

# Cyber Security & Wire Transfer Fraud

1

## Overview

- Cyber risks
- Business Email Compromise (BEC)
  - Phishing attempts
- Defenses
  - Passwords
- Wire transfers



2

# Cyber Risks

3

## Cyber Security in the Age of Cyber-Crime

- Types of attacks
  - Malware (Malicious Software)
  - Ransomware (Fast Growing)
  - Password Attacks (Guess Passwords)
  - Zero-Day Attacks (Who Knew?)
  - Insider Attacks (Disgruntled Employee)
- Other attacks
  - Man in the Middle (MitM) – Public WiFi
  - DDoS, APT, CSS, SQL Injection
  - Social Engineering (You Don't Say!)

4

## Real Estate Market

- Lucrative
  - Average wire transfer loss: \$200,000
  - Average bank robbery: \$7,000
- Multiple parties communicating electronically
  - Chain only as strong as weakest link
  - Transaction location irrelevant
- Fraud tools easily found online
  - Phishing kits & other technical tools
    - Little technical knowledge needed
  - Attorney, agency, broker, FSBO listings
- Fraudster sweatshops
  - Required minimum success hits per week



5

## Perpetrator Tactics

- Computer Intrusion
  - Malicious attachment or link
    - Activating gives computer access
    - Hacker monitors email traffic
    - Sends email from hacked account
- Social Engineering
  - Non-technical manipulation
    - Use of knowledge gained from hacked computer and publicly available resources
    - Exploit knowledge of chaos surrounding closing and last minute need to wire funds



6

## Losses



Reported U.S. losses due to business email compromise scams targeting the real estate, shown quarterly, with peak losses indicated. (Source: IC3)

7

7

## Best Practices Pillar 3 – Privacy & Information Security

- Adopt and maintain a written privacy & information security plan to protect Non-public Personal Information (NPPI) as required by local, state and federal law
  - Physical Security
  - Network Security
  - Disposal
  - Disaster Management Plan
  - Training
  - Use of Service Providers
  - Notification

**AMERICAN  
LAND TITLE  
ASSOCIATION**



8

8

# Business Email Compromise

## BEC Real Estate Fraud

1. Gain access to email account (“hack”)
2. Monitor for pending transactions
3. Commandeer real email address & create lookalike email addresses (“spoof”) for other participants
4. Email bogus wire transfer instructions
5. Funds wired to criminal-controlled account
6. Funds dispersed and trail goes cold



## Account Takeover



11

11

## Computer Intrusion

- Malware (malicious software)
  - Display unwanted advertising
  - Disrupt computer operations
  - Gather sensitive information
  - Gain access to private computer systems



**The Fund**  
ALWAYS DRIVEN™

12

12

## Bogus Email to Agent

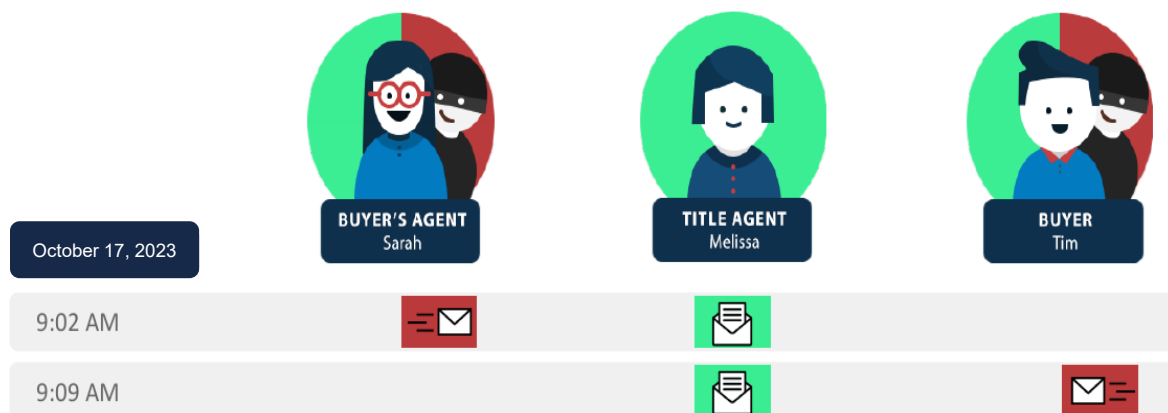


**The Fund**  
ALWAYS DRIVEN<sup>®</sup>

13

13

## Spoofed Buyer Email

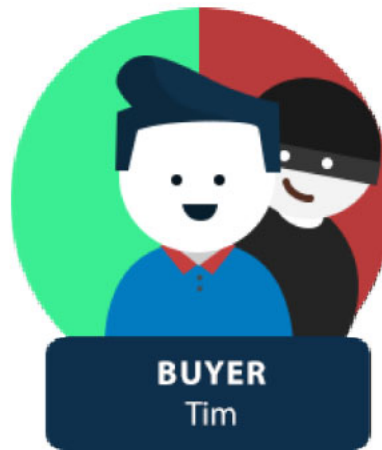


14

14

## Spoofed Email

- Tim:  
[tsmith@gmail.com](mailto:tsmith@gmail.com)
- Fraudulent Tim:  
[tsmith1@gmail.com](mailto:tsmith1@gmail.com)



The Fund<sup>®</sup>  
ALWAYS DRIVEN<sup>™</sup>

15

15

## Agent Emails “Parties”

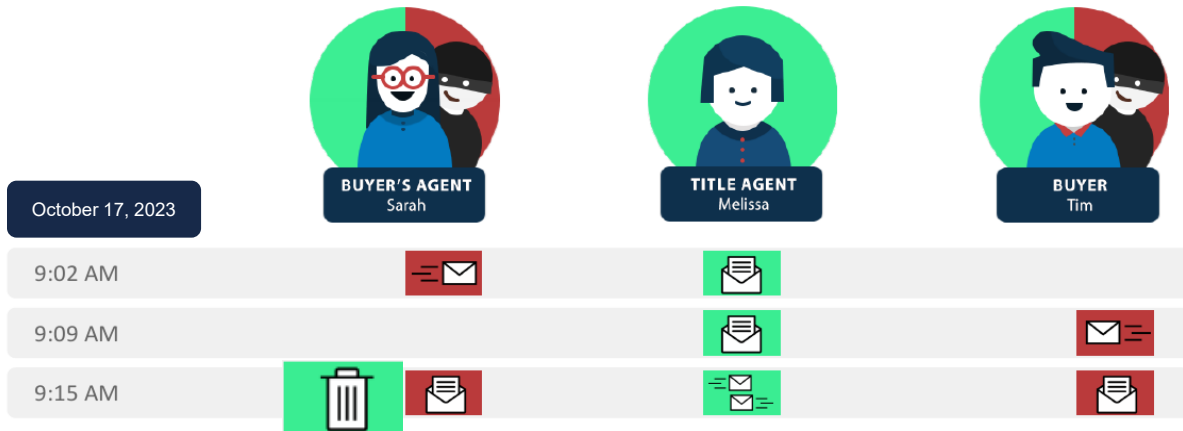


16

16



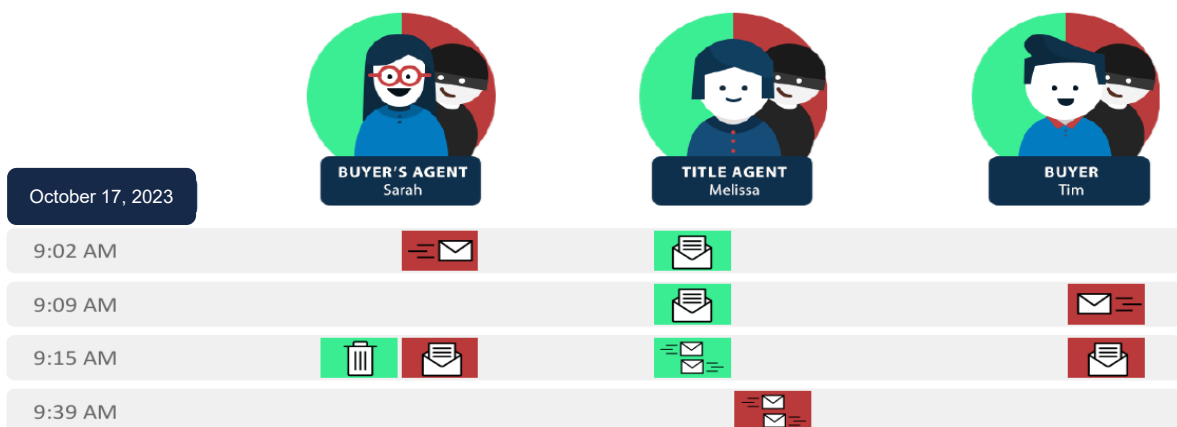
## Auto-deleted



17

17

## Spoofed Agent Email



18

18

## Spoofed Email

- Melissa:  
[mdombrowski@suntitleagency.com](mailto:mdombrowski@suntitleagency.com)
- Fraudulent Melissa:  
[mdombrowski@suntitleagency.com](mailto:mdombrowski@suntitleagency.com)

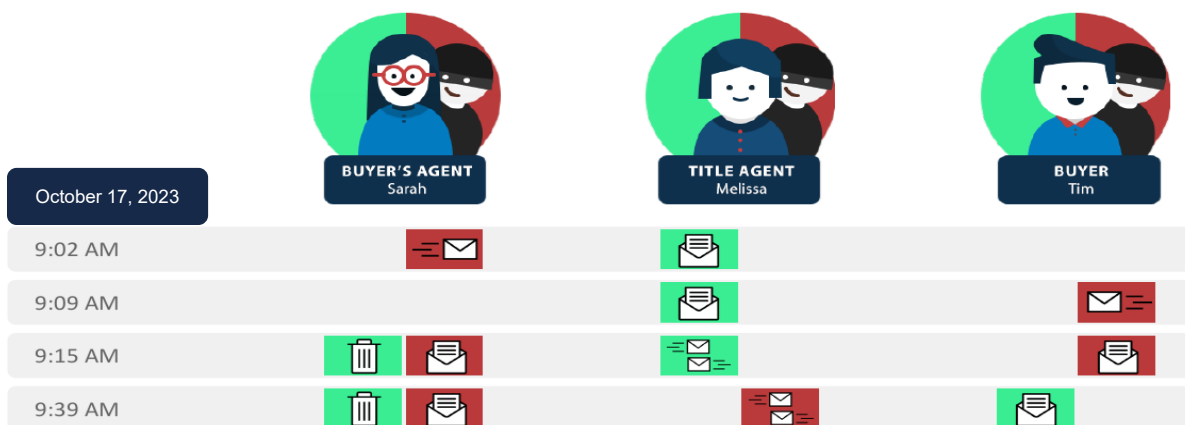


**The Fund**  
ALWAYS DRIVEN<sup>®</sup>

19

19

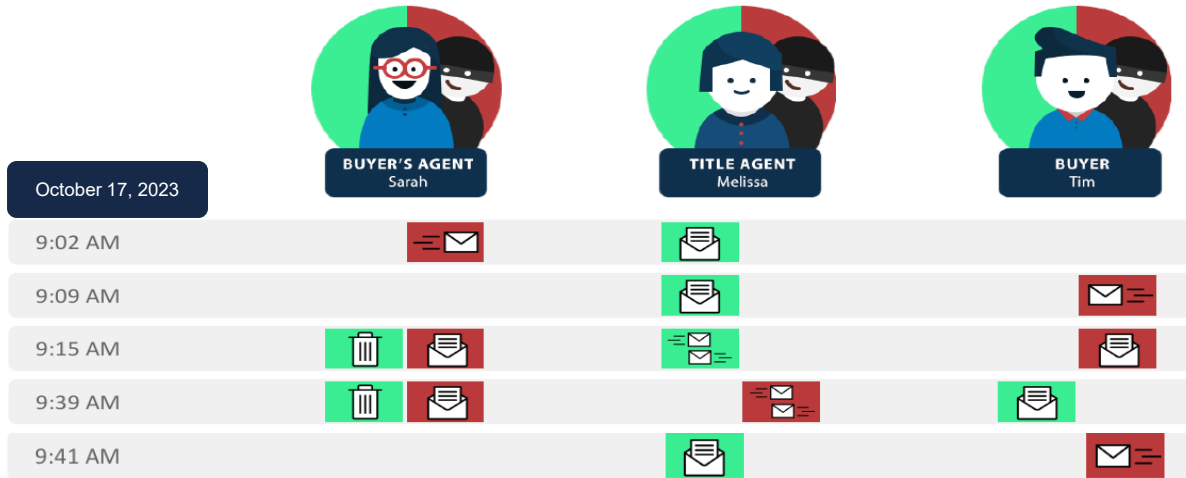
## Auto-delete / Buyer Opens



20

20

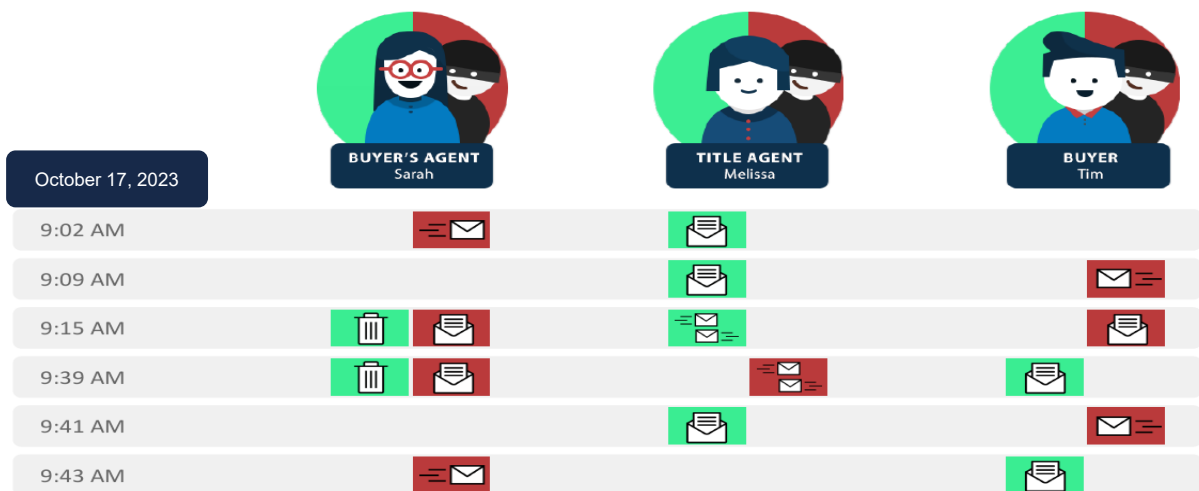
## Spoofed Buyer Email



21

21

## Bogus Email to Buyer



22

22

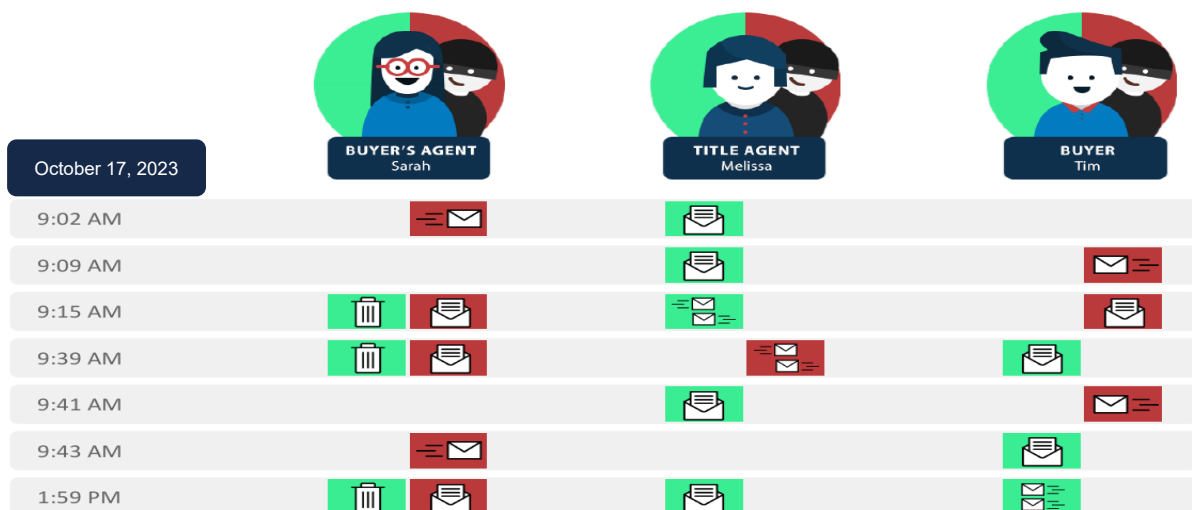
## Buyer Initiates Transfer



23

23

## Buyer Confirms Wire



24

24

# Phishing Attempts

25

## Phishing Attempts

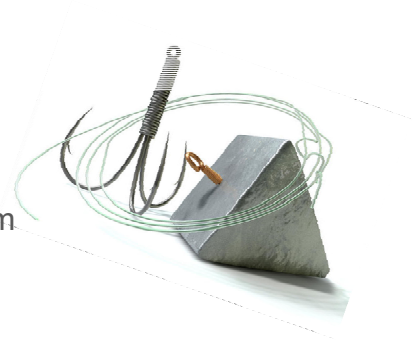
- Very Commonly Deployed Cybertheft
- Unsuspecting Individuals in Email
- Attempts to Collect Sensitive Information
- Login Credentials, CC#, Etc.
- Links to Fraudulent Websites
- Looks Legitimate on the Surface
- Uses Social Engineering
- Looks and Feels Familiar
- Spear Phishing: Advanced, Very Targeted



26

## Hook, Line & Sinkers

- Launch & wait
  - Broker, agency & title firm targets
  - Multiple email accounts receive malignant spam
  - Victim's "click" silently downloads malware
- Malware responds
  - Sets up new default rules for account
  - Auto-forwards to fraudster's server any email containing keywords (e.g., purchase, escrow, contract, down payment, cash, etc.)
  - Auto-delete replies to hacker initiated email
- "Mines" account for NPPI, etc.



27

27

## Phishing Attempts

- Intruder seeks access to computer system by enticing user to "click" email attachment or link to malicious site
- Forged messages appear to be from legitimate, real estate-related sources
  - "DocuSign"
  - "Dropbox"
  - "Real" underwriters, banks, title companies
    - Letterhead/signature blocks of actual parties reproduced
  - Once "clicked"
    - Malware infects system &
    - "SPAMs" user contact list
- Intruder can read/alter/redirect messages to defraud parties of infected systems

28

28

## Example

### Preliminary CD and Contract

Kathy Hale <julia.beems@ucdenver.edu>

Sent: Thu 12/8/2016 8:57 AM

To: Renee Realtor, Tom Title Agent

Message: Preliminary CD.htm (12 KB)

Good Morning,

Attached is the initial CD for my client (based on preliminary fees that you sent over). Can you please advise on revised/added fees (tax prorations, HOA dues, etc)?

Preliminary CD and Contract is enclosed via encrypted secure OUTLOOK PDF format

Kathy Hale  
Assistant  
John E. Robinson  
Key Financial, Inc.  
161 Belle Forest Circle  
Nashville, TN 37221  
323-892-5021

From: Katie Bennett <kbenett@lawyersadvantages.com> Sent: Mon 3/5/2018 10:47 AM  
To: John St. Lawrence  
Cc:  
Subject: Deed\*\*Title Payoff Amount Update Needed\*\*69 Union Street  
Message: SCAN1606\_000.pdf.htm (14 KB)

Hello,

Attached are the Statements, Deed, Title Commitment, and Payoff for 69 Union Street – scheduled to close on Monday, 3/9, at 4PM at Unity Real Estate. We will send the balance of the Real Estate Closing Documents upon completion.

Please let us know if you have any questions or need anything additional.

Have an Excellent day!

**Katie Bennett** | Settlement Pre-Processor | Lawyers Advantage Title Group

Phone: 410-480-2890 | Fax: 410-480-1575

8000 Main Street, Ellicott City, MD 21043

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

**\*WIRE FRAUD TREND ALERT\*** We have seen an increase in fraudulent wire instructions received via email. Protect yourself by always verbally confirming wire instructions with your beneficiary directly on a substantiated phone number before wiring.

29

29

## Example

On Wed, Oct 18, 2017 at 12:01 PM, Dolores Heventhal <dolores.nglawfl@gmail.com> wrote:

Guillaume,

Please find attached HUD & Wiring Instructions for the above referenced transaction. Amount to close this transactions is (\$262,687.37)

Proceed to the bank to wire the funds before your bank's closing hour and provide me a copy of receipt afterwards.

Kindly acknowledge the receipt of this email.

Sincerely,

Dolores Heventhal

Title Processor  
NUGENT & GROUND, LLC  
Attorneys and Counselors at Law

The Galleria Corporate Centre  
2455 E. Sunrise Blvd., Suite 807  
Fort Lauderdale, FL 33304

Phone ☎: 954.537.1717

Fax 📠: 954.537.1606



**Trusted & Verified**

*Due to the amount of fraudulent cashier's checks circulating in Florida, we will require all cash to close be tendered in the form of a WIRE transfer only.*

30

30

## Example

On Wed, Oct 18, 2017 at 9:35 AM, Guillaume J. Charmes <[guillaume@charmes.net](mailto:guillaume@charmes.net)> wrote:

Dolores, Marisela,

What is the "County tax" that has been added? Living in Broward for quite a while now, I don't recall paying county tax when I lived in, bought or sold a property.

Also, there seems to be some confusion around the property tax. The HUD says the sellers will pay \$2,331.12 to the escrow, so I am understanding that I will pay the taxes and use that fund to pay the owner's part. However, the sellers are requesting me to place that amount in an escrow waiting for them to pay the tax.

Please advise.

Regards,

—

Guillaume J. Charmes  
Software Engineer  
<http://blog.charmes.net>

31

31

## Example

From: Dolores Heventhal <[dolores.nglawfl@gmail.com](mailto:dolores.nglawfl@gmail.com)>

Date: Wed, Oct 18, 2017 at 12:53 PM

Subject: Re: HUD & Wiring Instructions

To: "Guillaume J. Charmes" <[guillaume@charmes.net](mailto:guillaume@charmes.net)>

Cc: [mariselajnglawfl@gmail.com](mailto:mariselajnglawfl@gmail.com), christian Guerin <[miamis225@aol.com](mailto:miamis225@aol.com)>, BEA CLAUDE <[yamilano@hotmail.fr](mailto:yamilano@hotmail.fr)>

Guillaume,

The sellers will be responsible for the County tax which will be paid by them at closing. Your amount due to close is (\$262,687.37). Seller will pay \$2,331.12 - County tax to the escrow at closing.

See attached wiring instructions once again. What time will the wire be sent?

Kindly acknowledge the receipt of this email.

Sincerely,

Dolores Heventhal

Title Processor  
NUGENT & GROUND, LLC  
*Attorneys and Counselors at Law*

The Galleria Corporate Centre  
2455 E. Sunrise Blvd., Suite 807  
Fort Lauderdale, FL 33304

Phone ☎: 954.537.1717  
Fax 📠: 954.537.1606



**Trusted & Verified**

*Due to the amount of fraudulent cashier's checks circulating in Florida, we will require all cash to close be tendered in the form of a WIRE transfer only.*

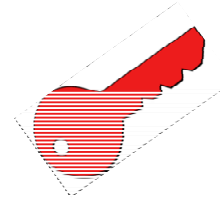
32

32



## “Avoid” the Phishing Tricks

1. Urgency or Threats
2. Pressure to Do Something
3. Request Sensitive Information
4. Spelling and Grammar Issues
5. Odd Email Addresses (To, From, Reply)
6. Too Good to Be True
7. Call the Sender to Confirm
8. Common Sense



## Defenses

## Cyber Security

- Antivirus Software
- Firewalls
- Encryption
- Password Protection
- Email Security
- Data Backups
- 3rd Party Assessment
- Patch Management
- Vulnerability Scan
- 2FA or MFA

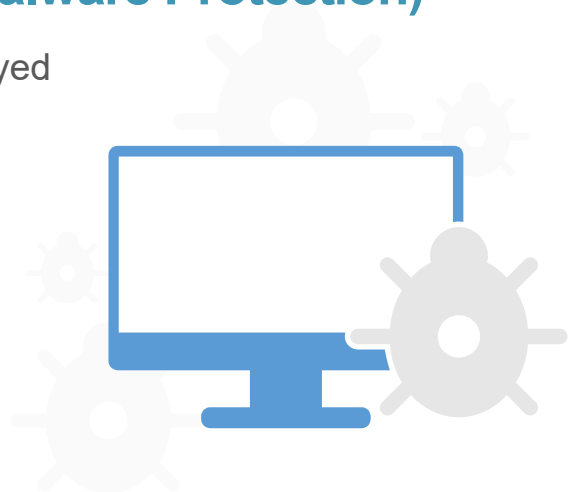


35

35

## Antivirus Software – (Malware Protection)

- Most common protection deployed
- Defends against most Malware
- Ransomware Protection
- Drive-by Protection
- Desktop and Server Protection
- Gateway (Internet) Protection
- Keep it Updated!



36

36

## Firewalls – (Hardware or Software)

- Adds a Layer of Protection
- Prevents Unauthorized Access
- Protects at the Gateway
- Protects at the Computer
- Provide Intrusion Protection
- Blocks Network Attacks



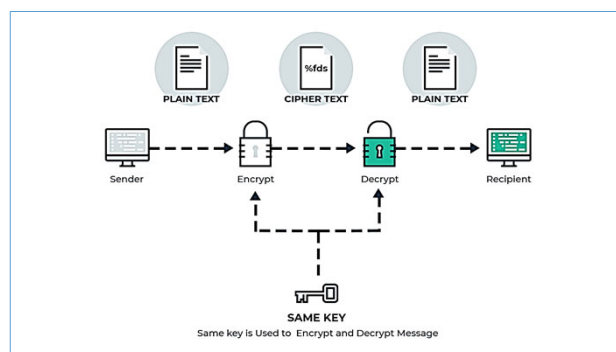
The Fund<sup>®</sup>  
ALWAYS DRIVEN<sup>™</sup>

37

37

## Encryption

- The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot

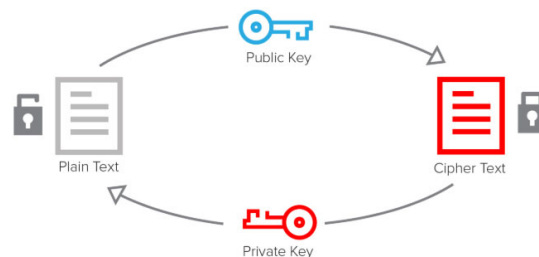


38

38

## Encryption – (Hardware or Software)

- Strong Data Protection
- Makes Data Unreadable to Hackers
- Protects Stored Data (file, volume, disk)
- Protects Data in Transit (https)
- Secure Email with Encryption
- Protects NPI, PII, PHI



39

39

## Passwords – Unique to each site

- If your common password is discovered
  - Will have access to all accounts which use that password
- New rule – have better passwords & less changes
  - More compliance
  - Longer passwords are better passwords

### Too Simple

H0use

Cat in the Hat

My beautiful red house

### Better

BigHouse\$123

Correct horse battery staple

Seashell glaring molasses invisible



**LONG PASSWORDS ARE STRONG PASSWORDS**

40

40

## Password Managers

- Encrypted vault for login credentials
  - May also save
    - Notes
    - Insurance cards
    - Credit card information
- Issue security alerts
- Generate passwords
- Streamlines logins
- Break bad habits
  - Unique passwords
  - Change passwords
- LastPass
- Dashlane
- 1Password
- Keeper
- Sticky password
- Intel's True Key
- RoboForm
- Iolo Technologies
- EveryKey
- My PassLock

41

41

## Password Multipart Authentication

- Process – How to know its really you
- Five common authentication factors
  - 1 Something you know
    - Password, address, other names, first car, etc.
  - 2 Something you have
    - Site sends a code or token witch expires within a short time
  - 3 Something you are
    - Fingerprint, retina, iris, voice, fact, etc.
  - 4 Somewhere you are
    - IP address – it knows your computer
  - 5 Something you do
    - Gestures or touches



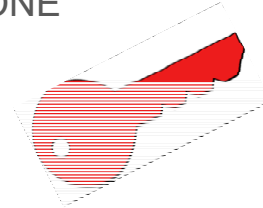
**The Fund**  
ALWAYS DRIVEN™

42

42

## Passwords – Tips

1. Don't use obvious personal information
2. Don't re-use passwords
3. Don't share your passwords – with ANYONE
  - Don't post your passwords
4. Use unique password for each site
5. Use password manager
6. Change your password regularly, or
  - Indication that you have been hacked
7. Use multi-factor authentication
  - Just turn it ON



## Email Security

- Protects Against Malicious Emails
- Built-in Malware Protection
- Ransomware
- Attachments, Payloads
- Spam Filtering
- Phishing Attacks
- Spear-Phishing
- Secure Email Transfer



## Cyber Fraud Defense

- Do not use **free email accounts** for business purposes (e.g., AOL, Gmail, Yahoo, etc.)
  - Easier to hack
- Create contact information log at the outset of transaction with all parties' phone numbers



45

45

## Data Backups

- Critical to Have a Backup
- Something Will Go Wrong
  - Accidental Deletion
  - Rogue Employee
  - Corrupted File
  - Hacker Activity (Ransomware)
- Backups are the Solution
- Easy to Setup and Maintain
- Keep You in Business



46

46

## Third Party Assessment

- Consider a 3rd party vendor
  - Security assessments
  - Risk assessments
  - Discovery & remediation
- Sign-up for notifications with product vendors
- Stay in the know with security websites
- Attend local cyber security workshops
- Register for cyber security webinars



47

47

## Resources

- IT Security Awareness Training
  - SANS: <https://www.sans.org/security-awareness-training>
  - SANS Ouch!: <https://www.sans.org/ouch>
- Phishing Tests/Tools
  - KnowBe4: <https://www.knowbe4.com/resources>
  - Phishme: <https://phishme.com/free>
- Multi-Factor Authentication: <https://twofactorauth.org>
- Security News: [www.krebsonsecurity.com](http://www.krebsonsecurity.com)
- Mail System Check: <https://mxtoolbox.com>
- Breach Check: <https://haveibeenpwned.com/>
- Best Practices: <https://www.cisecurity.org>

48

48



## Cyber Fraud Defense

- Have parties sign funds transfer agreement at beginning of transaction
- If procedure changes confirm by calling phone number in log
- Beware of pressure to quickly change payment arrangements
  - Slow down
  - Stay in control of the transaction
- Verbal confirmation includes reading wire instructions (just like confirming legal descriptions)
- Implement two-part authentication on all wire transfers



49

49

# Wire Transfers



50

50

## Wire Transfer – Facts

- Wire transfer fraud in US Real Estate only – 2018 statistics
  - \$149,457,144.00 in 2018
  - \$ 12,454,759.50 per month!
  - **\$ 409,471.63 EVERY DAY! And growing**
- FBI – labeled the scams as “business email compromise” or BEC

 **Fraudsters create urgency – MUST BE DONE NOW!!!**

- 2018 - Florida national ranking for BEC fraud
  - Number of victims – 3rd
  - Amount of funds lost – 4<sup>th</sup>



51

51

## Wire Transfer

- Warn, warn, warn clients; then warn again
  - Websites
  - Communications – emails etc.
  - Send separate notice to clients & real estate agents
- Call for verification – let client know ahead of time

 **Verify – verify – verify**





 **Think!!**



52

52

## Wire Transfer – VERIFY

-  **Verify account holder information with receiving bank prior to initiating the wire transfer!**
-  **Verify wire account information on payoff letter – use known number!**
-  **Verify wire account information of seller – use known number!**
-  **Verify the ABA number –**
  - [routingnumber.aba.com/default1.aspx](http://routingnumber.aba.com/default1.aspx)
  - [Routingnumber.com](http://Routingnumber.com)
  - Google bank – i.e. USAA aba number
  - <https://bank.codes/us-routing-number/bank/>



53

53

## Wire Transfers – Warning Verbiage

- Be aware! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS call us immediately to verify the information prior to sending funds.
- Due to increased fraud, buyers, sellers and lenders should confirm all wiring instructions by phone directly with our office before transferring funds.
- WARNING! WIRE FRAUD ADVISORY: Wire fraud and email hacking/phishing attacks are on the increase! If you have an escrow or closing transaction with us and you receive an email containing Wire Transfer Instructions, DO NOT RESPOND TO THE EMAIL! Instead, call your escrow officer/closer immediately, using previously known contact information and NOT information provided in the email, to verify the information prior to sending funds.

54

54

## Wire Transfers – Use Outgoing Wire Checklist

ALTA Information Security Committee  
Outgoing Wire Preparation Checklist  
V.2.0 08-19-2019

---

### ALTA Outgoing Wire Preparation Checklist

Visit the ALTA Website: <https://www.alta.org/business-tools/information-security.cfm>

**Date:** \_\_\_\_\_

**File Number:** \_\_\_\_\_

**Company Name/Location:** \_\_\_\_\_

55

55

## Wire Transfers – Use Outgoing Wire Checklist

1. Review the source of wiring instructions
  - Originally
  - Where they changes, if so what was the verification of the change
2. Verify instruction received
  - How sent
  - Call trusted number to ensure receipt
  - List wire creator & authorizer
3. Verify delivery of wired funds
  - Call to verify receipt



56

56

## Wire Transfers – Best Laid Plans of Mice & Men

- No matter how many warning or how careful you are – something will go wrong
- Review insurance to ensure proper coverage
  - Losses from wire fraud
    - Email is hacked and false information is sent out
    - Fraudster obtains information and uses it to defraud a party – information may have come from another party in the transaction

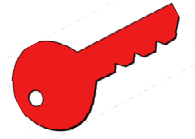
 Have a plan – **SPEED IS OF THE ESSENCE**

## Wire Transfers – ALTA Rapid Response Plan

1. Alert company management & internal wire fraud response team
2. Report to sending & receiving banks
3. Report to law enforcement
4. Call sending bank to confirm recall request has been processed
5. Inform parties in the transaction – using known numbers
6. Check with your plan to see if you need to secure internally
7. Consider contacting insurance carrier(s)
8. If wired out of the US, hire attorney in that country to help recovery
9. Document your response
10. File complaint with FBI



## Wire Transfers TIPS

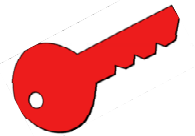


- 1. Call, don't email wire instructions
  - If you receive email instructions – do not use the number in the email to verify the instructions
- 2. Use secure portals for communications
- 3. Verify all wire transfers instructions and portal invitations
  - Known numbers
- 4. Be suspicious
  - Be wary of email requesting changes in information
- 5. Forward, don't reply
  - If email came from look-a-like address it will then go to correct mail address

59

59

## Wire Transfers TIPS



- 6. Confirm everything
  - Have bank confirm the name and account prior to sending the wire
- 7. Verify that the funds transferred immediately
- 8. Confirm receipt of wires
- 9. Sender of wire to initiate phone calls verifying information
- 10. Warn all parties of BEC and wire fraud

60

60