ Names</td>
<td>Pets’ Names</td>
</tr>
<tr>
<td>Parents’ Names</td>
<td>Your Schools</td>
</tr>
<tr>
<td>Relationship</td>
<td>Kids’ Schools</td>
</tr>
<tr>
<td>Favorite Food</td>
<td>Hospital Visits</td>
</tr>
<tr>
<td>Vacation Spots</td>
<td>Dentist &amp; Doctor</td>
</tr>
<tr>
<td>Hometown</td>
<td>Success Stories</td>
</tr>
<tr>
<td></td>
<td>Life’s Tragedies &amp; Rest of Your Life</td>
</tr>
</tbody>
</table>

**REMEMBER THIS!**
We Invite Them In!

Access #5 – We Hire Them And Give Them a Password

How Do Criminals Gain Access?

Stories of Actual Breaches

Personally, I’m always ready to learn, although I not always like being taught.

- Winston Churchill
False Sense of Cyber Security – It DID Happen To Me!

Cyber-Fraud War Stories

Experience is a hard teacher. The test is given first, the lesson afterwards

- Anonymous

War Stories

#1 Ransomware / Cryptolocker

• Computer or Network is compromised
• Computer Locked
• Data Encrypted
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America (Article 1, Section 8, Clause 8; Article 206; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were selected:
Your IP address was used to visit websites containing pornography, child pornography, pedophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography. Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents etc. Here is a complete list of encrypted files, and you can personally verify this.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

To obtain the private key for this computer, you need to pay 100,000 / 300 EUROS / similar amount in another currency.

Click Next to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.
False Sense of Cyber Security – It Cannot Happen To Me?

Jonathan W. Biggs, VP Risk Management & Education

Stories of Actual Breaches

#1 Ransomware / Cryptolocker

False Sense of Cyber Security – It Cannot Happen To Me!

IMAGINE YOUR PICTURE HERE

Your Computer has been locked!

To unlock your computer and avoid legal consequences, you are obligated to pay a release fee of $100. Popple through Green Dot.

Doubled In Last 6 Months of 2015

Global Mentions With Ransomware
War Stories

#2 Network Intrusions

- Gain Access To Data Source, Computer or Network
- Steal More Than Account Numbers
- Steal Ability To Open Accounts
- Steal Ability To Verify Information at Banks, etc.
- Steal Ability To Verify Information at Retirement Accounts
- Steal Ability To Perpetrate a Crime in Your Name
**War Stories**

#3 Account Hacked
False Sense of Cyber Security – It Cannot DID Happen To Me!

War Stories

#4 Phishing Emails

Pretending To Be From:

- Banks
- IRS
- Credit Card Companies
- Ebay.com
- Amazon.com
- Amazon.com
- Paypal.com
- Mortgage Companies
- Social Media (Such as Facebook)

Jonathan W. Biggs, VP Risk Management & Education

January 2017
False Sense of Cyber Security – It Cannot Happen To Me!

Jonathan W. Biggs, VP Risk Management & Education

Stories of Actual Breaches
War Stories
#4 Phishing Emails

False Sense of Cyber Security – It Cannot Happen To Me!

*Hover Over Links To See True Identity*

IGotYou@FailToHover.com

http://YouWishItWasWells.com

http://GiveMeYourPassword.com

Look alike IRS webpage

Internal Revenue Service
United States Department of the Treasury

Tax Refund

Get Tax Refund on your VISA or MasterCard

Please enter your Social Security Number and a valid Credit/Debit Card where you want the refund to be made.

Social Security Number

Credit/Debit Card

Please enter the following information here:

Name on card:
Card Number:
Expiration Date: mm/yy
CVV Code:

Refund Amount: $134.80

Note: For security reasons, we recommend that you close your browser after you have finished the refund process.
War Stories

#5 Social Engineering – Spear Phishing

- Fraudster tricks you into sending money to wrong place
- Frustrating & Infuriating
- Banks Tell You That They Sent Money Exactly Where You Told Them To Send It
- Will Not Put It Back
- Sellers’ Proceeds
- Buyers’ Funds
- Even Payoffs - Watch Out - Big Numbers

**BIG AREA OF FRAUD RIGHT NOW**
#5 Social Engineering – Spear Phishing

**From:** Jason McClain <cliff.hward@mail.com>  
**Sent:** Tuesday, March 15, 2016 9:04 AM  
**To:**  
**Subject:** 403 Topaz Drive Morton, IL 61550

Good morning Angi,  

We need your assistance as regards to the above mentioned property, We need disbursement done as a wire transfer to a different bank, as we just got advised by my financial advisor. Inform us about this as soon as possible in order to send you bank details required for the wire.  

Jason C McClain & Renee W McClain

---

**From:** Jason McClain <cliff.hward@mail.com>  
**Sent:** Tuesday, March 15, 2016 10:34 AM  
**To:**  
**Subject:** Re: RE: 403 Topaz Drive Morton, IL 61550

Thanks for getting back. We would like you to cancel the check as we out of town and won’t be back for some weeks. Kindly cancel the check. How will you like us to send the wiring instructions to you? Here or Should we fax it...  

Jason C McClain

---

Calls for a Change  
Poor grammar and states they will be out of town for a long time.
False Sense of Cyber Security - It Cannot **DID** Happen To Me!

Stories of Actual Breaches

#5 Social Engineering – Spear Phishing

![Image of a blackboard with social engineering message]

**Social Engineering**

The clever manipulation of the natural human tendency to trust.

From: Jason McClain <mc.jason@mail.com>
Sent: Tuesday, March 15, 2016 11:58 AM
To: [Redacted]
Subject: Re: RE: RE: 403 Topaz Drive Morton, IL 61550

How much is your international wiring fee?

Wiring instructions below:

Account name: NEIUIA Trade co. ltd (in beneficiary of Jason & Renee McClain) it is a corporate account
Account number: 58233274113638
Swift code: HSBCNINH
Bank: HSBC BANK HONG KONG
Bank address: Queens road central, Hong kong

Looking forward to seeing the Wire confirmation slip

Thanks
Jason C McClain

Different email being used here.

Out of Country

It's not common to have a corporate account with individual beneficiary names. Also misspelled Corporate.
War Stories

#5 Social Engineering – Spear Phishing

- Person or Person’s Digitally Compromised
- Gain Information
- Information Used To Gain Confidence
- Confidence Used To Exploit Someone or Gain Advantage
  - Think Old Time Confidence Man
  - Think About Dating and Relationships
  - Think About Contract Negotiations
- Sometimes Confidence and Information Used To Steal
- Then It Becomes Criminal
War Stories

#5 Social Engineering – Spear Phishing

Spouse’s Name
Kids’ Names
Parents’ Names
Relationship
Favorite Food
Vacation Spots
Hometown
Your Birthday
Family Birthdays
Employment
Pets’ Names
Your Schools
Kids’ Schools
Hospital Visits
Dentist & Doctor
Success Stories
Tragedies & Rest of Your Life

REMEMBER THIS!

> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team

You received this mandatory email service announcement to update you about
important changes to your Google product or account.
False Sense of Cyber Security – It Cannot Did Happen To Me!

Stories of Actual Breaches

War Stories

#5 Social Engineering – Spear Phishing

W. I. R. E. when you Wire

1. Proper Identification
2. Verbal Confirmation
3. Delivery Verification

What

I

R

E

require

Every

Time

Investors Title
## False Sense of Cyber Security – It Cannot Happen To Me!

**War Stories**

**#6 Employee Theft**

<table>
<thead>
<tr>
<th>Employee Theft Statistics</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount stolen annually from U.S. businesses by employees</td>
<td>$50,000,000,000</td>
</tr>
<tr>
<td>Percent of annual revenues lost to theft or fraud</td>
<td>7 %</td>
</tr>
<tr>
<td>Percent of employees who have stolen at least once from their employer</td>
<td>75 %</td>
</tr>
<tr>
<td>Percent of employees who have stolen at least twice from their employer</td>
<td>37.5 %</td>
</tr>
<tr>
<td>Percent of all business bankruptcies caused by employee theft</td>
<td>33 %</td>
</tr>
</tbody>
</table>

2015 Numbers
False Sense of Cyber Security – It **DID** Happen To Me!

**Stories of Actual Breaches**

**War Stories**

#6 Employee Theft

<table>
<thead>
<tr>
<th>Amounts Stolen</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1,000,000 and up</td>
<td>25.3 %</td>
</tr>
<tr>
<td>$500,000 – $999,999</td>
<td>9.6 %</td>
</tr>
<tr>
<td>$100,000 – $499,999</td>
<td>28.2 %</td>
</tr>
<tr>
<td>$10,000 – $49,999</td>
<td>16.8 %</td>
</tr>
<tr>
<td>$1,000 – $9,999</td>
<td>7 %</td>
</tr>
<tr>
<td>$1,000 or less</td>
<td>1.9 %</td>
</tr>
</tbody>
</table>

**2015 Numbers**

- Median Amount: $175,000
- 25.3% of breaches involved theft of amounts $1,000,000 and up
- 9.6% of breaches involved theft of amounts $500,000 – $999,999
- 28.2% of breaches involved theft of amounts $100,000 – $499,999
- 16.8% of breaches involved theft of amounts $10,000 – $49,999
- 7% of breaches involved theft of amounts $1,000 – $9,999
- 1.9% of breaches involved theft of amounts $1,000 or less

Investors Title

---

**Demographics**

<table>
<thead>
<tr>
<th>Demographics</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Men</td>
<td>59.1 %</td>
</tr>
<tr>
<td>Women</td>
<td>40.9 %</td>
</tr>
<tr>
<td>High School Degree</td>
<td>34 %</td>
</tr>
<tr>
<td>Some College</td>
<td>21 %</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>34 %</td>
</tr>
<tr>
<td>Postgraduate Degree</td>
<td>11 %</td>
</tr>
</tbody>
</table>

**2015 Numbers**

- 26% discovered by employee tip
- Median amount: $175,000

Investors Title
Preventive Medicine Plan

**C. Y. B. E. R.**

Can

You

Be

Entirely

Ready?

---

Preventive Medicine Plan

1. Risk Assessment
2. Privacy Officer
3. Access Limited To Authorized Personnel Only
4. Physical Security of NPI
5. Digital and Electronic Security aka Network Security
6. Disposal and Decommissioning of NPI
7. Disaster Management Plan
8. Oversight of Service Provider Handling NPI
10. Audit Procedures And Oversight of Information Security Program
11. Cyber-Fraud Insurance
Preventive Medicine Plan

Element #1 – Risk Assessment

- Unauthorized access to NPI within the Company records
- Unauthorized request for access to the Company records
- Interception of data during transmission
- Loss of data in a natural disaster
- Corruption of data or systems
- Misplacement or loss of paper records containing NPI
- Compromise of NPI from disposal of records or equipment
- Unauthorized or unintended disclosure of electronic or printed NPI
- Failure to adequately monitor third party service providers and risks that third party providers could improperly use NPI

Preventive Medicine Plan - Information Security

Element #2 – Privacy Officer

- Assess the Risks to NPI
- Assess Procedures for Monitoring Potential Threats To NPI
- Evaluate Procedures for and Methods of Detecting, Preventing and Responding to Identified Threats
Preventive Medicine Plan - Information Security

Element #3 – Access Limited To Authorized Personnel
- Acknowledge Policy
- Criminal Background Checks (Going Back 5 Years)
  - Pre-Hire
  - Every 3 Years Post Hire
- Only Authorized Employees Access NPI
- Assign User Rights To Employee
- Terminate Employee Privileges Immediately Upon Separation

False Sense of Cyber Security – It Cannot DID Happen To Me!

Preventive Medicine Plan - Information Security

Element #4 – Physical Security of NPI
- Clean Desk Policy
- Privacy Policy
- Employee Access to NPI
- Physical/Location Security
- Removable Media
False Sense of Cyber Security – It Cannot Happen To Me!

So What Do I Do?

Preventive Medicine Plan – Information Security

Element #5 – Digital & Electronic Security/Network Security

- Digital Security - Updated Systems, including OS security updates
- Backup Data - Performed Daily and Stored in a Secure Offsite Location.
- Internet Security - Antivirus, Anti-Malware, Firewalls Anti-Spyware
- Password Policy – Strong Passwords Changed At Least Every 3 Months
- Encrypted Email – Use it

Element #6 – Disposal and Decommissioning of NPI

- Paper & Files Containing NPI
- Computers and Digital Devices Containing NPI
Preventive Medicine Plan - Information Security

Element #7 – Disaster Management Plan

- Create an Information Systems Disaster Recovery Plan
- Protect Against:
  - Interruption To Business
  - Hardware Failures
  - Software Failures
  - Environmental Events
  - Theft

Element #8 – Oversight of Service Provider Handling NPI

Types of Third Party Service Providers

- Independent Searchers
- Couriers
- Janitorial Service
- Alarm Company
- HVAC, Plumbing, Electrical
- Off Site Storage
- IT Professionals
Preventive Medicine Plan - Information Security

Element #9 – Notification of Security Breaches for NPI

- All Employees and Third Party Service Providers Should Report Breaches of the Information Security Policy.
- If a Breach Occurs, Everyone Should Work with Affected Clients, Consumers, and Local Law Enforcement as appropriate.

Element #10 – Audit Procedures And Oversight of Information Security Program

- Should Test Systems for Proper Operation
- Should Review Policies Annually For Potential New Threats and Security Measures
- Should Review Professional Best Practices for New Procedures and Protections
- Should Stay On Top of Information Security
Preventive Medicine Plan - Information Security

Element #11 – Cyber-Fraud Insurance

When All Else Fails;
Have a Plan B -
Cyber-Fraud Insurance

I TOLD YOU SO . . . Comes 2 Ways

1) When You Look In The Mirror After A Loss

2) When Your Insurance Agent Tells You, When He Gives You a Check

Either Way, I Told You So Is Coming.
Thank You

Credits and Other Sites For Information

- http://invtitle.com
- http://alta.org/bestpractices
- https://www.fbi.gov/investigate/cyber
- https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/

Other than Investors Title Logos and Images, No Claim of Ownership is Made to Any of The Other Images Contained Herein