



Cyber Fraud Closing Checklist

Cyber Crime prevention in the real estate closing process is your responsibility. Potential home buyers lose hundreds of millions(\$446 million) of dollars every year thinking this will happen to somebody else. The best way to avoid a catastrophic financial loss is to be educated and proactive. Below are some steps you can take to protect yourself from fraudsters who are trying to steal from you.

Know the closing process and the professionals you are working with.

Verify all names, phone numbers and e-mail addresses to ensure you are always working with your team of trusted professionals. Build a rapport with these individuals.

Use encrypted e-mail to share nonpublic information (NPI)

When discussing or sending NPI, verify that all trusted parties involved with the transaction are using encrypted e-mail.

Use best password practices

Utilize a password manager, multi-factor authentication, different passwords for different accounts and complex passwords . It is also recommended by cyber security experts that you change your password every 3 months.

Never click on unknown attachments or links

Doing so can download malware onto your device which could lead to a ransomware event or lead you to a fraudulent website that appears legitimate.

Avoid doing business over public and unsecured Wi-Fi networks.

Using an unsecured network makes you more vulnerable and potentially compromises your information. Avoid using public networks in areas such as restaurants, hotels, airports, etc., to better minimize risk. If you must connect to an unsecured network, using a Virtual Private Network (VPN) will provide an additional layer of security.

Keep your anti-virus software and firewall up to date.

Routinely check and perform software updates. While they can feel like an annoyance, installing those updates decreases your vulnerability to cyberattacks.

Be Suspicious of any changes to wiring instructions.

Always verify any changes with your trusted team member(s), using the contact information that was initially established. Your title company with NEVER change their bank account or wiring instructions during your transaction.

Cyber crime isn't limited to e-mail

Artificial intelligence tools for voice cloning are changing the game for cybercriminals. Stay vigilant and always verify with your trusted team member(s) following phone conversations that discuss transactional information.

Protect your money

Confirm everything by asking your bank to confirm the name on the account before sending a wire. Verify immediately by calling the title company to confirm they received your money.