REALTOR SECURITY: MASTER CHECKLIST

PROTECT YOUR ACCOUNTS

☐ Use a unique, long password for every work account; aim for 15+ characters when creating passwords (or use a randomly generated password).
☐ Use a brokerage-approved password manager; never reuse your email password.
☐ Enable MFA for email, brokerage systems, bank accounts, and cloud storage; prefer passkeys or security keys when available.
☐ Deny any unexpected sign-in approval; investigate unusual login alerts and review recovery methods.
☐ Check email forwarding rules, active sessions, connected apps, and account-recovery information.

SECURE YOUR DEVICES AND WORKSPACE

☐ Turn on automatic updates for Windows/macOS, phones, browsers, and apps; replace unsupported software.
☐ Keep built-in or approved antivirus/endpoint protection active and updated; investigate warnings promptly.
☐ Use a device PIN/password, biometric unlock, short auto-lock, full-disk encryption, and device-finding/remote-wipe features.
☐ Separate work from shared family devices and accounts; use approved work profiles if a dedicated device is not possible.
☐ Protect home/office Wi-Fi with WPA2-AES or WPA3, updated router firmware, and a strong router administrator password.
☐ Back up important work data through approved systems; confirm that recovery/restoration works.

SAFEGUARD CLIENTS AND TRANSACTIONS

☐ Use an approved secure portal for IDs, Social Security numbers, tax returns, bank details, and other sensitive documents.
☐ Before sending, check the recipient, attachments, permissions, and whether the information is actually necessary.
☐ Treat unsolicited links, QR codes, password-reset requests, and voice messages as unverified—even with perfect grammar.
☐ Explain wire fraud early; independently call the title company using a trusted number before any wire is initiated.
☐ Escalate unusual seller identity circumstances, urgent requests, and any changed payment instructions before proceeding.

IF FRAUD IS SUSPECTED: STOP → CALL TRUSTED CONTACTS → CONTACT THE BANK → PRESERVE EVIDENCE → REPORT.

Do not wait to see whether a suspicious wire clears. For actual transfers, ask the originating bank's fraud department immediately for a recall and contact IC3.gov.

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.

This material is for educational purposes only and does not constitute legal advice. We assume no liability for errors or omissions. Backman Title Services LTD's underwriters are Old Republic National Title Insurance Company, First American Title Insurance Company, and Aliant National Title Company.

15-MINUTE SECURITY TUNE-UP

Start with the accounts and devices most likely to expose a client transaction.

FIRST 5 MINUTES — SECURE THE FRONT DOOR

☐ Open your email's Security settings. Confirm MFA is on; add a passkey/security key if offered.
☐ Check recent sign-in activity and remove unknown devices or sessions.
☐ Review account recovery email/phone and mailbox forwarding rules; report anything unfamiliar to IT.

NEXT 5 MINUTES — PROTECT YOUR DEVICES

☐ Windows 11: Settings → Windows Update; Windows Security → Virus & threat protection. Confirm protections and updates are active.
☐ Mac: System Settings → General → Software Update; Privacy & Security → FileVault.
☐ iPhone/iPad: Settings → General → Software Update; Face ID/Touch ID & Passcode; Find My.
☐ Android: Settings → Security & privacy and System → Software update (menu names vary); enable Find My Device.
☐ On every device: lock automatically, use a secure PIN/passcode, and do not share work sign-ins with family members.

FINAL 5 MINUTES — PREVENT REPEAT PROBLEMS

☐ Identify where your work passwords are kept. Switch reused passwords to unique ones stored in an approved manager.
☐ Bookmark official brokerage, title, lender, and banking login pages. Avoid search ads when signing in.
☐ Verify that documents are backed up in a company-approved, access-controlled location.

WHAT NEEDS A BROKERAGE OR IT DECISION?

Ask IT: Which password manager, cloud-storage portal, antivirus product, backup system, and incident-reporting channel are approved?
Personal devices: If your brokerage allows personal devices, use a managed work profile and never make the device available to others while logged into work accounts.
Wi-Fi: Use WPA3 or WPA2-AES, change default router admin credentials, update router firmware, and avoid sensitive work on an untrusted public connection.

KEEP CLIENT INFORMATION PRIVATE

The most useful rule: collect less, transmit securely, and verify before sharing.

WHERE SENSITIVE INFORMATION BELONGS

Use the approved secure portal: Government IDs, Social Security numbers, bank statements, tax returns, wire instructions, loan applications, and other sensitive records.
Avoid ordinary email and texting: Do not attach sensitive records to a conventional message or paste account numbers into a group text.
Use only approved storage: No personal cloud drives, family shared folders, personal email archives, or unnecessary local copies.

THE 10-SECOND "BEFORE YOU SEND" CHECK

☐ Am I sending only what this recipient needs?
☐ Is the address / number correct? Watch autofill and reply-all.
☐ Does the attachment contain hidden pages, signatures, account numbers, or unrelated client data?
☐ Does this link grant access only to the right person, for the right duration?
☐ Would a secure portal or a phone call be safer?

RECOGNIZE SOCIAL ENGINEERING — EVEN WHEN IT LOOKS POLISHED

☐ A familiar name or logo is not proof of who sent a message; an account may be compromised.
☐ An unexpected QR code can lead to a fake login page; preview the destination and navigate independently.
☐ A text, voice message, or video can be AI-generated; verify unusual instructions through an independently known channel.
☐ Never give anyone a one-time code or approve an MFA request you did not initiate.
☐ Pause at pressure tactics: "urgent," "confidential," "new account," "closing today," or "don't call."

IF YOUR EMAIL LOOKS COMPROMISED

Immediately: Report to brokerage IT/security; from a trusted device reset credentials, revoke unknown sessions and review forwarding rules, connected apps and recovery methods. Warn affected transaction partners by trusted phone numbers. Preserve relevant messages.

STOP WIRE FRAUD & SELLER IMPERSONATION

Use a repeatable verification process on EVERY transaction—not just suspicious ones.

TEACH EVERY BUYER THESE FOUR RULES

☐ Get wire instructions only through the process established directly with the title company.

☐ Before sending funds, call the title company at a number you independently confirmed earlier.

☐ Read back the receiving bank, beneficiary name, account/routing details, and amount with the authorized recipient.

☐ If instructions "change" or a new recipient appears, STOP. Do not use numbers or links in that message.

WHEN A SELLER OR PROPERTY NEEDS EXTRA SCRUTINY

Property flags: Vacant land, free-and-clear property, tax-mailing-address mismatch, unusual price, or an accelerated cash sale.

Seller flags: Won't speak by phone/video or appear for identification, communicates only electronically, presses for quick proceeds, or insists on an unapproved notary.

Next step: Call the title company early; independently verify seller contact details and coordinate enhanced identity/notary review. No single flag proves fraud.

EXAMPLE: AN APPARENT CHANGE OF WIRE INSTRUCTIONS

Message: "Our bank is having issues; please wire the buyer's funds to this new account immediately."

Agent response: Do not forward it as genuine or tell the buyer to act. Stop funding instructions, telephone a previously verified escrow contact, notify the brokerage, and preserve the original message.

REUSABLE CLIENT LANGUAGE

"Cybercriminals impersonate real estate professionals and sometimes enter an actual email conversation. Please do not wire money based only on an email or text. Before transferring funds, call the title company at the number we independently verified together. If anything changes, stop and call."

RAPID RESPONSE: MINUTES MATTER

Use this page when there is a suspicious message, compromised account, or fraudulent payment.

IF A FRAUDULENT WIRE WAS SENT: ACT IMMEDIATELY

1. Have the sender call the originating bank's FRAUD department immediately and request a recall or reversal; ask the bank about contacting the receiving bank and applicable indemnity/hold-harmless documentation.
2. Contact the escrow/title company and brokerage management through independently known phone numbers; pause disbursements and notify appropriate parties without spreading unverified claims.
3. Contact law enforcement promptly; submit a detailed report to the FBI Internet Crime Complaint Center at IC3.gov. A recent transfer may warrant contacting the local FBI field office.
4. Save original emails (with full headers), texts, wire confirmations, dates, amounts, account information and phone logs; preserve evidence through approved secure channels.
5. Continue coordinating with the bank, law enforcement, broker, escrow and appropriate insurer/underwriter. Document actions and times.

IF YOU CLICKED A LINK, SHARED A CODE, OR LOST YOUR DEVICE

☐ Stop using the suspicious site; report the incident to brokerage IT/security immediately.
☐ If credentials may be exposed, reset them from a trusted device and revoke sessions; report unexpected MFA approvals.
☐ If a device may have malware, follow IT instructions to isolate, investigate and restore it; do not erase potential evidence without guidance.
☐ Notify relevant transaction partners using independently trusted contact information if a transaction could be affected.

WHAT NOT TO DO

☐ Do not wait until tomorrow to contact the bank.
☐ Do not reply to the suspicious sender to "confirm" a payment change.
☐ Do not publicly email documents containing client identifiers or bank information as evidence.
☐ Do not promise recovered funds; a recall request is not a guarantee.

Official reporting: www.ic3.gov | FBI guidance: www.ic3.gov/CrimeInfo/BEC

UTAH TOOLS & CONTINUING HABITS

Useful resources and a simple monthly maintenance routine.

UTAH PROPERTY-RECORDING ALERTS

Invite clients to subscribe to their county recorder's official Property Watch / property-recording notification service where available. Alerts are notifications, not a substitute for title insurance or identity verification.

Salt Lake: https://slco.org/data-services/PropertyWatch/PropertyWatch.aspx
Utah: https://property-watch.utahcounty.gov/
Weber: https://www.webercountyutah.gov/forms/property_watch/
Davis: https://www.co.davis.ut.us/recorder/property-alert
Washington: https://www.washco.utah.gov/2021/11/04/sign-up-for-property-watch/
Cache: https://www.cachecounty.org/recorder/propertywatch/faq.html
Box Elder: https://erecord.boxeldercountyut.gov/eaglesoftware/eagleweb/fraudGuardSignup.jsp
Wasatch: https://kane.utah.gov/gov/dept/it/property-watch/

OTHER RESOURCES

- Check exposed email addresses: haveibeenpwned.com (a breach match is a signal to review passwords, not proof that an account is currently compromised).
- Report internet fraud: IC3.gov; use a local law-enforcement report as appropriate.
- Learn the basics: CISA "Secure Our World" — cisa.gov/secure-our-world.

REPEAT EVERY MONTH / EVERY TRANSACTION

☐ Monthly: review account sign-in alerts, forwarding rules, connected apps, updates, backups and lost-device controls.

☐ With every new client: give the wire-fraud warning before financial instructions enter the conversation.

☐ Before every high-risk seller transaction: tell the title company what identity concerns exist and agree on verification steps.

☐ After every incident: document what happened, escalate, and follow the brokerage response plan.