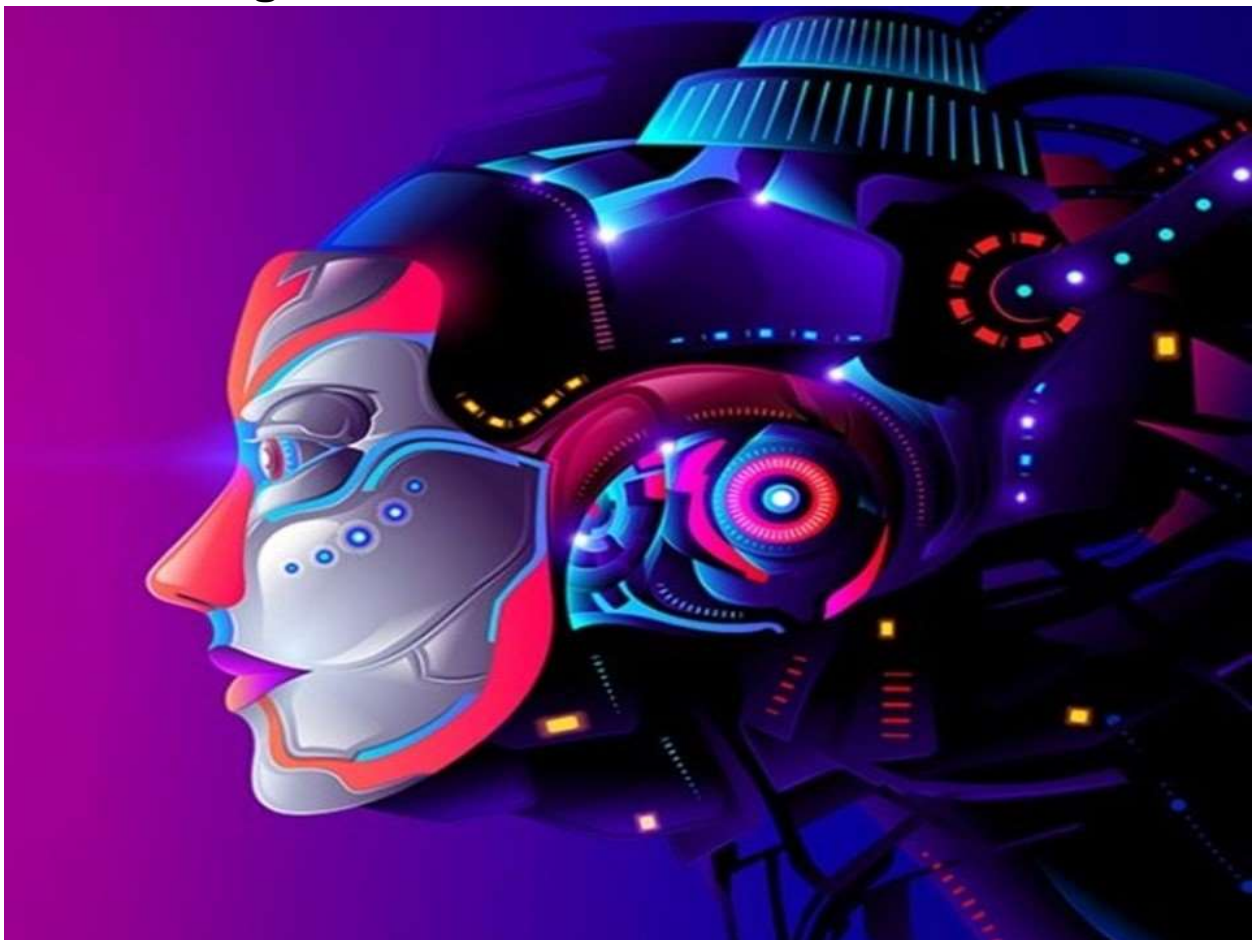




Presents

Cons, Scams & Hacks

Protecting Real Estate Clients in an Internet World



Written by: Brian Pate
In Person Course Number:
Synchronous Course Number:

Copyright 2023 Brian Pate Seminars

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.

Commission Rule 58A .1705: Attendance & Participation Requirements

(a) In order to receive credit for completing an approved continuing education course, a broker shall:

- (1) attend at least 90 percent of the scheduled instructional hours for the course;
- (2) provide his or her legal name and license number to the course sponsor;
- (3) present his or her pocket card or photo identification card, if necessary; and
- (4) personally perform all work required to complete the course.

(b) With the instructor or the sponsor's permission, a 10 percent absence allowance may be permitted at any time during the course, except that it may not be used to skip the last 10 percent of the course unless the absence is:

- (1) approved by the instructor; and
- (2) for circumstances beyond the broker's control that could not have been reasonably foreseen by the broker, such as:
 - (A) an illness;
 - (B) a family emergency; or
 - (C) acts of God.

Comments and complaints about the course, education provider, or instructor may be directed in writing to:

North Carolina Real Estate Commission

Education and Licensing Division

P.O. Box 17100

Raleigh, NC 27619-7100

Email address: educ@ncrec.gov

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.**

You may check your **current year's** CE credits online at the Commission's website <https://www.ncrec.gov/>. 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 the 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 the 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.

About The Author

Brian Pate – Realtor®, Real Estate Instructor

Email: brian@paterealty.com

Phone: 919-669-4575

Brian Pate has been a well-respected real estate professional for 30 years. During his time in the business, he has served as an agent, manager, instructor, coach and trainer for over 20,000 real estate students. In addition, the teams he has managed and coached have produced over \$2 billion in real estate sales under his leadership.



Since 1993, Brian Pate has been an integral part of the real estate scene in central North Carolina. Based in Wake Forest for over 25 years, he has seen massive growth in the area and experienced three recessions, as well as rate fluctuations from 16%, down to less than 3% and back up to 7%. He also continued to sell real estate and teach during the Covid-19 pandemic from March of 2020 through 2022 as lock down and masking orders were eliminated.

His early days of real estate sales began on August 2, 1993 when he joined Fonville Morisey, at the time the #1 independent real estate firm in the Triangle region, and one of the top 50 independent real estate companies in the United States.

Other than a 2.5-year stint at Coldwell Banker, Pate was with Fonville Morisey from 1993-2012 when he left management to get back into sales. In 2012, he established Brian Pate Seminars to continue teaching in addition to selling real estate. In 2014, he set a goal to create one of the top 100 teams in the Triangle Multiple Listing Service (TMLS) within 5 years. In 2017 and 2018, that goal was reached with the help of some fantastic teammates that averaged over \$35 million per year in real estate sales. Also, during those two years, Brian taught over 5,000 students in real estate classes and began coaching other agents to help grow their business.

Brian served two stints as CEO/Team Leader at Keller Williams Preferred in Raleigh, NC with over 350 agents and during that time, the office became the #1 listing office in the Triangle MLS.

Today, Brian continues to sell real estate as an independent broker with Pate Realty Group, write classes and teach on a regular basis. He also runs a coaching program for new, experienced and top producing agents in addition to teaching regulatory and training classes.

He lives in Wake Forest, North Carolina with his wife Kirke. Together they have four children between the ages of 19 and 24. They also have three dogs; a coonhound, a black lab and a yellow lab. They love to travel and have a slight obsession with baseball, with a goal of seeing a game at every Major League Baseball stadium in the next 10 years. Kirke and Brian also love to shag dance and spend their non-baseball weekends practicing their steps.



Why This Course Was Written

Cybersecurity is paramount for real estate licensees in this day and age as scammers and hackers are everywhere. With over \$10.3 billion in losses in 2022 (the most recent data available), cybersecurity needs improvement.



As Kevin Mitnick, the world's most famous hacker says, "Companies spend millions of dollars on firewalls, encryption and secure access devices, and it is all wasted money. None of these measures address the weakest link in the security chain... people."

This course was written to address that weak link, people. Throughout this course, students will be put through exercises that teach them how to avoid pitfalls of cybersecurity.

By the end of this class, students will be able to:

1. Identify the top 10 cyber risks and how to defend against them.
2. Differentiate between safe and dangerous emails.
3. Explain why real estate is such a high value target for hackers.
4. Define the top 5 real estate scams and how to defend against them.
5. Navigate artificial intelligence safely and to provide value to consumers.
6. Discover ways to safely navigate new technologies.

Student Notes

Where Are We Going Today?

Segment 1- Statistics and Top 10 Cyber Security Threats in 2023

Internet Crime Statistics	8
IC3 Recover Team/Steps to Take When Wire Fraud Occurs	11
Top 10 Security Threats	12

Segment 2- Real Estate Scams/Prevention

Busting Myths	14
Top 5 Common Real Estate Scams	15
Prevention	19

Segment 3- Artificial Intelligence

What is Artificial Intelligence?	19
Deepfakes	24
Digital Impersonation and How to Protect Online Accounts	25
OpenAI Chat GPT	27
OpenAI Examples	32

Segment 4- Other Issues/New Technology

Does Privacy Exist?	39
Email Security- The Weakest Link	40
Burner Email Accounts	42
Get Off Public WiFi	42
Mobile Hotspot/Avoid Public Computers	43
Secure vs Encrypted Email	44

Segment 1:

Statistics and Cybersecurity Threats

Learning Objectives

By the end of this section, attendees will be able to:

- 1. Identify the top 10 cybersecurity threats.**
 - 2. Explain how the risks translate to the real estate business.**
 - 3. Explore ways to protect consumers before, during and after the transaction.**
-

Some of the biggest names in industry were hacked in 2022. Big names including CashApp, Twitter and Uber, just to name a few. With more than 142 million people affected by those three, you would think people and corporations would focus more on preventing hacks. [PPT Slide 8](#)

Yet Meta (parent company of Facebook), agreed to settle a lawsuit in 2022 that alleged they illegally shared data for political purposes back in 2016 during the presidential election. You have likely heard of the Cambridge Analytica fiasco that was front and center for over two years after the election. [PPT Slide 9](#)

Victims of cybercrime lost over \$10.3 BILLION in 2022 alone and the number is expected to continue growing. Over the last five years, the Federal Trade Commission has received an average of 651,800 complaints annually. That doesn't even count the folks who are too embarrassed to admit they were scammed in one way or another. [PPT Slide 10](#)

Each year, the Federal Trade Commission (FTC) gathers data from consumers in order to publish the *Consumer Sentinel Network DataBook*. The purpose of the book is to make information on cybercrimes, do not call list violations and other pertinent information available to law enforcement agencies across the country.

Published in February each year, the data book reports statistical data breaking down different types of cons, scams and hacks from the previous year. The most recent printing of this book is from February 2023. [PPT Slide 12](#)

In that edition, over 5.2 million reports came into the agency with almost half of them being fraud reports. The top three categories for 2022 were; 1. Identity theft, 2. Imposter scams and 3. Credit bureaus, info furnishers and report users. Of the 2.4 million fraud reports involving potential financial loss, over 26% reported an actual loss. The median loss was \$650 and the total losses were \$8.8 billion. [PPT Slide 13](#)

The method most often used to scam consumers was phishing through both email and text. At this point, every real estate licensee has received a text about health insurance, getting your Google profile to the number one ranking or the extended warranty for your car.

Why do consumers keep getting these types of emails and texts? Because they work! Over 300,000 US citizens reported being scammed by a phishing attack. One might think it was mostly against the elderly but that could not be further from the truth. It is across all ages, all education levels and all income levels that are being affected. **PPT Slide 14**

As one would expect, the Federal Bureau of Investigation (FBI) generally leads US enforcement of cybercrimes. Because of the nature of contemporary crime, the FBI has established the Internet Crime Complaint Center. Also known as IC3, it is intelligence driven and threat focused. They collect data, identify trends and pursue threats and react to consumer complaints. **PPT Slide 15**

Filing a complaint is actually very easy. On the front page of their web site, there is a red button that says "File a Complaint." With the click of a button consumers can engage the assistance of the most knowledgeable group of crime fighters trained for this specific task. **PPT Slide 16**

Today's cyber landscape has provided ample opportunities for criminals and adversaries to target US networks, attack critical infrastructure, hold money and data for ransom, facilitate large-scale fraud schemes and threaten our national security.

In this day and age, Cyber Risk is Business Risk and Cyber Security is National Security. Small business owners, including real estate practitioners, must be aware of the pitfalls of cyber threats and prepare in advance to defend themselves against attacks from many different angles.

There is no shortage of recent examples showing the wide-ranging economic and national security effects of cybercrimes. Cyber threats emanate from around the world and we have witnessed the scope and sophistication of these scams and attacks deepen.

Because cyberattacks and cyber-enabled frauds continue to affect our everyday lives, the FBI's Internet Crime Complaint Center (IC3) is critical to combatting the cyber threat. The IC3 serves as a public resource to submit reports of cyberattacks and incidents, which allows us to collect data, identify trends, and pursue the threat at hand. In 2022, the IC3 received 800,944 complaints, which is a 5 percent decrease from 2021. However, the potential total loss has grown from \$6.9 billion in 2021 to more than \$10.2 billion in 2022.

Student Notes

While the number of reported ransomware incidents has decreased, not everyone who has experienced a ransomware incident has reported to the IC3. As such, ransomware remains a serious threat to the public and to our economy, and the FBI and our partners will remain focused on disrupting ransomware actors and increasing the risks of engaging in this activity.

The public can play a crucial role by taking proactive measures to prevent and prepare for a potential cyberattack and, if there is an incident, by reporting it to the FBI through the IC3. Though cybercriminals are continuously seeking to make their attacks more resilient, more disruptive, and harder to counter, public reporting to the IC3 helps us gain a better understanding of the threats we face daily.

What is IC3? (Internet Crime Complaint Center)

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities. They are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world.

To do that, the FBI leverages the IC3 as a mechanism to gather intelligence and internet crime so that we can support the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet facilitated crimes.

As of December 31, 2022, the IC3 has received over seven million complaints. The IC3 mission to provide the public and their partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber-enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report.

Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness. The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful and in the aggregate. That is, when these individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds.

Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally. To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends.

The success of these efforts is directly related to the quality of the data submitted by the public through the public, www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.

The IC3 Recovery Asset Team (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis. **PPT Slide 18**

Goals of RAT-Financial Institution Partnership

- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, and W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device.

Steps to Take When Wire Fraud Occurs (from the IC3 division) PPT Slide 19

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 also have received your wire.
5. Contact local authorities and file a police report.

Did you know the FBI has a cybercriminal "Most Wanted" list? In the style of the wild west, cyber criminals get the face all over the internet to warn consumers. Unfortunately, many of them are outside of the United States and that makes tracking them down much more difficult.

Student Notes

What are the top 10 cyber security threats?

Your Ranking		Actual
—	Insider Threats	—
—	Nation-backed cyber attacks	—
—	Supply chain attacks	—
—	Hacktivism	—
—	Ransomware	—
—	Social engineering and phishing attacks	—
—	IoT security	—
—	Lack of cyber security resources	—
—	Cryptojacking	—
—	Cloud security	—

Student Notes

Segment 2:

Real Estate Scams and Prevention

Learning Objectives

By the end of this section, attendees will be able to:

- 1. Identify the 5 most common real estate scams.**
 - 2. Explain Myth vs Fact in 7 specific cases.**
 - 3. Set up multi-factor authentication on email.**
 - 4. Compare the difference between a land scam and a deed scam.**
 - 5. Explain why one should never use public WIFI.**
-

Real Estate is an easy target for scammers for multiple reasons. First, there is a large amount of public information available about any house in this day and age. Finding information about who lives where, how much they paid for it, how long they have lived there and much more is very easy. One does not have to be clandestine in order to get a plethora of information about a homeowner. [PPT Slide 39](#)

Additionally, there is a ton of detailed communication in a real estate transaction. Real estate agents communicate with their clients, closing attorneys, inspectors and the other agents on a constant basis. When the pace is high, agents can get careless and click on an email that is only slightly different and BOOM! The hack is complete and full access is granted to the scammer.

Real estate closings are targets because of the large sums of money that can be obtained by criminals. Checks wired from a buyer's bank to the closing attorney and seller funds wired from the closing attorney to the seller's bank are prime targets because they are "big hits." For a comparison, the average bank robbery yields \$7,500 for the criminal while the average real estate scam nets over \$100,000.

Finally, the lax security standards of independent contractors in the real estate business makes agents easy targets. In North Carolina alone, there are over 100,000 real estate licensees. Most of them use Gmail or Outlook for their email client for business. Believe it or not, there are still over 1.5 million people using AOL for their email. Email security will be discussed later in this class. [PPT Slide 40](#)

Student Notes

Busting Myths

1. Birds will die if they eat uncooked rice flung at newlyweds.
2. If you eat Mentos and Diet Coke simultaneously, your stomach will explode.
3. Sugar makes children hyper.

All of the above myths are actually false. Those with children may argue that sugar does make children hyper, but studies from Harvard and Stanford have proven otherwise. It is amazing what consumers believe these days. After all, those infomercials on TV in the middle of the night are there for a reason... they work! **PPT Slide 41**

As stated earlier, all real estate licensees are a target no matter how big or little their business is. Even an agent that only sells one house per year is at risk. If you have a computer or a cell phone, you are a target, even if you are broke!

Some say that cyber fraud and wire fraud only happen to sloppy attorneys and brokers. That is not the case. Some of the best agents in the business as well as some of the top attorneys in North Carolina have been victims of wire fraud. Without precautions and being diligent all the time, risk grows.

There is always that person that things, "It won't ever happen to me." Murphy's Law is a bear in real estate. Agents will only a short time of experience in the real estate industry will tell you to prepare for the worst and hope for the best. Licensees must protect themselves and be vigilant at all times.

Some agents think they will know right away if they are hacked. This is especially true with email. Gmail is not immune. Below are stats from Gmail for a 12-month period.

- 788,000 login credentials were taken using keyloggers (spyware which reports all of your keyboard entries to a third party).
- 12,000,000 were taken by phishing (this is where a user is tricked into revealing their info, sometimes through fake e-mails or clone websites).
- 3,300,000,000 pieces of information in relation to Gmail accounts by third-party data breaches. (This would be, for example, a shopping website being compromised. This by proxy revealing your e-mail address as a customer).

Shockingly, these numbers are from 2017! It has become so difficult for Google to keep up with it, they don't even report the numbers anymore. With 1.8 billion active Gmail users, Google is definitely trying to stay ahead of the curve when it comes to Gmail patches.

Student Notes

Virus protection is also not enough by itself. A good computer virus software is only as good as the programmers. There are security patches coming out all the time for different systems due to found holes that can be exploited. That doesn't mean you should skip the virus protection. It is only a piece of a good cybersecurity system.

How often do you change your password? It is strong? Are you using "Password123" for your login password? If so, congratulations! It is the most popular password in the United States. Even a great password can eventually be cracked. It is why we must have layers of protection when it comes to cybersecurity.

Two-factor or multi-factor authentication (MFA) is the best way to protect yourself from hackers for any login. Users that have both a strong password and multi-factor authentication in almost every case. MFA will be discussed later in this segment.

Top 5 Common Real Estate Scams

1. **Business Email Compromise**
2. **Wire Fraud**
3. **Investment Scams**
4. **Land Scams**
5. **Deed Scams**



PPT Slide 50

Business Email Compromise

Business Email Compromise (BEC) is a sophisticated cybercrime tactic that targets organizations and individuals by exploiting vulnerabilities in email communication. It is a form of social engineering that involves manipulating individuals into taking actions or disclosing sensitive information by impersonating trusted entities.

For real estate agents, the compromise often happens for a multitude of reasons. Often, agents are using a free email service when they get hacked. In addition, although they may have virus protection on their computer at home, they may not have it on their phone. As a result, when an agent gets a text or email with a link and clicks on it, the doors to all of the private information is wide open.

BEC attacks typically involve a fraudster posing as a high-ranking executive, a vendor, or a trusted business partner. They employ various techniques, such as email spoofing, phishing, and malware, to deceive the target and gain their trust. The ultimate goal is to deceive the target into performing fraudulent transactions, wire transfers, or disclosing confidential data.

The success of a BEC attack relies on careful planning and meticulous research. Attackers often gather information about their targets from publicly available sources or by compromising email accounts. They then use this information to craft highly convincing messages that appear legitimate, making it difficult for the recipient to detect the fraudulent nature of the communication.

BEC attacks have severe consequences for businesses. They can result in financial loss, damage to reputation, and compromise sensitive data. Organizations should implement robust security measures to protect against BEC attacks, including multi-factor authentication, employee awareness training, email filtering systems, and strict verification processes for financial transactions.

To stay safe from BEC attacks, individuals and businesses should exercise caution when responding to email requests involving financial transactions or sensitive information. Verifying the authenticity of email senders through alternative means, such as phone calls, can provide an additional layer of protection. It is crucial to remain vigilant and skeptical of unexpected or urgent requests, especially those involving financial matters, and report any suspicious activity to the appropriate authorities. **PPT Slide 51**

Wire Fraud

Wire fraud refers to the illegal and deceptive act of using electronic communications, particularly wire transfers or electronic funds transfers, to deceive individuals or organizations for financial gain. It is a form of fraud that takes advantage of the speed and convenience of electronic transactions to carry out unlawful activities.

Wire fraud typically involves a fraudster who employs various tactics, such as phishing emails, fraudulent websites, or social engineering, to trick victims into sending money or sensitive information. These criminals often impersonate legitimate individuals or organizations, using sophisticated techniques to appear trustworthy and legitimate.

The consequences of wire fraud can be devastating for victims. Financial losses can be substantial, and personal or business information may be compromised, leading to identity theft or further fraudulent activities. Wire fraud schemes can target individuals, businesses, or even financial institutions, exploiting vulnerabilities in communication channels and financial systems.

To protect against wire fraud, it is essential to maintain a high level of awareness and skepticism when engaging in electronic transactions. Individuals should be cautious of unexpected or suspicious requests for money or personal information, especially when received through email or other electronic communication platforms. Verifying the legitimacy of requests through independent means, such as contacting the sender directly through verified contact information, can help prevent falling victim to wire fraud.

Organizations should implement robust security measures, including employee training on identifying and reporting fraudulent activities, strong authentication processes for financial transactions, and continuous monitoring of electronic communications for potential threats.

By being vigilant, staying informed about the latest fraud techniques, and employing appropriate security measures, individuals and organizations can minimize the risk of falling victim to wire fraud.

For real estate agents, the criminal often calls or emails the closing attorney or the agent and tricks the consumer into using false wiring instructions. This can happen when the buyer wires funds to the attorney for closing or when the attorney wires funds to the seller after closing for their proceeds. Again, agents should be vigilant making sure clients see the wire fraud warning on the contract and are reminded constantly throughout the contract to close process. [PPT Slide 52](#)

Investment Scams

Investment scams often happen when the criminal gets access to the closing information. The scammer then calls the buyer and says, “Hi Mr. Jones, I’m Frank from the closing attorney’s office for your closing on Tuesday. I need you to wire the total amount \$21,395.87 to the following routing number and account number.” Because the scammer has the exact amount the buyer is expecting to send, there is no suspicion that this could be a criminal.

Unfortunately, the buyer doesn’t find out until the real attorney calls for the check due at closing. This is when it can be tragic for a home buyer that has been saving for years, only to have their down payment disappear into cyber space. By the time anyone realizes, the bank account where the money was sent is closed and the criminal has made his escape. [PPT Slide 53](#)

Land Scams aka Seller Deed Fraud

Land scams refer to fraudulent schemes or deceptive practices that target individuals or businesses in relation to the buying, selling, or ownership of land or real estate properties. These scams aim to exploit the desire for lucrative real estate investments or homeownership, often resulting in financial loss and legal complications for the victims.

Land scams can take various forms, such as fake property listings, unauthorized land sales, identity theft, or fraudulent title transfers. Scammers may use forged documents, false identities, or misleading marketing tactics to deceive potential buyers or property owners. They may promise unrealistic returns on investment, offer properties at significantly discounted prices, or create a sense of urgency to pressure victims into making hasty decisions.

The consequences of falling victim to land scams can be severe. Victims may lose their hard-earned money, face legal disputes over ownership rights, or find themselves unknowingly involved in illegal activities. Additionally, the emotional and psychological toll of being defrauded can be significant, causing stress, anxiety, and a loss of trust in future real estate transactions.

To protect against land scams, it is crucial to exercise caution and due diligence when engaging in real estate transactions. Conducting thorough research on the property and its ownership history, verifying the legitimacy of sellers or agents, and consulting legal professionals can help identify potential scams and mitigate risks.

Individuals should be wary of overly enticing offers, pressure tactics, or requests for large upfront payments without proper documentation. Scrutinizing contracts and seeking independent appraisals or inspections can provide additional safeguards against land scams.

Furthermore, staying informed about common land scam techniques and reporting any suspicious activities to the appropriate authorities can help protect others from falling victim to similar fraudulent schemes.

By being vigilant, conducting proper research, and seeking professional advice, individuals can minimize the risk of being deceived in land transactions and safeguard their investments and property rights. **PPT Slide 54**

Deed Scams

Deed scams refer to fraudulent schemes or deceptive practices that target property owners by manipulating or falsifying property deeds. These scams aim to unlawfully transfer ownership of properties, often leading to financial loss and legal complications for the victims.

In a deed scam, fraudsters exploit vulnerabilities in the property ownership process to carry out their fraudulent activities. They may forge signatures, create counterfeit deeds, or manipulate existing documents to make it appear as though the property has been sold or transferred to them without the owner's knowledge or consent. Scammers may target vacant or abandoned properties, properties owned by elderly individuals, or homes with absentee owners.

In one such scam, the criminal targets elderly home buyers who recently closed. The scammer knocks on the door, tells the owner they are from the attorney's office and an error was made on the deed. Then the scammer asks the seller to sign the "corrected deed," which is actually a new deed transferring ownership to the scammer. Once signed and recorded, the property could be taken from the owner.

The consequences of falling victim to a deed scam can be devastating. Victims may face eviction from their own properties, lose their investment, or find themselves entangled in lengthy and costly legal battles to prove their rightful ownership. Deed scams can have long-lasting financial, emotional, and psychological impacts on the victims.

To protect against deed scams, property owners should be proactive in safeguarding their property rights. Regularly monitoring property records, conducting title searches, and verifying the authenticity of any deed changes or transfers can help detect fraudulent activity. It is crucial to review all documents carefully and consult legal professionals if there are any doubts or discrepancies.

By being vigilant, maintaining accurate records, and seeking legal advice when necessary, property owners can reduce the risk of becoming victims of deed scams and protect their property rights and investments. **PPT Slide 55**

Student Notes

Prevention

In today's digital world, email security is of utmost importance. Protecting your email from being hacked is crucial to safeguard your personal information, sensitive data, and prevent unauthorized access to your accounts. Here are some essential steps to help you prevent your email from being hacked:

1. Use strong, unique passwords: Create complex passwords that include a combination of letters, numbers, and special characters. Avoid using easily guessable information, such as your name or birthdate. Additionally, use a unique password for each of your online accounts to prevent a domino effect if one account is compromised.
2. Enable two-factor authentication (2FA): Enable 2FA for your email accounts whenever possible. This adds an extra layer of security by requiring a second form of authentication, such as a verification code sent to your mobile device, in addition to your password.
3. Be cautious with email attachments and links: Exercise caution when opening email attachments or clicking on links, especially if they come from unknown or suspicious sources. These can be phishing attempts that trick you into revealing your login credentials or downloading malware onto your device.
4. Keep your software up to date: Regularly update your operating system, web browser, and email client to ensure you have the latest security patches and bug fixes. Outdated software can have vulnerabilities that hackers can exploit.
5. Use antivirus and antimalware software: Install reputable security software on your devices to detect and prevent malicious programs. Keep the software updated to stay protected against the latest threats.
6. Be cautious of public Wi-Fi networks: Avoid accessing your email on public Wi-Fi networks, as they are often unsecured and prone to eavesdropping. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your internet traffic.
7. Regularly monitor your accounts: Keep an eye on your email account for any suspicious activities, such as unfamiliar emails, password reset notifications, or changes to your account settings. Report any suspicious activities to your email service provider immediately.

By implementing these preventive measures, you can significantly reduce the risk of your email being hacked. Remember, staying vigilant, using strong security practices, and being cautious with your online activities are essential for maintaining the privacy and security of your email accounts. **PPT Slide 57**

Use Two Factor/Multi Factor Authentication

In an era of increasing cybersecurity threats, relying solely on passwords for account security is no longer sufficient. That's where multi-factor authentication (MFA) comes into play. MFA is a security method that adds an extra layer of protection to your online accounts by requiring multiple forms of verification before granting access. Here's how MFA works:

1. Something you know: This is typically your password, which you enter as the first factor during the login process. It serves as the initial layer of security.

2. Something you have: The second factor involves something physical that you possess, such as a smartphone, a hardware token, or a security key. This factor generates a unique, time-sensitive code or prompts a push notification to your device.

3. Something you are: The third factor is based on biometric characteristics unique to you, such as your fingerprint, iris pattern, or facial recognition. Biometric authentication adds an additional layer of security and convenience.

To enable MFA, you first need to activate it within your account settings. When you log in, you'll be prompted to provide the additional factor(s) of authentication. This could involve entering the code from your authentication app, inserting a security key, or using your fingerprint.

MFA significantly enhances account security because even if someone obtains or guesses your password, they won't be able to access your account without the additional factors. It adds a crucial barrier that makes it much harder for unauthorized individuals to breach your accounts.

Implementing MFA is relatively straightforward, and many online platforms and services offer it as an option. By enabling MFA, you can greatly enhance the security of your accounts and protect your sensitive information from unauthorized access. **PPT Slide 60**

Stay Off of Public WIFI

Public Wi-Fi networks are ubiquitous and convenient, providing internet access in coffee shops, airports, hotels, and other public places. While they offer immediate connectivity, there are significant risks associated with using public Wi-Fi that make it advisable to exercise caution and avoid them whenever possible. Here's why:

1. Lack of security: Public Wi-Fi networks are often unsecured, meaning that the data transmitted over these networks can be easily intercepted by hackers. Without encryption, sensitive information such as login credentials, credit card details, or personal data can be exposed to prying eyes.

2. Man-in-the-Middle attacks: Public Wi-Fi networks are vulnerable to man-in-the-middle attacks, where an attacker intercepts the communication between your device and the network. This allows them to eavesdrop on your online activities, capture sensitive information, or even inject malware into your device.

3. Fake networks: Cybercriminals may set up fake Wi-Fi networks with names similar to legitimate ones to trick unsuspecting users. By connecting to these networks, users unwittingly provide the attackers access to their devices and information.

4. Malware distribution: Public Wi-Fi networks can serve as breeding grounds for malware. Hackers can inject malicious software into these networks, and anyone connected to them may unknowingly download malware onto their devices.

To protect your online security and privacy, it is advisable to use a secure, password-protected network whenever possible, such as your home or office Wi-Fi. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your internet traffic and ensure secure communication.

Additionally, avoid accessing sensitive information or performing financial transactions while connected to public networks.

By being cautious and mindful of the risks associated with public Wi-Fi, you can protect your personal information and maintain a safer online experience. **PPT Slide 65**

Beware of the Internet of Things

The Internet of Things (IoT) has revolutionized the way we interact with technology, connecting everyday objects to the internet and enabling seamless communication between devices. While the IoT offers numerous benefits, it also presents significant risks that users should be aware of. Here are some key risks associated with the Internet of Things:

1. **Security vulnerabilities:** Many IoT devices lack robust security measures, making them vulnerable to cyberattacks. Weak passwords, unpatched software, and insufficient encryption can expose devices and networks to hacking, data breaches, and unauthorized access.
2. **Data privacy concerns:** IoT devices collect vast amounts of data, including personal information and behavioral patterns. If not adequately protected, this data can be exploited or exposed, leading to privacy violations, identity theft, or misuse by third parties.
3. **Lack of standardization:** The IoT landscape is fragmented, with a multitude of devices from different manufacturers operating on various platforms. This lack of standardization makes it challenging to implement consistent security protocols and increases the risk of compatibility issues and vulnerabilities.
4. **Physical risks:** IoT devices that control critical infrastructure, such as smart home systems or medical devices, pose physical risks if they are compromised. Malicious actors could manipulate or disable these devices, leading to property damage, personal harm, or even loss of life.
5. **Network congestion and reliability:** With the proliferation of IoT devices, network congestion can become a concern, leading to slow or unreliable internet connectivity. Additionally, reliance on interconnected devices creates a single point of failure, where a disruption in one device or system can have cascading effects on the entire network.

To mitigate these risks, users should prioritize IoT security. This includes using strong, unique passwords, regularly updating device software, configuring privacy settings, and carefully selecting IoT devices from reputable manufacturers. Implementing network segmentation, using firewalls, and considering the use of IoT security solutions can further enhance protection.

As the IoT continues to expand, it is crucial for individuals, businesses, and policymakers to address these risks proactively to ensure a secure and trustworthy IoT ecosystem. **PPT Slide 69**

Slow Down and Don't Feed The Phish

Phishing has become one of the most prevalent and dangerous online threats in recent years. It is a deceptive technique employed by cybercriminals to trick individuals into divulging sensitive information, such as passwords, credit card details, or personal data. Phishing attacks typically occur via email, instant messaging, or fraudulent websites, and they can have serious consequences. Here's what you need to know about phishing:

1. **Deceptive communication:** Phishing attacks often involve emails or messages that appear to come from legitimate sources, such as banks, social media platforms, or trusted organizations. They use

sophisticated techniques to create a sense of urgency or fear, prompting victims to click on malicious links or provide confidential information.

2. Fake websites and forms: Phishing emails or messages may direct recipients to counterfeit websites designed to mimic legitimate ones. These fake sites trick users into entering their login credentials or other personal information, which the attackers then capture and exploit.

3. Financial and identity theft: The ultimate goal of phishing attacks is to steal sensitive information to commit financial fraud or identity theft. With the obtained data, cybercriminals can access bank accounts, make unauthorized transactions, or assume someone's identity for fraudulent activities.

4. Spear phishing and whaling: Phishing techniques have evolved to target specific individuals or organizations through highly personalized attacks. Spear phishing focuses on individuals, while whaling targets high-profile executives or individuals with access to valuable information or assets.

To protect yourself from phishing attacks, it is crucial to be vigilant and employ best practices:

- Be cautious of unexpected or suspicious emails, especially those requesting personal information or financial transactions.
- Verify the legitimacy of websites by checking for secure connections (<https://>) and validating the website's URL.
- Be wary of clicking on links in emails or messages; instead, manually type the website address in your browser.
- Keep your devices and software up to date with the latest security patches and antivirus software.
- Educate yourself and your colleagues about phishing techniques and encourage a culture of cybersecurity awareness.

By staying informed, being vigilant, and adopting preventive measures, you can protect yourself and your sensitive information from falling victim to phishing attacks.

Student Notes

Segment 3:

Artificial Intelligence

Learning Objectives

By the end of this section, attendees will be able to:

- 1. Define Artificial Intelligence.**
 - 2. Explain what precautions licensees should take when using AI.**
 - 3. Identify methods to recognize the use of AI or Deepfakes.**
 - 4. Use OpenAI effectively and in a safe manner.**
-

What is Artificial Intelligence

Machines that have been taught to think, reason, and learn like people are said to have artificial intelligence (AI), which is a simulation of human intelligence. In order to build intelligent machines that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and natural language processing, AI entails the development and application of cutting-edge algorithms that can analyze and interpret vast amounts of data. [PPT Slide 76](#)

AI comes in a variety of forms, including:

1. **Reactive AI:** This kind of AI lacks the capacity to create memories or draw on prior experiences when making judgments. It reacts in a programmed manner to a specific stimulus. For instance, a computer program that can defeat a human champion in chess but is otherwise powerless. [PPT Slide 78](#)
2. **Limited Memory AI:** It has access to historical information to improve decision-making. Self-driving cars employ this kind of artificial intelligence since they have access to vital information about the route and its surroundings. [PPT Slide 79](#)
3. **Theories of Mind AI:** This kind of AI is valuable in social interactions because it can comprehend the emotions, motives, goals, and beliefs of people. Although this model is still in its early stages of development, it has enormous potential for use in the fields of mental health and emotional support. [PPT Slide 80](#)
4. **Self-Aware AI:** This is a sophisticated type of AI that can be challenging to foresee or imagine. Self-aware AI would essentially be able to consider its own existence and perhaps even its own logic. [PPT Slide 81](#)

The world we live in is being rapidly altered by artificial intelligence. Voice recognition, chatbots, financial portfolios, and political campaigning are just a few examples of how artificial intelligence has made things possible that were previously impractical or prohibitive. Although it can make life easier and

more convenient, it also brings up significant moral dilemmas regarding the roles of machines and people.

When utilized in fields like facial identification, credit scoring, or automated facial recognition, artificial intelligence (AI) has the potential to transform healthcare diagnosis, monitoring, and treatment. However, it also carries considerable hazards. These instances highlight the urgent requirement for industry and government leaders to cooperate together on open governance frameworks to guarantee the unbiased and moral application of AI.

There are a wide variety of applications for artificial intelligence that have both advantages and draw criticism. To investigate and use the full potential of intelligent technology, this field will need ongoing investment from companies and organizations of all kinds.

Student Notes

Deepfakes

Artificial intelligence (AI) and deep learning algorithms are used in deepfakes, which are changed or manipulated movies and images. These can include believable face-editing in hilarious videos, unlicensed imitation, and fake news. [PPT Slide 83](#)

Data gathering, training, and generation are the three crucial processes in the creation of a deepfake.

Data collection is the initial phase, which involves gathering a target person's millions of photographs, videos, and audio snippets from online social media platforms, search engines, and other public sources. To get rid of extraneous information or duplicates, the data is sorted, arranged, and labeled after collection. The system learns the targeted person's facial expressions, body language, and emotional states better the more data there is to go on.

Artificial neural networks that act as information processing systems make up the developed deep learning algorithms. These algorithms examine the patterns in the data and formulate a group of conditional probabilities that characterize the patterns of the person's various facial expressions, feelings, or movements.

Then training data, which consists of image or video sequences, is presented to the algorithms. Convolutional neural networks (CNNs), which are layers of digital filters, examine the training data frame by frame to find patterns that can be utilized to recreate or mix the target person's visual identity in the context of a new image or video.

Generation: The final phase in the deepfake generation process is stitching a computer-generated image or video onto the original footage using trained deep learning algorithms. The process of "mapping the new identity" involves the algorithm projecting the movement, form, and perspective of the source footage onto the newly produced face, movement, or body.

The output must go through a number of post-processing phases, including splicing, noise reduction, texture transfer, color re-matching, and animation retargeting, to guarantee the deepfake movie appears realistic.

The deepfake films are evaluated and put through quality control after the procedure is finished to make sure they closely enough resemble the target person to avoid detection. Currently, anyone with the necessary computer processor speed, training data, and software can produce a convincing deepfake video using even basic deepfake approaches.

Deepfake technology ultimately has a tremendous impact on society, from media and entertainment to national security and interpersonal interactions. To reduce the possibility of utilizing deepfakes for malicious purposes, ethical use and raising awareness of them are essential.

Student Notes

Digital Impersonation and How to Protect Online Accounts

Has anyone ever stolen your identity on social media to make a fake account? I had this happen to me recently and received a call from a very angry woman in Texas. Once I figured out what was going on and helped her to understand what happened, I decided to dig deeper into "Digital Impersonation," to help others learn how to protect online accounts. **PPT Slide 84**

Digital impersonation involves the creation of a fake or false online identity for various purposes like cyberstalking, online defamation, fraud, etc. It has become a growing trend in recent years, and the impact of this behavior is significant.

The problem with digital impersonation is that it allows people to hide online, making it harder to identify the culprits. People who use digital identity can damage the reputation of a company, individual, or organization by posting false or defamatory content on the internet.

One of the most common forms of digital impersonation is catfishing. Catfishing involves creating a fake identity, often using stolen images and personal information of other people, and then using it to lure unsuspecting victims into romantic relationships. The average victim lost \$15,000 to catfishing in 2021. Impersonators will often hide their true identity, which makes it difficult for the victims to discover the truth about the person they are talking to.

Another form of digital impersonation is cyberstalking. Perpetrators will usually create fake online identities to stalk or harass individuals. They'll write harmful things about their victim on social media, send threatening or harassing messages or intimidatory statements that can cause emotional distress and physical harm to their victims. Cyberstalking can be more dangerous than traditional stalking because the perpetrators can hide behind anonymity and reach their targets pretty easily.

If someone is cyberstalking to you, here are some steps to take; 1. Ask the perpetrator to stop. Once you no longer consent to communication, they are legally required to stop. 2. If they continue to communicate, save all evidence. Every conversation should be saved and keep a diary or journal chronologically. 3. File a police report. 4. If they are contacting you using a specific app, file a complaint with that app provider. 5. Contact a lawyer to file a restraining order. Everyone deserves to feel safe on and off line.

In addition, fake online identities are also used for financial fraud. Scammers and fraudsters will often create convincing online personas to gain access to people's financial information or extract money from the victim. This method is commonly referred to as "phishing," where the cybercriminal impersonates a legitimate company or person to trick the victim into providing their personal and financial details.

So how can people protect themselves from digital impersonation? The truth is there's no foolproof method to defend oneself entirely against digital impersonation. Cybercriminals always come up with new tactics and technology to keep themselves ahead. However, some essential precautions can prevent these cybercrimes:

1. Be aware of the risks of online anonymity: Before sharing any personal information online, think about the risks involved. Do not put too much personal info online or share too much with strangers.
2. Protection of Social Media Accounts: Keep your social media accounts private, set strong passwords, and avoid accepting friend requests from unknown people. If you are trying to meet new people online, click on the profile and verify it is a real account and not a bot. By spending 15 seconds to verify that a user is who they say they are can save you headaches down the road.
3. Verify the identity of the people: When you receive emails from unknown sources, do not open any attachments, avoid clicking on any undecipherable links, or replying to any such communications in case of doubt. Attachments as small as 7KB can wipe out sector zero on your hard drive meaning your computer will never boot again. Don't click on links that you aren't expecting.

4. Avoid oversharing of personal information online: Try to avoid sharing too much about your personal life online. Cybercriminals tend to target people who put too much personal information on their online platforms. Also, be careful about sharing your location constantly. If you post that you are leaving for one week vacation, criminals can move from online to actually breaking into your home.

5. Use a reputable Antivirus and Firewall Application: With the right antivirus application and excellent firewall settings, you can significantly reduce the risks of identity theft or other problematic activities.

In conclusion, digital impersonation is a serious issue that can cause damage to people's lives, reputations, and finances. To reduce the risk of being a victim, it's necessary to take basic cyber safety precautions, avoid exposing too much personal information, and build awareness of the risks associated with online anonymity. While no system or safety guideline is foolproof, it's imperative to identify and educate yourself in the ever-evolving threats.

Student Notes



What is OpenAI ChatGPT?

OpenAI, a pioneering research organization in the field of artificial intelligence, has made significant strides in developing advanced language models capable of engaging in dynamic and interactive conversations. One of their most impressive creations is ChatGPT, an AI-powered chatbot designed to simulate human-like conversations.

Launched on November 1, 2022, the software reached over 100 million users in one month. ChatGPT is an innovative language model that leverages OpenAI's GPT-3.5 and 4.0 architecture. It has been trained

on a massive dataset of diverse internet text, allowing it to generate contextually relevant responses to user prompts. OpenAI's ongoing research and continual improvements have led to the development of a highly conversational AI that can assist users in various tasks, provide information, and even engage in creative exchanges.

There is a free version of the software but often users will get a message that says, "Sorry, we are too busy." With a paid account, providing different levels based on user needs, the account is always available, yet it can be slow at times due to a large volume of users. **PPT Slide 86**

Primarily, the goal of OpenAI (available in the App Store on Apple iOS) is to digitize and democratize all data available on the internet. It is so compelling; it drew a \$10 million investment from Microsoft. **PPT Slide 87**

The versatility of ChatGPT enables it to excel in a wide range of applications. From providing customer support and virtual assistants to facilitating language learning and brainstorming ideas, ChatGPT's applications are virtually limitless. It can offer personalized recommendations, generate product descriptions, assist with technical queries, and even engage in casual conversations to provide companionship.

OpenAI emphasizes the concept of "human-in-the-loop" when it comes to ChatGPT. It recognizes the importance of combining human expertise with AI capabilities to ensure optimal outcomes. OpenAI actively encourages user feedback and utilizes human reviewers to identify and mitigate biases and inaccuracies. This collaborative approach helps refine the model, making it safer, more reliable, and better aligned with human values.

As with any AI technology, ethical considerations are crucial. OpenAI is committed to addressing concerns surrounding biases, misinformation, and potential misuse of ChatGPT. They actively invest in research to enhance the model's behavior, ensure user privacy, and implement guidelines that prioritize user safety and security.

OpenAI's ChatGPT is revolutionizing the way we interact with AI. By enabling dynamic, human-like conversations, ChatGPT has the potential to transform industries, streamline processes, and enhance user experiences. OpenAI's commitment to continuous improvement and ethical considerations paves the way for responsible AI deployment, promoting a future where humans and AI collaborate harmoniously to achieve unprecedented advancements.

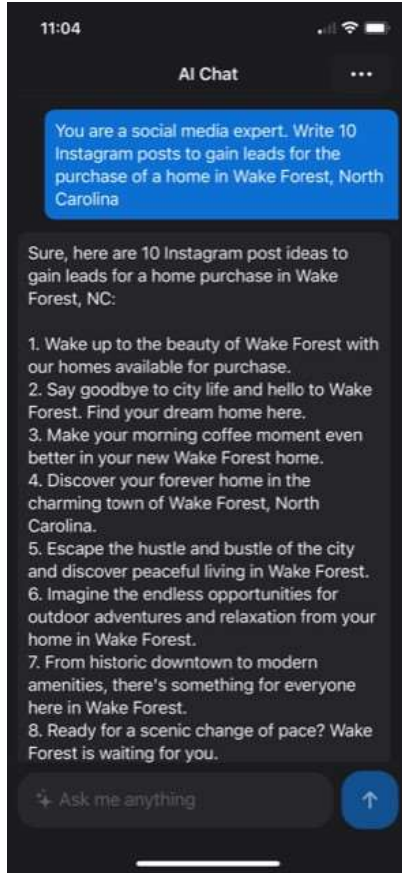
Benefits of Artificial Intelligence for Realtors

As technology evolves, it's becoming increasingly necessary for real estate agents to make use of any tools at their disposal to better serve their clients. One such tool that has gained popularity among realtors is chatGPT. ChatGPT is an Artificial Intelligence (AI) powered assistant that helps real estate agents automate routine tasks, streamline communication with clients and leads, and carry out predictive analysis of their market. Let's look at some of the benefits of artificial intelligence for Realtors.

ChatGPT helps real estate agents save time. As an AI-powered assistant, it helps agents automate specific tasks such as writing property descriptions, creating social media posts, and blog writing. With chatGPT,

real estate agents can focus on more meaningful activities, such as finding new buyers, maintaining relationships with clients, and closing deals quickly.

At this early stage of its popularity, chatGPT is used by Realtors for simple tasks. However, using the Application Programming Interface (API) from OpenAI, it can be taught to do many other tasks.



For example, if an agent has written over 500 property descriptions, those descriptions can be uploaded and analyzed so that the technology not only writes future descriptions, but does so in the tone and style of the author.

The system can also be fed data to reorganize it, categorize it or present it in a new way.

Some systems have the ability to provide real estate agents with important insights into their market trends through data analysis. Advancements in machine learning will also allow systems to monitor data through social media and other relevant online channels. Once the data has been collected, the real estate agent can use that data to tailor marketing strategies to specific audiences.

Ultimately, AI will improve the speed and effectiveness of real estate transactions. Systems will be able to learn from previous transactions and provide insight into what buyers and sellers are looking for. With this information, real estate agents will be able to more quickly identify quality leads and close deals more quickly.

The adoption of AI by Realtors will be a great help in revolutionizing the customer experience, delivering quality services to clients and streamline routine tasks. Although it has been around for a while, AI

is finally starting to gain traction amongst real estate agents and is going to be a game changer for agents that embrace it. **PPT Slide 88**

Agents using ChatGPT will have to be very careful when using the software. The source of the content is the internet so accuracy is not always at the forefront. Because GPT3 is only indexed through December 31, 2021, users should make sure they are using a paid version which upgrades to the 4.0 system.

Proofreading of ChatGPT results for licensees is a must. It has been known to “make up” information to fill space the same way a high school student makes up information for a paper that must fill at least three pages.

Additionally, and maybe most importantly, ChatGPT has no concept of Fair Housing laws and often violates them. The words used will have to be massaged for users, especially when describing a property.

PPT Slide 89

AI & Copyright

Despite the fact that copyright law is grounded in human authorship and dates back to a Supreme Court ruling from the 1880s, a number of instances employing cutting-edge AI technology are currently contesting that rule of law. The US Copyright office released a statement on March 16, 2023 saying they would treat generative AI situations on a case-by-case basis. [PPT Slide 90](#)

Regardless of copyright rules, licensees should remember that all OpenAI results are sourced from the internet meaning there is likely copyright infringement on anything used. As a result, it is advisable to not use anything with AI on public sites like blogs, websites or social media posts without giving proper credit to original authors. [PPT Slide 91](#)

We are already seeing a few examples that show the complex legal problems with AI-generated works.



In one instance, plaintiff Stephen Thaler is suing the United States Copyright Office (in *Thaler v. Perlmutter*) because it disallowed him copyright on a picture created by his artificial intelligence program, the Creativity Machine.

He asserts that he and the AI generator agreed to create it as a work-for-hire. "Thaler argues that human authorship isn't required and, therefore, his work should be entitled to protection," Hecht said, despite numerous denials by the Copyright Office.

It has been noted that Thaler has said he will, if necessary, challenge his case to the Supreme Court. [PPT Slide 92](#)

In another instance, a writer and artist used AI to produce graphics and write the text for a graphic novel. When it was discovered that the images were AI-generated, the Copyright Office first awarded her protection but limited the registration to the text and image arrangement. However, the author insists that she didn't merely enter a prompt. She grabbed the photograph and instructed AI to modify it till it reflected her preferences.

The stock photo industry behemoth Getty photos sued Stability AI Inc. last year for exploiting 12 million Getty photos and their associated metadata to train its system, and Hecht concluded by describing this instance. In order to train their system, an AI developer uses the work of others. This allows AI to create new works based on the originals. [PPT Slide 93](#)

For real estate professionals and others wishing to exploit this developing technology, the instances raise several questions. However, Articles 2 and 12 of the Code of Ethics provide direction.

Article 2 holds that “REALTORS® shall avoid exaggeration, misrepresentation or concealment of pertinent facts relating to the property or the transaction.” Article 12 says, “REALTORS® shall be honest and truthful in their real estate communications and shall present a true picture in their advertising, marketing and other representations.”

It is against those two Articles to use AI to repair a structural break in a wall, but it is acceptable to remove a hose and bucket that were unintentionally captured in a photo.

Three things to remember to use AI as safely as possible:

1. Always check the accuracy of articles produced by AI.
2. Avoid utilizing AI to produce a work that you intend to be able to defend.
3. Never presume that any content from a third party was produced by AI and is thus freely usable. Always obtain written authorization before using someone else's creation in any fashion, and keep the authorization letter. **PPT Slide 94**

Student Notes

Open AI Examples

Prompt: You are a Realtor. Write a description in less than 100 words about the Town of Cary, NC

Response: Discover the charm of Cary, NC, a vibrant town nestled in the heart of the Research Triangle. With its idyllic setting, Cary offers a perfect blend of small town charm and urban amenities. Boasting top-rated schools, beautiful parks, and a strong sense of community, it's an ideal place to call home. Enjoy a thriving arts scene, diverse dining options, and world class shopping destinations. Whether you're seeking outdoor adventures, cultural experiences, or career opportunities, Cary has it all. Experience the best of suburban living with easy access to the bustling cities of Raleigh and Durham. Welcome to Cary, where quality of life meets endless possibilities.

Student Notes

Open AI Examples

Prompt: You are a social media expert. Write an Instagram post with less than 100 words about downtown Durham, north Carolina

Response: 🏙️ Discover the vibrant heart of North Carolina - Downtown Durham! 🎉 Immerse yourself in the perfect blend of history, culture, and modernity. Stroll down the bustling streets lined with unique shops, eclectic art galleries, and farm-to-table eateries. Experience the energy of the Bull City as you explore the historic Durham Bulls Athletic Park or catch a show at the iconic DPAC. Indulge in locally brewed craft beers and indulge your taste buds with culinary delights from award-winning chefs. From its rich history to its thriving creative scene, Downtown Durham has something for everyone. 🌟 #DurhamNC #BullCity #DiscoverDurham

Student Notes

Open AI Examples

Prompt: You are a Realtor. Write a property description for the home at 212 E Winston Street, Youngsville, NC.

Response: Introducing a dream home at 212 E Winston Street in the charming town of Youngsville, NC! 🏡 Nestled on a picturesque lot, this stunning property offers the perfect blend of elegance and comfort. Step inside to discover a spacious open floor plan bathed in natural light. The gourmet kitchen features high-end appliances and a center island, ideal for culinary creations. Relax in the luxurious master suite with a spa like ensuite bathroom. Enjoy outdoor living at its finest with a covered porch and a meticulously landscaped backyard. Conveniently located near schools, parks, and shopping, this home is a true gem. Welcome to your forever home! #YoungsvilleNC #DreamHome #ForSale

Student Notes

Chat GPT Clears the US Medical Licensing Examination

Researchers from Massachusetts General Hospital (MGH) and AnsibleHealth, a technology-enabled medical practice providing care to medically complex chronic respiratory disease patients, found in a recent study that the artificial intelligence (AI) chatbot ChatGPT can pass the United States Medical Licensing Exam (USMLE) — findings that may highlight the tool’s potential use cases in medical education.

Recent hype and concerns around the use of ChatGPT in healthcare, such as digital mental health service Koko’s reported use of the tool in an experiment to help develop responses to users, have raised questions about its use cases.

To evaluate one aspect of ChatGPT’s potential utility, the researchers evaluated its performance on the USMLE, which consists of three standardized tests that medical students must pass to obtain a medical license.

To do this, the research team obtained publicly available test questions from the June 2022 sample exam released on the official USMLE website. Questions were then screened, and any question requiring visual assessment was removed.

From there, the questions were formatted in three ways: open-ended prompting, such as ‘What would be the patient’s diagnosis based on the information provided?’; multiple choice single answer without forced justification, such as ‘The patient’s condition is mostly caused by which of the following pathogens?’; or multiple choice single answer with forced justification, such as ‘Which of the following is the most likely reason for the patient’s nocturnal symptoms? Explain your rationale for each choice.’

Each question was then put into the model separately to reduce the tool’s memory retention bias.

During testing, the researchers found that the model performed at or near the passing threshold of 60 percent accuracy without specialized input from clinician trainers. They stated that this is the first time AI has done so.

The researchers also discovered upon evaluating the reasoning behind the tool’s responses that ChatGPT displayed understandable reasoning and valid clinical insights, which led to increased confidence in trust and explainability. **PPT Slide 99**

Transforming Property Management: The Impact of Artificial Intelligence

Artificial intelligence (AI) has emerged as a disruptive force across various industries, and the property management sector is no exception. With its ability to analyze vast amounts of data and automate routine tasks, AI is poised to revolutionize the property management industry. **PPT Slide 101**

AI-powered systems can streamline property management operations by automating processes such as rent collection, maintenance requests, and lease renewals. Machine learning algorithms can analyze historical data to predict maintenance needs, optimize rental pricing, and even identify potential risks. This not only saves time and reduces human error but also allows property managers to focus on more strategic tasks.

AI can significantly enhance the tenant experience by offering personalized services and efficient communication channels. Virtual assistants and chatbots can promptly address tenant queries, provide real-time updates, and facilitate seamless interactions. AI-powered platforms can also simplify the rental application process, enabling tenants to find suitable properties more efficiently.

AI-powered surveillance systems equipped with facial recognition technology and video analytics can improve property security. These systems can detect unauthorized access, monitor common areas, and send real-time alerts in the event of suspicious activities. Property owners and managers can proactively address security concerns, ensuring the safety of residents and assets.

The vast amount of data generated in the property management industry can be harnessed by AI algorithms to provide valuable insights. AI can analyze market trends, tenant preferences, and financial data to optimize rental pricing, identify investment opportunities, and improve overall portfolio performance. Data-driven decision making empowers property managers to make informed choices that maximize profitability and mitigate risks. **PPT Slide 102**

AI-Powered Property Valuation

The emerging trend of AI-powered property valuation is revolutionizing the real estate industry. Utilizing advanced algorithms and machine learning, AI can analyze vast amounts of data to accurately estimate property values. By considering factors such as location, market trends, historical sales data, and property characteristics, AI-powered valuation models provide faster and more objective assessments. This technology enables real estate professionals to make informed decisions regarding pricing, investment opportunities, and risk assessment. AI-powered property valuation not only enhances efficiency but also reduces human bias, leading to fairer and more reliable property appraisals in the ever-evolving real estate market. **PPT Slide 104**

AI and Predictive Analytics

The use of AI and predictive analytics in real estate has transformed the industry by providing valuable insights, optimizing decision-making, and improving operational efficiency. AI algorithms can analyze vast amounts of data, including market trends, demographic information, historical sales data, and property characteristics, to identify patterns and predict future outcomes.

AI can analyze public records for family changes like death, divorce and birth to identify sellers who may be interested in selling. In addition, AI can monitor social media posts to identify potential sellers and buyers based on their posting pattern. Along with that, AI has the ability to monitor human interactions on web sites, including Google searches like, "Move to Denver."

By leveraging predictive analytics, real estate professionals can make more informed decisions regarding property investments, pricing, and marketing strategies. AI models can accurately forecast property values, rental demand, and market trends, enabling investors to identify lucrative opportunities and mitigate risks. Real estate agents can utilize predictive analytics to identify potential buyers and sellers, tailor marketing campaigns, and enhance customer experiences.

Furthermore, AI-powered tools streamline operations by automating routine tasks such as property searches, lead generation, and document processing. This improves efficiency, reduces costs, and allows professionals to focus on higher-value activities.

In summary, the integration of AI and predictive analytics in real estate empowers industry professionals to make data-driven decisions, optimize strategies, and enhance overall performance. The application of these technologies will continue to reshape the real estate landscape, making it more efficient, transparent, and responsive to market dynamics. **PPT Slide 106**

Identifying AI Generated Content

Identifying AI-generated content has become increasingly important as artificial intelligence technology advances and its applications expand. AI models like OpenAI's GPT-4 have demonstrated remarkable abilities to generate human-like text, making it challenging to distinguish between AI-generated content and content created by humans. However, several key indicators can help identify AI-generated content.

First, a lack of coherence or inconsistency in the generated text can be a telltale sign of AI involvement. AI models may produce grammatically incorrect sentences, illogical arguments, or abrupt changes in style or tone.

Second, assessing the context and knowledge presented in the content can provide clues. AI-generated content may lack real-world context, historical accuracy, or specific nuances that human-generated content often possesses. Unusual or unrealistic claims, unfamiliar references, or incorrect information can raise suspicions.

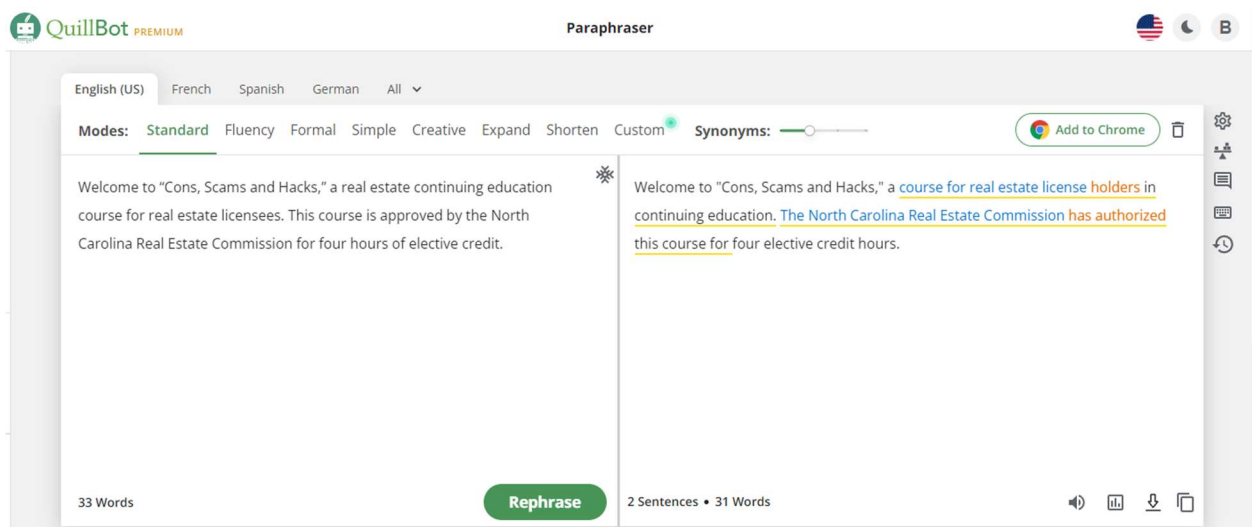
Third, examining the response time and volume of content production can offer insights. AI models can generate content at an incredible speed and produce a vast quantity of responses in a short time frame, which would be difficult for a human to replicate.

Lastly, considering the purpose and intent of the content is crucial. AI-generated content may exhibit generic or formulaic patterns, lacking a personal touch or human emotion. It may also be designed to persuade or manipulate rather than engage in authentic communication.

As AI technology advances, it is vital to develop effective methods and tools to identify AI-generated content. This enables users to critically evaluate the information they encounter, maintain transparency and trust, and make informed decisions in an increasingly AI-driven world. **PPT Slide 107**

Using an AI content detector or AI text classifier like Originality.AI can enable the user to identify AI created content.

Quillbot.com



Quillbot.com is an online writing tool that utilizes artificial intelligence to assist users in improving their writing. It employs advanced algorithms to analyze the input text and generate alternative suggestions, paraphrases, and summaries. Quillbot.com helps users enhance their writing by offering synonyms, rephrasing sentences, and providing additional context. It can be used to improve the clarity, coherence, and overall quality of written content. Whether it's academic papers, blog posts, or professional emails, Quillbot.com aims to support users in expressing their ideas more effectively and efficiently. **PPT Slide 108**

Student Notes

Segment 4:

Other Issues/New Technology

Learning Objectives

By the end of this section, attendees will be able to:

- 1. Explain why people are the weakest link in cybersecurity.**
 - 2. Describe how new technologies operate including Threads, Ring By Name and Apple Vision Pro.**
 - 3. Explain the dangers of Digital Transaction Management**
-

Does Privacy Exist? [PPT Slide 113](#)

In today's world, privacy is a rare thing. As seen in the video, there are very few places other than inside of one's own home that provide privacy anymore.

As a result, licensees must realize they are being held liable for not protecting client information that leads to the theft of wires. In 2021, the North Carolina Real Estate Commission told licensees in the General Update and the BICUP that licensees should not be involved in the exchange of money beyond delivery of the Due Diligence Fee and Earnest Money. [PPT Slide 114](#)

Agents were being caught in the middle of wire fraud and being held accountable. The good news is that licensees got the message. The number of complaints about wire fraud have been reduced at least at the real estate regulatory level.

This is good news for agents as lost wire funds are usually gone forever and those losses are rarely covered under errors and omissions insurance policies. Real estate companies should invest in cyber insurance to protect in the event of a data breach. [PPT Slide 115](#)

As licensees have noted, the wire fraud notice on the Offer To Purchase and Contract (Form 2-T) has helped to prevent issues for both buyers and sellers. In addition, the National Association of Realtors put a recommendation out in 2019 for agents to include on their email signatures. [PPT Slide 116](#)

Student Notes

Email Security- The Weakest Link

In today's digital age, securing email from hacking is of utmost importance. With cyber threats and hacking attempts becoming increasingly sophisticated, implementing robust security measures is crucial to protect sensitive information. Here are several essential steps to enhance email security:

1. **Strong Passwords:** Ensure you use unique, complex passwords for your email accounts. Combine uppercase and lowercase letters, numbers, and special characters, and avoid easily guessable information like birthdays or common phrases.
2. **Multi-Factor Authentication (MFA):** Enable MFA on your email accounts. This adds an extra layer of security by requiring a second verification step, such as a code sent to your phone, in addition to your password.
3. **Phishing Awareness:** Be cautious of phishing attempts, where attackers pose as trustworthy entities to trick you into revealing sensitive information. Avoid clicking on suspicious links or downloading attachments from unknown senders.
4. **Regular Software Updates:** Keep your email client, antivirus software, and operating system up to date. Software updates often include security patches that address vulnerabilities and protect against new threats.
5. **Encryption:** Use email encryption tools or services that encrypt your messages, making them unreadable to unauthorized parties. Look for end-to-end encryption options to ensure secure communication.
6. **Spam Filters:** Activate spam filters to reduce the risk of malicious emails reaching your inbox. These filters can identify and block suspicious or unsolicited messages.
7. **Secure Networks:** Avoid accessing your email from public Wi-Fi networks or unsecured connections. Use a virtual private network (VPN) to encrypt your internet traffic and protect your data.
8. **Employee Education:** Educate yourself and your team on email security best practices, including recognizing phishing attempts, avoiding suspicious links, and maintaining good password hygiene.

By implementing these measures, you can significantly enhance the security of email accounts and safeguard personal and confidential information from hacking attempts. Remember, staying vigilant and proactive is key to maintaining email security in an ever-evolving digital landscape. **PPT Slide 118**

Student Notes

What to Do After You've Been Hacked

1. Change your password.
2. Set up MFA.
3. Keep software up-to-date.
4. Email your contacts and let them know.

Don't wait to do this. Do it immediately. The quicker you get on it, the fewer the damages.

Some real estate companies may choose to hire a third-party provider for email monitoring, especially if there are more than 10 agents in the company. [PPT Slide 119](#)

Establishing Your Own Domain

One great way to secure your email is by having your own domain and hiring a third party to host it.

Licensees should own their own domain rather than having one provided by the company. When the agent leaves to go to another company, the original company retains the old website and can use it to their advantage.

By owning one's own domain, there is control and the only thing that changes on the website or with the email hosting is the logo.

There are many providers of websites that will also host your email domain. Talk to friends in the business and get recommendations before jumping into the deep end with an expensive site that may overwhelm you. [PPT Slide 120](#)

Student Notes



Burner Email Accounts

Burner email accounts offer numerous benefits when it comes to maintaining online privacy and protecting personal information. These temporary or disposable email accounts provide a layer of security and control over the flow of emails.

Firstly, burner email accounts help protect against spam and unwanted solicitations. By creating a separate email address for specific purposes, such as signing up for newsletters or online services, individuals can prevent their primary email accounts from being flooded with promotional emails and potentially compromising their privacy.

Secondly, burner email accounts reduce the risk of data breaches and unauthorized access. If a burner email account is compromised or subjected to a data breach, the impact is limited since it is not linked to a person's primary email address or other sensitive information. This helps individuals maintain control over their personal data and minimizes the potential consequences of a security breach.

Lastly, burner email accounts allow individuals to maintain anonymity when engaging in online activities. By using a temporary email address, individuals can browse and communicate without revealing their real identity, providing an additional layer of privacy and security.

Overall, burner email accounts provide a convenient and effective way to manage online interactions, protect against spam, safeguard personal information, and maintain a certain level of anonymity. **PPT Slide 122**

Get Off Public Wi-Fi

Using public Wi-Fi networks can be convenient, but it poses significant risks to personal security and privacy. Here is why people should exercise caution when connecting to public Wi-Fi:

Firstly, public Wi-Fi networks are prime targets for hackers and cybercriminals. These networks are often unsecured, making it easier for malicious individuals to intercept data transmitted between devices. This puts sensitive information, such as passwords, banking details, and personal data, at risk of being compromised.

Secondly, public Wi-Fi networks lack encryption, leaving data vulnerable to interception. Without encryption, any data transmitted over the network can be easily accessed and exploited by hackers.

Thirdly, man-in-the-middle attacks are common on public Wi-Fi networks. Hackers can position themselves between a user and the Wi-Fi hotspot, intercepting and altering data exchanged between the two parties without their knowledge.

Lastly, public Wi-Fi networks may be operated by malicious actors or set up to lure unsuspecting users into sharing sensitive information. These "fake" networks, also known as rogue hotspots, mimic legitimate networks to deceive users and collect their personal data.

To mitigate these risks, it is advisable to avoid accessing sensitive information, such as online banking or personal accounts, while connected to public Wi-Fi. Instead, consider using a virtual private network (VPN) to encrypt your data or rely on cellular data networks for secure internet access. Prioritizing personal security and privacy is essential in today's digitally connected world. **PPT Slide 123**

Get Proficient with Your Phone's Mobile Hotspot

Using a phone's mobile hotspot offers several compelling reasons for individuals seeking a secure and reliable internet connection. Here are some key advantages:

A mobile hotspot provides a private and encrypted network connection. Unlike public Wi-Fi networks, which are often unsecured, using a mobile hotspot allows individuals to create their own personal network with password protection. This ensures that their data remains secure and inaccessible to unauthorized parties.

Mobile hotspots offer greater reliability and stability compared to public Wi-Fi. While public networks can be congested and suffer from slow speeds or frequent disconnections, mobile hotspots leverage cellular networks, providing a more consistent and reliable internet experience.

Hotspots also offer flexibility and convenience, allowing individuals to access the internet wherever they have cellular network coverage. This is particularly beneficial in situations where public Wi-Fi is unavailable or unreliable, such as during travel or in remote areas.

Using a mobile hotspot provides individuals with greater control over their data usage and costs. They can monitor their data consumption and choose suitable data plans to suit their needs, preventing unexpected charges or limitations imposed by public Wi-Fi providers.

Overall, using a mobile hotspot ensures a secure, reliable, and flexible internet connection, making it an ideal choice for individuals who prioritize privacy, dependability, and control over their online experience. **PPT Slide 124**

Avoid Using Public Computers

Using public computers poses significant risks to personal security and privacy. Public computers, such as those found in libraries or internet cafes, may have compromised security measures or outdated software, making them vulnerable to malware or keyloggers. Logging into personal accounts on public computers can expose sensitive information, including passwords and financial details. Additionally, public computers may lack proper privacy settings, allowing others to access personal files or browsing

history. To safeguard personal information and maintain privacy, it is advisable to avoid using public computers for sensitive tasks. Instead, using personal devices or trusted computers with up-to-date security measures provides a safer and more secure computing environment. **PPT Slide 125**

Secure Email vs Encrypted Email

Secure email and encrypted email are two distinct concepts that aim to protect the confidentiality and integrity of email communications, but they approach security in different ways.

Secure email refers to the overall security measures implemented to safeguard email communication. This includes various components such as secure email protocols (e.g., HTTPS), secure authentication mechanisms (e.g., multi-factor authentication), spam filters, and antivirus scanning. Secure email focuses on protecting the email infrastructure, preventing unauthorized access to email accounts, and ensuring that email transmission occurs through secure channels.

On the other hand, encrypted email specifically focuses on securing the content of the email itself. Encryption is a process that transforms the plain text of an email message into an unreadable format, known as ciphertext. Only the intended recipient with the appropriate decryption key can convert the ciphertext back into readable plain text. Encryption ensures that even if an unauthorized party intercepts the email, they will not be able to decipher its content.

While secure email encompasses various security measures to protect the email infrastructure, encrypted email specifically protects the content of the email from unauthorized access or interception. Both secure email and encrypted email play crucial roles in ensuring the privacy and security of email communication. Implementing secure email protocols and using end-to-end encryption for sensitive or confidential messages provides a comprehensive approach to protecting the confidentiality and integrity of email exchanges. **PPT Slide 126**

Student Notes

Trade Unsubscribe for Block

When faced with unwanted or spam emails, it is often more effective to block the sender rather than simply relying on the unsubscribe feature. Here are some recommendations to consider:

1. **Reduced Risk:** Blocking email senders minimizes the risk of potential harm or security breaches. Unsubscribing from suspicious or unknown senders may confirm the validity of your email address, leading to more spam or phishing attempts. Blocking ensures that future emails from the sender are automatically diverted to your spam folder or prevented from reaching your inbox altogether.

2. **Time and Effort Savings:**

Unsubscribing from unwanted emails can be time-consuming, especially if you receive numerous unsolicited messages. Blocking the sender directly eliminates the need to repeatedly go through the unsubscribe process, saving time and effort.



3. **Permanent Solution:** While unsubscribing may stop some unwanted emails, it doesn't guarantee a permanent solution. Blocked senders, however, are prevented from contacting you further, providing a more effective long-term solution to manage unwanted communications.

4. **Enhanced Control:** Blocking email senders grants you greater control over your inbox. It allows you to create a personalized list of approved senders, ensuring that you only receive emails from trusted sources.

5. **Spam Filtering Support:** Most email service providers have robust spam filters that can learn from your actions. By blocking and reporting unwanted senders, you contribute to the ongoing improvement of spam filtering algorithms, benefiting not only yourself but also other users. **PPT Slide 127**

Don't Use Business Email for Social Media Accounts

Using a business email for social media accounts may not be the best practice due to several reasons. Here are a few key points to consider:

Separation of Personal and Professional: Maintaining a clear distinction between personal and professional communication is important. By using a personal email for social media accounts, you can keep your personal online presence separate from your business-related activities. This ensures that personal messages, notifications, and social media interactions do not get mixed up with important business emails.

Privacy and Security: Social media platforms often require users to provide personal information during registration. By using a business email, you risk exposing sensitive business-related information to

potential privacy breaches. It is preferable to keep business and personal information separate, reducing the chances of unauthorized access or potential data leaks.

Brand Consistency: Using a dedicated business email for social media accounts allows you to maintain brand consistency and professionalism. It reinforces your business identity and helps establish a more credible and unified online presence.

Easier Transition: If there are personnel changes within your organization or you need to transfer account management responsibilities, having a separate business email associated with social media accounts simplifies the transition process. It ensures a smooth handover without compromising personal accounts or data.

Organization and Efficiency: By keeping social media accounts separate from your business email, you can manage your communication more effectively. It helps declutter your inbox, prevents distractions, and allows you to prioritize important business-related emails without getting overwhelmed by social media notifications.

Using a personal email for social media accounts instead of a business email is advisable. It promotes privacy, security, brand consistency, and efficient communication management. Separating personal and professional accounts ensures a more streamlined and effective online presence for both individuals and businesses. [PPT Slide 128](#)

Don't Open Attachments Without Verification

In an era where cyber threats and malicious attacks are prevalent, exercising caution and verifying the content of email attachments and text messages is crucial. Here are compelling reasons why one should never open an email attachment or click on a text message without proper verification:

Opening unknown email attachments or clicking on suspicious links can lead to the installation of malware or viruses on your device. These malicious programs can compromise your data, steal sensitive information, and cause significant damage to your system.

Email attachments and text messages can be used as tools for phishing attacks, where cybercriminals impersonate legitimate entities to deceive users and extract personal or financial information. Clicking on malicious links within these messages can lead to identity theft or financial loss.

Email attachments, particularly those in the form of seemingly harmless documents or files, can contain ransomware. When opened, ransomware encrypts files on your device and demands a ransom to regain access. Falling victim to a ransomware attack can result in financial loss and significant disruption to your personal or professional life.

Malicious attachments and text messages may employ social engineering tactics to manipulate users into taking harmful actions. They may create a sense of urgency, fear, or curiosity to prompt individuals to click on links or open attachments without proper verification.

Attackers can send emails or text messages that appear to come from a trusted source or known contact. However, these messages can be forged or spoofed, aiming to trick recipients into downloading malicious attachments or visiting compromised websites.

To protect yourself from these risks, it is essential to verify the source and legitimacy of any email attachment or text message before taking any action. Verify the sender's identity, cross-reference with known contacts, and assess the content for inconsistencies or red flags. Additionally, rely on robust antivirus software and anti-malware tools to scan attachments before opening them.

By adopting a cautious and vigilant approach, you can mitigate the potential risks associated with opening unsolicited email attachments or clicking on suspicious text message links. Prioritizing verification and exercising skepticism serve as a crucial defense against cyber threats, safeguarding your personal and financial well-being in the digital age. **PPT Slide 129**

Threads for Instagram

Threads from Instagram is a standalone messaging app designed to facilitate intimate and private communication between close friends. It offers a more focused and streamlined experience compared to the broader functionality of the main Instagram platform. Threads aims to foster genuine connections by enabling users to share updates, photos, videos, and messages with a select group of contacts.

Many compare the platform to Twitter. There are many experts in the industry that expect Twitter to sue Meta, the parent company of Facebook, Instagram and Threads, for infringement of intellectual property.

The app emphasizes real-time sharing and personal updates, as it automatically syncs with the user's Instagram Close Friends list. This feature allows for seamless communication and sharing within a trusted circle of friends. Threads also includes a status feature called "Auto Status" that uses location data and user activity to provide automatic updates on what a user is doing throughout the day.

Privacy is a central focus of Threads, with the option to customize and control who can reach out and share content. It also includes privacy settings to limit data sharing with the main Instagram app. Threads provides end-to-end encryption for messages, ensuring that the content remains private and secure.

With Threads, Instagram aims to provide a dedicated space for authentic and meaningful conversations among close friends, while allowing users to maintain control over their privacy. It provides a more intimate and focused platform for users to connect, share, and communicate with their inner circles in a private and secure manner. **PPT Slide 131**

Apple Vision Pro VR Headset

The Apple Vision Pro VR headset represents a significant leap forward in the virtual reality (VR) industry. Combining cutting-edge technology, sleek design, and the renowned Apple ecosystem, this headset offers a captivating and immersive VR experience.

One of the standout features of the Apple Vision Pro VR headset is its advanced visual capabilities. Equipped with high-resolution displays, precise tracking sensors, and a wide field of view, the headset delivers stunning visuals that transport users to virtual worlds with remarkable clarity and realism. Apple's commitment to excellence in display technology is expected to result in a visually breathtaking VR experience.

Furthermore, the integration with Apple's ecosystem is a notable advantage. With seamless compatibility across various Apple devices and services, users can easily access a wide range of VR content, applications, and experiences. The headset is likely to leverage the power of Apple's proprietary chips, ensuring smooth performance and efficient power consumption.

Apple's emphasis on user comfort and convenience is expected to be reflected in the design of the Vision Pro VR headset. Lightweight and ergonomically designed, it aims to provide a comfortable fit even during extended VR sessions. The inclusion of high-quality audio and intuitive controls further enhances the immersive experience.

In terms of content, Apple's vast ecosystem and collaboration with developers are likely to offer a diverse selection of VR experiences. Whether it's gaming, educational applications, or productivity tools, users can expect a range of compelling content options to explore. [PPT Slide 132](#)

Digital Transaction Management (DTM)

Digital transaction management (DTM) has revolutionized the real estate industry by streamlining and digitizing the various processes involved in property transactions. From document signing and sharing to contract management and secure storage, digital transaction management platforms have transformed how real estate transactions are conducted. Here are some key benefits of digital transaction management in real estate:

DTM eliminates the need for physical paperwork and manual processes. It allows real estate professionals to handle documents electronically, reducing administrative burdens and saving time. With the ability to track and manage documents in real-time, the entire transaction process becomes more efficient.

Digital platforms provide easy access to transaction documents from anywhere and at any time. Multiple parties involved in the transaction, such as buyers, sellers, agents, and lenders, can collaborate seamlessly, share information, and make updates in a secure and centralized environment.

DTM platforms prioritize data security and compliance with industry regulations. They offer robust encryption, secure storage, and audit trails to protect sensitive information. This helps maintain the integrity of documents and ensures compliance with legal requirements.

Platforms also enhance transparency by providing a clear trail of document history, changes, and communications. Parties involved can easily track the progress of the transaction, view updates, and maintain an accurate record of all interactions.

Adopting digital transaction management reduces costs associated with printing, mailing, and storing physical documents. It also minimizes the risk of errors, lost paperwork, and delays, resulting in cost savings and improved overall operational efficiency.

Overall, DTM has streamlined and modernized real estate transactions, offering enhanced efficiency, accessibility, security, and compliance. Its ability to digitize and automate processes provides a seamless experience for all parties involved, ultimately transforming how real estate transactions are conducted in the digital age. **PPT Slide 133**

Ring By Name

Ring By Name is a company that offers a unique and innovative service for personalized audio greetings through text or email. The company specializes in creating customized name pronunciations for individuals and businesses, ensuring that their names are accurately pronounced in voice recordings, phone systems, and other audio applications.

The process of how Ring By Name works is simple yet effective. Users provide the company with the correct pronunciation of their names or the names of their employees, colleagues, or clients. This information can be submitted through an online form or via a phone call. Ring By Name's team of experts then works diligently to produce high-quality audio recordings that accurately capture the intended pronunciation.

The recorded name pronunciations are delivered in various audio file formats, allowing seamless integration into phone systems, voicemail greetings, and other audio platforms. Users can easily upload the files or use Ring By Name's API to integrate the personalized recordings into their communication systems.

By using artificial intelligence to analyze the communication with the client, the system makes recommendations on the next steps for clients and identifies those that might be selling sooner rather than later.

The benefits of Ring By Name's services are significant. Accurate name pronunciations contribute to professional and personalized communication, helping individuals and businesses establish rapport, respect, and a positive impression. It ensures that names are pronounced correctly, avoiding potential embarrassment or miscommunication. **PPT Slide 134**

Student Notes



Presents:



Copyright Information for Cons, Scams and Hacks

Under United States Copyright Law, Section 107, the doctrine of fair use permits the limited use of copyrighted materials without obtaining permission from the copyright owner for purposes such as criticism, comment, new reporting, teaching, scholarship or research. The application of fair use depends on a case-by-case analysis, considering the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use upon the potential market for the copyrighted work.

All materials used in this course including photographs, video or otherwise are for educational purposes only.

If you have questions or concerns regarding the fair use of copyrighted materials in this course, please contact the author, Brian Pate at brian@paterealty.com.



Presents:

Cons, Scams & Hacks

Protecting Clients in an Internet World



Written by Brian Pate
Copyright 2023 Brian Pate Seminars