

Cons, Scams & Hacks

Protecting Real Estate Clients in an Internet World



**With Over 50 Tips &
Tools to Protect Them
and You!**

Student Playbook

North Carolina Real Estate Commission

Continuing Education

Student Information Sheet

READ IMMEDIATELY UPON CHECKING IN

Basic CE Requirement (21 NCAC 58A.1702)

The CE requirement to maintain a license on active status is **eight (8) classroom hours per year** (each license period) consisting of the four (4) hour Real Estate Update course (mandatory for all licensees) and a four (4) hour elective. The content of the Update course changes each year.

Important Points to Note

- Newly licensed licensees do NOT need to take any CE prior to their **first license renewal** but must satisfy the CE requirement prior to their **second license renewal**.
- A course may not be taken for CE credit twice in the same license period. Make sure you have not already taken this course during the current license period.
- If your license is **inactive**, you should check with the Commission to ascertain the amount of CE you need to activate your license.

Attendance Requirement

In order to receive CE credit for a course, students must attend the entire scheduled class session. Sponsors and instructors may, on an individual basis, excuse a student for good reason for up to 10% of the scheduled class session (20 minutes for a 4 hours class session); however, a student must attend a minimum of 90% of the scheduled class session in order to receive a course completion certificate and CE credit. No exceptions to the 90% attendance requirement are permitted for any reason.

Student Participation Requirement

To help assure that the mandatory continuing education program will be one of high quality, the Commission requires that students comply with the following student participation standards:

A student shall direct his active attention to the instruction being provided and refrain from engaging in activities unrelated to the instruction which are distracting to other students or the instructor, or which otherwise disrupt the orderly conduct of a class. **Examples of Prohibited Conduct:** Sleeping; reading a newspaper or book; performing office work; carrying on a conversation with another student; making or receiving a phone call on a cellular phone; receiving a page on a pager that makes a noise; loudly rattling or shifting papers; or repeatedly interrupting and/or challenging the instructor in a manner that disrupts the teaching of the course.

Sponsors and instructors are required to enforce the student participation standards. Sponsors have been directed to NOT issue a course completion certificate to a licensee who violates the standards and sponsors must report inappropriate behavior to the Commission.

Course Completion Reporting

Sponsors are responsible for reporting course completion information to the Commission via the Internet within **7 days of course completion**. Licensees are responsible for assuring that the real estate license number that they provide to the course sponsor is correct.

Licensees may address comments/complaints about courses, instructors, and/or sponsors to:

Continuing Education Officer
North Carolina Real Estate Commission
P.O. Box 17100
Raleigh, North Carolina 27619-7100

Certificates of Course Completion

Course sponsors will provide each licensee who satisfactorily completes an approved CE course a Certificate of Completion on a form prescribed by the Commission within 15 calendar days following a course. The certificate should be retained as the licensee's personal record of course completion. **It should not be submitted to the Commission unless the Commission specifically requests it.**

Check the Label of Your Newsletter

The number of continuing education credit hours credited by the Commission to your licensee record for the current license period as of a stated date will appear on the mailing label of each edition of the Commission's newsletter. You may also check your **current year's** CE credits online at the Commission's website: www.ncrec.state.nc.us. You will need to log in under Licensee Login using your license number and pin number. If you are unsure of your pin number, please follow the instructions on our website.

Please avoid calling the Commission office to verify the crediting of continuing education credit hours to your license record unless you believe that an error has been made. Please use our website to verify that your credit hours have been reported. Your cooperation in this regard will be especially needed during the May 15 - June30 period each year.

Why This Course Was Written

A pretty good argument can be made that with all the risks that exist throughout the real estate profession, cybersecurity today should be at the top of the list. Millions of dollars of hard-earned client money is at risk. Professional reputations and entire brokerages are at risk. Cybercrime has become the #1 criminal activity in America.

As Kevin Mitnick, “The World’s Most Famous Hacker” has said:

Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s all wasted money. None of these measures address the weakest link in the security chain...people.



This course was written to address the weakest link in the security chain. People. We will explore our habits and the weaknesses that hackers and cybercriminals use to compromise the real estate profession. The class is full of practical tips and tools that will help keep you and your clients safer in an internet world. We have broken the course down into 4 modules:

- **Risks We All Face**
- **Scams & Cons in Real Estate**
- **Wire Fraud in Real Estate**
- **North Carolina Case Studies**

Student Notes



About the Author, Terry Wilson, DREI

Terry Wilson, DREI, is a leading real estate instructor with Superior School of Real Estate in North Carolina. With thousands of students and over a decade of live classroom experience Terry has excellent educational skills. His knowledge of the actual practice of real estate is bolstered by the fact that he is the founder and Broker-in-Charge of Wilson Realty, LLC., a brokerage firm with nearly 100 practicing agents that he works with daily.

Terry is a recognized voice on National Public Radio and the host of the Real Estate Great Debates podcast. In this course Terry combines his passion for teaching, his practical knowledge of the business and his technical expertise as a 20-year IBM corporate executive.

About the Producer, Len Elder, JD, DREI, CDEI



Len Elder, DREI, is the Senior Instructor and Curriculum Developer for Superior School of Real Estate. With over 40,000 hours of live classroom presentations and teaching, Len has excelled to the top of his field and is recognized nationally as an author, speaker, course developer and a Distinguished Real Estate Instructor (DREI) by the national Real Estate Educators Association.

With a B.A. degree in Speech Communications & Broadcasting and a law degree from Capital University, Len brings a multi-disciplinary approach into the classroom. His professional life spans the private practice of law, the mortgage banking industry, the real estate profession and the educational profession. He has served on numerous committees. Len is the 2018 North Carolina Real Estate Instructor of the Year, author of the national 2018 Course of the Year and holds several other awards. More than anything else, Len believes that real estate education ought to have real value, be engaging and help real estate professionals in their careers.

Table of Contents / Course Outline

| | |
|---|-----------|
| Module 1 – Risks We All Face | 8 |
| The Internet of Things | 10 |
| Who’s Guarding the Door | 11 |
| The Escalation of the identity Theft Crises | 12 |
| An Overview of Identity Theft | 13 |
| The Deep & Dark Web | 15 |
| The Role of the Federal Bureau of Investigation | 16 |
| The Department of Justice | 17 |
| Top Ten Internet Cons & Scams | 17 |
| The Nigerian Prince Scam | 17 |
| Phishing Scams | 18 |
| Facebook Password Scams | 21 |
| The Secret Shopper Scams | 21 |
| Gift Card Scams | 22 |
| Hitman & Extortion Scams | 22 |
| Scareware | 23 |
| Electronic Greeting Cards | 23 |
| Malware & Viruses | 24 |
| Cookies & Browsing History | 24 |
| Module 2 – Scams & Cons in Real Estate | 27 |
| The Ten Most Common Real Estate Scams | 28 |
| Hijacked Listings | 29 |
| Rental Scams | 29 |
| Component Part Scams | 31 |
| Moving Company Scams | 31 |
| Deed Scams | 32 |
| Mortgage Fraud | 33 |
| Open House Thefts | 35 |
| Fake REALTORS® and Attorneys | 36 |
| Ransomware Attacks | 37 |

| | |
|---|-----------|
| SSL Certificates | 38 |
| Cybersecurity for Small Business | 39 |
| Module 3 – Wire Fraud | 40 |
| Bain vs. Platinum Realty | 41 |
| Colorado Couple Loses \$272,000 Due to Real Estate Wire Fraud | 42 |
| The 2019 IC3 Wire Fraud Report | 43 |
| Steps to Take When Wire Fraud Occurs | 44 |
| Licensees and Email Security | 45 |
| Ten Best Practices for Email Security | 47 |
| Use Strong & Unique Passwords | 47 |
| Use Multiple Email accounts | 47 |
| Get Off Public Wi-Fi | 48 |
| Get Proficient with Your Mobile Phone’s Hotspot | 49 |
| Use Two Factor Authentication | 49 |
| Use Email Encryption | 50 |
| Beware the Phish | 52 |
| Trade Unsubscribe fo Spam Filters | 52 |
| Don’t Use Business Emails for Social Media | 52 |
| Don’t Open Attachments Without Verification | 52 |
| Module 4 – North Carolina Case Studies | 53 |
| By the Numbers | 54 |
| A lesson in Stolen Wires & Hold Harmless Hurdles | 54 |
| NC State Bar Formal Ethics Opinions | 57 |
| The Surprise Liens | 58 |
| Craigslist Rental Scandal Hits Raleigh Area | 59 |
| The Role and Responsibility of NC Real Estate Licensees | 60 |

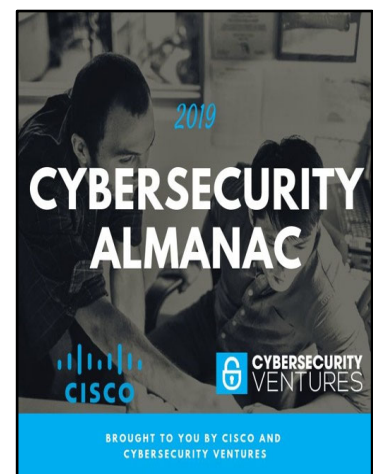


Module 1

Risks We All Face

Cisco and Cybersecurity Ventures teamed up in 2019 to produce a comprehensive report on the nature and extent of cybersecurity breaches. Among some of their findings:

- Cybercrime has become the fastest growing crime in the United States.
- Cybercrime has grown to over a \$1.5 trillion industry
- Nearly 70% of businesses have experienced some form of cybersecurity attack.
- One out of every 50 emails contain malicious content.
- Attacks occur every 14 seconds.
- Estimated losses by 2021 will top \$6 trillion.
- Cybercrime has become most costly than all the world's natural disasters.
- Computer crimes are more profitable than the entire world's illegal drug trade.



Student Notes

The nature and extent of compromised databases and consumer information on the internet has reached epic proportions involving the theft and misuse of everything from dates of birth, social security numbers, passwords, credit cards, bank accounts and fund transfers.

Huge breaches of data are occurring, and we have all heard of major companies whose data has been hacked or compromised over the last decade.

| Company | Accounts Hacked | Date |
|-----------------|------------------------|----------------------|
| Linkedin | 100 Million | June 2012 |
| Target | 110 Million | November 2013 |
| Yahoo | 3 Billion | August 2013 |
| Uber | 57 Million | November 2016 |
| Equifax | 145 Million | July 2017 |
| Marriott | 500 Million | June 2018 |
| Facebook | 540 Million | March 2019 |

One of the country's leading cybersecurity experts and consultants is Robert Herjavec, who appears regularly on Shark Tank. Robert is the CEO of the Herjavec Group, and has called cybersecurity "the greatest threat to small business."

Student Notes

Herjavec produces the Official Annual Cybercrime Report. One of the key additional pieces of insight that Herjavec brings to cybercrime discussions is the revelation that we are only experiencing the tip of the iceberg when it comes to protecting information and data on the internet. The sheer volume of information and

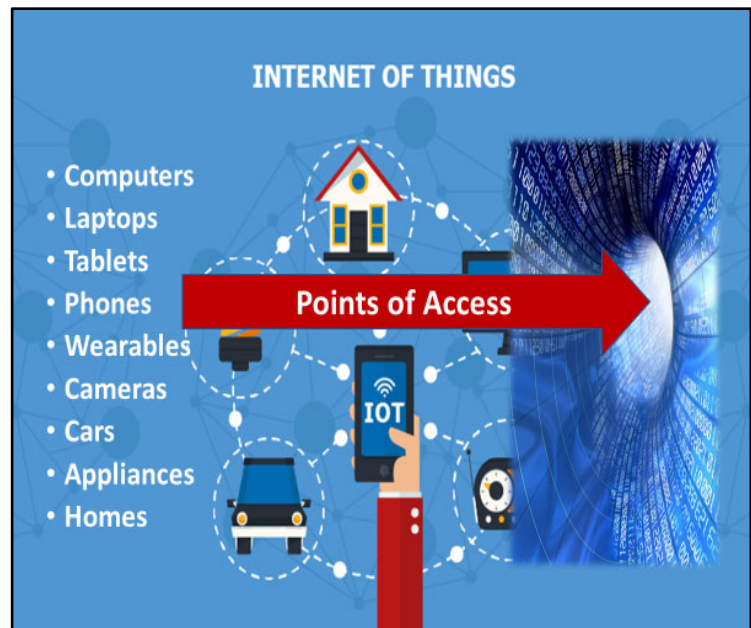
the massively growing amounts of data will make cybersecurity a monumental task in the years ahead.

- By 2021 data volume will be 100 times greater than it was in 2016
- By 2020 there will be 200 billion devices connected to the internet compared with just the 2 billion devices in 2006
- There are 300 billion passwords to protect
- Every year over 111 billion lines of new code is written in the form of apps and programs requiring constant innovation in security

The Internet of Things

It was one thing when internet users had to protect just their computer or their laptop from malware, viruses and hacking. Today we live in the Internet of Things. Today all types of devices are connected to the internet and exchanging electronic information online.

Each new connected device creates another point of access for hackers and intrusion to infiltrate your internet security.



Student Notes

Who's Guarding the Door

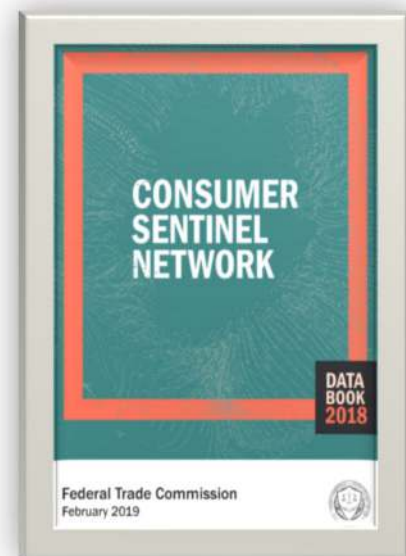
There are lots of different government agencies at the federal, state and local level that have some level of involvement in tracking and prosecuting cybercrime. In this course we are just focusing on the major players who are involved with cybercrime on a domestic basis.



The U.S. Federal Trade Commission is mostly involved in gathering data from consumers. The main repository for this data is the Consumer Sentinel Network that is compiled by the FTC based on the collection of information from consumers.

Consumer Sentinel is the unique investigative cyber tool that provides members of the Consumer Sentinel Network with access to millions of consumer complaints. Consumer Sentinel includes complaints about:

- Identity Theft
- Do-Not-Call Registry violations
- Computers, the Internet, and Online Auctions
- Telemarketing Scams
- Advance-fee Loans and Credit Scams
- Immigration Services
- Sweepstakes, Lotteries, and Prizes
- Business Opportunities and Work-at-Home Schemes
- Health and Weight Loss Products
- Debt Collection, Credit Reports, and Financial Matters



Consumer Sentinel is based on the premise that sharing information can make law enforcement even more effective. To that end, the Consumer Sentinel Network provides law enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors. The database is free to any federal, state or

local law enforcement agency. The entire project is premised on the idea that access to information and the sharing of cybercrime incidents can help law officials in identification and prosecution.

Student Notes

The Escalation of the Identity Theft Crisis

One of the fastest rising areas of cybercrime is identity theft. Credit card fraud ranks as the #1 type of criminal theft by the FTC with over 150,000 reported incidents per year. However, the nature of the theft has changed in recent years. Previously hackers and criminals stole credit cards, hacked credit card numbers and accounts and manufactured duplicate cards.



Sometimes our best efforts at trying to curtail crime has unintended consequences. The reason that the security chip was introduced was because the problem with magnetic strips is that they contain all of the cardholder information that would be necessary to make a purchase or to duplicate the card. Due to the rapid advances in technology the magnetic strip and its information became a lot easier to thieves to steal.

By contrast, the EMV (Europay, Mastercard & Visa) computer chips generate a unique code for each transaction that can only be used once. Thus, even if the chip information is stolen or there is a data breach at a retailer, thieves cannot do anything with the data collected from the chip. The chips made stealing the card, hacking the data or breaking into a vendor's database worthless.

Consequently, it became much more profitable and productive to steal identities rather than the card information. By stealing a person's identity, the thieves could then simply apply and get new cards issued in the victim's name. This practice has led to a spike in identity theft.



An Overview of Identity Theft

The primary access point for identity theft is the hacking of your accounts. When people duplicate passwords, fail to change and update passwords or use predictable and short passwords they are playing into the hands of cybercriminals engaged in identity theft. Here are some alarming identity theft statistics:

- Over 60% of people use the same password across multiple sites
- The average user has 26 password-protected sites
- The average user has only 5 different passwords across those sites
- More than 85% of Americans try to keep track of passwords by memorizing them in their heads
- On average it takes 170 days to detect a malicious attack
- 12345678 is cracked during a single sneeze
- It takes .2 seconds to crack a Google software engineer's password

Be Alert to the Warning Signs of Identity Theft

- Unexplained withdrawals from your bank account
- Calls from debt collectors about debts that aren't yours
- Debts appearing on your credit report that are not yours
- Notices from trusted vendors that your security was breached
- IRS notifications of multiple filings or delinquencies you don't understand
- Notices from social security of alterations or aberrations in your account



While there is no 100% way to prevent identity theft, there are several steps that can be taken to minimize the risks:

1. **Use a Password Generator to create stronger passwords for your accounts.**
2. **Review your bank statements on a regular basis.**
3. **Consider setting auto-alerts with your bank**
4. **Pull and review your credit report on an annual basis at AnnualCreditReport.com.**
5. **Review your official Social Security Report Annually.**
6. **Consider enrolling or subscribing to an identify theft service such as LifeLock or Advanced Identity Protector.**



Student Notes



The DEEP & DARK Web

Despite what consumers believe is a huge amount of information on the worldwide accessible through search engines like Google, Bing and Internet Explorer, only about 1% of internet is visible through public search engines. All that is searched in traditional browser bars is like the tip of the iceberg.

Most of the internet is actually in the Deep Web. The Deep Web is not necessarily a bad thing. It is used by academics, governments, law enforcement agencies where databases and information is kept from the public view. Specialized software is used to block web crawlers and public search engines. The Deep Web of private information composes about 90% of internet information.

The remaining 9% is the Dark Web where illegal and illicit activity is conducted using software programs such as TOR that hide the information and make it invisible, encrypted, encoded and unable to trace IP addresses. It is this arena that stolen identity information, credit cards and social security numbers are distributed and sold. If you are a victim of a hacker, chances are your information ended up in the Dark Web.



The Role of the Federal Bureau of Investigation

The FBI is the U.S. lead investigation and enforcement agency on cybercrime. The FBI has now assembled an entire Cybercrime Division. This division operates several Cybercrime task forces and investigates matters that are channeled through the Internet Crime Complaint Center (IC3).

Anyone can file a complaint with IC3. If you are ever a victim of cybercrime or identity theft, filing a complaint with the FBI is a good idea. The complaint process is simple and direct. Just go to their website: www.ic3.gov.



Federal Bureau of Investigation

Internet Crime Complaint Center(IC3)



Home
File a Complaint
Press Room
News
About IC3

Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

File a Complaint

Welcome to the IC3

🔍

Site Navigation

Alert Archive

FAQs

Disclaimer

Privacy Notice

Internet Crime Prevention Tips

Internet Crime Schemes

Annual Report

The Department of Justice

Although the U.S. Department of Justice has a Computer Crime and Intellectual Property Section (CCIPS) gets involved in cybercrime issues, their focus is mostly on international crime. The DOJ spearheads a coordinated effort between the United States, Europe, Australia and Asia known as Operation Shadow Web to disable and apprehend international criminals involved in computer crimes.

It may sound like an episode out of Netflix's hit series, Blacklist, but the FBI and DOJ have assembled a list of the 41 Most Wanted Cybercriminals in the U.S. and abroad and are engaged in active attempts to apprehend and halt their operations.



The Top 10 Internet Cons & Scams

The Nigerian Prince Scam

These scams involve someone overseas offering you a share in a large sum of money or a payment on the condition that you help them transfer the money out of their country. They initially originated in Nigeria, but today they come from all over the world. Initial contact is out of the blue by email, social media or text message.

Either in the initial contact or follow up the scammer will seek information about your bank account so they can transfer the money, or else the scammer requests that

you pay what will become an unending stream of fees and charges that are necessary for you to receive “your share” of the funds.

Today this scam still creates losses of about \$700,000 annually in the United States. If you are surprised that people still “fall” for this scam it is important to realize that while the initial scams depended on the victim providing bank account information or funds, the widespread use of this scam have caused it to take on different forms and different ways of targeting its victim.

The email itself is often a phishing scam where the opening of the email infects your computer or gives hackers access to your data. So even if you responded by emailing back a message that says: “Stop scamming people. You are a disgrace.” May have left you victim to this scam. In fact, scammers are now using the pretense of law enforcement to gain your participation.

Phishing Scams

Phishing scams are defined as fraudulent attempts to obtain information such as passwords, usernames and credit cards in an electronic communication. Phishing can appear in a variety of ways, but the most common is an email that informs consumers that they need to reset accounts, login differently or make password corrections to their account. Learning to recognize or identify phishing emails is an important skill in this era of cybercrime and hackers.

The Federal Investigation Bureau

Washington, DC

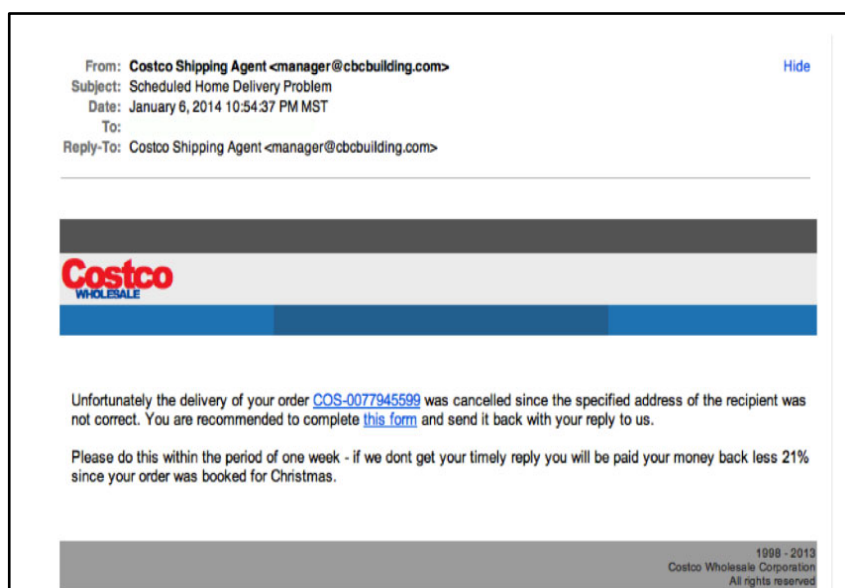
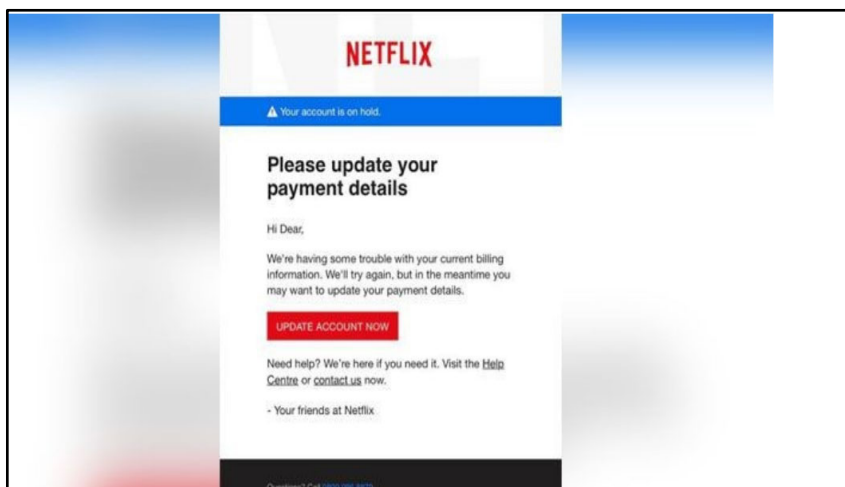
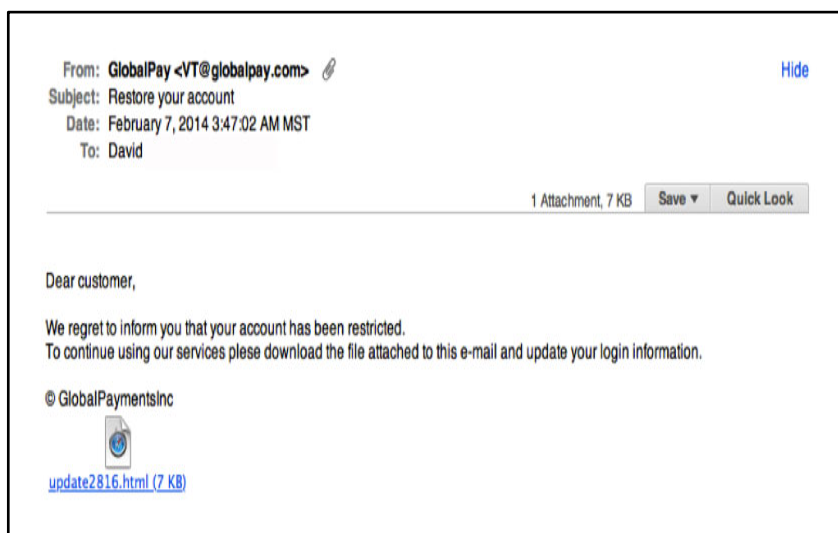
Our office has come to investigate scams involving foreigners emailing Americans and asking for funds. We start investigation.

If you received such an email, click on link below to add you to government database.

We look forward to share with you proceeds recovered in prosecution.

Student Notes

MARK the RED FLAG WARNING SIGNS





Because phishing has become so prevalent and fictitious emails are the number one way that hackers gain access, there are things that you can do to minimize the risk. Being cognizant of the RED FLAG warning signs we just discussed is critical. Here are some additional insights and tips.

1. Delete generically addresses emails
2. Know that embedded links don't authenticate
3. Be cognizant of grammatical errors
4. Use your own link to access companies and sites
5. Use the web tool to verify sites



Check The Domain of Suspicious Emails

In Outlook right click on the email and select "View Message Details"

LinkedIn Welcome
[EXTERNAL] Len, see... 10:26 AM
Kickstart your network by... contacts ...

Dawn Fellers
[EXTERNAL] Mid Term Assessment Test 9:44 AM
No problem! I will let him know! Dawn Fellers Ed...

The CE Shop
[EXTERNAL] The 📅's ticking -- save 40% 9:03 AM
Take advantage of this one-day deal! To view this...

Yesterday

Message details

Received: from BN6PR06MB2626 namprd06.prod.outlook.com (2603:10b6:805:ca:37) by SH6PR06MB4206 namprd06.prod.outlook.com with HTTPS via SH6PR16CA0060 NAMPRD16.PROD.OUTLOOK.COM: Wed, 21 Aug 2019 13:44:13 -0000
Authentication-Results: mckissoc.com; dkim=none (message not signed)
headerfrom=mckissoc.com; dmarc=none action=none
headerfrom=mckissoc.com

Received: from BN6PR06MB2595 namprd06.prod.outlook.com (10.173.144.10) by BN6PR06MB2626 namprd06.prod.outlook.com (10.173.145.22) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2178.18 Wed, 21 Aug 2019 13:44:12 +0000

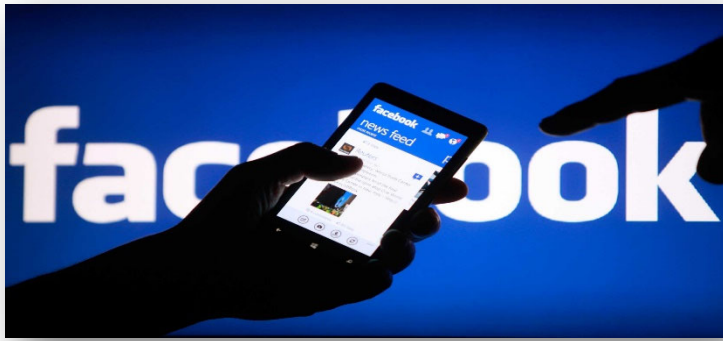
Received: from BN6PR06MB2595 namprd06.prod.outlook.com ([fe80:7b05:558:2575:5454]) by BN6PR06MB2595 namprd06.prod.outlook.com ([fe80:7b05:558:2575:5454]) with mapi id 15.20.2178.018 Wed, 21 Aug 2019 13:44:12 +0000

Content-Type: application/ms-tnef; name="winmail.dat"

From: Dawn Fellers <dawn.fellers@mckissoc.com>
To: Len Elder <len.elder@mckissoc.com>

Thread-Topic: [EXTERNAL] Mid Term Assessment Test
Thread-Index: AQHVA3i6hRuH+OyuGGZx/mcTBWkCtHAqA/tKCAAR/Q0A=

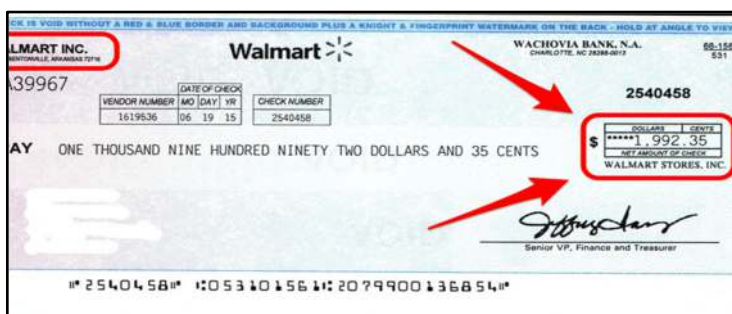
Forward emails to reportphishing@antiphishing.org



**What passwords
have you given away
on Facebook?**

Student Notes

The Secret Shopper Scams



There are legitimate secret shopper companies and jobs in the current marketplace. There are also a lot of scams surrounding this opportunity. The most common is the receipt of a solicitation to be a mystery shopper. Be wary of offers that charge fees

upfront or require some type of paid certification. Often these scams involve sending you a check, instructing the mystery shopper to deduct out a certain amount for their services and write a check for the remainder to another entity or company. Inevitably the check sent bounces and the consumer is on the hook for the check they sent.

Gift Card Scams

There have recently been a lot of scams surrounding gift cards. These come in a variety of formats. Gift cards are often out in the open on display racks and easily accessible. Beneath a tab on the card is a bar code for activation and a PIN. Scammers can gain access to the bar code and the PIN. Once the card is activated, they steal the money that is on the gift card.

Student Notes

The reason that things like gift card scams are discussed in a real estate course is because real estate agents encounter all these scams and cons in their daily lives. The instructor should constantly reinforce the fact that as professionals, when a licensee's data or devices are compromised, they not only put themselves at risk but also expose all the clients, customers and other professionals they work with to the risks as well.

One of the newest and most popular twists on the gift card scam is for the scammer to impersonate a friend, relative, co-worker or boss. The scammer then asks a consumer to purchase gift cards because they are needing for work, emergency, jail bond, hospitalization or because someone is stranded. Once the cards are obtained the consumer is asked to provide information on the back of the card and the money is stolen. These scams have become so widespread that major companies, like Walmart, that sell thousands of dollars in gift cards have posted gift card fraud prevention notices on their websites.

Hitman & Extortion Scams

The second most popular crime in 2018 was extortion. In that year alone 51,146 victims lost a total of \$83,357,901 to criminals. Usually the criminal threatened physical or financial harm or the release of sensitive or incriminating data. The rise in these crimes between 2017 and 2018 represented a 242% increase.



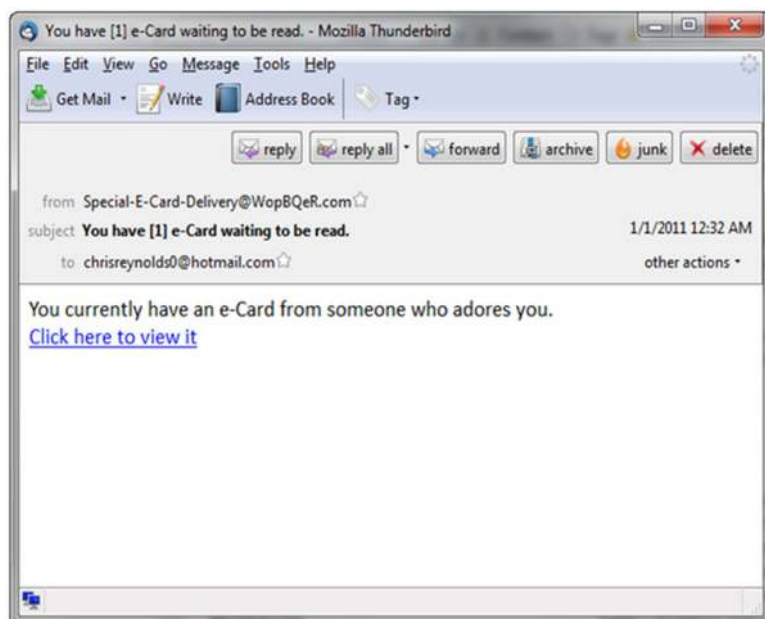
Scareware

It's becoming increasingly difficult to stay ahead of the scammers. Due to the recent dissemination of cybercrime instances, scammers have learned to use the fear of hacking to create additional scams. Pop-up screens and notices are now generated that inform the consumer that their computer is infected and urge them to immediately click on a link to scan their computer or install a "Fix." Such messages almost always are the virus or malware. Clicking on the links gives hackers access to the device and information on the device is compromised. Some warning signs of false computer safety messages often include:

- Dire warnings
- Pop-ups
- Unknown company names
- Offers to scan immediately



Electronic Greeting Cards



Who wouldn't like to receive an electronic greeting card from a friend or a secret admirer? Messages that say you have an e-card waiting for you, but which do not identify the sender are almost always a link to malware and viruses. Legitimate e-card companies and messages always tell you who the card is from. Electronic greeting card emails and messages which do not identify the sender of the card should be deleted.

Malware & Viruses

Malware is a contraction of the phrase “malicious software” and there are dozens of viruses and malware programs written as code every year. There are various forms including worms, viruses, trojans, adware and spyware that can infect your device and cause any number of problems.



Nearly everyone of these programs requires the user to be an accomplice in the cyberattack by clicking on a link, opening files or downloading programs. While the differences between such programs and the way they operate are technical issues which the average consumer user does not need to understand, the ghosting malwares of Adware and Spyware are the most problematic.

A ghosting malware is one that rests on your computer and allows the computer to continue to operate, however, it enables the computer to do more than you ever intended. Adware targets your computer to open various solicitations and ads as annoying pop-up screens (many which are malicious in nature). The pop-ups are notoriously hard to close without you inadvertently opening the offer or scam.

Spyware operates totally in the background and allows the criminal to not only see everything displayed on your screen but also to track every keystroke made on your computer, from the log-in to your email to the signing in on your online banking and credit card accounts.

Cookies & Browsing History

Most internet browsers, whether Chrome, Firefox, Internet Explorer or Bing contain a program that is storing the history of searches made on the internet. It's the reason that once you have been to a site that when you type a few letters in the search bar the previous search you conducted appears as a search choice. The various programs which store and record this history are called cookies. Most websites also have cookies that store information about your visit to the site. They capture such things as the number of pages you viewed, the number of visits you made, the IP address of your computer and your log in information.

In and of themselves cookies are not a bad thing. They are useful to those who operate websites, consumers and they add assistance to your internet searches. However, over time these cookies can slow the operation of your computer and affect its operation. These little bits of your browser history also can be hacked to provide a accurate with more information about you and what you do on a regular basis on the internet. Clearing cookies and caches will not only help your device operate better but will also provide you greater privacy and safety in using the internet.




Since each browser operates differently you should research the browser you commonly use. There are several “How To” videos on YouTube and Google which will walk you through some simple steps to change browser settings, automatically delete cookies and clear them periodically to prevent issues.

You can find various instructions and information about cookies and managing the properly by visiting [usa.gov/optout-instructions.com](https://www.usa.gov/optout-instructions.com).



Student Notes

Many of the risks and issues that we have discussed can be greatly minimized with a high-quality anti-virus, malware protection software. All users should install a reliable product from a known vendor and keep the program up to date.

| | | |
|--|---|--|
| <p>Best Overall</p>  | <p>Webroot</p> <p>9.9</p> <p>★★★★★ (3,823)</p> <ul style="list-style-type: none"> ✓ Protects Windows, Mac, Android, and iOS ✓ Real-time anti phishing ✓ 21-time PC Magazine award winner ✓ 70-day money-back guarantee ✓ 24/7 customer support <p>More ▾</p> | <p>WEBROOT</p> <p>Visit Site >></p> <p>Over 207 people chose this site today!</p> <p>\$39.99</p> <p>\$19.99</p> <p>50% Off</p> |
| <p>Most Comprehensive</p>  | <p>Norton 360 by Symantec</p> <p>9.0</p> <p>★★★★★ (3,041)</p> <ul style="list-style-type: none"> ✓ Protects Windows, Mac, Android, and iOS ✓ Parental controls included ✓ LifeLock™ security with select plans ✓ Million Dollar Protection Package ✓ 24/7 customer support <p>More ▾</p> | <p>Norton</p> <p>Visit Site >></p> <p>\$59.99</p> <p>\$39.99</p> <p>\$50 Off</p> <p><i>Plus applicable sales tax</i></p> |
|  | <p>McAfee</p> <p>8.8</p> <p>★★★★★ (2,181)</p> <ul style="list-style-type: none"> ✓ Protects Windows, Mac, Android, and iOS ✓ Parental controls included ✓ Permanently deletes sensitive digital files ✓ 30-day money-back guarantee ✓ 24/7 customer support <p>More ▾</p> | <p>McAfee</p> <p>Visit Site >></p> <p>\$69.99</p> <p>\$24.99</p> <p>\$45 Off</p> |



Student Notes

MODULE 2 SCAMS & CONS IN REAL ESTATE



Module 2 Scams & Cons in Real Estate

It should come as no surprise that the entire real estate industry is a huge target for cybercriminals. Whether you are an individual real estate licensee, a brokerage, a closing attorney, a real estate law firm, a title company or a mortgage lender you are highly at risk for scams and security breaches. Here are the top reasons why the real estate industry is such a lucrative target for cybercriminals:

- **There is lots of public information**
- **There is lots of communication**
- **There are constant transfers of money**
- **There are lax security standards by individual participants**

It is amazing the wealth of information regarding real estate that hackers and criminals have access to without having to steal anything and without being clandestine. This happens because of the vast amount of real estate information in the public records and due to the advertising and marketing conducted by real estate professionals. Think about what is immediately and easily accessible:

- The name of the owner
- Documents regarding the property
- Tax records
- Legal descriptions
- Liens & encumbrances
- Status of marketing
- Identities of those in the transaction
- Tons of background and biographical information



Student Notes

As real estate professionals we have a duty to safeguard and protect our client's information. And although real estate agents may believe that they don't have information worth stealing, the reality is that on your devices is a ton of information that is extremely valuable to cybercriminals. Real estate professionals are often in custody of all of the following which needs to be safeguarded. PPT Slide 81

- Client identity
- Closing disclosures
- Social security numbers
- Legal names
- Status of properties
- Financial information
- Bank account information



The Top 10 Most Common Real Estate Scams



There are dozens of scams perpetrated every day in the real estate industry. It is one of the reasons why all of the information in Module 1 is critical to you as a real estate professional. When our computers and devices are compromised, we are not only exposing ourselves to cybercriminals, we are exposing all the people with whom we work and communicate.

Hijacked Listings

We advertise and market properties across the entire internet spectrum. It is therefore reasonably easy for a cybercriminal to gather information about a listed property including its address, sales price, the real estate professionals involved and the owner. Cybercriminals gather this information publicly and then use that information to advertise the property on other sites such as Craigslist or eBay. Once posted they can collect deposits on offers, charge fees or offer the property for rent.

Student Notes

Rental Scams

Hijacked listings most often involve rental scams. The criminal simply does the following:

1. Gather home information from the internet
2. Establish an email similar to the listing agent
3. Advertise the property for rent on other sites
4. Offer fake leases and collect security deposits



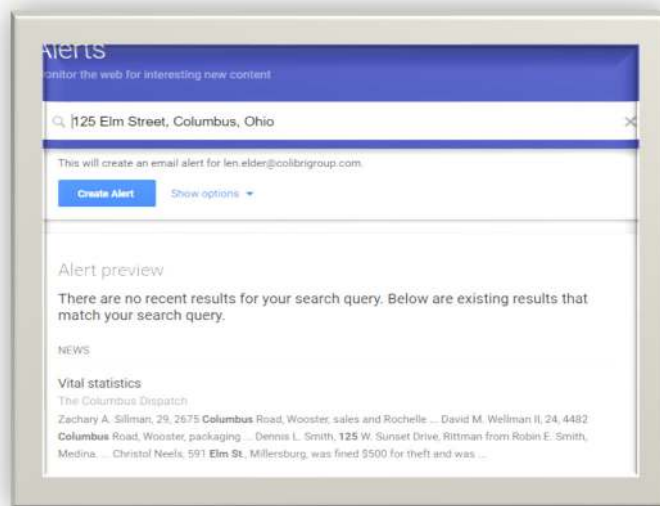
Student Notes



What Conversations Should We Be Having with Clients?

Using Google Alerts to Protect You and Your Clients

Google alerts is a FREE tool that you can use to set alerts in the Google search engine. By simply searching “Google Alerts” a user can set a browser search that is conducted 24 hours a day, 7 days a week. When information is posted to the internet that matches the search terms, the user is sent an email by Google alerting them that new information has been added to the internet containing those words or phrases. Real estate professionals should consider setting Google Alerts for:



- Their name
- Addresses of properties they have listed or which they manage

Student Notes

Component Part Scams



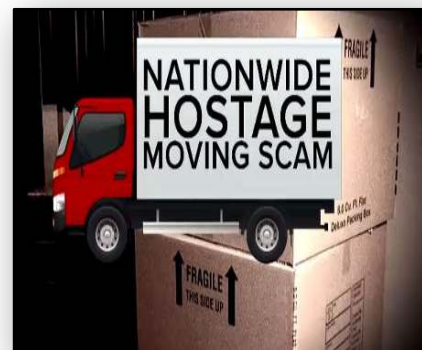
Many current markets have attracted flippers and investors who are purchasing, rehabbing and relisting properties. Component part scams started primarily with these types of sellers and what is known as an arc fault circuit interrupter (AFCI). AFCI's are advanced circuit breakers that reduce electrical fire threats and are required by some jurisdictions to comply with building codes. The breakers can be extremely expensive as compared to traditional circuit breakers.

The scammers list a property for sale that contains such breakers and at some point, prior to closing, revisit the home as the owner or seller and swap out the expensive breakers for cheaper ones. Let's face it, most homeowners would never notice. The illegal practices of swapping out component parts has now spread to HVAC units, water heaters and other components of the home removed and swapped after a home inspection. The items targeted are usually things that a typical homeowner or buyer's agent would never check on final walkthrough.

Think about expanding your final walkthrough list to include component part items such as the HVAC, smaller appliances such as the dishwasher, garbage disposal, garage door opener, electrical panels and water heaters.

Moving Company Scams

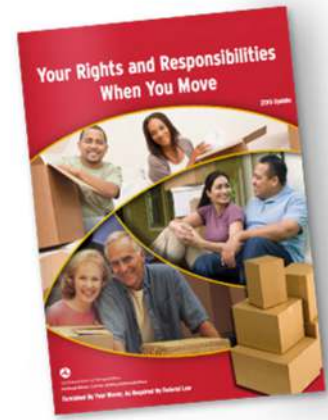
Recently there has been an increase in moving company scams. Such scams have involved everything from holding property hostage upon payment of additional fees and hidden costs to disappearing movers who steal the entire contents of a home. These problems occur more frequently for buyers who are moving across stateliness and may be unfamiliar with reputable companies who



engage in interstate moves. Always encourage and remind your clients to fully investigate moving companies before entrusting all of their belongings to one of them.

Moving companies that engage in interstate moves are subject to the Federal Motor Carrier Safety Administration regulations which are contained in Title 49 of the U.S. Code. These companies are required to comply with certain consumer protection provisions that are contained in federal law and must:

- Provide the required informational pamphlet of rights and responsibilities of homeowners
- Provide a binding estimate prior to taking custody of the consumer's belongings
- Not hold property hostage for unpaid fees and charges



Deed Scams

Remember what public information is available. It is easy for a cybercriminal to obtain a copy of a Warranty Deed to a property. It is also easy for criminals to obtain contact information for the homeowner and to know when properties are listed for sale.

A criminal can create a transfer Deed for the seller. By establishing an email similar to that of the listing agent the criminal then sends the seller a transfer Deed to sign and get notarized informing them that it is part of the closing process. Sometimes criminals approach owners appearing as lenders and request as part of the refinance process to sign a Warranty Deed. No legitimate lender EVER requires the signing of a Warranty Deed as part of the lending process.

You can help by educating consumers that the signing of a Warranty Deed transfers ownership of the property. Advise consumers that they should NEVER sign a Warranty Deed without consulting an attorney and fully understanding the nature of the documents that they are signing.

Mortgage Fraud

Mortgage fraud occurs when any borrower or individual materially misrepresents information which a lender utilizes as the basis for a loan.



Because mortgage fraud has a very broad definition it can occur in many forms and is usually tracked and reported based on the following categories:

Occupancy fraud occurs when mortgage applicants deliberately misrepresent their intended use of a property (primary residence, secondary residence or investment). Programs, pricing and underwriting guidelines are impacted by a property's intended occupancy.

Income fraud includes misrepresentation of the existence, continuance, source, or amount of income used to qualify. It also includes the misrepresentation or omission of certain debts and liabilities

Transaction fraud occurs when the nature of the transaction is misrepresented such as undisclosed agreements between parties and falsified down payments and earnest money deposits. This risk includes third party risk, non-arms length transactions and straw buyers.



Across all categories mortgage fraud has been steadily rising since 2010. The number of cases accelerated between 2017 and 2020. Core Logic's Mortgage Fraud Report indicates that in 2018 Out of every 109 loan applications 1 contained fraudulent information. Financial institutions have a statutory and regulatory duty to monitor, detect and report suspicious activities that may involve mortgage fraud under the federal Bank Secrecy Act (BSA). The Financial Crimes Enforcement Network (FinCEN), the agency under the U.S. Department of the Treasury works with the Federal Bureau of Investigation to collect SAR (Suspicious Activity Reports) and undertake investigations along with financial institutions.



The top 10 riskiest states for mortgage fraud include New York, New Jersey, Florida, District of Columbia, New Mexico, Illinois, Georgia, Nevada, California and Oklahoma.



The biggest risks and more frequent occurrences are with investors. Fraud rates for investor properties are 88% higher than other consumers with much of the fraud coming from the misrepresentation of occupancy. Part of the explanation may be the number of poorly informed and educated consumers who are given inappropriate and sometimes illegal advice on many of the “Get Rich Quick in Real Estate” investment seminars.

For out-of-state investors the numbers are even more staggering with 80% higher delinquency rates, and foreclosure rates 114% higher than other loans.

With the number of Out of State Investors (OOSI) increasing over 25% in the last 6 years these numbers are alarming.

Every borrower who completes a standard 1003 Fannie Mae Uniform Residential Loan Application certifies that the information contained in the application is true and that if there are any material changes that they will notify the lender. Licensees who knowingly allow a borrower to commit mortgage fraud can be charged with conspiracy.

Right above their signature in Section IX of the loan application every borrower acknowledges and agrees that:

- The loan application information is true and correct
- They have made no intentional or negligent misrepresentations
- The property will be occupied as represented
- The lender may rely on the information in the loan application
- The borrower will inform the lender of any material changes that occur between the time of loan application and the date of closing

Steering Clear of Loan Fraud

1. **Don't allow borrowers to misrepresent occupancy**
2. **Properly handle and deposit all due diligence fees and earnest money deposits**
3. **Make certain due diligence fees and earnest money deposits are accurately reflected in the contract**
4. **Don't create or condone outside the transaction agreements between the parties**
5. **Get all the agreement and money accurately reflected on the closing disclosure**



Open House Thefts

Homes that are on the market have always been a target of thieves and criminals. Widespread use of the internet and the posting of home information across the web has increased the problem. Thieves no longer need to stalk around in the middle of the night searching for a home to burglarize. They can preview their targets on the internet by viewing virtual tours which depict furniture, artwork and valuables along with the locations of windows, doors and alarm systems.



When criminals attend open houses and the agent is distracted with other guests common practices include the theft of prescription drugs, spare keys and the unlocking of doors and windows for later intrusion. A perfect window of opportunity is created between the posted time that the open house ends and the owner returns between 4:00 and 6:00 on a Sunday afternoon.

Agents should be aware of these issues, take precautions and have lengthy discussions with sellers about securing valuables and medications during an open house and alert homeowners to the security risks that exist.

Student Notes

Fake REALTORS® and Attorneys

There have been multiple instances recently of individuals posing as fake real estate professionals or attorneys and taking advantage of unsuspecting consumers.



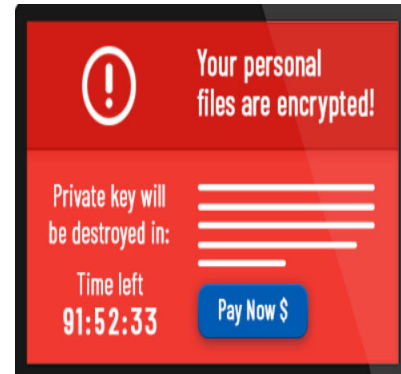
When imposters pose as agents, they most often offer to write a contract and obtain deposits from consumers. Posing as an attorney opens the door to requesting signatures on documents such as deeds and transfers of the property, issuing wire instructions and collecting deposits. As imposter rental agents, criminals draft fake leases and collect security deposits.

Both professions are heavily regulated, and it is relatively simple for a consumer to check with official websites and agencies to make certain they are truly dealing with licensed professionals.

Student Notes

RANSOMWARE ATTACKS

Ransomware is malware that is designed to deny access to a computer system or data until ransom is paid. The malware is usually spread through phishing email or links. Over the last couple of years incidents of ransomware attacks have increased 350%. Payment is usually demanded from the network or data owners in the form of Bitcoin or cryptocurrency which cannot be traced.



There have been a lot of ransomware attacks and many of them have been part of the national news cycle:

- Metrolist MLS in California with 20,000 members
- City of Baltimore
- Monroe College
- City of Atlanta
- 23 Texas towns

Student Notes

The Best Defense Against Ransomware Attacks

The best defense against ransomware attacks is to have all data backed up and stored somewhere other than the network server or your device. There are lots of effective data backup systems to choose from. Carbonite is a national company that specializes in the secure backup of computer data and boasts the story of a RE/MAX real estate professional, Sandler Dickson of Tallahassee, Florida who defeated a ransomware attack with Carbonite. Sandler and his wife are prominent Tallahassee agents who had

on their computer tons of information about real estate deals past and present. They included real estate documentation, floor plan graphics and close to 25,000 pictures of properties.

When the computers were infected with ransomware that locked up all of their data, the Dickson's were able to simply wipe the entire computer clean and rebuild it from scratch. Carbonite made it possible for them to restore all of the original data.

In addition to Carbonite, cloud based backup and external hard drive backups are available. External hard drives (often called Passports) are relatively inexpensive, easy to use and can store a lot of data. Real estate professionals should have a regular and routine plan for backing up data.

SSL Certificates

SSL stands for Secure Socket Layer and involves datafiles that are encrypted on a web server. These files create a secure and encrypted connection from servers to browsers.

Consumers are used to SSL secured websites because they are frequently utilized on any website that is exchanging with consumers:

- Credit card transactions
- Data transfers
- Logins

SSL certification is now becoming the norm on any site with which a consumer exchanges information, downloads data or logs in. For example, a real estate website where a potential buyer can create a profile or search for homes.



Student Notes

There are a lot of companies, such as Go Daddy that provide SSL certification which will make your consumers feel more secure in dealing with your website. The cost of SSL certification is relatively inexpensive. If you deal with a lot of consumers and the exchange of information with them on your website, you may want to explore SSL certification and security.

Cybersecurity for Small Business

In today's high-tech world there is no such thing as any information or system being 100% secure. Anything data can be stolen. Any system can be hacked or compromised.

Cybercriminals, like most criminals, look for windows of opportunity and target the low hanging fruit. One of the biggest reasons that real estate professionals have become a preferred target is due to the lax security concerns and inattention to the issues we are addressing in this course. A large percentage of real estate professionals handle a ton of sensitive and financial data. A lot of real estate professionals are operating businesses in a cybercriminal world and regularly engage in the reckless practices of:

- Using simple and repetitive passwords
- Operating email accounts without any security
- Using devices with no security protection
- Accessing public Wi-Fi systems
- Failing to back up or store data properly

While you can never be 100% safe, some simple implementation of the tips and tools discussed in this course can help protect you and your clients and assist you in operating in a safer environment.

Student Notes



Module 3

Wire Fraud in Real Estate



Let's Play Hacker Smacker

Indicate whether the following statement are True or False

1. Hackers usually target major businesses with a lot of records.
TRUE **FALSE**
2. As a real estate professional all client emails should be encrypted.
TRUE **FALSE**
3. Errors and omissions insurance covers lost wires.
TRUE **FALSE**
4. Once I have lost a wire there is nothing that I can do.
TRUE **FALSE**
5. Licensees should only log on to secure public Wi-Fi's.
TRUE **FALSE**
6. Real estate professionals can be held liable even if they never touched the wire instructions and did not have anything to do with sending the wire.
TRUE **FALSE**

Student Notes

Bain vs. Platinum Realty

Jerry Bain was a buyer purchasing a home. Defendant Kathryn Sylvia Coleman acted as the sellers' real estate agent and was affiliated with the Defendant, Platinum Realty, LLC. To fund the purchase, Bain, who planned on paying cash was instructed to wire \$196,622.67 to the title company. Unbeknownst to the parties involved, a criminal was intercepting emails between the title company, agent and Bain. Bain had actually been sent hacked wiring instructions which instructed him to wire the funds straight to the criminals account. The email that Bain received was allegedly from the listing agent, Kathryn Sylvia Coleman's email. Once the funds were sent, they could not be recovered and so Bain sued the agent, the firm and others.



At trial the jury found that the listing agent was 85% responsible for the losses and that Mr. Bain was responsible for 15% of the fault. A judgment was entered against Ms. Coleman in the amount of \$167,129.27. It was from this judgment that Ms. Coleman filed an appeal because the evidence was clear that she did not create the fraudulent email that contained the wire instructions.

In reviewing the case, the Court of Appeals acknowledged that while the listing agent may not have sent the fraudulent email that the jury was entitled to their conclusion that she acted without reasonable care in the handling of client communications and that she was negligent in not protecting the client in their transmission of funds.

Student Notes



Colorado Couple Loses \$272,000 Due to Real Estate Wire Fraud

James and Candace Butcher were ready to finalize the purchase of their dream retirement home, and at closing time wired \$272,000 from their bank following instructions they received

by email. Within minutes, the money had vanished.

Unbeknownst to the Colorado couple, the email account for the real estate settlement company had been hacked, and fraudsters had altered the wiring instruction to make off with the hefty sum representing a big chunk of the Butchers' life savings, according to a lawsuit filed in state court. The Butchers, forced to move into their son's basement instead of their dream home, eventually reached a confidential settlement in a lawsuit against their real estate agent, bank and settlement company, according to their lawyer Ian Hicks.

The problem is growing as hackers take advantage of lax security in the chain of businesses involved in real estate and a potential for a large payoff.

"In these cases, the fraudster knows all of the particulars of the transaction, things that are completely confidential, things they should not know," said Hicks, who is

involved in more than a dozen similar cases across the United States. Numerous cases have been filed in courts around the country seeking restitution from various parties. One couple in the US capital Washington claimed to have lost \$1.5 million in a similar fraud scheme.

It may be difficult to establish liability, but Hicks said that "consumers are not going to be careless with their life savings" and that the real estate professionals have a responsibility to ensure the security of their systems, and to give customers adequate information.

The lawsuit filed by Hicks for the Butchers said that "the scam that befell the Butchers was well-known in the real estate industry and easily preventable."

The 2018 IC3 Wire Fraud Report

The FBI's Internet Crime Complaint Center (IC3) has identified real estate wire fraud as a major target of cybercriminals.

- 20,237 victims have lost \$1.6 billion
- Losses up 1,100% since 2016
- Number of actual attempts unknown
- Interactions are becoming more sophisticated
- Wire fraud is extremely lucrative



According to the Federal Bureau of Investigation, the average amount stolen in a typical bank robbery is only \$3,816. The average amount stolen through wire fraud is \$129,427. For most consumers and the business professionals wire fraud is particularly devastating. Because the perpetrators of wire fraud use "money mules" to transfer the money across various accounts and countries in the blink of an eye, once funds are wired to an inappropriate account they are usually gone forever. Very few wire fraud thefts are ever recovered. For the professionals and businesses involved, most of them are on the hook personally for the losses, which are usually excluded from coverage under standard E&O policies.

When dealing with wire instructions there are some basic safeguard procedures which should be followed. Those who handle wire instructions should employ all of the following processes:

1. Use a wire confirmation checklist
2. Try to use overnight delivery or landline faxes for instructions
3. Use encrypted email
4. Confirm the wire verbally



Steps to Take When Wire Fraud Occurs



1. Contact your bank and initiate a “SWIFT recall’ on the wire transfer that left your bank.
2. File a complaint with the FBI’s Internet Crime Complaint Center (IC3)
3. Contact your local FBI field office and provide the IC3 complaint number.
4. Contact all banks that may have received the wire.
5. Contact local authorities and file a police report.

Student Notes

Every wire sent or received should involve proper identification and verification of the authenticity of the instructions, verbal confirmation of the instructions with the appropriate party and verification of the delivery of the wire. Attorneys and lenders are experts at protecting wires and all of them have in place set processes and procedures for verification. Real estate professionals by contrast tend to be the weak link in the chain.

The Best Advice for Real Estate Professionals



Consider This Addition to Your Emails

READ THIS!!!

WIRE FRAUD: During your representation by Wilson Realty Co., LLC, you will NEVER be asked via email to wire or send funds to ANYONE, not even an attorney.

DO NOT COMPLY WITH ANY EMAIL INSTRUCTIONS FROM THIS OFFICE TO WIRE FUNDS!

WIRE FRAUD ALERT

MIKE EBYND ATEBL

The National Association of REALTORS® has published the following as an addition that licensees may wish to consider adding to their email signature line. NAR cautions that the Notice should never serve as a substitute for educating your clients and other participants in real estate transactions about email wire fraud.

IMPORTANT NOTICE: Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.

Licensees & Email Security



Just because licensees may decide to never touch or become involved in the wiring of money or the wiring instructions does not, as the Bain case indicates, protect agents from liability. Licensees have a duty to protect and promote their client's interests and are charged with the responsibility of exercising reasonable care in their handling of a transaction.

Student Notes

Not utilizing proper email security is the biggest enabler to cons, scams and the loss of wires.

The entire problem tracks back to email security and the lax standards of real estate professionals in protecting the communications with the clients, customers and other

YOU are the Weakest Link in the Chain



professionals involved in the transaction. Real estate professionals are by far the weakest link. The Dodd Frank Act and the requirements of TRID (TILA RESPA Integrated Disclosure) Rules from Congress and the Consumer Financial Protection Bureau (CFPB) forced lenders and closing agents, such as attorneys, to employ safeguards and security

protocols in the handling of consumer financial information. Those rules were never applied to real estate professionals. Accordingly, nearly all of the wire fraud cases get tracked back to a breach of the emails that were being used by the real estate professional.

Student Notes

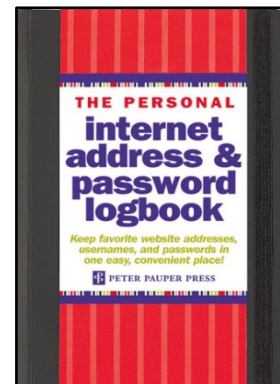


TEN BEST PRACTICES FOR EMAIL SECURITY

1. Use Strong & Unique Passwords

Everything we discussed earlier in this course about passwords applies twice as much to the passwords you utilize to access your email. Email account passwords should:

- Use 8-14 characters
- Include #'s and symbols
- Employ unpredictable capitalization
- Omit your name
- Use multiple passwords
- Change them every 30-90 days
- Use a password generator



2. Use Multiple Email Accounts

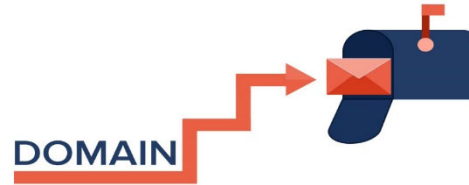
Nearly everything you do on the internet today requires an email address. No one would expect real estate agents to stop making hotel, flight or car reservations. No one expects agents to cease online shopping from retailers or Amazon. Keep your audible account. Use social media. Just stop providing such sites with the same email address you use to communicate with clients from which you exchange transactional information.

Establish multiple emails for various uses. Using Gmail and yahoo accounts is fine for a lot of applications with proper attention to the security issues we have discussed. Because they are such huge databases, they are a target for hackers. If your brokerage has an established domain for emails use that domain and ONLY use that email for business purposes and communicating with clients.



If your brokerage does not have an established firm domain email, then establishing your own domain for emails is inexpensive and simple. Not only does it add to your level of professionalism, but it provides less risk of hacking. There are several companies that can help you set up your own email domain:

- Godaddy.com
- Wordpress.com
- Wix.com
- Fitssmallbusiness.com



3. Get Off Public Wi-Fi

According to a recent study about 70% of people constantly connect to public Wi-Fi and have no hesitation or concerns about doing so. There are dozens of videos on YouTube with instructions of how to hack public Wi-Fi and gain access to other devices. Many of them have hundreds of thousands of views.



The most common method of attack is known as “Man in the Middle.” In this simple technique, traffic is intercepted between a user’s device and the destination by making the victim’s device think the hacker’s machine is the access point to the internet. A similar, albeit more sinister, method is called the “Evil Twin.” Here’s how it works: You log on to the free Wi-Fi in your hotel room, thinking you’re joining the hotel’s network. But somewhere nearby, a hacker is boosting a stronger Wi-Fi signal off of their laptop, tricking you into using it by labeling it with the hotel’s name. Trying to save a few bucks, and recognizing the name of the hotel, you innocently connect to the hacker’s network. As you surf the web or do your online banking, all your activity is being monitored by this stranger.

Some individuals claim they never log a laptop or tablet onto public Wi-Fi, just their phones. If you have access to your emails, text messages, accounts and documents on your phone, the same risks apply.

4. Get Proficient with Your Phone's Mobile Hotspot

Rather than connecting to public Wi-Fi most smartphones today have mobile hotspots or virtual private networks (VPN's). You can create a much more secure internet connection by connecting to your own portable network than by connecting to public Wi-Fi. Such services are easily accessible through the settings on your mobile device.

Although your carrier may charge you an additional fee for unlimited data and the speed that you require, such charges are always much cheaper than the ramifications of a security breach.



5. Use Two Factor Authentication

Email security experts strongly recommend two factor authentication for your accounts. It doesn't matter what type of account you have or the email program you are using, two factor authentication is easy to set up and utilize.

Essentially when you attempt to log into one of your accounts with your password a random temporary code is generated that requires you to enter that number or password before gaining access to the site. This additional process means that even if your password is hacked, cybercriminals are unable to use the password due to the added security.

Student Notes

6. Use Email Encryption

Today there are multiple programs that can encrypt email. Trusted vendors like Citrix and Barracuda offer a wide range of encryption software. Standard email programs like Microsoft 365 Outlook allow for emails to be encrypted without the installation of special software.

Within Outlook 365 under the Permissions button has now been replaced with an encryption option. There is a mistaken belief that so long as real estate professionals are not transmitting wire instructions, account numbers and sensitive information that the emails they send are innocuous and do not create a cybersecurity risk for their clients.

Student Notes

Can You Identify the Cybersecurity Risk in Each of the Following Seemingly Innocent Emails?

The screenshot shows an "Email Template" window in Outlook 365. The "TITLE" field is labeled "Required" and contains the text "Buyer". A black oval with white text "VALID & LEGITIMATE EMAIL" is overlaid on the "TITLE" field. The "SUB" field contains the text "Your Closing Disclosure". Below the fields is a rich text editor with the following content: "Valerie & Tom, Attached is a copy of your Closing Disclosure. When you have a few minutes please review it. If you have questions please call me so we can discuss. Your Buyer's Agent". A red arrow pointing right with the text "And THEN" is overlaid on the bottom right of the email body. At the bottom of the window, there is a "Add attachment" button, a yellow button labeled "PDF Buyer's Closing Disclosure", and "Cancel" and "Save" buttons.

Email Template

TITLE

Seller

Required

SUB

Congratulations You Have a Contract For Sale

B

I

U

¶

•

A

T

↶

↷

📎

🗑️

☰

☷

☰

☷

↺

↻

<>

Doug & Mary,

CONGRATULATIONS! Based on your acceptance of the buyer's offer, your home is now under contract. I am attaching a copy of the fully executed Purchase Contract for your records.

Your Listing Agent

And THEN

📎 Add attachment

PDF Purchase Contract

Cancel

Save

Email Template

VALID & LEGITIMATE EMAIL

TITLE *

Seller

Required

SUB

Congratulations You Have a Contract For Sale

B I U A T

Shawna,
CONGRATULATIONS! As I discussed with you the seller accepted your offer and you are on your way to owning a new home. I have delivered the due diligence check you wrote to the seller. Please make arrangements to pay the \$5,000 earnest money to the trust account of Sam Walker, Attorney at Walker & Reed, 125 N. Main Street.

Your Buyer's Agent

And THEN

Add attachment

PDF Copy of DDF Check

Cancel

Save

Email Template

TITLE * **Seller** Required

SUB **Congratulations**

VALID & LEGITIMATE EMAIL

B I U **A T**

Melissa,
 The closing attorney contacted me and the Deed has been recorded. Your check is ready to pick up at the attorney's office.
 Please make arrangements to do so with Sam Walker, Attorney at Walker & Reed, 125 N. Main Street.
 Your Listing Agent

And THEN

Add attachment

Cancel Save

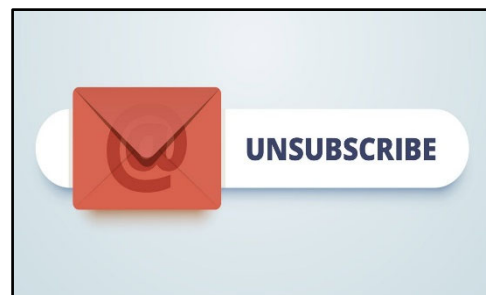
7. Beware the Phish

Because the most common way that data and devices get compromised is with some type of phishing virus, know the warning signs of phishing emails. These scams are the best reasons why all your devices should have an anti-malware, anti-virus program installed on them.

8. Trade Unsubscribe for Spam Filters

The Federal CAN SPAM Act requires that mass emails contain an unsubscribe link. Now criminals are sending out unsolicited emails where the unsubscribe link contains a virus or malware. Here are some reasons why choosing “unsubscribe” may not be the best thing to do:

- By responding to the email, you have positively confirmed that your email address is correct and that it belongs to an actual live person.
- If your response goes back via email your email contained meta data identifying your email software and other functions of the program you are using
- If your response opened a separate browser bar you may be giving away even more about yourself through the activation of cookies
- Your response may have routed you through the website of a scammer and now malware, adware and spyware have been installed on your device



Instead consider setting or adjusting the spam filters on your email. Occasionally you should just delete the unwanted emails in bulk by deleting all contents of your spam folder.

9. Don't Use Business Emails for Social Media

10. Don't Open Attachments Without Verification

Student Notes

MODULE 4 NORTH CAROLINA CASE STUDIES



Module 4 North Carolina Case Studies

NC Ranks in the Top 5 States for Cybercrime Losses

TOP 10 STATES BY VICTIM LOSS¹⁷



**According to
the FBI,
North
Carolina
residents
lost \$137
Million in
2018**

By the Numbers

According to the Consumer Sentinel Network maintained by the FTC not only does North Carolina rank in the top 5 states for cybercrime, it also ranks 15th for identity theft and 16th for fraud. Identity theft alone was responsible for 32% of all theft types with credit card fraud making up another 31% of theft losses.

Although the median loss per reported incident is only \$324, the total lost annually is nearly \$30 million. In NC alone, over 11,481 people have reported having their identity stolen.



A Lesson in Stolen Wires & Hold Harmless Hurdles

It was late November 2016, and **Jon and Dorothy Little** were all set to close on a \$200,000 home in Hendersonville, North Carolina. Just prior to the closing date on Dec. 2 their realtor sent an email to the Little's and to the law firm handling the closing, asking the settlement firm for instructions on wiring the money to an escrow account.

It appeared that the attorney with the closing firm responded with wiring instructions as requested, attaching a document that had the law firm's logo and some bank account information that was represented as the seller's account number. The Little's realtor sent the wire on Thursday morning, the day before settlement.

"We went to closing at 1 p.m. on Friday, and after we signed all the papers, we asked the lawyers if we were going to get back the extra money we had sent them, because they hadn't be able to give us an exact amount in the wiring instructions. At that point they told us they had never gotten the money."

After some disagreement, both legitimate parties to the transaction agreed that someone's email had been hacked by the fraudsters and was used to divert the wired funds to an account the criminals controlled. The hackers had forged a copy of the law firm's letterhead, and beneath it placed their own Bank of America account information.

The owner of the Bank of America account appears to have been a willing or unwitting accomplice — also known as a “money mule” — recruited through work-at-home job schemes to receive and forward funds stolen from hacked business accounts. In this case, the money mule wired all but 10 percent of the money (a typical money mule commission) to an account at TD Bank.

MONEY MULING



Fortunately for the Littles, the FBI succeeded in having the resulting \$180,000 wire transfer frozen once it hit the TD Bank account. However, efforts to recover the stolen funds were stymied immediately when the Littles' credit union refused to give Bank of America a so-called “hold harmless” agreement that the bigger bank wanted as a legal guarantee before agreeing to help.

Charisse Castagnoli, an adjunct professor of law at the **John Marshall Law School**, said banks have a fiduciary duty to their customers to honor their requests in good faith, and as such they tend to be very nervous legally about colluding with another bank to reverse payment instructions by one of their own customers. The “hold harmless” agreement is usually sought by the bank which received a fraudulent wire transfer, Castagnoli said, and it requires the responding bank to assume any and all liability for costs that the requesting bank may later incur should the owner of account which received the fraudulent wire decide to dispute the payment reversal.

“When it comes to wire fraud cases the banks have to move very quickly because once the wires make it outside the U.S. to foreign banks, the money is usually as good

as gone,” Castagnoli said. “The receiver or transferee usually insists on a hold harmless agreement because they’re moving the money on behalf of their own account holder, kind of going against their own client which is a big ‘no-no’ when you’re a fiduciary.”

But in this case, the credit union in which the Littles had invested virtually all of their money for more than 40 years decided it could not in good faith provide that hold harmless agreement, because doing so would stipulate that the credit union affirms the victim (the Littles) hadn’t willingly and knowing initiated the wire, when in fact they had.

“I talked to the wire dept multiple times,” Mr. Little said of the folks at his financial institution, Atlanta, Ga.-based **Delta Community Credit Union (DCCU)**. “They finally put me through to the vice president of loss prevention at the credit union. I’m not sure they even believed all that was going on. They finally came back and told me they couldn’t do it. Their rules would not allow them to send a hold harmless letter because I had asked them to do something and they had done it. They had a big meeting last week with apparently the CEO of the credit union and several other people. Then they called me on Monday again and told me they would not could not do it.”

The Littles had to cancel the contract on the house they were prepared to occupy in December. Most of their cash was tied up in this account that the banks were haggling over, and so they opted to get a heavily mortgaged small townhome instead, with the intention of paying off the mortgage when their stolen funds are returned.

“We canceled the contract on the house because the sellers really needed to sell it,” Jon Little said. Eventually the bank informed the Littles that the other bank would soon have its hold harmless letter — freeing up their \$180,000 after more than four months in legal limbo.

The Littles’ story has a fairly happy ending, however most of the other few dozen stories previously featured on this blog about wayward mortgage, escrow and payroll payments wound up with the victim losing six figures at least.

Student Notes

North Carolina State Bar Formal Ethics Opinions on Funds Stolen by 3rd Parties



The North Carolina State Bar has been asked to provide a formal ethics opinion on the liability of attorneys when a third-party steals funds from the lawyer's trust account. When presented with a scenario of an attorney involved in real estate closing where information was hacked (other than the attorney's which resulted in the loss of wired funds, here was the opinion of the NC State Bar:

Inquiry #5:

Lawyer is retained to close a real estate transaction. Prior to the closing, Lawyer obtains information relevant to the closing, including the seller's name and mailing address. Lawyer also receives into his trust account the funds necessary for the closing. Lawyer's normal practice after the closing is to record the deed and disburse the funds. Lawyer then mails a trust account check to the seller in the amount of the seller proceeds.

Hacker gains access to information relating to the real estate transaction by hacking the email of one of the parties (lawyer, realtor, or seller). Hacker then creates a "spoof" email address that is similar to realtor's or seller's email address (only one letter is different). Hacker emails Lawyer with disbursement instructions directing Lawyer to wire funds to the account identified in the email instead of mailing a check to seller at the address included in Lawyer's file as previously instructed.² Lawyer follows the instructions in the email without first implementing security measures such as contacting the seller by phone at the phone number included in Lawyer's file to confirm the wiring instructions. After the closing and disbursement, the true seller calls Lawyer and demands his funds. Lawyer goes to Bank to request reversal of the wire. Bank refuses to reverse the wire and will not cooperate or communicate with Lawyer without a subpoena.

While pursuing other legal remedies, does Lawyer have a professional responsibility to replace the stolen funds?

Opinion #5:

Yes. Lawyers must use reasonable care to prevent third parties from gaining access to client funds held in the trust account. A lawyer has a duty to implement reasonable security measures. Lawyer did not verify the disbursement change by calling seller at the phone number listed in Lawyer's file or confirming seller's email address. These were reasonable security measures that, if implemented, could have prevented the theft. Lawyer is, therefore, professionally responsible and must replace the funds stolen by Hacker. If it is later determined that Bank is legally responsible, or insurance covers the stolen funds, Lawyer may be reimbursed.

Student Notes



The Surprise Liens

A resident of the Dilworth neighborhood near Freedom Park in Charlotte was in the process of refinancing her home. During that process she was notified of a \$500,000 lien that had been placed against her home of which she had no knowledge.

Upon talking with other homeowners, she discovered that nine other homes in the area had received letters from the Cherokee Nation of Moors who called Charlotte the "Imperial City" saying that the aboriginal moors have been resurrected and that the homes were located on their land. The letter demanded a "sovereign soil tax" of \$500,000.

Although attorneys have called the letters and the liens "bogus" the homeowners will have to file and pursue a quiet title action in order to remove the liens from their property.

The Dilworth incident is presented here because a lot of real estate fraud may involve placing liens of which the homeowner has no notice on properties. It occurs a lot in refinance and mortgage fraud. Eventually the issue has to be confronted before a property can be sold or refinanced. Such instances lead to a good discussion.



1. Should homeowners be advised to regularly check their property for liens?

2. How often?

3. What is the process of doing that in your area?

Craigslist Rental Scandal Hits Raleigh Area

Wesley Diggers thought he had found the deal of the century. Homes in the River Ridge subdivision in southwest Raleigh rent for around \$1,500 a month. A couple agreed to rent a home they found on Craigslist for \$900 a month, including utilities. Diggers wired the man he thought was the landlord \$1,800 and began to move.

Although Diggers never met the man whom he thought was the landlord, when Diggers entered the code into the lockbox, he was able to get the key. He never suspected a thing.



After calling the number on the sign in the front yard belonging to American Homes for Rent, Diggers discovered that they were the legal owners of the home, had no knowledge of who he was and never received money from him.

Student Notes

The Role & Responsibility of NC Real Estate Licensees

Protecting clients from internet cons, scams and particularly the loss of wired money is an important issue for North Carolina real estate licensees. Not only do such breaches create financial hardship and often result in civil litigation for the parties and entities involved, such actions can lead to NCREC disciplinary actions.

The language of General Statutes 93A-6(a)(8) and (10) provide that a licensee can face disciplinary action for:

- Unworthiness and incompetence, as well as
- Any other conduct which constitutes improper, fraudulent or dishonest dealing

When consumers begin to lack faith in the real estate profession and the individuals to whom they have entrusted their most valuable asset, everyone loses. Now more than ever, real estate professionals must step up and work together to protect and promote the interests of consumers.



Student Notes