

# Wire Fraud: The Cyber Threat to the Real Estate Industry

Be Vigilant and Make the Phone Call!



Scott Stevenson, Esq.  
CEO, Northwest Title

Scott.Stevenson@nwttitle.com  
614-610-9909 (direct)

## You and Your Clients Are Under Attack!



## You and Your Clients Are Under Attack!

Why The Real Estate Industry?

1. Path of Least Resistance
  - Customer Service Oriented
2. Electronic Transfers of Funds for Real Estate Closings
3. Social Media & Internet Friendly



### 3 CYBER FRAUD LAWS



**Law #1:** There will always be cyber fraud

Cyber fraud does not disappear, but is transformed

**Law #2:**



**Law #3:** Cyber fraud follows the path of least resistance



## You and Your Clients Are Under Attack!



## Cyber Fraud in Real Estate Headlines

### Attorney Hacked 1.9M deposit lost:

- A Manhattan couple wired a \$1.9 million earnest money deposit for their new co-op but learned that the messages from an AOL e-mail account hid a crucial detail: They got conned.
- Robert Millard, a managing partner at Realm Partners, and his wife, Bethany, blame their real estate attorney, Patricia Doran, for "cybercriminals" stealing the 10 percent deposit intended for a Manhattan co-op they were buying for \$19.4 million, according to a new lawsuit filed in New York State Supreme Court.
- The Millards claim that Doran's use of an AOL e-mail account and her lack of computer security essentially served as a neon sign welcoming hackers to snatch their money.



## Cyber Fraud in Real Estate Headlines

### Going After **Sellers and Buyers** with Fake Realtor and Title Company Looking Emails:

- Usually a home buyer/seller gets an email from what appears to be the real estate agent or a title company requesting a transfer of funds for escrow or the down payment.
- The email appears to be coming from the company handling the transaction, the agent, attorney or title insurance officer.
- "One person we heard about doing this was slick — he knew the terms about closing and said all the right words," said Mary Frances Burleson, CEO of Dallas' Ebby Halliday Realtors.

## Cyber Fraud in Real Estate Headlines



It only takes one person in the transaction to click on the wrong email link to start this process and allow the cybercriminal into a transaction.



## Social Engineering & Computer Intrusion Techniques



## Social Engineering

### Social Engineering:

Is the psychological manipulation of people into performing actions or divulging confidential information.

A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

**Social  
Engineering**



The clever  
manipulation  
of the natural human  
tendency to trust!

## Social Engineering & Computer Intrusion Techniques

Today's Forms of Social Engineering:

- Vishing or Phone Phishing
- Phishing
- Spear Phishing



## Social Engineering & Computer Intrusion Techniques

### Vishing or Phone Phishing:

The victim is prompted to call or log into "their bank" via a phone number or provided link in order to "verify" information. A typical "vishing" system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords.



### FRAUD NOTICE

FRAUDULENT PHONE CALLS REQUESTING INFORMATION



## Social Engineering & Computer Intrusion Techniques

### Phishing:

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided.

The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN or a credit card number.



## Social Engineering & Computer Intrusion Techniques

### Spear Phishing

Is a targeted form of phishing in which fraudulent emails target specific organizations in an effort to gain access to confidential information.

The objective of spear phishing and phishing are ultimately the same—to trick a target into opening an attachment or click on a malicious embedded link.



### The Usual Suspect:

#### What Phishing Emails Looked Like Before 2016

They were fraught with “red flags” that would give the receiver an opportunity to quickly realize the email was “Phishing”

**From:** University of California <[biblioteca@al.ce.gov.br](mailto:biblioteca@al.ce.gov.br)> ← Odd "from" address  
**Date:** March 18, 2012 2:31:53 PM PDT  
**To:** [webteam@ucdavis.edu](mailto:webteam@ucdavis.edu) ← Unprofessional punctuation  
**Subject:** Protect Your Email Now!!!! ← Unprofessional punctuation  
**Reply-To:** [University@dns1.al.ce.gov.br](mailto:University@dns1.al.ce.gov.br), [of@dns1.al.ce.gov.br](mailto:of@dns1.al.ce.gov.br), [California@dns1.al.ce.gov.br](mailto:California@dns1.al.ce.gov.br) ← Odd "reply" addresses

## UC DAVIS

Your email account has been reported for numerous spams Activities from a foreign ip recently. As a result of this the UC Davis ITS has received advice to suspend your account.

However, you might not be the one promoting this Spam as your email account might have been compromised.

To protect your account from sending spam mails, You are to confirm your true ownership of this account by Clicking on this link below to Login and confirm in one simple step. On receipt of the requested information, the UC Davis Web-Mail email support shall block your account from Spam.

<http://www.123contactform.com/form-302435/University-Of-California> ← Links to external websites

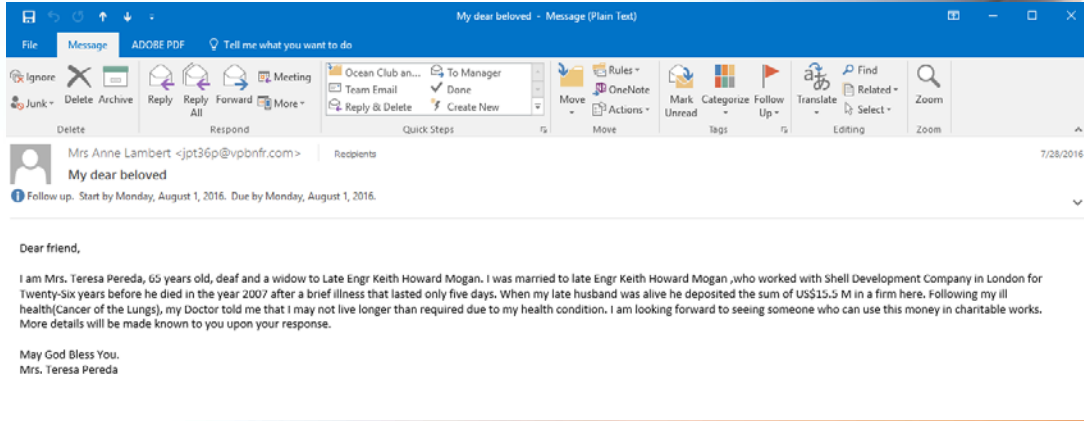
Failure to do this will violate the UC Davis Web-Mail terms & conditions. This will render your account inactive. ← Use of threats

**NOTE!!!** You will be sent a password reset message In next seven (7) working days after undergoing this process for Security reasons.

---

University of California, Davis One Shields Avenue Davis, CA 95616 (530) 752-1011  
 Questions or comments? | Last update: March 16, 2012  
 Copyright © The Regents of the University of California, Davis campus. All rights reserved.

## The Usual Suspect: Not Long To Live, give my money to Charity please!



☀ ID: 133 - Account Alert! (Oct. 2015)



Microsoft account team (outlook.teeam@outlook.com) Add to contacts 12:15 AM

To: account-security-nonreply@account.microsoft.com



Dear Outlook user,

You have some blocked incoming mails due to our maintenance problem.

In order to rectify this problem, you are required to follow the below link to verify and use your account normally.

Please click below to unlock your messages, it takes a few seconds.

**Verify Your Account**

<http://spapparelsindia.in/Aprons/outlook.com/login.html>

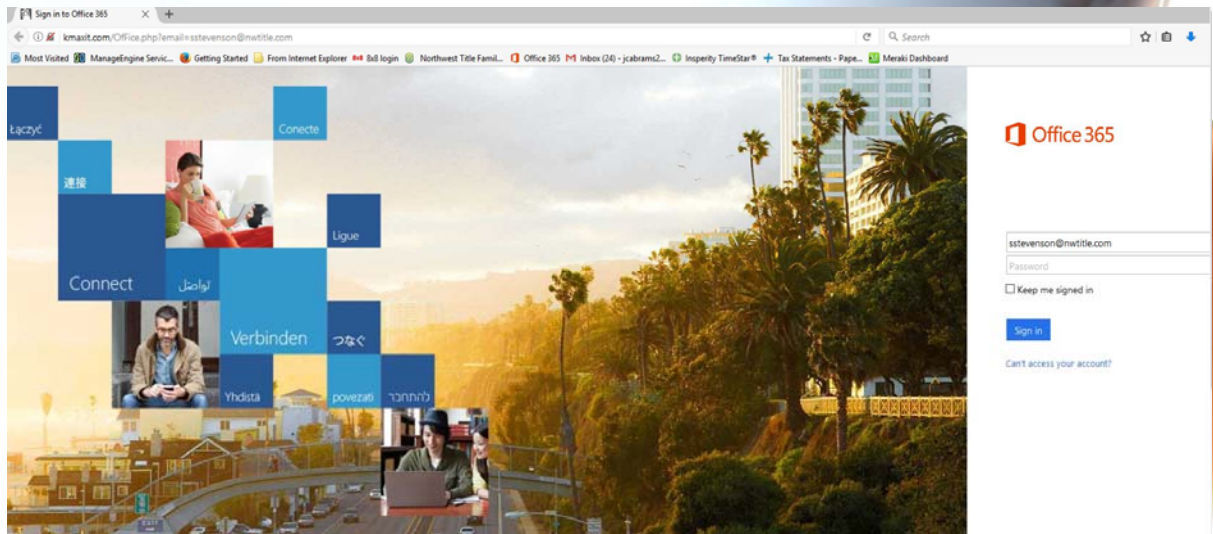
We apologize for any inconvenience and appreciate your understanding.

Thanks.

The Microsoft account team™



### Fraudulent Landing Page Seeks Login & Password



Step 1:  
Locating  
target is as  
easy as using  
Zillow!

**CONTACT AGENT** **Spear Phishing a Real Estate Seller** EXPAND CLOSE

Public View Owner View

**248 E Gay St # TH33,  
Columbus, OH 43215**

**FOR SALE**  
**\$539,900**

EST. MORTGAGE  
\$2,118/mo

**CONTACT AGENT**  
**Lari Madosky Shaw**  
★★★★★ (3)  
8 Recent sales  
Coldwell Banker King  
Thompson - Arlington /  
Clintonville / Grandview  
Regional  
(614) 619-9141

## Spear Phishing a Real Estate Seller

Step 2:  
Search for  
property  
address on  
Auditor's  
Web Site!

Clarence E. Mingo, II  
Franklin County Auditor

Our Office | Your Property | **Search** | On-Line Tools | Reference | Contact Us

ParcelID: 010-290109-00 | Map-Rt: 010-T191-064-00  
**HOEPFNER LARRY A** | 248 E GAY ST

1 of 1  
Return to Search Results

**Actions**

- Neighborhood Sales
- Proximity Search
- Printable Version
- Custom Report Builder

**Reports**

- Proximity Report
- Map Report
- Parcel Summary
- Parcel Detail

**Social Media Links**

View Google Map

**Most Recent Transfer**

Step 3:  
Search for Seller in all  
Social Media to locate  
emails, phone numbers,  
personal information,  
habits, likes/dislikes,  
family, etc.

Search for people, jobs, companies, and more...

Home | Profile | My Network | Learning | Jobs | Interests

**Larry Hoepfner** 2nd

C-Level Executive | Business Operations |  
 larryhoepfner@gmail.com | (614) 309-1397  
 Columbus, Ohio Area | Sports

Previous: Columbus Blue Jackets, Fox Sports Florida,  
 MediaOne/Continental Cablevision

Education: University of Miami - School of Business

Connect | Send Larry InMail | 500+ connections

https://www.linkedin.com/in/larryhoepfner

**Background**

**Summary**

Larry Hoepfner  
 larryhoepfner@gmail.com  
 614-309-1397

Senior-level corporate executive and sports / entertainment business operations expert, with two decades of proven experience in roles including Executive Vice President of Business Operations. Offer diverse portfolio of strengths encompassing revenue and business development, marketing management and strategic planning proficiencies. Track record entails accountability for organization's P&L – spanning \$80+ million in revenues, \$8 million budgets, and 85 staff – and oversight of teams charged with securing \$24 million in corporate sponsorships and local television rights as well as \$35 million in ticket sales.

## Spear Phishing a Real Estate Seller

Step 4:  
Copy  
Realtor's  
headshot



Step 5:  
Create new email  
account in  
Hotmail/gmail/etc.  
using Realtor's name  
for the email address.

## Real or Fake?

**Real or Fake?**

Confirmation about your Chase account - Message

File Message ADOBE PDF Tell me what you want to do

Ignore Delete Archive Reply Reply Forward Meeting example fraud... To Manager  
Junk Delete Archive Reply Reply Forward All Team Email Done  
Delete Respond Reply & Delete Create New Move OneNote Mark Unread Categorize Follow Up Translate Related Select

Thu 3/30/2017 9:24 AM

Chase <no-reply@alertsp.chase.com>  
Confirmation about your Chase account

To jonathan.holfinger@gmail.com; Escrow Admin; Justin Luke; Paul Nyikes; Scott Stevenson

**CHASE**

We're confirming that you recently:

- changed your Account Alert preferences, or
- updated the Chase Mobile(R) app on your device, or
- updated your device's operating system.

If you have not performed any of the actions mentioned above, please log on to [www.chase.com](http://www.chase.com) or call 1-877-CHASEPC (1-877-242-7372) immediately.

To see all of the Alerts available to you, please log on to [www.Chase.com](http://www.Chase.com).

To reply to this Alert, please send us a secure message from your inbox on [www.Chase.com](http://www.Chase.com).

**Real**

Confirmation about your Chase account - Message

File Message ADOBE PDF Tell me what you want to do

Ignore Delete Archive Reply Reply Forward Meeting example fraud... To Manager  
Junk Delete Archive Reply Reply Forward All Team Email Done  
Delete Respond Reply & Delete Create New Move OneNote Mark Unread Categorize Follow Up Translate Related Select

Thu 3/30/2017 9:24 AM

Chase <no-reply@alertsp.chase.com>  
Confirmation about your Chase account

To jonathan.holfinger@gmail.com; Escrow Admin; Justin Luke; Paul Nyikes; Scott Stevenson

**CHASE**

We're confirming that you recently:

- changed your Account Alert preferences, or
- updated the Chase Mobile(R) app on your device, or
- updated your device's operating system.

If you have not performed any of the actions mentioned above, please log on to <http://www.chase.com> or call 1-877-CHASEPC (1-877-242-7372) immediately.

To see all of the Alerts available to you, please log on to [www.Chase.com](http://www.Chase.com).

To reply to this Alert, please send us a secure message from your inbox on [www.Chase.com](http://www.Chase.com).

Real or Fake?

Mailbox full "s Stevenson"

File Message ADOBE PDF Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward More Meeting Moving Memb... To Manager Team Email Done Reply & Delete Create New Rules OneNote Mark Categorize Follow Unread Tags

Mon 3/27/2017 3:08 PM

Mail Support <mailsupport@emailsrv.net>  
Mailbox full "s Stevenson@nwtitle.com"

To Scott Stevenson

You forwarded this message on 3/27/2017 3:25 PM.

Dear user: s Stevenson

4 messages pending delivery,

**Because your mailbox "s Stevenson" is full.**

**50687 MB 50688 MB**

You can not receive/send new messages. Please click the URL below to increase your mailbox size.

<http://nwtitle.com/s Stevenson/&path=/mail/upgrade>

Webmail Admin

Copyright (c) Webmail 2001-2017. All rights reserved

Real or Fake?

You have r

File Message ADOBE PDF Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward More Meeting Moving Memb... To Manager Team Email Done Reply & Delete Create New Rules OneNote Mark Categorize Follow Unread Tags

Wed 3/29/2017 11:56 AM

Facebook 3 friend request <notification+vy760h3detfw@arrowtitle.com>  
You have notifications pending

To joelle@quixnet.net

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

**facebook**

Hi,

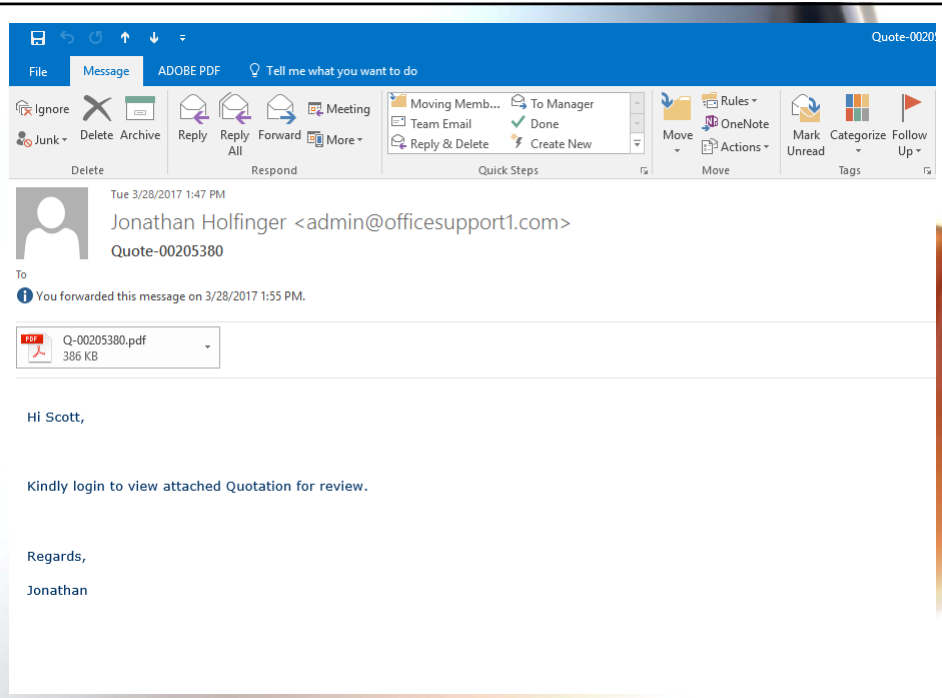
Here's some activity you have missed on Facebook.

3 friend request

[Go To Facebook](#) [See All Notifications](#)

This message was sent to [joelle@quixnet.net](mailto:joelle@quixnet.net). If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).  
Facebook, Inc. Attention: Department 415 P.O. Box 10005 Palo Alto CA 94303

## Real or Fake?





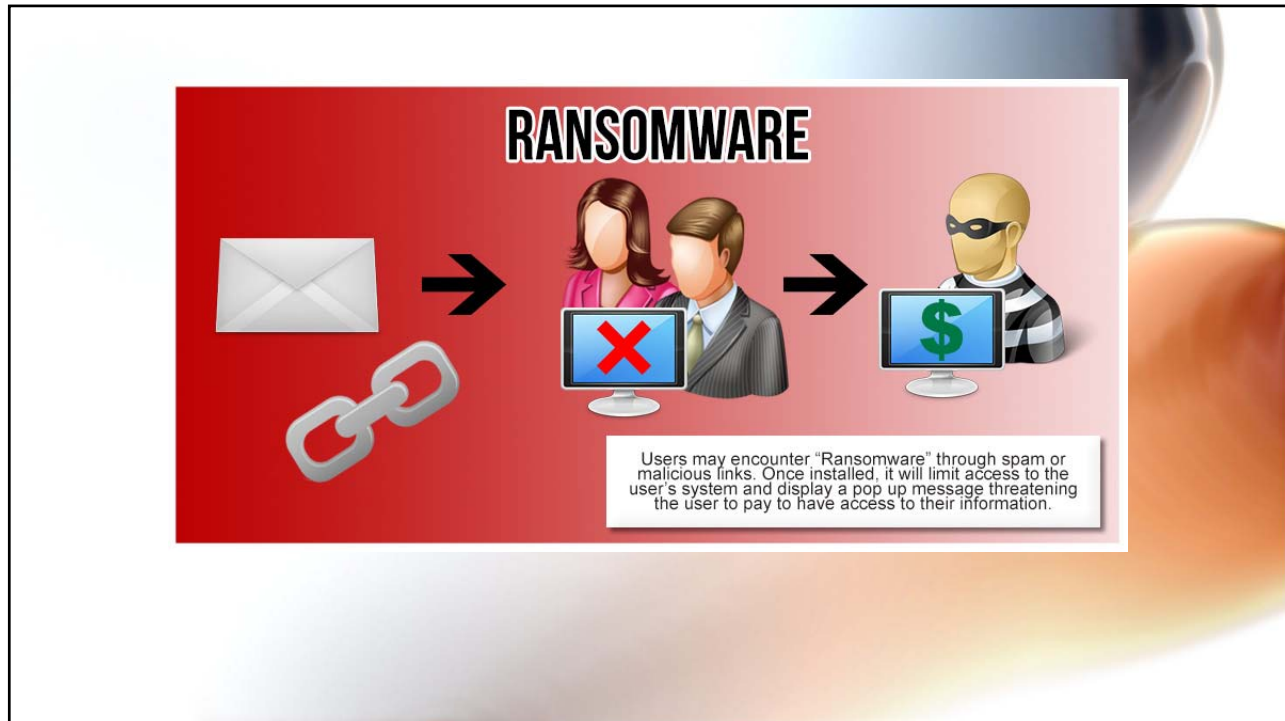
Your money  
or your data

**Ransomware**  
From the beginning of the year, ransomware attacks have bombarded like never before. In total, there is an increase of 500% in malware spread.

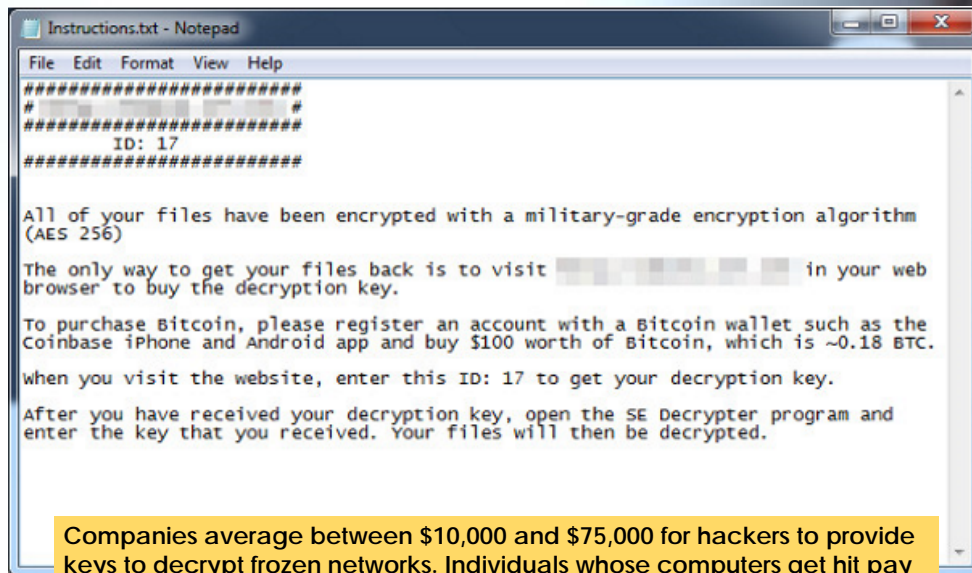
Growth in Ransomware Infections




Month	Infections
Dec-15	30,000
Jan-16	28,000
Feb-16	30,000
Mar-16	55,000
Apr-16	38,000




## Ransomware




Companies average between \$10,000 and \$75,000 for hackers to provide keys to decrypt frozen networks. Individuals whose computers get hit pay as little as \$100 to \$300 to unlock their encrypted files.



**LickingCounty**  
licounty.com: Your Link to Licking County Services





**Newark, Ohio: January 30<sup>th</sup> through February 15<sup>th</sup>, 2017**


- The more than 1,000 county employees were without working office phones, email and internet access.
- Some data from Jan. 30 and Jan. 31 could not be retrieved, so employees are recreating lost data.
- 150 County Servers had to be rebuilt
- 9-1-1 services stopped
- No real estate transactions were processed during this time.



## Have I Sufficiently Scared You Yet?



## Protecting Yourself and Your Client

 Word of the Day

# vigilant

*adjective* [vij-uh-luhnt]



keenly watchful  
to detect  
danger; wary.

Dictionary.com

1. Passwords & Password Managers
2. 2-Step Verification of all Accounts
3. Anti-Fraud Disclosure To Consumers
4. Add anti-fraud language to your email signature
5. Get Professional IT Help for your business and home computers
6. Cyber Liability Insurance Policy

## Protecting Yourself and Your Client

**PASSWORDS ARE LIKE  
UNDERPANTS**



Change them often, keep them private and never share them with anyone.

## Protecting Yourself and Your Client

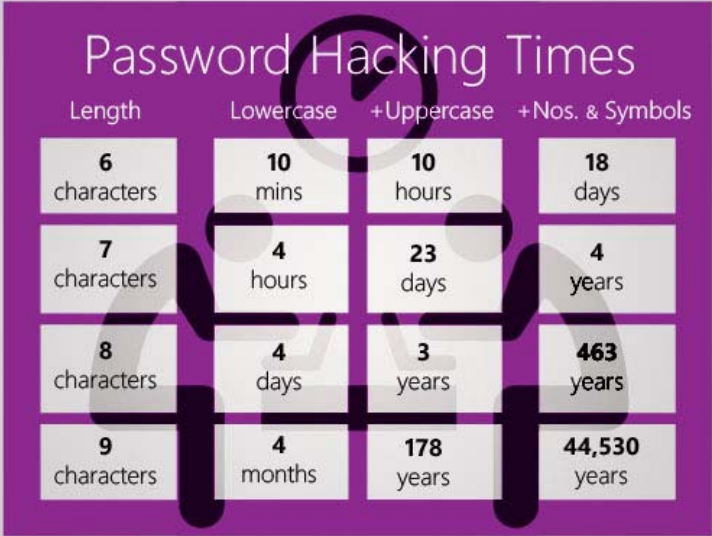
### The 50 Most Used Passwords

- |              |              |                |              |             |
|--------------|--------------|----------------|--------------|-------------|
| 1. 123456    | 11. 123123   | 21. mustang    | 31. 7777777  | 41. harley  |
| 2. password  | 12. baseball | 22. 666666     | 32. f*cky*u  | 42. zxcvbnm |
| 3. 12345678  | 13. abc123   | 23. qwertyuiop | 33. qazwsx   | 43. asdfgh  |
| 4. qwerty    | 14. football | 24. 123321     | 34. jordan   | 44. buster  |
| 5. 123456789 | 15. monkey   | 25. 1234...890 | 35. jennifer | 45. andrew  |
| 6. 12345     | 16. letmein  | 26. p*s*y      | 36. 123qwe   | 46. batman  |
| 7. 1234      | 17. shadow   | 27. superman   | 37. 121212   | 47. soccer  |
| 8. 111111    | 18. master   | 28. 270        | 38. killer   | 48. tigger  |
| 9. 1234567   | 19. 696969   | 29. 654321     | 39. trustno1 | 49. charlie |
| 10. dragon   | 20. michael  | 30. 1qaz2wsx   | 40. hunter   | 50. robert  |

Howsecureismypassword.net

Password Hacking Times

Length	Lowercase	+Uppercase	+Nos. & Symbols
6 characters	10 mins	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	44,530 years



## Protecting Yourself and Your Client

LastPass \*\*\*\*

RoboForm

### Passwords Manager

One Master Password to access the account

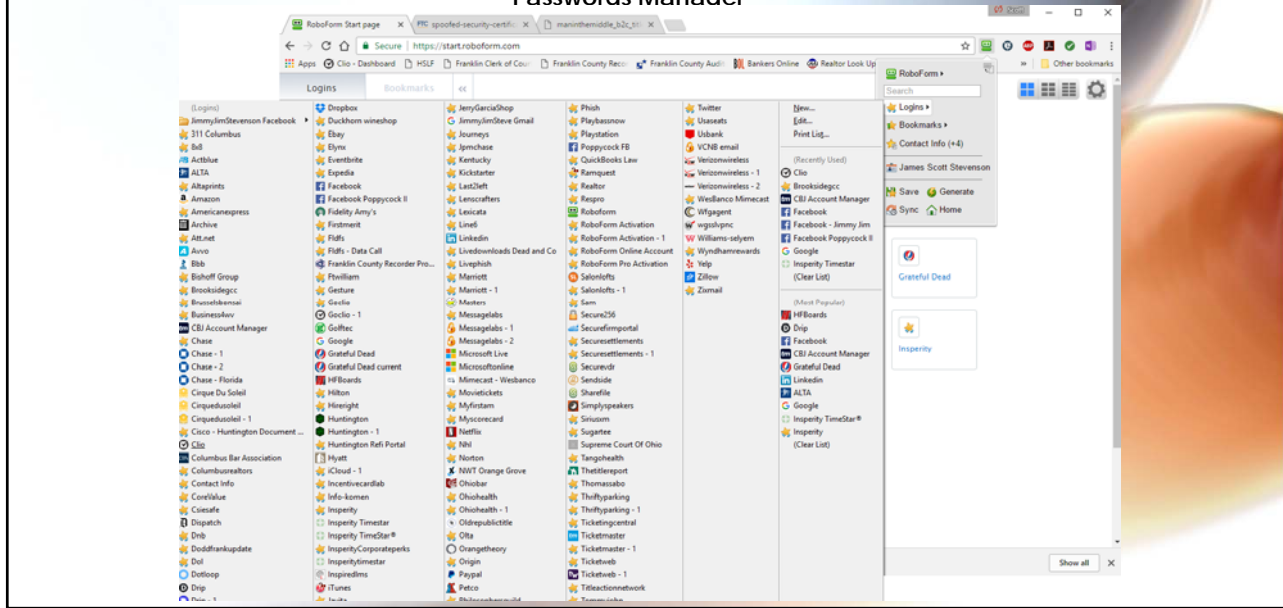
Access the your passwords on any device

Saves and even Creates passwords "X3\$asicke!()<.1"



# Protecting Yourself and Your Client

## Passwords Manager



## 2-Step Verification of Password: Just Do It!

# EMAILS FOR SALE: DARK WEB VENDOR PEDDLES DECRYPTED GMAIL, YAHOO ACCOUNTS

RT.COM 2 DAYS



Published time: 7 Mar, 2017 04:13

TOP NEWS TODAY

## 2-Step Verification of Password: Just Do It!

### EMAILS FOR SALE: DARK WEB VENDOR PEDDLES DECRYPTED GMAIL, YAHOO ACCOUNTS

Published 1 hour 11 min ago



TOP NEWS TODAY

- One million accounts could be compromised and for sale on the dark web.
- A user called SunTzu583 is auctioning off 500,000 Gmail accounts for 0.0219 bitcoin (\$28.24) in one auction and 450,000 in another for 0.0199 bitcoin (\$25.74).

The compromised accounts occurred between 2010 until 2016, through third parties such as: **Tumblr, LastFM, Adobe, Dropbox, Xbox 360, MySpace, Flash Flash Revolution, LookBook, etc.**

However, it is recommended that users affected by breaches in the past change their passwords

## 2-Step Verification of Password: Just Do It!

When you enable **2-Step Verification** (also known as **two-factor authentication**), you add an extra layer of security to your account. You sign in with something you know (your password) and something you have (a code sent to your phone).

### What are Login Approvals?

Login Approvals is an extra layer of security that uses your phone to protect your account.

#### How it works



When logging in from an unknown browser, you'll need a security code.



You can only get security codes from your phone. [?]

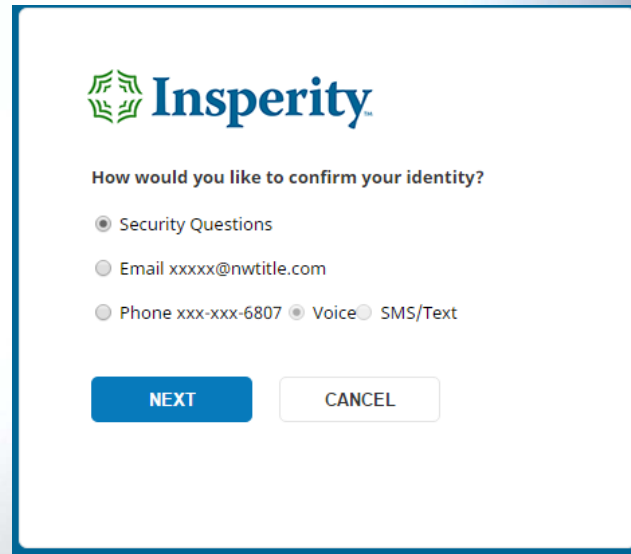



By entering the code, you can prove that it's really you trying to log in.

**Get Started**

Cancel

## 2-Step Verification of Password: Just Do It!

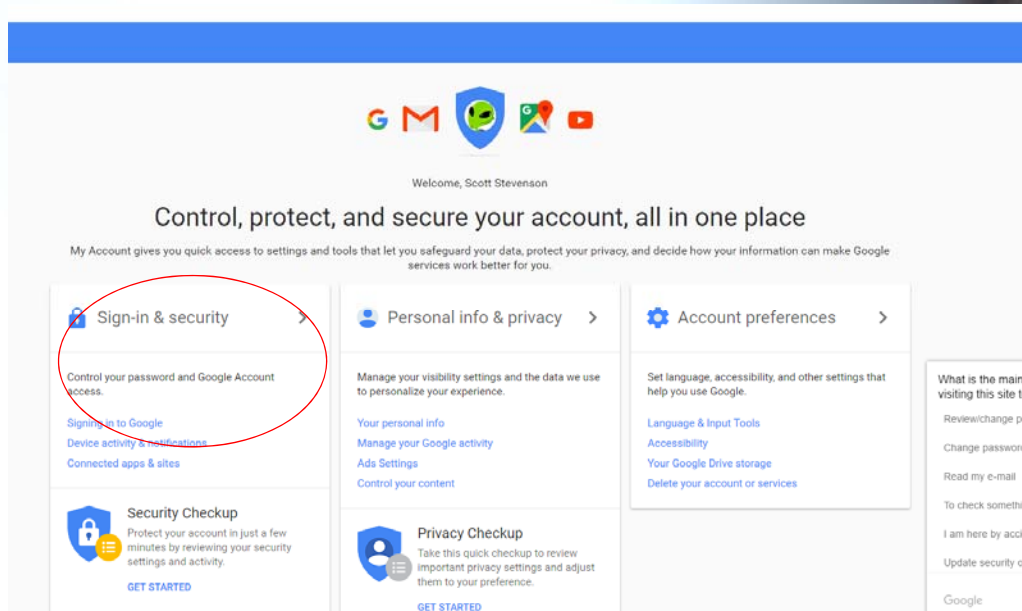


 **Insperity**

How would you like to confirm your identity?

Security Questions  
 Email xxxxx@nwtitle.com  
 Phone xxx-xxx-6807  Voice  SMS/Text






## 2-Step Verification of Password: Just Do It!

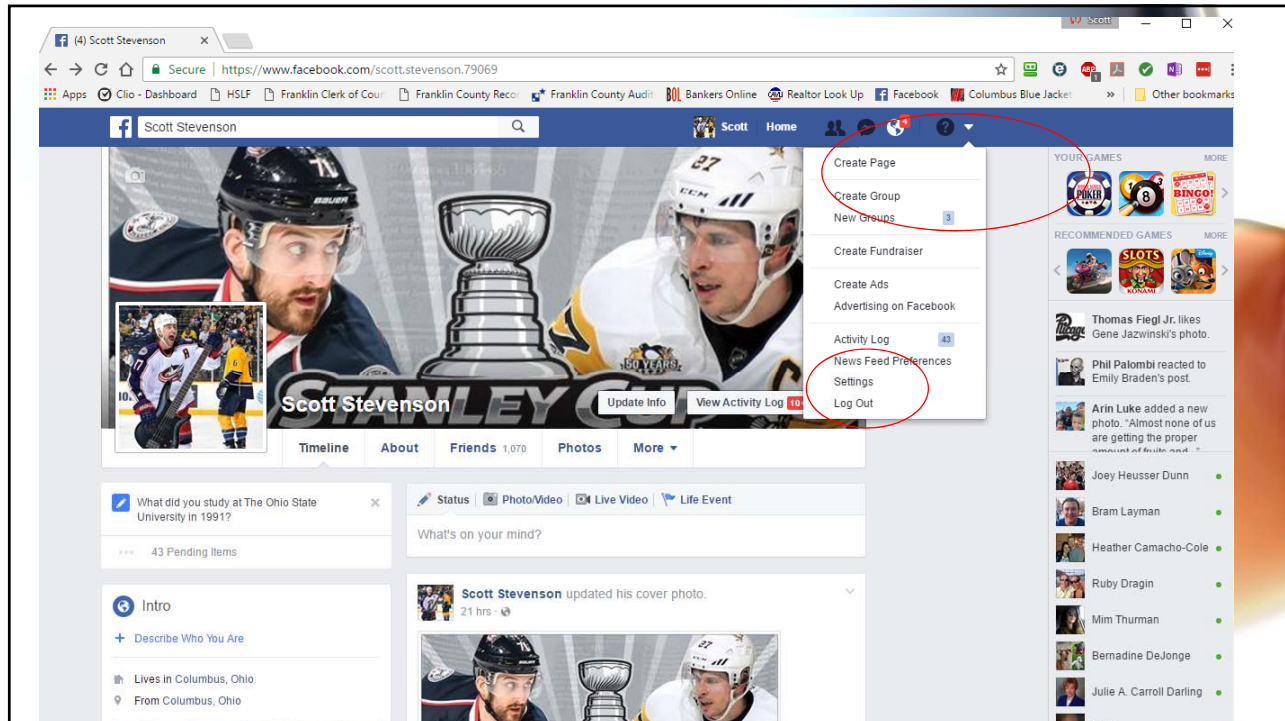


Welcome, Scott Stevenson

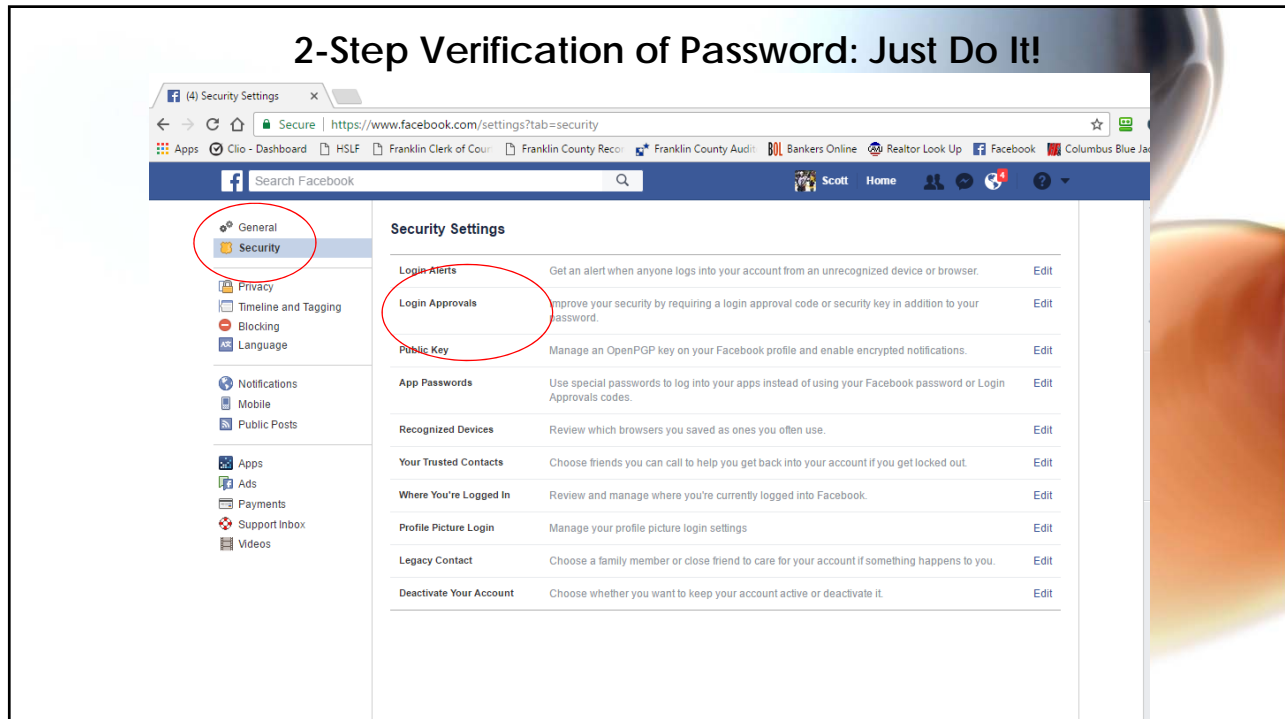
Control, protect, and secure your account, all in one place

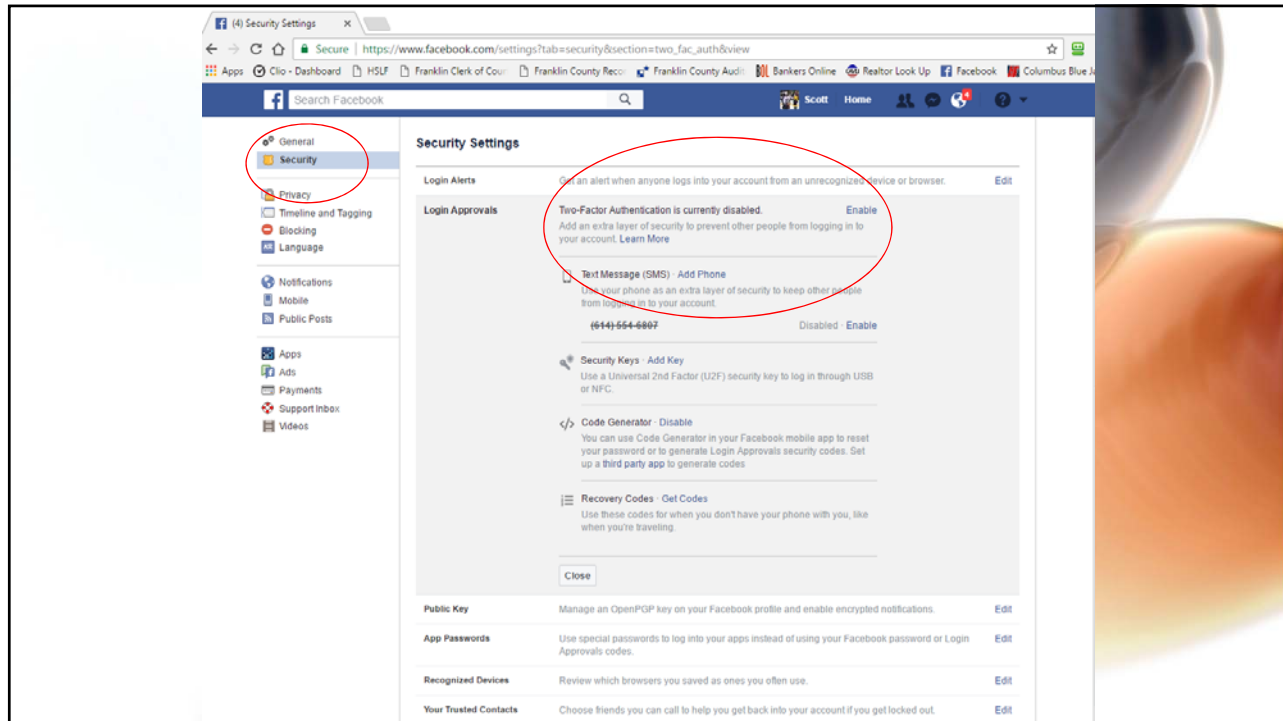
My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

<p> <b>Sign-in &amp; security</b></p> <p>Control your password and Google Account access.</p> <p><a href="#">Signing in to Google</a>  <a href="#">Device activity &amp; notifications</a>  <a href="#">Connected apps &amp; sites</a></p> <p> <b>Security Checkup</b>        Protect your account in just a few minutes by reviewing your security settings and activity.  <a href="#">GET STARTED</a></p>	<p> <b>Personal info &amp; privacy</b></p> <p>Manage your visibility settings and the data we use to personalize your experience.</p> <p>Your personal info  <a href="#">Manage your Google activity</a>  <a href="#">Ads Settings</a>  <a href="#">Control your content</a></p> <p> <b>Privacy Checkup</b>        Take this quick checkup to review important privacy settings and adjust them to your preference.  <a href="#">GET STARTED</a></p>	<p> <b>Account preferences</b></p> <p>Set language, accessibility, and other settings that help you use Google.</p> <p><a href="#">Language &amp; Input Tools</a>  <a href="#">Accessibility</a>  <a href="#">Your Google Drive storage</a>  <a href="#">Delete your account or services</a></p>	<p>What is the main reason for visiting this site today?</p> <p><a href="#">Review/change personal info</a></p> <p><a href="#">Change password</a></p> <p><a href="#">Read my e-mail</a></p> <p>To check something out, I am here by accident.</p> <p><a href="#">Update security or privacy settings</a></p> <p>Google</p>
---	--	---	---



## 2-Step Verification of Password: Just Do It!





# Protecting Yourself and Your Client

## ANTI-FRAUD DISCLOSURE TO CONSUMERS

Electronic communications such as email, text messages and social media messaging, are neither secure nor confidential. While **[Real Estate Brokerage]** has adopted policies and procedures to aid in avoiding fraud, even the best security protections can still be bypassed by unauthorized parties. **[Real Estate Brokerage]** will never send you any electronic communication with instructions to transfer funds or to provide nonpublic personal information, such as credit card or debit numbers or bank account and/or routing numbers.

YOU SHOULD NEVER TRANSMIT NONPUBLIC PERSONAL INFORMATION, SUCH AS CREDIT OR DEBIT CARD NUMBERS OR BANK ACCOUNT OR ROUTING NUMBERS, BY EMAIL OR OTHER UNSECURED ELECTRONIC COMMUNICATION. EMAILS ATTEMPTING TO INDUCE FRAUDULENT WIRE TRANSFERS ARE COMMON AND MAY APPEAR TO COME FROM A TRUSTED SOURCE.

If you receive any electronic communication directing you to transfer funds or provide nonpublic personal information, EVEN IF THAT ELECTRONIC COMMUNICATION APPEARS TO BE FROM **[Real Estate Brokerage]**, do not respond to it and immediately contact **[Real Estate Brokerage]**. Such requests, even if they may otherwise appear to be from **[Real Estate Brokerage]** are likely part of a scheme to defraud you by stealing funds from you or using your identity to commit a crime.

To notify **[Real Estate Brokerage]** of suspected fraud related to your real estate transaction, contact: **[designate email address and phone number that will be monitored for prompt local action and notification to Company]**.

ACKNOWLEDGMENT: I/we have read this Anti-Fraud Disclosure Statement and understand that **[Real Estate Brokerage]** will never send me/us any electronic communication with instructions to transfer funds or provide financial account numbers or other nonpublic personal information.

Signature (Date)



## Protecting Yourself and Your Client

### II. Email Signature TAG LANGUAGE\*

"Reminder: email is not secure or confidential. [Real Estate Brokerage] will never request that you send funds or nonpublic personal information, such as credit card or debit card numbers or bank account and/or routing numbers, by email. If you receive an email message concerning any transaction involving [Real Estate Brokerage], and the email requests that you send funds or provide nonpublic personal information, do not respond to the email and immediately contact [Real Estate Brokerage]. To notify [Real Estate Brokerage] of suspected email fraud, contact: [designate email address and phone number that will be monitored for prompt local action and notification to Company].



**WE DO NOT ACCEPT OR REQUEST**  
 CHANGES TO WIRING INSTRUCTIONS VIA EMAIL OR FAX.  
**Always call to verify.**

## Protecting Your Business: Cyber Liability Policy for real estate professionals

### Cyber Liability Insurance

(also called Cyber Risk Insurance and Data Breach Insurance)

is a type of small business insurance that covers the cost of dealing with the fallout of a data or monetary breach.

#### What Client Information do you maintain on your computer?

1. Bank Approval Information?
2. Social Security numbers?
3. Mortgage Payoff Account information/numbers?
4. Bank account information?
5. Driver's license numbers?

# Protecting Your Business: Cyber Liability Policy for real estate professionals

## How Cyber Liability Insurance Protects Real Estate and Title Businesses:

- **Cyber extortion expenses.** Sometimes cyber criminals hold your information "hostage" until you pay them. This is called "cyber extortion" and your insurance policy can help you pay the ransom.
- **Legal expenses.** After a data breach, your affected clients might decide to sue your business. Even if those lawsuits never reach a courtroom, you'll still have to pay for legal counsel and possibly a settlement.
- **Notification of affected parties.** In most states, the law requires businesses to notify affected parties after a data breach. Depending on the number of individuals involved, this could end up costing your business a significant amount of time — and money.
- **Credit monitoring services.** You may want to offer affected parties credit monitoring services in order to regain their trust and repair your relationship. Your insurance policy can help you pay for these services.
- **A marketing campaign.** After a data breach, your reputation may be tarnished — which is why your insurance policy helps you finance a marketing campaign to restore your image in the community.

# Cyber Insurance Coverage Comparison



	E&O Policy Endo 1	E&O Policy Endo 2	Package Cyber Policy	Privacy Policy A	Cyber Policy A	Cyber Policy B	Cyber Policy C
Privacy Liability (data breach)	Red	Green	Yellow	Green	Green	Green	Green
Cyber Liability (computer related breach)	Red	Green	Yellow	Green	Green	Green	Green
Notification Costs	Yellow	Green	Yellow	Green	Yellow	Green	Green
System Damage	Red	Green	Yellow	Green	Green	Green	Green
Business Interruption	Red	Green	Yellow	Green	Green	Green	Green
Multimedia Liability	Red	Green	Yellow	Green	Green	Green	Green
Cyber Threats/Extortion	Red	Green	Yellow	Green	Yellow	Green	Yellow
Funds Transfer Fraud	Red	Green	Yellow	Red	Red	Yellow	Green
Social Engineering (Loss of Funds)	Red	Green	Yellow	Red	Red	Yellow	Green
Reputational Damage/Public Relations	Red	Green	Yellow	Red	Red	Yellow	Green
Regulatory Actions & Investigations	Red	Green	Yellow	Red	Red	Yellow	Green
Retro Coverage	Yellow	Green	Yellow	Red	Green	Green	Green
Hotline/Risk Portal	Red	Green	Red	Green	Green	Green	Green
Average Cost	\$0	\$300	\$0	\$700	\$3,000	\$1,500	\$2,000
Legend:	Covered up to policy limit	Green					
	No Coverage	Red					
	Limited Coverage	Yellow					

## Where To Go For Outside Help

Bobby Kneisel  
CEO  
KTech Solutions  
[bobby.kneisel@ktechsolutionsllc.com](mailto:bobby.kneisel@ktechsolutionsllc.com)  
614.398.0999



Cyber Security:  
Protecting Brokerages

## Where To Go For Outside Help

Matthew J. Wyen  
CEO/ Co-Owner Simplicity Virtual  
[Matt.wyen@simplicityvirtual.com](mailto:Matt.wyen@simplicityvirtual.com)  
(614) 401-8138

Main Office - 614-721-4333  
Tech Support - 614-721-3337

website:  
<https://simplicityvirtual.com>



Cyber Security:  
Protecting your Small Business

# Where To Go For Cyber Insurance

Kaitlin Kelly  
 Fran Kelly Professional  
 Liability LLC

[www.TitleLiability.com](http://www.TitleLiability.com)

Direct: 610-413-2574

Office: 610-478-0400

Fax: 412-281-4716



Cyber Insurance:  
 Protecting Your Small Business

## Reduce Your Risk of Cyber-Fraud by Practicing Good Cyber Hygiene

- Do not click on suspicious emails, attachments or links
- Keep your operating system up to date on all devices
- Install antivirus software on all devices and keep it up to date
- Keep your firewall turned ON
- Turnoff, lock, or set to "time-out" when your computer/device is not in use
- Use strong passwords and change them every 90 days
- Do not use personal information for passwords, rather: one upper/lower; one special character; one number, etc.
- Consider individual employee accounts; non-shared email accounts
- Be careful what you download
- Avoid websites you don't trust
- Do not send wire information or other business sensitive data



# Wire Fraud: The Cyber Threat to the Real Estate Industry

Be Vigilant and Make the Phone Call!



**Scott Stevenson, Esq.**  
CEO, Northwest Title

**Scott.Stevenson@nwttitle.com**  
614-610-9909 (direct)