

EBOOK

# HOA Board Member's Guide

to Cybersecurity

---

# CONTENTS

- 3** Introduction
- 4** Recognize Phishing Emails
- 5** Be Cautious of Smishing
- 6** Use Strong, Unique Passwords
- 7** Enable Two-Factor Authentication (2FA)
- 8** Be Wary of Public Wi-Fi
- 9** Secure Financial Transactions
- 10** Conclusion



A person wearing a dark hoodie is hunched over a laptop, working in a server room. The background shows server racks with red and blue lights.

## INTRODUCTION

Cybersecurity is essential to protecting your homeowners' association's (HOA's) finances, sensitive data, and reputation.

As a board member, you hold responsibility for safeguarding your association against cyber threats. This guide will help you build strong cybersecurity habits to minimize risks for the association and your personal security.

## RECOGNIZE PHISHING EMAILS

Phishing involves deceptive emails designed to trick you into sharing sensitive information, such as passwords or financial details.

These emails often appear to come from legitimate sources.

**Example:** You receive an email claiming to be from your bank requesting that you verify account details via a provided link.

**Tip:** Always verify the sender's email address. Avoid clicking on links or downloading attachments from unknown sources. Contact the sender directly through verified channels to confirm the email's authenticity.



## BE CAUTIOUS OF SMISHING

Much like phishing, smishing involves fraudulent text messages designed to trick you into providing personal information or clicking malicious links.

These messages often appear to come from trusted sources.

**Example:** You receive a text claiming to be from your bank, stating there is an urgent issue with your account and asking you to click a link to resolve it.

**Tip:** Avoid clicking on links in unsolicited text messages. Verify the sender by contacting them directly through verified channels. Be especially wary of urgent or alarming language in text messages.



## USE STRONG, UNIQUE PASSWORDS

Weak passwords are a gateway for hackers to access sensitive data. Reusing passwords across platforms increases vulnerability.

**Example:** A board member's email account is hacked because they reused their password from a breached e-commerce site.

**Tip:** Create passwords with at least 12 characters using a mix of letters, numbers, and symbols. Consider using a password manager to store and generate unique passwords securely.



## ENABLE TWO-FACTOR AUTHENTICATION (2FA)

2FA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, in addition to your password.

**Example:** A hacker attempts to log in to your banking portal using a password stolen via a successful phishing attempt or data breach but is stopped because they cannot provide the 2FA code sent to your phone.

**Tip:** Enable 2FA for all association-related accounts.



## BE WARY OF PUBLIC WI-FI

Public Wi-Fi networks can be insecure, making it easy for hackers to intercept data you send or receive.

**Example:** A board member uses public Wi-Fi at a coffee shop to access the association's financial records, exposing the information to potential hackers.

**Tip:** Avoid accessing sensitive information on public Wi-Fi. Use a Virtual Private Network (VPN) for secure connections when necessary.







## SECURE FINANCIAL TRANSACTIONS

Cybercriminals often target financial transactions to steal money or sensitive details.

**Example:** A fraudster sends an email impersonating a vendor, asking for payment to a different bank account.


**Tip:** Always verify payment requests through a secondary method, such as a phone call. Use secure payment platforms and implement checks for unusual transactions.

## CONCLUSION

By implementing these cybersecurity practices, you'll reduce your exposure to cyber risks and protect your community's assets. Cybersecurity is a shared responsibility, and proactive steps can make a significant difference. Make cybersecurity a priority for your board today.

CAMS is committed to safeguarding your private information. We will never ask for your bank or account information in any email. If you are concerned about a message, you can go directly to [www.camsmgt.com](http://www.camsmgt.com) in your browser to access the website.





At CAMS, our top priority is keeping all aspects of your community running seamlessly. We make leading and living in a managed community better and easier than ever.

Contact us to learn more today!



*Accredited Association Management Company (AAMC®)*  
**CAMS Has Provided Local, Trusted Guidance  
For Community Associations Since 1991.**

[www.camsmgt.com](http://www.camsmgt.com)

877.672.2267