# TIPS TO AVOID CYBER CRIME IN REAL ESTATE

## SECURE YOUR DEPOSIT OR PROCEEDS FROM WIRE FRAUD

- Wire fraud is common, especially in high-worth transactions like real estate, so prevention is key
- Always confirm emailed wire instructions by phone using contact information that DID NOT come with the emailed wire instructions
- In general, it is a good idea to obtain the phone number of the escrow/title officer for your transaction at the beginning
- If there are any changes to the contacts provided, always independently confirm them before wiring any money

## USE SECURE WIFI

- Use secure, encrypted WiFi connections
- Be skeptical of unsecured, public WiFi. Consider using a secure proxy server

## LIMIT SOCIAL MEDIA

- Do not provide your location information on social networks or check-in sites
- Criminals commonly find potential victims using this shared information

## USE EMAIL CAUTIOUSLY

- Enable *Two Factor Authentication* (most email services providers offer this service, which typically can be found in your *Profile Settings*)
- Check access details regularly to confirm that no compromise has occurred
    - With a Gmail account, for example, you can click on the *Details* link at the bottom of the page in your *Inbox*. This will show you any recent activity. If the *Location* information shows a foreign country, there may be reason for concern
- Your email services may offer alerts to notify you of any unusual activity and you should activate this service, if it is available
- Think carefully before you click on an embedded link and select only those from a confirmed legitimate source or destination you recognize
- When in doubt, contact the sender to confirm the email is legitimate or delete the email entirely
- Avoid sending personal information in emails or texts
- If you need to send personal information by email, use an encrypted email service
- This is a time to be overly cautious

## KEEP YOUR COMPUTER SECURITY UP-TO-DATE

- Install pending security updates to your computer. Consider enabling automatic updates
- MacOS – Updates are installed using the Mac App Store or by choosing *Software Update* from the Apple menu
- Windows 10 – Updates can be found in Settings. Select *Update & Security* and then *Check for Updates*

## INSTALL VIRUS PROTECTION

- Ensure that your virus protection subscription is active and that updates are installed

## ENABLE YOUR SYSTEM FIREWALL

- MacOS
  - Open *System Preferences* and then select *Security & Privacy*
  - Select the *Firewall* option and turn it on
- Windows 10
  - On Start, scroll down to *Windows System > Control Panel > System and Security > Windows Firewall*
  - Select *Turn Windows Firewall "On" or "Off."* You may be asked for an admin. password or to confirm your choice
  - Under the appropriate *Network Setting*, select Turn on *Windows Firewall*

## USE UNIQUE AND STRONG PASSWORDS

- Consider using an encrypted password vault that stores and encrypts your passwords and other private information locally, and not in a pooled or group storage (which presents a rich target for potential attacks)

## ACTIONS TO TAKE IF YOU SUSPECT FRAUDULENT ACTIVITY

- If you suspect fraudulent activity *immediately* take the following actions:
  - Notify the Federal Bureau of Investigation Internet Crime Complaint Center at http://www.ic3.gov/
  - Notify other parties involved in the transaction so they may take appropriate action and do not unknowingly facilitate any fraud
  - Change your usernames and passwords to reduce the risk of further fraudulent activity

## ADDITIONAL RESOURCES FOR TIPS & ADVICE:

- https://www.stopthinkconnect.org/
- https://www.onguardonline.gov/

CALIFORNIA
ASSOCIATION
OF REALTORS®