CyberPolicy | NATIONAL ASSOCIATION OF REALTORS® REALTOR BENEFITS® PROGRAM

# The Importance Of Owning Your Role In Cybersecurity


*CyberPolicy, a REALTOR Benefits® Program partner, is committed to help REALTORS® and REALTOR®-owned brokerages plan for, prevent and insure against cyber crime targeting the real estate industry with educational and cybersecurity resources.*

Cybersecurity can be a complex and intimidating topic for many real estate professionals. But, what may seem too large for any one person to solve can actually be a very manageable task with a little knowhow. In truth, the foundations of cybersecurity are decidedly non-technical and highlight the role of the individual internet user. With some basic understanding and a little guidance, you can see that cybersecurity relies on the collective actions of individuals within a brokerage rather than complex or expensive software.

Read on to learn how you can own your role in cybersecurity and strengthen the integrity of your real estate business.

**Know what hackers are looking for**
Hackers are primarily after identity data, credit card information is their secondary target.

Identity data is any information that can be used to identify a specific user, employee, contractor, client, or consumer. This includes names, addresses, email addresses, social security numbers, and more. In many cases, a name, SSN and birthdate are enough to steal someone's identity causing immense financial and credit damage.

While stolen credit cards are bad news, stolen identity data found on financial documents is much worse. Hackers love to pilfer real estate documents to resell on the dark web. Digital black-marketers actually prefer financial documents to stolen credit cards. Credit cards can be canceled and they expire, offering a limited window of value. This is not the case for SSNs, names or birth dates, which live on indefinitely. Even a deceased person's identity data can be used for nefarious purposes. If you handle customer identity data, it is your job to protect that information.

**Implement non-technical identity data management procedures**
Knowing exactly what cyber criminals are looking for makes it easier to safeguard that valuable information and protect your real estate business. Here are handful of non-technical approaches that will enable you protect identity data:

**Understand that not all data needs to be saved.** Protect your clients by not saving some information. After all, it can't be stolen if you don't have it. Many CRM and lead gen applications

collect more data than is needed. Adjust the default settings of any apps that your brokerage uses to retain only the information that is needed to create and maintain a relationship with clients.

**Train your staff to be skeptical.** Phishing and social engineering scams are used by hackers to fool real estate professionals and their clients into sharing personal or financial information. Email is the primary tool that hackers use to deliver scams to unsuspecting recipients, so this is where you want to be on the lookout. Train your team to identify suspicious emails. As a general rule: Be weary of all messages from unknown senders and NEVER share information, click links, or download attachments from anyone that you don't know. This can be difficult given the nature of the real estate industry, but it is important to remain vigilant and on the lookout for anything suspicious.

**Silo your data based on who needs it most.** Not every member of your brokerage needs access to identity data. Segment access based on a need-to-know basis. Fewer access points to sensitive data offers fewer opportunities for a hacker to weasel in and cause problems.

**Accountability of the broker-owner**

Any business conducted online or with a connected device carries a certain set of risks. That's the reality of the tech-enabled world that we work in today. Literally every brokerage that hires employees or contractors, handles financial documents, or stores client data needs to consider the possibility of a data breach. As a broker-owner, the outcome of any breach falls squarely on your shoulders. Data is one of the most valuable and vulnerable assets that any brokerage manages. Unfortunately, many agents and brokers don't learn this fact until it's too late, because anytime there is a data breach, lawsuits can be expected to follow.

A cyber insurance policy covers your real estate business in the event of a hack or data breach that results in financial damages - both direct and litigatory. This type of business insurance covers a brokerage's intangible assets like digital files and data. Cyber insurance may seem novel to many, but it has become a necessary form of coverage for real estate professionals that use the internet.

**Common sense cybersecurity practices and training are the first line of defense. Cyber insurance is the final piece.** Visit CyberPolicy's page or give CyberPolicy a call at (844) 293-7440 to learn more about the cyber liability insurance program available exclusively to REALTOR®-owned brokerages through NAR's REALTOR Benefits® Program.

These articles are not the product of the National Association of REALTORS®, and may not reflect NAR's viewpoint or position on these topics and NAR does not verify the accuracy of the content.

**Amber Bachman**
*Director of Cyber*

CyberPolicy®