CYBERCRIME AND CYBER SECURITY

Jessica Edgerton, Associate Counsel, NAR
Nobody is Safe.

By 2019, the annual global cost of cybercrime = est. $2.1 Trillion.

Source: Juniper Research
It’s Not Just The Big Guys.

• In 2015, forty-three percent of all cyberattacks were leveraged at small to midsized businesses (250 or less employees.)*
• Dangerous misconception: “I’m too small to bother with.”
• Cybercriminals know that the small guys are less protected.

* Source: Symantec 2016 Cybersecurity Report
Estimated price tag on a successful cybercrime for a small to midsized business:

$690,000

Source: Ponemon Institute
Cybercrime Financial Loss is Correlated With:

- Direct theft of funds – fraud/scams/extortion.
- Loss of critical/sensitive/confidential data.
- Business disruption, downtime.
- System clean-up, data/program recovery.
- Post-breach IT & business consultation fees.
- Reputational damage to business.
Cybercriminals ♥ Real Estate

- Smaller to mid-sized companies.
- Busy professionals focused on clients, deals.
- Multiple separate players during transactions: Buyer, seller, buyer’s agent, seller’s agent, escrow agent, lawyer, mortgage broker, banks.
- Real estate purchase = large sums of money.
Real Estate Cyber Fraud
Du Jour:
Email Wire Fraud
Wire Fraud

• Hacker breaks into email account, sits quietly, collects info.
• Well timed email to buyer just before deal closes.
• Looks to be from agent, attorney, other trusted participant.
• Claims last minute change to wiring instructions.
• Buyer wires money to criminal.
• Criminal empties account immediately.
• Money is gone forever.
Scams of the Past

• Bad grammar and spelling
• Weird syntax
• Outrageous claims
• Quick money
• In your spam folder
GOV GODWIN EMEFELE <postmaster@cockycookie12.de>
!!!***+++ URGENT NOTICE +++***!!!

Dear <insert name>,

Is my pleasure inform YOU that your deliveryman has arrived at the airport with your cash trunk boxes value $8.3 million dollars US currency being your inheritance /compensation payment. \>>

Most importantly, you are advised to sending your full data to him on this email address reply, which include your Full Name, Current Residential Address, DIRECT CELL NUMBER, AND A COPY OF ANY IDENTITY CARD WITH SOCIAL SECURITY NUMBERICALS to verify that you are the right receiver to avoid mistake and enable him deliver your cash consignment boxes to your house without any further delay.

CONGRATULATION!!!
MR.GODWIN EMEFELE,  
EXECUTIVE GOVERNOR,  
CENTRAL BANK OF NIGERIA
New Scams

• Highly sophisticated organized crime;
• Virtually indistinguishable from legitimate email:
  - Comes from hacked account; or
  - Minute difference in email address;
• Looks to be from trusted source - in-the-know re: deal.
• Right timing, right tone, right information;
• Devastatingly successful.
Hi Everybody,

We’re almost to the finish line. Just got the heads up that there’s been a tweak to the wiring instructions – please see attached for new info. Let’s get this baby wrapped up today. Congrats again to all. Brenda, you and Roger and little Susie are going to love your new place on Franklin Road.

Cheers,
Jack

Jack Lawyern
Lawyern & Lawyern

Hand in Hand with Texas Homebuyers for Three Generations
Wire Fraud Damage Control: Best Practices

• Buyer: Contact financial institution(s).
• Buyer: Contact local FBI, police.
• Hacked entity: Change passwords.
• Hacked entity: Run anti-virus; scan IT systems.
• Everybody: Review insurance policy, contact insurance company as appropriate.
Wire Fraud Prevention: Best Practices

• Communicate and educate.
• Warn all parties: Be suspicious of wiring info sent via email.
• Consider implementing standard warning notice. (See NAR.realtor)
• Real estate agents/brokers: Avoid handling disposition of funds when possible.
• Buyers should call the intended recipient of wired funds immediately prior to sending, using an independently verified phone number.
• Develop security-conscious email & password practices.
Securing Your Email Account
How Does a Hacker Hack Email?

• Online tutorials for hacking into email.

• Favorite hacker tools for breaking into email:
  - Infected attachment/link in email installs malware, e.g.:
    • Keylogger (reads keystrokes.)
    • Zip Password Cracker Pro (“brute force attack”)
  – Exploiting your shoddy email password practices by guesswork, online research.
Best Email Practices

• Check junk mail, sent mail folders regularly for anomalies.
• Check email account settings: Email forwarding, folder settings.
• Regularly purge email.
• Use strong passwords.
• Consider using a password manager.
• Use two-factor (or multi-factor) authentication.
• Avoid doing business over unsecured wifi.
Best Email Practices

THINK BEFORE YOU CLICK.

• Ask yourself: Is this a trusted email?
• Hover mouse arrow over the email address of sender.
• If something seems fishy, DO NOT CLICK.
Whenever possible, avoid sending sensitive or confidential information via standard email.
Alternatives to Document Sharing via Standard Email

- **Faxing:**
  - E-delivery fax service – same possible issues as regular email.
  - Traditional fax: Be aware of where faxes will be printed out.
- **Encrypted Email (Recommended)**
- **Document Sharing or Transaction Management Platforms (Recommended)**

**NOTE:** KEEP LOGIN CREDENTIALS AND PASSWORDS SECURE.
BEYOND WIRE FRAUD: OTHER SCAMS AND TRAPS
Beyond Wire Fraud: Other Scams and Traps

• “Referral” Email Scam: Spoofed referral email. (Malware.)
• “Overpayment” Scam: Buyer sends false payment, demands partial refund. (Check fraud.)
• Fake DocuSign Email Scam (Malware).
Fake ("Spoofed") DocuSign Emails

Erase emails with subject lines similar to:


- Completed: realtors.org - Wire Transfer Instructions for jedgerton Document Ready for Signature
Fake (“Spoofed”) DocuSign Emails

• Do not click on links in a “DocuSign” email if you don’t recognize the sender.
• Look for a unique code in the email. If there isn’t one, don’t trust the email.
• When a code does appear in the email, access your documents directly from www.docusign.com by entering the code directly on the website.
• Report suspicious emails to spam@docusign.com
• DocuSign provides robust tips and tools for combating scams. For more info:
Recommended: Enter this code directly at DocuSign site to access documents

From: Michael Strickland (michael.strickland@docusign.com)

Hello Phillip Buckingham,
Please review the documents and sign immediately.
Best,
Michael

Alternately, you can access these documents by visiting docusign.com, clicking the "Access Document" link, and using this security code:

8A5A4DDADB5490AAC0D358ED675F ****

DocuSign. The fastest way to get a signature.

This message was sent to you by Michael Strickland who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.
RANSOMWARE
WANNACRY/WANNACRYPT
Ransomware Triage:

- Disconnect from network and power off.
- Consult with IT professional, remove malware/run antivirus.
- Decide whether to pay.
  - Data, systems backed up?
  - Understand that there are no guarantees
- Report to FBI (Internet Crime Complaint Center).
Ransomware Prevention

• Keep operating systems patched and up-to-date.
• Update when prompted.
• BACK UP YOUR STUFF. (Data, critical programs.)
• Make sure backed-up files are separate, restricted.
• Restrict and silo systems, programs, and network access.
Takeaway:

Stay paranoid.

(In a healthy, non-freaking-out kind of way.)
Data Protection and Cybersecurity
Electronic Data is…

- A vital and increasingly valuable asset for all businesses…
- Resting on a fragile, porous, and incessantly changing security structure…
- Under constant criminal attack.
Criminals’ End Games in Data Breach

• Collect Personally Identifiable Information (PII) for identity theft
• Collect financial, credit card information
• Disruption
Personally Identifiable Information

Indiana Definition of PII (IC 24-4-14): Any of the following data when combined with first initial or name plus last name:

- Social security number
- Credit card numbers
- Financial account numbers
- Debit card numbers
- Access codes, security codes, or passwords
- Driver's license numbers
- State identification card numbers
Proper Handling of PII

- Know what PII you have in your systems. Take inventory. Protect PII, and dispose of it properly.
- Know your state laws regarding handling and transmitting PII.
- Don’t keep PII longer than you need it.
Two-Tier Data Breach Defense

• Leveraging the human element
• Leveraging the IT element
Leveraging the Human Element
People open the door…

Breaches are often traced back to in-house human behavior, rather than purely electronic infiltration:

• Falling for infected website links and clickbait;
• Clicking on infected links, attachments in emails;
• Employing shoddy password practices.
People can close the door.

- Habit modification - Yours, staff’s, licensees. (E.g., “think before you click”).
- Report possible infections, breaches.
- Stay up-to-date on scams, fraud: Take advantage of NAR’s resources. Subscribe to a free cybersecurity newsletter. Talk to your colleagues, partners, clients.
Implement and Follow Appropriate Policies

• Be aware of your state’s laws regarding cyber policies, practices.
• Whether or not your state mandates it, best practice is to have:
  – Document Retention and Destruction Policy
  – Cyber and Data Security Policy
  – Breach Notification Policy
• Make sure to review law regularly, update policies accordingly.
• Ensure staff, licensees are educated and following policies.
Leveraging the IT Element
IT Infrastructure Best Practices

• Keep antivirus software, firewalls active and up-to-date.
• Keep operating system and programs patched, and up-to-date.
• Regularly back up critical data, applications, and systems, as your budget and IT capacity allows.
• Consider conducting voluntary IT audits.
Don’t Forget Your Phone!

• Handhelds, tablets, mobiles are prime targets for attack.
• Beware malware apps. Think before you download.
• Beware unsolicited texts with links, requests for info.
• Beware pop-ups, push notifications.
• When in doubt, call your mobile provider.
• Update phone when updates are available.
• Back up data on your phone.
• Consider phone data encryption.
IT VENDOR CONSIDERATIONS
Engaging Technology Vendors

• Cloud Storage Providers
• Document Sharing Platforms
• Password Management Applications
• Website and App Developers
• Other Technology Providers
Engaging Technology Vendors

• Do due diligence re: vendor reputation, security
• Review vendor contract (with attorney if feasible) for:
  - Appropriate warranties, indemnifications
  - Unreasonable limitations on liability
• You may not have leverage to negotiate.
  - …So then what?
Engaging Technology Vendors

• Check vendor’s client lists for large companies.
• Bigger may be better when it comes to some providers.
• Small companies ride on security warranties leveraged by larger companies.
• Especially with cloud services, all clients benefit from same protections.
Cyber Insurance
Cyber Insurance

• Cyber Insurance still in “wild west” territory, but improving.
• Don’t purchase without reviewing current policy.
• Consult a specialist: In addition to cyber policies, ask about crime (“fidelity”) riders, social engineering endorsements, and other products that may bolster coverage in the wake of a cybercrime.
Cyber Insurance

• Be aware of what’s covered...and what’s NOT covered. Don’t assume.
  ✓ Ensure current E&O covers defense for suits related to alleged negligent acts leading to breach or other cyber crime.
  ✓ Crime coverage (also called “fidelity” insurance) and cyber policies may cover first-party losses for social engineering. Likely NOT covered: Third party losses (e.g., a client’s loss due to socially engineered wire fraud.)
  ✓ Ask what post-breach services are offered. Consultation services? Breach notification assistance? Breach notification cost coverage?

• Policies may become outdated quickly in light of new threats, so review regularly.
Cybersecurity and the Law: Managing Your Risk
State Law

• State law may require:
  - Various cybersecurity and data protection policies;
  - Notice following a breach exposing PII;
  - Encryption of PII during storage, electronic transit.

• Regularly check laws for new requirements.
A few Indiana Data Security Laws….

- Social Security Number Law (Indiana Code (IC) 4-1-10): Crime to disclose SSNs except under certain circumstances.
- Data Disposal Law (IC 24-4-14): Crime to dispose of certain sensitive personal information without taking specific steps to make it unreadable.
- Breach Notification Law (IC 4-1-11): Requires notification of potentially affected individuals following a systems breach.
Indiana: Penalties

• Intentional or reckless disclosure of a SSN: Felony. Up to 3 years' jail time and up to $10,000 in fines.
• Negligent SSN disclosure: Up to 1 year jail time; $5,000.
• Violation of data disposal law: Up to 1 year jail; $5,000.
State Law is in Flux. 2015 - 2016:

• 12 significant amendments to state breach notification laws
• 20 states, 1 territory now specify contents required in breach notifications
• 22 states now require notice to the attorney general under certain circumstances
• Expanding definitions of PII
• Increasing specificity for notification timeline requirements
Private Lawsuits

- Negligence, failure to take appropriate IT precautions when conducting business electronically, breach of contract.
- Breach of fiduciary duty as a real estate professional; failure to protect client’s assets.
- Failure to warn about cybercrime.
Federal

• No comprehensive federal cybersecurity law specific to real estate at this time.

• Federal Trade Commission: Charged with protecting consumers from “unfair or deceptive commercial practices.”
Federal Trade Commission

FTC has determined that “unfair and deceptive practices” include bad cybersecurity practices:

• Failure to provide reasonable protections for personally identifiable information in company’s possession and control;

• Failure to comply with own privacy and security policies.
Federal Trade Commission

Settlements include:

• Requiring business to take remedial measures;
• Audit, reporting requirements;
• Monetary fines.
Cybercrime is Devastating.

Sixty percent of small businesses that are victimized by a successful cybersecurity breach go out of business within six months.

- Source: Ponemon Institute
Key Takeaways

1. Implement appropriate policies and programs, keep them updated, and enforce them.
2. Educate and empower yourself, employees, licensees, business partners, clients.
3. Keep security programs, anti-virus up-to-date.
4. Back up crucial data and programs.
5. Stay up-to-date on applicable laws.
KEEP CALM AND CARRY ON.

• We are a technology-driven industry in a technology-driven world.

• Evaluate your business’s cybersecurity risk, then implement reasonable precautions within your budget.

• **Best defense: Education.**
National Association of REALTORS®: Resources

Wire Fraud Landing Page: https://www.nar.realtor/topics/wire-fraud
Video Alerts and Education:
https://www.nar.realtor/videos/wire-fraud-alert-for-buyers


Articles:
- http://www.nar.realtor/articles/request-to-redirect-funds-should-trigger-caution
Contact:

JESSICA EDGERTON

JEDGERTON@REALTORS.ORG