Key measures to protect your online identity.

- **Use Updated Antivirus Software**: Ensure that you have reliable antivirus software installed on all your devices. Keep the software up-to-date and run regular scans to detect and remove any malware or viruses. This practice also includes keeping virus definitions current to protect against the latest threats.
- **Keep Work Devices and Home/Family Devices Separate**: Use dedicated devices for work-related activities and separate devices for personal or family use. This reduces the risk of cross-contamination from malware or unauthorized access. It also helps maintain a clear boundary between professional and personal information, enhancing security and privacy for both.
- **Use Strong, Unique Passwords**: Create passwords that are long (at least 12 characters), combining uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like names or birthdates.
- **Activate Multi-Factor Authentication (MFA)**: Enable MFA on all accounts. This typically involves a second form of verification, such as a code sent to your phone or an authentication app, adding an extra layer of security.
- **Regularly Update Passwords**: Change passwords periodically and immediately update them if you suspect any account has been compromised.
- **Avoid Reusing Passwords**: Use a different password for each account to ensure that a breach on one platform doesn't compromise others.
- **Use a Password Manager**: Implement a reputable password manager to securely store and generate complex passwords, reducing the risk of forgetting them or using weak ones.
- **Enable Account Alerts**: Set up notifications for any unusual activity or login attempts on your accounts to stay informed about potential security breaches in real time.
- **Be Cautious with Phishing**: Stay vigilant against phishing attacks by not clicking on suspicious links or opening attachments from unknown senders. Verify the legitimacy of requests for personal information.
- **Regularly Update Software**: Keep all devices and software, including email clients and browsers, updated to protect against known vulnerabilities and exploits.
- **Secure Wi-Fi Networks**: Ensure your home and office Wi-Fi networks are secure by using strong passwords and encryption protocols (such as WPA3). Avoid using public Wi-Fi for sensitive transactions.
- **Backup Important Data**: Regularly back up important data to a secure, offline location. This ensures you can recover information in case of a ransomware attack or other data loss incident.
- **Use Encrypted Email Services**: Choose email providers that offer end-to-end encryption to ensure your communications are secure and cannot be easily intercepted by hackers.
- **Regularly Review Account Permissions**: Periodically check which apps and services have access to your email and other accounts. Revoke access for those you no longer use or recognize.
- **Educate Yourself on Social Engineering Tactics**: Learn about common social engineering tactics such as pretexting, baiting, and scareware so you can recognize and avoid falling victim to them.
- **Secure Your Devices**: Ensure all your devices (phones, tablets, computers) have security measures such as biometric locks (fingerprint or facial recognition), strong passwords, and are set to lock automatically after a short period of inactivity.
- **Implement Email Filtering**: Use advanced email filtering tools to help identify and block phishing attempts and spam before they reach your inbox, reducing the risk of accidentally clicking on malicious links.

SECURITY WARNING

Urgent Wire Fraud Warning!

Beware of Cyber Criminals Exploiting Real Estate Transactions!

Cyber criminals are actively exploiting real estate transactions! Fraudsters employ email compromise schemes to impersonate attorneys, realtors, lenders, and title companies, utilizing pirated accounts and deceptive practices to steal your money through fraudulent wire transfers.

CYBER CRIME

At Backman Title Services, we prioritize the security of your transactions. Before initiating a wire transfer, we will provide you with written instructions during our in-person settlement/closing. Note that these instructions won't change, and we will never request funds in an account under a different name.

If you receive conflicting wire instructions, ***STOP IMMEDIATELY*** and contact us using a known phone number—not a phone number provided in a potentially fraudulent email or text. We won't communicate changes to wire instructions via email.

BEWARE OF CYBER-CRIME!

All real estate transaction parties face wire fraud risks. Safeguard transactions with these recommendations:

SECURITY

1. **CHECK EMAIL SENDER:** Email communication from Backman Title comes from our domain (backmantitle.com) and never from public email domains (e.g., Gmail, Yahoo, MSN). Always watch for modified and misspelled domains.
2. **VERIFY INSTRUCTIONS:** Backman Title operates branches in Utah; we don't have out-of-state locations or accounts. Call Backman Title Services independently to confirm wire instructions. Avoid using email-provided phone numbers.
3. **NO CHANGES TO OUR INSTRUCTIONS:** Be cautious of claims about changes; suspect fraud if instructions conflict. Contact us or your Real Estate Agent.
4. **CONFIRM ACCOUNT NAMES:** Our Trust Accounts will ALWAYS be under the name of Backman Title Services Trust Account. If the instructions you received are any variation of that account name, they should be considered fraudulent.
5. **VERIFY FUNDS RECEIPT:** ***IMMEDIATELY*** after sending funds, contact us to confirm receipt. Always use trusted numbers; avoid clicking links in emails.

Backman Title Services

Backman Title is not responsible for money sent to an incorrect account by you.

Only your diligence can prevent wire fraud and other criminal activities and your attention is crucial!

If you have any concerns or questions, do not hesitate to reach out to us using verified contact information.

Backman Title Services

Wire Fraud Rapid Response Checklist

What to do when you find out a client has received fake wire instructions & cyber criminals are stealing money.

Time is of the essence – act fast!

1. **Alert other stakeholders - Inform the parties to the transaction (buyer, seller, real estate agents, loan officer/broker, split title company etc.)**
   - **By phone** using known, trusted, phone numbers for verbal verification.

     If you're unsure about what to say, here's a sample: *"There appears to have been [attempted] wire fraud associated with this transaction. We recommend that you review your email security and update passwords and take any other appropriate security measures immediately. For the remainder of this transaction, all communication will occur using known, trusted, telephone numbers."*
   - **By email**, here is sample email:

     Subject; Warning - Wire Fraud!

     Everyone;

     We have been notified that cyber criminals have compromised this transaction; they are reading emails, and they are trying to steal money.

     1- Forward this warning email to everyone involved in this real estate transaction.

     2- Ask everyone to be vigilant and proceed with EXTREME CAUTION.

     3- Do not wire transfer any money until you have called the recipient, using a known telephone number, not one provided in an email and verified the recipients wire transfer information and the wire transfer amount.
2. **Contact Banks - Sending and Receiving Banks (Coordinate quickly!)**
   - Your client will need to contact their bank themselves, but you have helpful information to share, too.
   - Your client must contact the credit union or bank's fraud department and request a recall of the wire be sent to the receiving bank because of fraud. Help them remember to have the details of the fraudulent instructions and provide those details.
   - Ask the sending credit union or bank to initiate the FBI's Financial Fraud Kill Chain.
   - They can call the receiving bank's fraud department to notify them that you have requested a recall of the wire because of fraud. Provide the details for the wire and request that the account be frozen.
3. **Instruct the victim to send Backman a copy of the fraudulent email and wire transfer instructions.**
   - To allow analysis of the fraudulent email's header and metadata, the recipient of the suspicious message should create a new email and send the email they received as an attachment. The client can save original email using the "Save As" or "Download" option in their email client. The saved email, containing the necessary information, can then be attached to the fresh message. This allows us to conduct a comprehensive analysis and helps formulate an effective response against the cyber threat.

Backman Title Services

Protecting Against Wire Fraud in Real Estate Transactions: A Vital Alert for Real Estate Agents

Remain Vigilant and Proactive

According to the FBI's 2022 report, victims of business email compromise reported staggering losses exceeding **$2.7 BILLION**. The Internet Crime Complaint Center (IC3) receives **over 2,175 COMPLAINTS PER DAY**

Warning: Fraudulent Wiring Instructions

1. Beware of Web-based Email Accounts: Exercise caution with free, web-based email accounts, as they are susceptible to hacking.
2. Always Verify Payment Instructions: Confirm any changes in payment instructions and validate requests for fund transfers.
3. Beware of Requests for Secrecy or Urgency: Use caution with requests for secrecy or using high pressure tactics.
4. Call, Don't Email: Confirm all wiring instructions via phone before transferring funds, using the phone number from the title company's official website or business card.
5. Be Suspicious of Changes: Title companies rarely alter wiring instructions and payment information. Be wary of unexpected changes.
6. Confirm All Details: Ask your bank to confirm not only the account number but also the name on the account before initiating a wire transfer.
7. Immediate Verification: Call the title company or real estate agent immediately to validate the receipt of funds, especially within the first 2 hours.
8. Forward, Don't Reply: When responding to emails, hit forward instead of reply, and manually type in the recipient's email address to avoid falling victim to fraudulent addresses.

If You Suspect You Might Be a Victim

1- Use a known phone number to call the supposed sender for authentication. 2- Notify financial institutions and escrow agents involved in the transaction immediately. 3- Contact local law enforcement and file a complaint with the FBI's Internet Crime Complaint Center.

Additional Tips to Recognize and Combat Wire Fraud

- Be wary of changes to wire instructions, especially regarding language, timing, or amounts.
- Implement additional callback procedures using a known, independently verified telephone number.
- Exercise caution with instructions marked as rush, urgent, or secret.
- SWIFT codes are typical for international accounts, not domestic bank or credit union accounts
- Treat email instructions, especially late in the transaction, with suspicion.
- Avoid wiring funds to unknown, new, or foreign banks.
- Question instructions with unusual explanations, such as overfunding due to uncertain international exchange rates.

Backman Title Services

Protecting Against Email Compromise: A Vital Alert for Real Estate Agents

Identifying Suspicious Emails

1. Bad Grammar and Spelling: Be wary of misspellings and poorly translated content, as these are common indicators of phishing attempts.
2. Email Format and Logos: Legitimate emails often use HTML, featuring a mix of text and images, including the company's logo. Plain text emails or those lacking images, especially without the company logo, may be signs of illegitimate correspondence.
3. Urgent Requests: Exercise caution when faced with urgent requests for personal information, such as Social Security numbers or bank details. Verify the legitimacy of the request before taking any action.
4. Suspicious Attachments: Beware of high-risk attachment file types like .exe, .scr, .zip, .com, and .bat. - Verify the sender's legitimacy before opening attachments and scrutinize the context of why the attachment is being sent.
5. Links in the Email: Hover over links before clicking to ensure they match the preview provided by your email platform. If in doubt, open a new browser window and type the URL directly into the address bar.
6. Work Email Usage: Reserve your work email for professional purposes only; avoid using it for personal signups on social media or loyalty programs.

Additional Security Measures

1. Review Account Settings: Periodically check your Sent folder to ensure emails aren't being sent without your knowledge. Be vigilant against compromised email accounts.
2. Recognizing Red Flags: Pay attention to generic greetings, unusual urgency, offers that seem too good to be true, and poor grammar.
3. Be cautious of emails asking you to click hyperlinks.
4. Verify domain names to prevent falling victim to spoofed emails.
5. Header Analysis: Utilize a header analyzer if you suspect the From: address is fraudulent to verify the sender's identity.

Alerts of Account Compromise:

1. Investigate if customers or colleagues report receiving "spam" messages from your account.
2. Take immediate action if you receive replies to emails you didn't send or notice unusual account settings.

Utah Association of REALTORS®
REALTOR®

EQUAL HOUSING OPPORTUNITY

WIRE FRAUD ALERT DISCLOSURE

This is a legally binding document. If not understood, consult an attorney.

THIS WIRE FRAUD ALERT DISCLOSURE is provided by _____(the "Company") Including _____(the "Agent") to _____ _____ (the "Buyer or Seller') in connection with the purchase of any property.

WARNING NOTICE: There are instances where cyber criminals are hacking the email accounts of parties involved in a real estate transaction and are sending emails with fake wiring instructions. These emails look convincing and legitimate. **Never trust wiring instructions sent via email**. You must **always** confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. **Never** wire money without double-checking that the wiring instructions are correct.

In every real estate transaction, the Buyer or Seller is advised to:

1) **Never** trust wiring instructions sent via email.

2) **Never** send personal information such as social security numbers, bank account numbers and credit card numbers, unless it is through secured/encrypted email or personal delivery to the intended recipient.

3) **Never** click on attachments or links from unfamiliar sources. These attachments or links may contain malware that may allow a hacker to access your emails, accounts, and any other information on your computer.

4) **Always** independently confirm wiring instructions by personally speaking with the intended recipient of the wire to confirm the routing number and account number.

5) **Always** confirm that the contact information for the wire transfer recipient is legitimate. Call a verified number.

6) **Always** take steps to secure the system you are using with your email account such as using strong passwords and secure WiFi.

RECEIPT AND ACKNOWLEDGEMENT OF BUYER

By signing below, I acknowledge that I have read and understand and have received a copy of this WIRE FRAUD ALERT DISCLOSURE. If I believe that I have received suspicious wire transfer instructions, I should immediately notify my lender, title agent, and REALTOR®. Also, I understand that I should immediately report suspicious wire transfer instructions to Salt Lake City FBI field office at (801) 579-1400 or file a complaint at www.ic3.gov. For additional information, please refer to the following links:
Federal Bureau of Investigation: http://www.fbi.gov
National White Collar Crime Center: http://www.nw3c.org
On Guard Online: http://www.onguardonline.gov

_____ _____
Buyer or Seller Signature Date Buyer or Seller Signature Date

The Forensics *of* Wire Fraud

Language Fingerprints

Language fingerprints can be found in emails, letters, transaction documents, wire instructions, and payoff statements.

Knowing what words fraudsters use and how they use them can help you spot and stop a crime happening right before your eyes.

FRAUDSTER LEXICON

Certain words – or types of words – are used frequently by fraudsters to manipulate you into doing what they want. If you spot the fraudster's lexicon, please STOP to review the transaction as a whole, and consider you may be dealing with a fraudster.

"KINDLY"

The #1 word used by fraudsters is "kindly." Most cybercrime is committed by overseas fraudsters where this word is part of their vernacular instead of the word "please." If someone uses the word "kindly" or uses it repeatedly in one communication, chances are you are communicating with a fraudster.

WORDS INDICATING FRIENDSHIP

Words of friendship convey familiarity, trust, and can include someone being overly complimentary about your role in the transaction. The fraudsters use this technique to lower your guard by playing on your ego's desire to be liked. You are more likely to go the extra mile for a "friend" or "pal" and overlook discrepancies and red flags for people you like and trust.

Tucker Hodgson
Backman Title Services, LTD
8012957676
thodgson@backmantitle.com

Language Fingerprints

RISK WORDS

Risk words imply a possible negative action or outcome to you personally and, at their core, are a latent threat to your financial security, invoking a fear response. Risk words including "concern," "prevent," "failure," and "avoid" all imply there are consequences to not following the request.

NEGATIVE WORDS

Any instruction you receive that tells says you "must not," "shall not," "never," or "do not do [something]" is a red flag. Consider what they are instructing you not to do and if it makes sense in the transaction. Do they not want you to verify something, call or email someone specific, or not use a telephone or email address you previously used throughout the transaction?

GOD OR RELIGION-TYPE WORDS

Culturally, words with religious overtones are not used in real estate transactions in the United States, but that isn't necessarily the case in foreign countries. If someone refers to God or uses other words with religious overtones in an email or any written communication, consider a fraudster from a country where that is acceptable or even expected in a business transaction may be impersonating a party.

FRAUDSTER GRAMMAR

Since most cybercrime originates from overseas, the fraudster may have a poor command of the English language and grammar. Communications or instructions that contain any of the following grammatical errors are a red flag for fraud:

- Missed punctuation
- Misuse of punctuation
- Misspelled words
- Incorrect spacing or formatting
- Capitalization errors
- Improper syntax
- Improper verb usage
- Improper verb tense usage

STOP.

THINK. VERIFY.

ALWAYS carefully compare updated payoff statements with the original, and be suspect of last-minute changes in wire instructions.

If you suspect fraudulent activity, escalate to your local First American policy-issuing title agent for additional review. Wire and other disbursement instructions received by email should be confirmed by phone, using a known or confirmed number.

WIRE INSTRUCTIONS

Wire instructions and payoff statements can contain language fingerprints too! Be on the lookout for:

- Different font or type size from the rest of the document
- Sender's location shown on a faxed document does not match party's purported location
- Payoff amount differs from a previously received payoff statement, or calculation of payoff amount doesn't add up
- Receiving bank does not match payoff statement bank
- Beneficiary's name on the account differs from party or lender
- Address or phone number listed in the statement is different than contact information that is independently verified
- Email address is different or contains variations
- Rush requests or sense of urgency
- Wire is going to a bank in a country outside of US or different from where the party is located

AMD: 07/2022

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

FRAUDSTERS are impersonating property owners to illegally sell commercial or residential property. Sophisticated fraudsters are using the real property owner's Social Security and driver's license numbers in the transaction, as well as legitimate notary credentials, which may be applied without the notary's knowledge.

Fraudsters prefer to use email and text messages to communicate, allowing them to mask themselves and commit crime from anywhere.

Due to the types of property being targeted, it can take months or years for the actual property owner to discover the fraud. Property monitoring services offered by county recorder's offices are helpful, especially if the fraud is discovered prior to the transfer of money.

Where approved by state regulators, consumers can purchase the American Land Title Association (ALTA) Homeowner's Policy of Title Insurance for additional fraud protection.

WATCH FOR RED FLAGS

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A PROPERTY

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property
- Has a different address than the owner's address or tax mailing address
- Has no outstanding mortgage or liens
- Is for sale or sold below market value

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A SELLER

- Wants a quick sale, generally in less than three weeks, and may not negotiate fees
- Wants a cash buyer
- Is refusing to attend the signing and claims to be out of state or country
- Is difficult to reach via phone and only wants to communicate by text or email, or refuses to meet via video call
- Demands proceeds be wired
- Refuses or is unable to complete multifactor authentication or identity verification
- Wants to use their own notary

SHUTTERSTOCK / TANYA ANTUSENOK

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

AMERICAN LAND TITLE ASSOCIATION

TAKE PRECAUTIONS

CONTACT SELLER USING INDEPENDENT SOURCES

- Contact the seller directly at an independently discovered and validated phone number
- Mail the seller at the address on tax records, property address, and grantee address (if different)
- Ask the real estate agent if they have personal or verified knowledge of the seller's identity

MANAGE THE NOTARIZATION

- Require the notarization be performed by a vetted and approved remote online notary, if authorized in your state
- If remote online notarization is not available, the title company should select the notary. Examples include arranging for the seller to go to an attorney's office, title agency, or bank that utilizes a credential scanner or multifactor authentication to execute documents

VERIFY THE SELLER'S IDENTITY

- Send the seller a link to go through identity verification using a third-party service provider (credential analysis, KBA, etc.)
- Run the seller's email and phone number through a verification program
- Ask conversational questions to ascertain seller's knowledge of property information not readily available in public records
- Conduct additional due diligence as needed

USE THE PUBLIC RECORD

- Compare the seller's signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value

CONTROL THE DISBURSEMENT

- Use a wire verification service or confirm wire instructions match account details on seller's disbursement authorization form
- Require a copy of a voided check with a disbursement authorization form
- Require that a check be sent for seller proceeds rather than a wire

FILE FRAUD REPORTS

- IC3.gov
- Local law enforcement
- State law enforcement, including the state bureau of investigation and state attorney general
- Secretary of state for notary violations

FIGHT FRAUD WITH INDUSTRY PARTNERS

- Educate real estate professionals in your community, such as country recorders, real estate agents, real estate listing platforms, banks, and lenders
- Host educational events at the local or state level
- Alert your title insurance underwriter of fraud attempts

SHUTTERSTOCK / TANYA ANTUSENOK