2020-2021 General Update Course

Section Three
Cybersecurity

FOR DISCUSSION

1. Kristi, a broker with ABC Realty, is updating documentation in a transaction file while at a local coffee shop. Kristi uses the public Wi-Fi and sends her client a reminder via email to sign the engagement letter for the closing attorney's office. Because Kristi has worked with the attorney previously, she has a copy of the attorney's wiring instructions, so she attaches a copy of the wiring instructions in the email to her client.

   What did Kristi do wrong? ______________________________________

2. Sandra, a broker with Houz Realty, uses her smartphone to access transaction files and client information. One day while Sandra is searching for listings, a text message pops up, with a link to set up delivery preferences for a package. Sandra does not remember ordering a package, but she clicks on the link anyway.

   Has Sandra compromised the information of her clients?

   ____

3. Joe, a BIC with Farm Realty, answers a call one day. He receives an unfamiliar call from Tom, who claims to be a representative with the firm's cloud storage provider, Documents R' Us. Tom informs Joe of a new upgrade, and during the conversation Joe states that the firm is not paying for an additional service. Tom convinces Joe that the upgrade is needed and free. Joe then provides his email address, receives an email with a link, and clicks on it.

   What, if anything, has Joe done wrong?

   ____

LEARNING OBJECTIVES

By the end of this section, you should be able to:

- describe common types of cybersecurity attacks in real estate transactions;
- list best practices for brokers to prevent wire fraud, and
- describe fraudulent activities that have become more prevalent during the COVID-19 pandemic.

TERMINOLOGY

The following definitions are provided by the Cybersecurity and Infrastructure Security Agency (CISA).

- Cybersecurity: The art of protecting network, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality and integrity, and availability of information.
- Malware: Software designed to steal sensitive information, and/or gain access to private computer systems.
- Ransomware: A type of malicious software or malware designed to deny access to a computer system or data until a ransom is paid.

The division of the Department of Justice / FBI that tracks and investigates computer crime is IC3

Report
Internet Crime
to the FBI
www.ic3.gov
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FEDERAL BUREAU OF INVESTIGATION
INTERNET CRIME COMPLAINT CENTER
IC3
INTERNET CRIME COMPLAINT CENTER

TYPES OF CYBERSECURITY ATTACKS

Business Email Compromise/Email Account Compromise (*BEC/EAC)*

According to the Internet Crime Complaint Center (hereafter known as IC3), business email compromise/email account compromise (hereafter known as BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

Following is a common fact scenario for BEC/EAC scams in real estate transactions:

1. Unbeknownst to the account holder, the email account of an individual in the transaction is hacked (broker, attorney, mortgage representative, buyer, or seller).
2. The hacker monitors email communications for transaction details such as closing costs, property location, and/or funds to be wired.
3. The hacker creates and sends a "spoof" email with instructions for the wire transfer on behalf of the attorney or broker to the buyer or seller. The hacker's email address and the style of the email closely resembles that of the original account holder, so the recipient is unlikely to realize it is not an authentic communication.

Also, it is important to note that this scam is not always associated with a transfer of funds request. Business emails can also be compromised to gain access to an employees' Personal Identifiable Information or Wage and Tax Statement (W-2) forms according to IC3.

⚠ BIC ALERT: BICs should consider specifying in their office policy the types of email accounts that are permissible for brokers to use (e.g. free email accounts, firm email accounts, encrypted emails) to help prevent their email from being compromised.

Case Analysis: A Business Email Compromise

- The buyers entered into a contract to buy a property for $180,000 and did not intend to obtain mortgage financing to purchase the property. The buyers indicated their closing date would be in two weeks.
- A hacker obtained the name of an employee at the closing attorney's office and created a fake email address for the employee.
- The email contained a misspelled word and utilized a public email account (e.g. samm@gmail.com).

- The hacker sent an email masquerading as the attorney's employee to the buyer's agent asking for the buyer's email address.
- The buyer's agent responded to the hacker with the email address of the buyers and asked to reschedule the closing for ten calendar days later.
- The hacker responded to the buyer's agent and confirmed the new closing date and asked when they would receive the down payment from the buyers.
- The buyer's agent forwarded the email to the buyers. The email did not include any wire fraud verbiage or warning.
- The hacker sent an email directly to the buyers asking if they received the new wiring instructions and for them to wire the funds to escrow immediately.
- The buyers responded to the email from the hacker inquiring about the new instructions.
- The hacker responded to the email with an attachment that included the new wiring instructions and the amount to be escrowed of $175,854.30.
- The buyers made two wire transfers to the account specified in the hacker's wiring instructions.
- The wire fraud was not discovered until a couple of weeks later when recovery of the money was not possible.

Based upon the facts, what could the buyer's agent have done differently to better protect the buyers?

____

____

____

____

What could the buyers have done differently?

____

____

Brokers should continuously remind clients about wire fraud and potential scams even though wire fraud information is included in various contract forms.

Cloud Storage Attacks

How do you store transaction files and documents for brokerage activities? Do you store this information in a cloud? As brokers conduct more real estate transactions virtually, the importance of ensuring the security of transaction files and personal data may require additional safety protocols.

Therefore, cloud data storage providers allow brokers and brokerage firms to secure their data, collaborate more effectively with others, and access information with convenience from a variety of locations. However, cloud storage providers are susceptible to cyber-attacks just like any other individual or business. According to Virtua, a data protection solutions company, hackers may attack cloud storage providers by retrieving the passwords of users or the security tokens of the computer.

Brokers who use the “cloud” for storage should implement the following practices to minimize the likelihood of a cyber-attack on their cloud storage:

- create a unique password with a mixture of letters, special characters, and numbers (e.g. 20 or more characters represent a strong password);
- change the password frequently;
- clear caches regularly;
- refrain from saving passwords on your computer;
- disable automatic synchronization of data; and
- encrypt files.

Although cloud providers have a responsibility to safeguard the information of its customers, brokers are obligated to secure transaction files as well. If there is a breach which leads to a potential loss suffered by a client, a broker may be held liable.

⚠ BIC ALERT: BICs should consider implementing “best practices” to prevent a cyber-attack in their office policies. Additionally, in cases of a breach, recovery protocols should be addressed.

Malware

According to the Cybersecurity Infrastructure Security Agency (hereafter known as CISA), malware is software that disrupts service, steals sensitive information and gains access to private computer systems. The most commonly used malware is spyware or Trojans. Hackers utilize this type of software to retrieve financial information, personal information (e.g. social security number, credit card number), and client data.

Historically, malware has been delivered via phishing emails. Phishing emails are used by hackers to trick you into giving them personal, confidential information. According to the Federal Trade Commission, the emails resemble emails from trusted sources; however, they usually:

- have incorrect grammar, punctuation;
- indicate a problem with your account;
- insist that you take immediate action to verify an account;
- include a fake invoice;
- offer free merchandise or a coupon; or
- inform you to click on a link to make a payment.

Ransomware

According to CISA, ransomware is a type of malicious software or malware designed to deny access to a computer system or data until a ransom is paid. It is usually disseminated in a link within an email or disguised as an attachment. Once the link or attachment is clicked, the device and/or network is infected with ransomware.

The Federal Bureau of Investigation (hereafter known as the FBI), states that cybercriminals are becoming more sophisticated and are sending legitimate websites with malicious codes or phishing emails.

Once the infection occurs, the malware encrypts the files, attached drives, and other computers on the network. This attack will lead to inaccessible data and a request for a ransom payment in exchange for a decryption key to retrieve lost data.

The FBI does not support paying a ransom due to the probability that a decryption key may not be received. Some of the following tips are recommended by the FBI to prevent ransomware attacks:

- educate employees on ransomware attacks;
- install anti-virus and anti-malware software; and
- back up data regularly.

Crypto-Jacking

Have you ever noticed that your computer is performing poorly, for example, operating slowly or overheating for no reason? If so, your computer may be infected with malware that runs unknowingly in the background. An example of this type of malware attack is crypto-jacking.

Crypto-jacking is a popular alternative to ransomware attacks because hackers can make more money with less risk of exposure. Crypto-jacking occurs when:

- victims receive a legitimate looking email that encourages them to click on a link; or
- hackers inject a code on a website.

Whatever method hackers use to distribute the code, once the code is enabled, it runs in the background on the victim's computer while it is in use. The hacker uses the victim's computer only as a hub to perform illegal activities and does not steal any of the victim's information. Therefore, this type of cyber-attack will not be obvious. A pop-up window will not appear nor will files be held hostage or lost. An individual who has been a victim of crypto-jacking will experience a computer than operates differently and more slowly.

Brokers can protect the operating systems of their computers by:

- scanning for malware;
- monitoring computer usage;
- using ad blockers to block malicious codes in online advertisements;
- closing out browsers after each use; and
- not clicking on ads or links without verification.

Smishing

Brokers communicate with a multitude of individuals daily who never become their clients or parties in a transaction. Therefore, brokers should exercise extreme caution when receiving text messages, links, or attachments from unknown sources.

One type of scam that brokers could experience is smishing. Smishing is similar to phishing scams that are sent via email. It involves links or attachments being sent via text and occurs when hackers use mobile devices such as tablets and phones, to gain access to confidential information.

Tech Support Scams

On a daily basis, brokers are filtering through emails, text messages, and answering phone calls. This activity makes brokers susceptible to tech support scams.

Tech support scams are conducted by scammers who call and pretend to be a computer technician from a well-known company. The scammers indicate that a problem has been found with your computer and often ask for remote access to run a fictitious diagnostic test. Additionally, the scammers insist on receiving payment to fix a problem that does not exist.

Also, the scammers may use pop-up windows that indicate an error has occurred with your operating system or antivirus software. A telephone number is usually included in the pop-up and individuals are instructed to call the number to receive technical assistance.

Brokers should be aware that legitimate technical support companies will not display a pop-up warning asking you to contact them about potential viruses or security problems.

In an effort to prevent technical support scams, brokers should:

- keep security software up-to-date;
- contact a trusted computer technician;
- not allow anyone control of their computer;
- not click links or attachments; and
- not provide their bank or credit card information over the telephone.

⚠ BIC ALERT: BICs should indicate in their firm policies who is authorized to make changes to services rendered by vendors.

BEST TIPS FOR PREVENTING WIRE FRAUD

Cybersecurity attacks and wire fraud are prevalent in brokerage transactions due to the nature of the business. The following are best practices as indicated by Old Republic Title, a title insurance company, for preventing wire fraud:

- secure devices and accounts (authenticate, encrypt, use strong passwords);
- be vigilant about educating brokers and clients about cybersecurity and wire transfer protocols;
- utilize cashier checks (cashier checks can be verified with the bank prior to funding);
- know the company's wire fraud policies and procedures;
- read all emails cautiously and slowly (analyze requests, check and verify sender's email address, use forward instead of reply);
- be suspicious of changes to wiring instructions; and
- remind clients to review wire fraud disclaimers.

The North Carolina Bar Association has provided guidance to attorneys that is also beneficial to brokers. They recommend the following to prevent fake wiring instruction scams:

- don't allow changes in disbursement methods to be made via email;
- confirm all wiring instructions with a phone call to a trusted number and initiate the call;
- confirm email addresses and encrypt all sensitive information; and
- require multiple people to review wiring instructions before sending wire transfers.

The North Carolina Bar Association's video can be accessed by clicking here: https://www.youtube.com/watch?v=mgI_QX1oK6E&feature=youtu.be&utm_source=Wiring+Instructions+Alert&utm_campaign=WiringInstructionsAlert&utm_medium=email

Additionally, the National Association of Realtors® provides a plethora of resources to ensure that brokers are equipped with the knowledge to prevent wire fraud and to educate their clients of its prevalence as well.

A wire fraud video developed by the National Association of Realtors® can be accessed here: https://www.youtube.com/watch?v=amPQEO1n1rM

COVID-19 and FRAUD

On April 8, 2020, the United States Department of Homeland Security (hereafter known as DHS), Cybersecurity and Infrastructure Security Agency (CISA), and the United Kingdom's National Cyber Security Centre (hereafter known as NSCC) issued an alert entitled, COVID-19 Exploited by Malicious Cyber Actors, AA20-099A.

The alert provides information regarding the types of cyberattacks that have occurred due to the COVID-19 global pandemic. Cyber criminals are conducting COVID-19 related scams by sending phishing emails and malware that use COVID-19 as a common theme. Additionally, due to the increase in curiosity that has occurred due to the pandemic, hackers are able to use social engineering to gain access to data, devices, and personal information.

Brokers should be aware of the following attacks specifically related to COVID-19:

- phishing emails that include an email subject line referencing COVID-19;
- smishing messages that request demographic information to receive governmental support or financial assistance; and
- exploitation of VPN's (Virtual Private Network) and remote access desktop programs by sending malicious files via email.

The NSCC has identified four red flags that can assist a broker in determining whether an email is phishing. The red flags are an email that:

- has an authoritative tone commanding an action;
- has an urgency with a timeline to complete the requested action;
- provokes emotions such as anxiety or nervousness if the action is not completed in a timely manner; or
- indicates that a product is scarce or in short supply.

Brokers have adapted their brokerage services to meet the needs of clients by offering virtual showings, teleconferences, and assisting them with scheduling virtual settlement conferences. On March 30, 2020, the Federal Bureau of Investigation (FBI) issued a press release entitled, FBI Warns of Teleconferencing and Online Classroom Hijacking during COVID-19 Pandemic.

The press release provided the following tips to prevent the hijacking of online meetings:

- create passwords for meetings and use a "virtual" waiting room to control the admittance of guests;
- do not share meeting room links on unrestricted, public social media posts;
- ensure screen sharing options are disabled and provide for "Host Only";
- ensure that current versions of the teleconferencing tools are employed; and
- implement telework polices that specify requirements for physical and information security.

Real estate transactions are still occurring during this pandemic and cybercriminals are still hacking business email accounts, sending phishing emails, and smishing messages to obtain confidential information for financial gain.

Old Republic Title has created a wire fraud prevention drill that can be used by any party in a real estate transaction to help prevent fraudulent activity especially during times of crisis such as COVID-19. The drill consists of three important steps:

STOP: Upon receiving a call with potential wiring instructions, hang up and tell the caller you will verify the information. If you receive an email or text message with wiring instructions, do not reply.

CALL: In an effort to make sure that the request you receive is legitimate, call a trusted, approved telephone number used in the past to contact individuals involved in the transaction or on the contract. Refrain from using telephone numbers given over the phone, in an email or text sent to you.

VERIFY: After calling the trusted number, speak with the person that allegedly called, emailed, or texted you to verify that the changes to the instructions are legitimate.

WAIT BEFORE YOU WIRE
WHAT YOU NEED TO KNOW
Hackers are targeting Real Estate Agents, Title Companies and others within the industry
Fraudulent wire instructions are being sent to Real Estate Agents, Title Agencies and Customers
Consumers are losing money
Wire fraud incidences are rising
WHAT YOU NEED TO DO
COMMUNICATE
Educate your customers to ALWAYS verify wire instructions BY PHONE BEFORE wiring
Use only KNOWN contact information. DON'T use the phone #'s in an email or hit "reply"
Be ESPECIALLY SUSPICIOUS of emails that change wiring instructions
PROTECT YOURSELF
Understand phishing and whaling
Verify email before clicking on link
Use strong passwords & change often
Use a sophisticated email provider and enable 2 factor authentication
Don't keep old emails past date needed
WHAT TO DO IF YOU THINK YOU'RE HACKED
IMMEDIATELY ASK SELLER TO VERIFY IF FUNDS WERE RECEIVED, IF NOT...
AND MONEY WAS WIRED TO A HACKER'S ACCOUNT
NOTIFY
the bank's security department ASAP!
LOCAL POLICE
LOCAL FBI &
FBI Internet
FBI
CONSULT YOUR ATTORNEY regarding data breach laws & notice requirements
CHANGE passwords

Brokers have a duty to receive education on the prevention of wire fraud and inform their clients of potential threats.

BICs should ensure brokers have access to adequate resources to prevent wire fraud and educate clients. Most importantly, protocols should be specified to assist brokers in reporting the fraud and possibly assist in the recovery of the lost funds.

ANSWERS TO DISCUSSION QUESTION

For Discussion on page 45:

1. Kristi, a broker with ABC Realty, is updating documentation in a transaction file while at a local coffee shop. Kristi uses the public Wi-Fi and sends her client a reminder via email to sign the engagement letter for the closing attorney's office. Because Kristi has worked with the attorney previously, she has a copy of the attorney's wiring instructions, so she attaches a copy of the wiring instructions in the email to her client.

   What did Kristi do wrong?
   Answer: Kristi should not use a public Wi-Fi to send personal, confidential information to clients. In addition, Kristi should not send wiring instructions to her client. Wiring instructions and protocols should be communicated directly to the client by the attorney's office and not via the broker.

2. Sandra, a broker with Houz Realty, uses her smartphone to access transaction files and client information. One day while Sandra is searching for listings, a text message pops up, with a link to set up delivery preferences for a package. Sandra does not remember ordering a package, but she clicks on the link anyway.

   Has Sandra compromised the information of her clients?
   Answer: Probably. Sandra should not click on links from unverified sources due to the potential of being hacked and client data being lost or stolen.

3. Joe, a BIC with Farm Realty, answers a call one day. He receives an unfamiliar call from Tom, who claims to be a representative with the firm's cloud storage provider, Documents R' Us. Tom informs Joe of a new upgrade, and during the conversation Joe states that the firm is not paying for an additional service. Tom convinces Joe that the upgrade is needed and free. Joe then provides his email address, receives an email with a link, and clicks on it.

   What, if anything, has Joe done wrong?
   Answer: Yes, Joe should not have given his email address to an unverified individual/company. Also, Joe should have verified the information from the representative by calling the company before providing his email address. In addition, Joe should not have clicked on any links from an unverified source.

Case Analysis on pages 47-48:

Based upon the facts, what could the buyer's agent have done differently to better protect the buyers?

> The buyer's agent should have called the attorney's office to question / verify the change in instructions. Also, the buyer's agent should have provided the buyers some information / education regarding potential risks of and best practices for wire transfers.

What could the buyers have done differently?

> The buyer's agent should have called the broker and/or attorney's office to question / verify the change in instructions.