REAL ESTATE BROKERS AND AGENTS

Cybersecurity Checklist

INTRODUCTION

Hi, my name is Garland Oakes, owner of South Atlantic Data and Design. As related to the world of Information Technology I can truly say that I have seen about every program used from listing properties to closing the sale. I have worked with appraisers, brokers, agents, and lawyers over my journey since I started in this field in 1997. Today I am sharing information to you as it relates to how we navigate future technologies in the real-estate business and keep our clients safe.

In today's digital age, the intersection of cybersecurity and real estate has become increasingly critical. As the real estate industry embraces technology for transactions, property management, and client communications, it simultaneously faces heightened risks of cyber threats. From data breaches to ransomware attacks, the stakes are high, making robust cybersecurity measures essential for protecting sensitive information and maintaining trust with clients.

Real estate professionals must navigate a complex landscape where safeguarding personal and financial data is paramount. This involves not only implementing advanced security protocols but also fostering a culture of cybersecurity awareness among staff and clients. With the potential for significant financial loss and reputational damage, understanding the nuances of cybersecurity in real estate is vital for ensuring a secure and thriving business environment.

As we delve deeper into this topic, we will explore the specific challenges the real estate sector faces in cybersecurity, best practices for risk management, and the role of technology in fortifying defenses against cyber threats.

1. EMAIL AND PASSWORDS

- Never click on unknown attachments or links, as doing so can download malware onto your device. Ransomware can cause the loss of critical information and data, including photos, documents, and financial records. If backups aren't available, these losses can be permanent.

- Use encrypted email, a transaction management platform, or a document-sharing program to *share sensitive information*. Free email addresses from sites such as GMAIL, OUTLOOK, HOTMAIL, YAHOO, and others have zero security to protect the information of your clients, colleagues, or other businesses.

- Carefully guard login and access credentials to email and other services used in a 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. Using names of pets or children should never be used. Lots of times people fill out questionnaires on social media with this information readily available for hackers to use against them. We recommend using 3 words that have zero meaning to each other that is easy to remember so it meets requirements.

- Do not use the same password for multiple accounts. If one of the accounts gets compromised such as your email then other accounts such as banking accounts would be easily accessible.

- Consider using a password manager. Password managers such as LastPass and Bitwarden help secure your password and make them easily accessible for retrieval.

- Use two-factor authentication whenever it is available. This helps prevent unwanted logins to your accounts and will help put a second layer of protection between your important data and the hackers.

2. OTHER IT-BASED SECURITY MEASURES

- Keep antivirus software and firewalls active and up-to-date. Antivirus and Malware protection is the number one way to keep your computer clean of hijackers. Viruses and Malware can leave you with a number of issues including ransomware which is the worst.

- Keep your operating system and programs patched and up-to-date. Patching your operating system is extremely important as vulnerabilities are the first line of attack.

- Regularly back up critical data, applications, and systems, and keep backed up data separate from online systems. Data is your most important resource, this can be collected over days, months, or years and can be very hard to recreate in a time efficient manner.

- Don’t download apps without verifying that they are legitimate and won’t install malware or breach privacy. Free isn’t always free, lots of apps have the ability to monitor your computer for those times you enter passwords which will give the hacker instant access.

- Don’t click on links in texts from unknown senders. Phishing scams are the number one way for hackers to gain access to your computer and your money.

3. LAW, POLICY, AND INSURANCE CONSIDERATIONS

- In collaboration with your IT company, develop a written disclosure warning clients of the possibility of transaction related cybercrime. South Atlantic Data and Design can work with you to create a Wire Fraud Email Notice Template that you and your counsel may adopt.

- 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 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 and electronic crime riders.

At **South Atlantic Data and Design**, we offer free no hassle consultations. Our main goal is to keep your businesses and clients safe while using technology to enhance your business. Please call us today at 276-618-2058 or 540-352-7083 to set either a face to face or video conference for your firm.

Website: www.southatlanticdata.com