CLASS BREAKDOWN

1) **Hacking & Scams Terms**
2) **Common Real Estate Scams**
3) **Best Practices**
4) **What To Do When Information Is Compromised**

There is a plethora of risks that making a career out of real estate entails. As a real estate professional, you need to not only make sure that your property is protected, but you also need to worry about interactions with clients, employees, tenants, investors, and a variety of other parties involved in your operations.

Cyber security statistics show that nearly every industry is being affected by cyber-attacks, and real estate is no exception. Property managers store sensitive client, customer, and tenant information such as Social Security numbers, credit card numbers, and more, making them a vulnerable target for data breaches. Real Estate deals with large sums of money with several individuals involved.

These attacks don't always have to be spearheaded by hackers and can be the result of social engineering in which employees were tricked into delivering sensitive information to hackers or a member of staff participating in criminal activity that results in severe financial losses for your organization. In fact, recent reports showed that insiders provide the information needed for 37% of data attacks in real estate.

We will go over common ways information is compromised, how to know how and why it happened, and how to reduce your risk by using the best computer practices for your business.

Hacking & Scam Terms (Hacking)

Hackers are criminals who gain unauthorized access to a network and devices, usually with the intent to steal sensitive data, such as financial information or company secrets. The growth of the Internet introduced new possibilities and spawned new industries, but also new downsides.

Tons of spam started to infiltrate email accounts, and computer viruses wreaked havoc on business networks. A new threat known as computer hacking extended the definition of thievery to include infiltrating your computer, stealing personal information, tricking you into revealing private data, and using that data to steal and extort personal information, such as business secrets, bank account credentials and even people's identities.

Hackers are people who break into internet-connected devices such as computers, tablets, and smartphones, usually with the intent to steal, change or delete information. Just as other thieves have malicious intent, hackers usually find their way into devices for negative purposes, however, one exception is “white hat hackers”, whom companies hire to break into their devices to find security flaws that need to be fixed.

Hackers may want to steal, alter, or delete information in your devices, and they often do so by installing malware (software used for malicious purposes) you might not even know is there. These thieves might get access to your most precious data before you're aware of a break-in.

Key takeaway: Hackers are interested in gaining unauthorized access to your devices to steal sensitive data and variety of motivations, ranging from financial gain to political goals. Awareness of these intentions can help you anticipate attacks that could affect your small business.

Hacking & Scam Terms (Hacking)

MALWARE

Malware is an umbrella term for any type of “malicious software” that’s designed to infiltrate your device without your knowledge. There are many types of malware, and each works differently in pursuit of its goals. Adware, spyware, Trojans, ransomware, and other programs all fall under the definition of malware. Malware isn’t just a threat to PC – Macs and mobile devices can also be targeted.

Most malware infections occur when you inadvertently perform an action that causes the malware to be downloaded. This action might be clicking a link in an email, visiting a malicious website, or free software download bundles. Mobile devices can also be infected via clicking links in text messages.

Once the malware has been installed, it infects your device and begins working towards the hackers’ goals. What separates the various types of malware from each other is how they go about doing this. You need may ask the advice of a security/IT specialist before trying anything to remedy malware or viruses.

ADWARE

Adware’s job is to create revenue for the developer by subjecting the victim to unwanted advertisements. Common types of adware include free games or browser toolbars. They collect personal data about the victim, then use it to personalize the ads they display.

Most adware is legally installed. Individuals are at greater risk of contracting adware than businesses and can be contracted on almost any device. Less-savvy internet users are generally at the most risk, as they’re the most likely to fall for common hacker tricks like offers that are too good to be true.

Hacking & Scam Terms (Hacking)

BROWSER HIJACKING

Browser hijacking occurs when unwanted software on an internet browser alters the activity of the browser. Internet browsers serve as the "window" to the internet, and people use them to search for information and either view it or interact with it. This often changes the home or start page when the browser is turned on.

Sometimes hackers drop malware into browsers to take users to websites used to capture critical information about them. The data could include user IDs, passwords, full names, addresses, social security numbers, and even answers to security questions — mother's maiden name, etc. Cybercriminals then use the information to access accounts that users log in to on the internet. In some instances, they can obtain financial data and steal a user's money or identity.

JUICE JACKING

With most mobile devices power supply and the data stream pass through the same cable. When your phone connects to another device, it pairs to that device and the devices can share information. During the charging process, the USB cord opens a pathway into your device that a cybercriminal may be able to exploit by copying your phone data and transfer it back to their own device. Other malware may help them gather data such as your GPS location, purchases, social media interactions, photos, and call logs.

While juice jacking is a real security threat, there is little evidence that it has become a widespread problem. Apple and Google have also added safety features to iOS and Android operating systems to help prevent juice jacking.

Hacking & Scam Terms (Hacking)

RANSOMWARE

Ransomware (typically activated by the victim clicking a link or opening an attachment) encrypts your files or data so you can't access them, you'll then see a message demanding a ransom payment to restore what they took. The number one rule is to never pay the ransom. This is now advice endorsed by the FBI. All that does is encourage cybercriminals to launch additional attacks against either you or someone else.

One potential option for removing ransomware is that you may be able to retrieve some encrypted files by using decryptors. To be clear: not all ransomware have had decryptors created for them. And even if there is a decryptor, it's not always clear if it's for right version of the malware. Another way to deal with a ransomware infection include downloading a security product known for remediation. You may not get your files back and for screen locking ransomware, a full system restore might be in order.

SCAREWARE

Scareware, as it turns out, is not that scary. It includes rogue security software and tech support scams. Scareware is a type of malware that leverages pop-up ads, fake websites, and social engineering tactics to manipulate online users into believing they need to buy or download software that's useless or malicious.

Encouraging users to act fast to address an alleged cybersecurity problem. As the name suggests, it scares users into handing over their confidential data to what they believe is a legitimate solution to their cybersecurity problem. The consequence of scareware can vary and includes credit card fraud or identity theft.

Hacking & Scam Terms (Hacking)

SPYWARE

Spyware, once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

Spyware can also be used to track a person's location and track the physical location of the victim, intercept their emails and texts, eavesdrop on their phone calls and record conversations, and access personal data, such as photos and videos.

Spyware can be difficult to detect; often, the first indication a user has that a computing device has been infected with spyware is a noticeable reduction in processor or network connection speeds. In the case of mobile devices, data usage and battery life.

TROJAN HORSE

A Trojan presents itself as legitimate software but hidden beneath its seemingly harmless exterior are malicious codes that can damage your devices. It makes up approximately half of all malware.

Most Trojan attacks start with tricking the user into downloading, installing, and executing the malware. A hacker might attach a Trojan installer to an email while employing social engineering to get you to open the attachment. If you do, your device will download and install the Trojan.

Hacking & Scam Terms (Scam)

Real estate is a common target for criminals due to the large sums of money involved in transactions as well as the sharing of sensitive information among multiple parties. Employing traditional scam techniques with technology to reach their targets.

Real estate is the third most common sector for fraud attempts behind construction and commercial services. Housing scams are prevalent across all aspects of the housing industry, with criminals targeting buyers, sellers, renter, owners, agents & brokerages.

Real estate transactions revolve around email and digital document transfer, which makes them vulnerable to cyberattacks. The FBI announced in its 2020 Internet Crime Report that complaints resulted in over $1.8 billion in losses in 2020 alone. With much money moving through unsecured channels agents not only need to be informed but keep their clients informed as well.

Key takeaway: Despite growing awareness around cybercrime, it continues to be a threat in the real estate industry. Being aware of common forms of fraud is an important step in avoiding scams.

Hacking & Scam Terms (Scam)

SOCIAL ENGINEERING

Social engineering refers to the manipulation of a target so that they give up key information to steal an individual's identity or compromising a credit card or bank account. Social engineering can be applied to obtain a company's trade secrets or exploit national security. Social engineering is illegal and can happen to an individual online or in person. There are many forms of social engineering attacks, but the most common is phishing.

For example, attackers might call a victim's bank, pretending to be the victim's spouse, claiming an emergency, to request access to the account. If the attacker can successfully socially engineer the bank's customer service by appealing to the representative's empathetic tendency, they may succeed in obtaining access to the victim's account and stealing the victim's money.

Similarly, an attacker might contact an email provider's customer service department to obtain a password reset, making it possible for the attacker to control a target's email account rather than hacking into that account.

Individuals can decrease their risk by avoiding giving out confidential information, being cautious when sharing information on social media, and not repeating passwords to your accounts. Additional ways to decrease hacking are using two-factor authentication, using fake or difficult-to-guess answers to account security questions, and keeping a close eye on financial accounts.

Attackers use surprisingly simple tactics in social engineering schemes, such as asking people for help or exploit victims by asking them to provide personally identifiable information such as maiden names, addresses, dates of birth, and social security numbers for missing or deceased loved ones because these pieces of information can later be used for identity theft.

Hacking & Scam Terms (Scam)

CATFISHING

When people intentionally misrepresent themselves online, adopting a fake identity or spinning stories about a past, they are, in colloquial terms "catfishing." Catfishing relationships typically remain online, with one person believing it is legitimate, and the other knowing it is not.

Catfishing involves throwing out the bait like attractive photos or words that suggest sincere interest and then stringing the victim along for a bit before escalating to requests for money or personal information. Not all catfishing involves financial scams, but when it does, catfishing can mislead individuals to think they are in a legitimate relationship to the point where they want to send money or help.

IDENTITY THEFT

Identity theft occurs when someone uses your identity in a crime or fraudulent act. Unlike a robbery or burglary, identity theft often occurs without the victim's knowledge. Most identity theft victims only find out after they see strange charges on their credit card statements or when they apply for a loan. While prevention is always the best policy, sometimes personal information is exposed through security breaches at banks or companies with which the victims do business.

Identity theft can happen even to well-prepared consumers and can happen to anyone, there are some things you can do to reduce your risk. If you think someone is using your personal information to open accounts, file taxes, or make purchases, visit www.IdentityTheft.gov to report the identity theft.

Hacking & Scam Terms (Scam)

PHISHING (EMAIL) / SMISHING (TEXT)

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Most phishing messages are delivered by email and are not personalized or targeted to a specific individual or company.

The content of a bulk phishing message varies widely depending on the goal of the attacker–common targets for impersonation include banks and financial services, email and cloud productivity providers, and streaming services.

To identify a scam email, double-check the email address it's coming from, you may find that the actual email address is suspicious. Most services will never ask for sensitive information via email, text message, or phone. If you receive an email or text that seems legitimate, but you're just not sure, contact them directly to check. Find the phone number from a source other than the email.

SPOOFING

Spoofing is when someone or something pretends to be something else to gain confidence, get access to systems, steal data, steal money, or spread malware.

Cybercriminals invoke the name of a big, trusted organization is enough to get victims to give up information or act. A spoofed email from PayPal or Amazon might inquire about purchases you never made. Concerned about their account, a victim might be motivated to click malicious links to a web page with a malware download or a faked login page.

Common Real Estate Scams

WIRE TRANSFER FRAUD

A common form of cybercrime is real estate wire fraud. This form of fraud often targets homebuyers as they navigate the process of buying a home. By hacking into email and other forms of communication, criminals can gain access to bank accounts, social security numbers, and other sensitive information. With this information, criminals can intercept transactions and steal hundreds of thousands of dollars from your clients.

HOME TITLE THEFT

Home title theft, also known as deed theft, deed fraud, or house stealing, occurs when the title to a property is obtained illegally without an owner's consent. Title theft often occurs at critical stages of sales and refinance transactions, where funds and sensitive information are passed between parties. Thieves often acquire the information they need to execute a title theft by assuming the identity of a real estate professional or third party. Deed theft recently made headlines in New York where a Long Island man forged deeds and falsified documents to acquire two properties in Harlem. Victims of home title theft are encouraged to report cases to the Federal Trade Commission (FTC).

MORTGAGE FRAUD SCAMS

Homebuying can be an intimidating and expensive process, so homebuyers may be misled by "no strings attached" loans. This type of mortgage scam may promise a loan with low interest rates or no closing costs. Once the loan is finalized, the new homeowner may discover higher interest rates and undisclosed fees. Avoiding these scams starts with working with reputable lenders and encouraging clients to carefully review their closing documents. Using a secure closing portal allows you to share documents and communicate with clients to help them understand all aspects of the closing process.

Common Real Estate Scams

FORECLOSURE RELIEF

Homeowners may fall behind on mortgage payments and risk losing their home. In this situation, scammers may offer foreclosure relief to homeowners desperate to save their property. Unfortunately, foreclosure relief scams have become more prevalent during the pandemic; targeting homeowners who may have lost their jobs. If financial challenges are preventing a borrower from fulfilling mortgage payments, encourage them to talk with their lender to identify options for modifying loans, requesting forbearance, or other solutions.

RENTAL SCAMS

According to research conducted by Apartment List, 5.2 million U.S. renters have lost money from rental fraud. Renters may experience a variety of scams, which can lead to different levels of financial loss. A common rental scam involves fake rental advertisements. In this case, a scammer creates an ad for an apartment and attempts to collect a deposit or lease payment from a potential tenant. The FTC warns that any payment requests—especially via wire transfer or cash—prior to meeting a landlord or signing a lease are red flags for rental scams. In other scenarios, scammers may lie about amenities to increase the rent.

MOVING SCAMS

Real estate scams don’t end when a homeowner receives the keys to their new home. Moving can provide additional opportunities for scams. Moving scams tend to fall into two categories: (1) companies that overcharge with undisclosed fees and (2) companies that accept a deposit and then disappear without a trace (with or without the mover’s belongings!). To avoid moving scams, the Federal Motor Carrier Safety Administration (FMCSA) recommends getting at least three quotes from potential companies and researching each company to ensure that they’re a reputable business. The FMCSA also warns that moving companies that request cash or large deposits are usually red flags for fraud.

Best Practices

They say an ounce of prevention is worth a pound of cure. Stay informed and keep others informed. There are many people involved in the real estate transaction process. Not only to you need to stay safe but help other stay safe. There are numerous scams that go out through mail, email, text, and phone calls with new scams being invented every year.

No matter how informed you are, not everyone involved in your business will be. You must consider all your coworkers, employees, and customers could do something that opens your business up to an attack or compromise of information.

We are going to employ a Takedown List. This technique has two advantages. First, it adds layers of protections with each thing you do. The more layers of protection you have the better. Second, if the worst would happen, you can show that you have done everything possible to prevent it. The following list of things to do, or not do, will be your takedown list.

Best Practices

TECHNOLOGY

Learn your devices. Google Tutorials / Classes at CSN

Install security software before you get hit with malware or viruses.

Back up your important data (files, documents, photos, videos, etc.)

Keep your operating systems and programs up to date.

Do not use the same password for multiple accounts.

Consider using a secure password manager.

Consider using a VPN (Virtual Private Network).

Use two-factor authentication whenever it is available.

Don’t use free email services (see helpful links). Ruthie recommends Outlook.

Use separate emails for business and personal use. Maybe even have another email just for throw away services.

Have a dedicated phone number for business. See Voice-over-internet-protocol (VoIP) Providers.

Don’t click on links in emails and texts from unknown senders.

Question all attachments, no matter who sends them to you.

Avoid doing business over public, unsecured Wi-Fi.

Be wary of using public devices and know who uses your devices.

Never download paid apps / programs for “FREE.”

Consider using different devices for business and personal.

Don’t use your or family names or important dates in any passwords.

Key takeaway: You don’t have to know how it works, but you must know how to find out how it works.

Best Practices

SOCIAL MEDIA

Be careful of who you friend or friend only people you know.

On Facebook, use lists to determine who see what you post.

Don't share private information on social media.

Don't participate in social media "quizzes" or "tests." They are data mining your personal information.

FINANCE

Read your credit card and bank statements weekly.

Never give your credit card number over the phone, unless you made the call and trust the business or person.

Never pay anything with Gift Cards. This is 100% always a scam.

Report suspicious transactions to your credit card company or bank.

Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries.

Shred any documents with personal or financial information on them.

BUSNIESS

Have business insurance that covers cybercrimes and hacking threats.

Use a transaction management platform, or a document-sharing program to share sensitive information.

Double check with your people (Broker / Lawyer / The Division / Tech Support).

Hire a technology professional for when assistance is needed.

Key takeaway: If you don't know, ask someone. Then ask two more people.

Best Practices

HELPFUL RESOURCES

All Links Found At: www.LasVegasAgentFormula.com/risk

Anti-Malware: https://www.malwarebytes.com/

Anti-Virus: https://www.avg.com/

Cyber Security Basics: https://www.malwarebytes.com/cybersecurity

Cyber Security Insurance: https://get.cyberpolicy.com/nar/ or https://cyberpolicy.com/

Facebook Lists: https://www.facebook.com/help/204604196335128

Fight Fraud Task Force: https://consumeraffairs.nv.gov/

Free Basic Computer Classes: https://www.northwestcareercollege.edu/basic-computer-classes.html

Internet Crime Complaint Center: https://www.ic3.gov/

Password Manager: https://www.cnet.com/tech/services-and-software/best-password-manager/

Scam Glossary: https://www.fcc.gov/scam-glossary

Secure Email: https://cybernews.com/secure-email-providers/

Virtual Private Network (VPN): https://www.cnet.com/tech/services-and-software/best-vpn/

Voice-over-internet-protocol (VoIP) Provider: https://www.techradar.com/news/best-voip-service

Great Information Source: https://www.ic3.gov/

What To Do When Information Is Compromised

If you don't know someone, find someone. Best to do this before you ever have a problem. As a business owner you need to hire someone to fall back on for when something happens.

DON'T PANIC. Panicking will lead to a greater mistake or consequence.

Stop using that device. Consult your technology professional.

If possible, run all anti-virus and anti-malware programs installed on your device.

As a last resort, take a picture of the screen with your phone then turn your computer off. This could be risky, but it will stop the computer from doing anything while you contact a professional to assist with your problem.

On another device change all your passwords. No Exceptions. If one password, security question or pin number is compromised, assume they all are.

If you think a virus has emailed your contact list, contact everyone in the list to warn them previous emails they got from you may be viruses.

What To Do When Information Is Compromised

REPORT CRIMES

If you think you need to involved Law enforcement…

Report a fraud or scam with the Fight Fraud Task Force (https://consumeraffairs.nv.gov/) or call the Better Business Bureau at 775.322.0657 or 702.320.4500.

If you are victim of Identity Theft, contact the police department in either the county of your residence or county in which the crime occurred to report the crime. If you fall victim to Identity Theft while using the Internet, you should file a report with the Internet Crime Complaint Center (https://www.ic3.gov/).

You can report a cybercrime to the Las Vegas Cyber Crime Task Force

https://www.lvmpd.com/en-us/cybercrime/Pages/default.aspx

More Info at https://ag.nv.gov/Hot_Topics/Victims/Report/