CYBERSECURITY CHECKLIST

BEST PRACTICES FOR REAL ESTATE PROFESSIONALS

Cybercrime can be devastating to real estate professionals and their clients. The following checklist offers some best practices to help you curb the risk of cybercrime. Because data protection and cybersecurity laws differ across the country, NAR recommends that you work with an attorney licensed in your state to help you develop cybersecurity-related programs, policies, and materials.

A. Email and Password Hygiene

- ✓ Never click on unknown attachments or links, as doing so can download malware onto your device.
- ✓ Use encrypted email, a transaction management platform, or a document-sharing program to share sensitive information.
- ✓ Carefully guard login and access credentials to email and other services used in the transaction.
- ✓ Regularly purge your email account, and archive important emails in a secure location.
- ✓ Use long, complicated passwords such as phrases or a combination of letters, numbers, symbols.
- ✓ Do not use the same password for multiple accounts.
- ✓ Consider using a password manager.
- ✓ Use two-factor authentication whenever it is available.
- ✓ Avoid doing business over unsecured wifi.

B. Other IT-based Security Measures

- ✓ Keep antivirus software and firewalls active and up-to-date.
- ✓ Keep your operating system and programs patched and up-to-date.
- ✓ Regularly back up critical data, applications, and systems, and keep backed up data separate from online systems.
- ✓ Don't download apps without verifying that they are legitimate and won't install malware or breach privacy.
- ✓ Don't click on links in texts from unknown senders.
- ✓ Prior to engaging any outside IT provider, review the applicable privacy policies and contracts with your attorney.

C. Law, Policy, and Insurance Considerations

- ✓ In collaboration with your attorney, develop a written disclosure warning clients of the possibility of transaction-related cybercrime. Recommend in the disclosure that buyers never wire money without first confirming the wiring instructions via a phone call to the intended recipient.
- ✓ Stay up-to-date on your state's laws regarding personally identifiable information, the development and maintenance of cyber and data-related business policies, and other legally required security-related business practices.
- ✓ Develop and implement the following policies:
  1. Document Retention and Destruction Policy
  2. Cyber and Data Security Policy
  3. Breach Response and Breach Notification Policy
- ✓ Ensure that your staff and licensees have reviewed and are following all implemented policies.
- ✓ Review your current insurance coverage, and ask your insurance agent about cyber insurance and the availability and applicability of products such as social engineering fraud endorsements and computer & electronic crime riders.

For more information about cybercrime and cybersecurity, please visit NAR.realtor's data privacy and security landing page. Questions can be directed to NAR Associate Counsel Jessica Edgerton at jedgerton@realtors.org.