Thieves are using evermore sophisticated scams to steal your identity and, ultimately, your down payment. To help protect yourself, consider these suggestions:



- Create strong passwords for your computer and smart devices and change them regularly.
- Add lock-out software that blocks access to your computer when you're not using it.
- Never access or send financial or personal information when connected to a free Wi-Fi hub or charging station.
- Seek referrals before choosing a lender. And never send sensitive information without first meeting the lender in person.
- Never open suspicious emails or attachments, even if they appear to be from your lender or Realtor®.
- Use caution if posting information about your purchase on social media, where it can be mined by scammers.
- Never email sensitive information. Instead, send it by courier, drop off the documents in person or use a secure, encrypted document-sharing platform.

Ask your Realtor and lender who will have access to your personal information and how it will be disposed of if it's not needed when your transaction is complete. Will it be shredded or stored in a secure location?

Work only with a lender who uses dual controls on wire transfers so no money can be moved until two employees independently

approve the transfer.

- Never wire funds until you have phoned a trusted source to confirm that all the information in the wiring instructions is accurate.
- Always be on the lookout for scams and impersonators.

