




# Cyberfraud & Real Estate

*with* **Karen Michaels, VP**

©2018 Fidelity National Title Group | Florida Agency



## What is Cyber Fraud?

When credit and financial information is stolen online by a hacker and used in a criminal manner.

Cyber crime is one of the fastest growing areas of crime in the United States.

The contents provided herein are for informational purposes only and are not intended to provide legal advice or opinions and should not be relied on for such purpose. Further, nothing within these materials is intended as an offer to create an attorney-client relationship and no such relationship is created based on the presentation of these materials.

Fidelity National Title Group, Chicago Title Insurance Company, Commonwealth Land Title Insurance Company and Fidelity National Title Insurance Company, and any and all parents, subsidiaries and related companies ("The Company") does not guarantee that the information reflects the most current legal developments nor that these materials are complete and/or without technical inaccuracies. Any parties receiving these materials should consult their own competent counsel for legal advice.

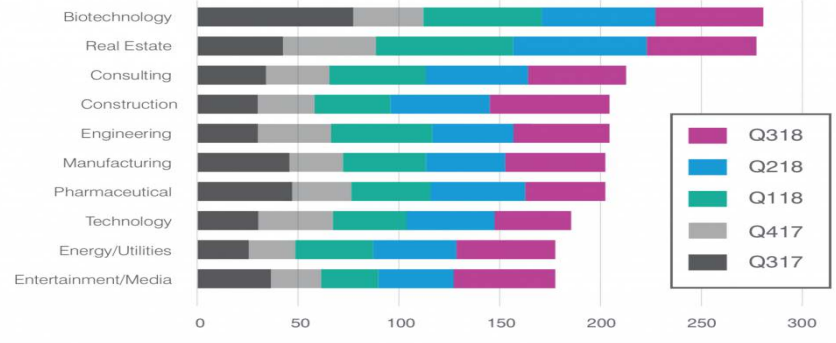
©2018 Fidelity National Title Group | Florida Agency



# Attacks by Industry

## Attacks by Industry

Biotech, medical device makers and real estate firms are targeted with email fraud more than other industries.



©2018 Fidelity National Title Group | Florida Agency



# Increasing!



©2018 Fidelity National Title Group | Florida Agency



## Cybersecurity Stats

1. Americans lost \$360 million in 2016, \$675 million in 2017 and over \$1 billion in 2018.
2. Cybercrime damages will hit \$6 trillion by 2021.
3. Cybersecurity spending to exceed \$1 trillion from 2017 to 2021.
4. Human attack surface to reach 6 billion people by 2022.
5. Global ransomware damage costs are predicted to exceed \$5 billion in 2017.

©2018 Fidelity National Title Group | Florida Agency



## Victims

### 2017 Victims by Age Group

Victims		
Age Range <sup>16</sup>	Total Count	Total Loss
Under 20	9,053	\$8,271,311
20 - 29	41,132	\$67,981,630
30 - 39	45,458	\$156,287,698
40 - 49	44,878	\$244,561,364
50 - 59	43,764	\$275,621,946
Over 60	49,523	\$342,531,972

©2018 Fidelity National Title Group | Florida Agency



## Cyber Crime Impact

Data breaches can impact a real estate business in 3 different ways

- Suffering financial harm from expenses resulting from the breach
- Legal risks from lawsuits from clients or others impacted
- Reputational risks from having to disclose the hack

©2018 Fidelity National Title Group | Florida Agency



## Types of Cyberfraud

Top 3 Types of Cyberfraud:

1. Phishing
2. Ransomware
3. Business Email Compromise Scam

©2018 Fidelity National Title Group | Florida Agency



## Phishing

- Real estate agents and title agents who respond, by opening a link, downloading a file or even replying can open the door to a gold mine of names, closing dates and money.
- By tracking email exchanges the hackers know who's buying, for how much, what the pay-off amount will be, and the timing of closing.

©2018 Fidelity National Title Group | Florida Agency



## Phishing

### Spotting Phishing Expeditions:

- Incorrect Grammar/Spelling/Text Body
- E-Mail Format/Absence of Logos/Plain Text
- Urgent Request for Personal Information
- Suspicious Attachments
- Links in the e-mail

©2018 Fidelity National Title Group | Florida Agency



## Phishing

The FBI recommends these safeguards to protect yourself from Phishing:

- Be suspicious of any unsolicited email requesting personal information or forms that ask for personal information
- Always compare the link in the email to the link that you are actually directed to
- Type the actual web address into the search bar instead of using a link
- Contact the actual business that supposedly sent the email

©2018 Fidelity National Title Group | Florida Agency



## Phishing Expedition - Result

Clicking on a link or opening an attachment in an email can result in Ransomware...

- *Ransomware* is an advanced malware that prevents you from accessing your PC or files until you pay a ransom

©2018 Fidelity National Title Group | Florida Agency



- Using the cookie tracking technology to steal financial information, passwords, and to take over your computer or system, in most cases anonymously.
- Intercepting emails related to financial information and stealing or changing data for financial gain (wire scams)
- A hacker impersonating a trusted friend, colleague, business, or your financial institution to access your personal information

©2018 Fidelity National Title Group | Florida Agency



## Ransomware

### **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 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia 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.**

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through \_\_\_\_\_

To pay the fine, you should enter the digits resulting code, which is located on the back of your \_\_\_\_\_ in the payment form and press OK (if you have several codes, enter them one after the other and press OK)



©2018 Fidelity National Title Group | Florida Agency



# Ransomware

**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.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / 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 server**.

Private key will be destroyed on  
**9/8/2013**  
**5:52 PM**

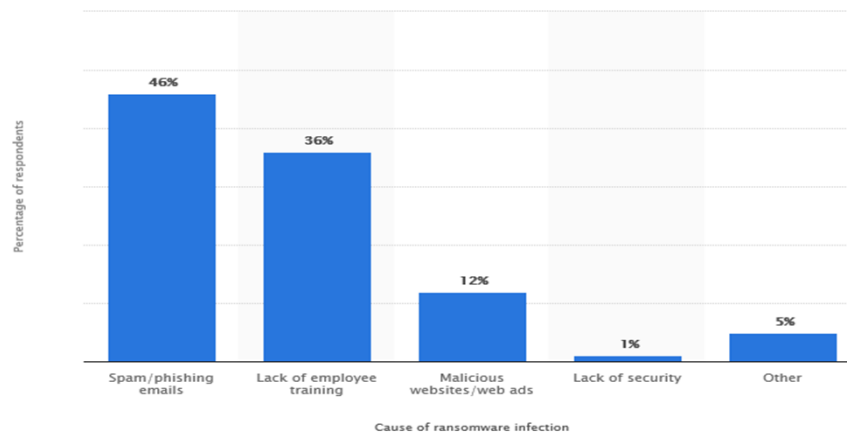
Time left:  
**56 : 16 : 12**

Next >>

©2018 Fidelity National Title Group | Florida Agency



# Ransomware



©2018 Fidelity National Title Group | Florida Agency





## Business Email Compromise

- Targets - Realtors, Loan Officers, Title Officers, and Escrow Officers
- Between December 2017 and May 2018, 136% increase in total losses.
- Fraudulent transfers have been sent globally to 115 countries.
- Since 2013, losses have topped \$12 billion.

©2018 Fidelity National Title Group | Florida Agency



©2018 Fidelity National Title Group | Florida Agency



## How It Works

- Intercepting emails related to financial information and stealing or changing data for financial gain (wire scams)
- Untrustworthy websites or emails containing bugs that track activity on your system
- Emails asking for financial or other personal private non-public information
- Uses a hacked email account or spoofed email account to initiate fraudulent transactions:
  - Email account is slightly different or has been altered. For example:
    - Legitimate email address: [john-doe@abc.com](mailto:john-doe@abc.com)
    - Fraudulent email address: [john\\_doe@abc.com](mailto:john_doe@abc.com) or [john-doe@abc.com](mailto:john-doe@abc.com)

©2018 Fidelity National Title Group | Florida Agency



## Other Methods for Hackers

- Using the cookie tracking technology to steal financial information, passwords, and to take over your computer or system, in most cases anonymously.
- A hacker impersonating a trusted friend, colleague, business, or your financial institution to access your personal information.
- Mouse-hack – using your wireless mouse to obtain passwords and other information on your computer.

©2018 Fidelity National Title Group | Florida Agency



## Who are The Hackers?

- Today's hackers are studying their marks closely.
- More sophisticated than before and not sending out emails with misspelled words or nonsensical messaging.
- They learn how to imitate the tone and style of an agent when emailing their victims.
- Once inside an agent's email, they get to know who's involved in the transaction which helps them come across as even more convincing.

©2018 Fidelity National Title Group | Florida Agency



## What Happens if You Do Get Hacked?

- Faster you take action afterward, the more likely you are to get some money back.
- Your bank might be able to recall the money, but only if you move quickly.
- Whether your bank can get the money back depends on whether or not the receiving bank has accepted it and whether there's a cancellation agreement in place between the two financial institutions or not.
- Whether you get your money back or not, you also want to report any incidences of wire fraud to the right authorities: the FBI, the Federal Trade Commission (FTC) and your local police force.

©2018 Fidelity National Title Group | Florida Agency



## Getting Hacked, contd.

- While reporting the wire fraud to the right authorities might not result in any action right away, it does help law enforcement to put together a case and begin to understand the patterns or methods a hacker might use to get private information and steal more victims' hard-earned money.
- Even if you do fall victim to wire fraud, your quick action is vital in preventing it from happening to other innocent homebuyers!

©2018 Fidelity National Title Group | Florida Agency



## Case Study #1

January 2019

- An Orlando couple wired a \$46,000 down payment to a title company they thought was legitimate, but later learned it was really a spoofed IP address for hackers based in South Africa.
- The home buyers were given the bad information by their real estate agent who forwarded wire instructions from what she thought was the title company.

©2018 Fidelity National Title Group | Florida Agency



## Case Study #1, contd.

- The real estate agreement warns clients not to “wire any funds without personally speaking directly to the office that is closing the transaction.”
- The agent never called to confirm with the title company that the instructions were legitimate.
- Buyer’s lawyer says the agent is accountable because she breached her own policy.

©2018 Fidelity National Title Group | Florida Agency



## Case Study #2

- Buyer was working with a real estate agent to purchase a property.
- Buyer was instructed to wire \$196,622.67 to the title company by his real estate agent.
- Unbeknownst to all involved, a criminal was intercepting e-mails exchanged between the title company, agent, and Buyer.
- Buyer had actually been sent hacked wiring instructions, which instructed him to wire funds straight to the criminal’s account.
- Once the funds were sent they could not be recovered and so Buyer sued the agent, the broker, and others.

©2018 Fidelity National Title Group | Florida Agency



## Case Study #2, contd.

- Kansas federal court upholds jury verdict that a real estate agent was 85% responsible for the Buyer's losses.
- The court rejected the broker's argument that she did not send the email because her email was hacked.
- Broker had to pay \$167,129 to Buyer.
- Bain vs. Platinum Realty, LLC, Dist. Court, D. Kansas 2018)

©2018 Fidelity National Title Group | Florida Agency



## Red Flags

- Email with new wire instructions.
- Message from someone you've never spoken with or met.
- Different email address than what was used previously.
- Missing usual warnings or signature lines.

©2018 Fidelity National Title Group | Florida Agency



## Red Flags, contd.

- Asks for NPI.
- Asks you to click a link to go to a form.
- Mysterious attachments.
- Name on recipient account is different.
- No email encryption

©2018 Fidelity National Title Group | Florida Agency



## NAR Tips to Prevent Losses

In May of 2016, the National Association of Realtors published an advisory warning of the risk of wire fraud in residential real estate transactions.

The NAR advisory listed recommendations to ensure the security of transactions but not limited to:

- 1) Build a **standard warning** about wire scams and avoid sending sensitive information over email.
- 2) At the beginning of every transaction, tell clients what **your communication practices** are.
- 3) If you, or your agents, do engage in a wire transfer with a client, **call them on the phone immediately** prior to the transfer of funds, so they know they're sending money to a legitimate source.
- 4) Always using strong passwords and change them **regularly**, and encourage your clients to do the same thing.
- 5) Brokers should consider **employing an IT staff person** who's responsible for monitoring, updating and implementing information security systems and procedures at your company.

©2018 Fidelity National Title Group | Florida Agency



## Additional Tips to Prevent Losses

- Always **verbally** verify closing and wire instructions with a verified employee at your title company.
- Educate your clients not to share personal information over email.
- Have your clients talk to their bank to not allow wire transfers without some checkpoint.
- Don't react immediately to email.
- Monitor the progress of the wire transfer to completion.
- Be vigilant!

©2018 Fidelity National Title Group | Florida Agency



## Additional Tips to Prevent Losses

- Use VPN for external connections.
- Set up your system to backup daily and in different ways.
- Use complex passwords.
- Add a lock out program to your system when your computer is not in use.
- Be aware of free Wi-Fi and don't access financial or other personal information on them.
- Use HTTPS when transferring personal or private non-public information. Always look for the "S".

©2018 Fidelity National Title Group | Florida Agency





## Additional Tips to Prevent Losses

- Do system updates to keep your browser, security system up to date.
- Shut off your computer at night!
- If it feels suspicious, it probably is.

### **Most Important Defense: Communication!!!**

- Inform buyers and sellers about scams early and ask them to call you if they receive an email about wiring funds

©2018 Fidelity National Title Group | Florida Agency



## Tools to Help Prevent Cyber Fraud

- Secure email systems
- Consider using a Password Manager
- Protect Mobile Devices
  - Create a timed out password or PIN to secure device
  - System Updates

©2018 Fidelity National Title Group | Florida Agency



## Tools to Help Prevent Cyber Fraud

- Resources
  - FBI Internet Crime Complaint – ([ic3.gov](http://ic3.gov))
  - The Financial Crimes Enforcement Network ([fincen.gov](http://fincen.gov))
  - American Land Title Association ([alta.org](http://alta.org))
  - Florida Realtors ([floridarealtors.org](http://floridarealtors.org))
  - National Association of Realtors ([nar.realtor](http://nar.realtor))

©2018 Fidelity National Title Group | Florida Agency



# THANK YOU!

©2018 Fidelity National Title Group | Florida Agency