

# **Cybersecurity: How Technology Can Ruin Your Business**

## **Course Description**

It is no longer a secret that with the proliferation of Wire Transfer Fraud, Listing Scams, and many other digital schemes, the real estate industry has become a major target for hackers and fraudsters. They realize REALTORS® are often involved in large transactions and gathering valuable information and typically don't have the proper training, tools, or resources to do so.

In this session, you will learn how to assess what current cybersecurity weaknesses you may have, how to protect yourself and your clients with very easy-to-implement low-tech solutions, and how to navigate several laws, NAR policies, and more to ensure you and your clients survive this perilous digital world.

This course is designed to elevate awareness, assist students in establishing policies and procedures, and raise the level of care offered to the consumer when we promise to protect and promote a client's best interests.

### **Direct Learning Objectives**

After attending this course, participants will be able to:

1. Describe how viruses and malware can infect your computer and mobile devices
2. Identify techniques to encrypt your data to avoid getting viruses and malware
3. Relate the importance of having a strong password policy
4. Define encryption and explain its important role in securing your data
5. Cite state & federal laws relating to technology that affect your job as a REALTOR® and your interactions with consumers
6. Identify what Social Engineering is & how it works
7. Identify what Phishing Scam is & how it works
8. Identify what Wire Transfer Fraud is and how it works
9. Relate how negative information online can affect your business.
10. List the steps needed to manage Your Online Reputation
11. Identify the differences, strengths, and weaknesses between Digital & Electronic Signatures
12. Explain the National Association of REALTORS® policies on technology and how they impact your business
13. Cite how state & federal laws affect your ability to advertise & market your business
14. List the steps required to ensure your Website is safe
15. List the steps required to ensure your Website is legally compliant
16. State the terms and dangers of copyright infringement
17. Identify safe media sources to avoid copyright infringement
18. Assess the importance of using proper online etiquette and how to handle online conflicts
19. Leverage tools and techniques to keep you and your technology devices safe
20. Assess what Company & Shared Device Policies you will want to implement
21. List steps required to ensure your Technology and Personal Safety
22. Define the steps you would take if You got hacked or were the victim of a digital crime
23. Define what Cyber Liability Insurance is and assess if you need it.
24. List the steps needed to create a Digital Security Policy