Stopping Community Association Social Engineering Fraud Starts with You

Ian H. Graham INSURANCE
An Aon Company

Community associations are not immune to social engineering fraud, which can lead to financial loss as well as a loss of trust in the board.[i] In social engineering fraud, a perpetrator intentionally misleads an individual by using psychology to manipulate them. Through the use of fraudulent phone calls, emails, text messages, social media posts and other means, the fraudster convinces the individual to divulge confidential information or otherwise disregard security protocols.[ii]

For example, a fraudster poses as a trusted vendor, using a nearly identical email address and logo as the vendor, to send an "urgent" request to a Board member. The email claims payment must be wired immediately to a new bank account to keep the vendor's business afloat. Under pressure and without confirming the request, the Board member wires the funds—unknowingly sending thousands of dollars directly to the criminal.

BE SUSPICIOUS OF:

1	Urgent requests for money that trigger an emotional response and discourage the recipient from taking the time to perform reasonable due diligence.
2	Requests ostensibly made by a trusted person but which are delivered using an atypical or unverifiable means of communication, or an email address which is different from the display name on the email.
3	Requests by an unknown person claiming to work for a trusted person, made in circumstances which discourage the recipient from seeking confirmation.
4	Requests for a payment or money transfer to be made to an unverified account or using unusual procedures.
5	Requests for the sharing of passwords or personal and/or financial information via email.
6	Suspicious links or attachments that appear unrelated to the sender and/or company.[iii]

MITIGATE THE RISK OF SOCIAL ENGINEERING:

1. Continually train, including simulation training, regarding social engineering schemes. Train to distinguish between a fraudulent, targeted phishing email and a legitimate one, and provide clear instructions if an email is suspected to be fraudulent. Train to avoid clicking on suspicious links from unknown senders.[iv]
2. Implement multifactor authentication for computer systems to provide an additional layer of security even if access credentials are compromised.[v]
3. Establish strong vendor controls. This includes maintaining a master list of all approved vendors and owners. Consider limiting the number of people who are able to transfer money, make purchases or make payments, and who are able to change vendor or owner accounts. Consider requiring dual authorization for large amounts of money. Create and follow policies and procedures to verify the receipt of inventory, supplies, goods or services against an invoice prior to making payment to a vendor.[vi]
4. Confirm money transfers and account requests with a direct call to the vendor using an authenticated phone number provided before the transfer or change request was received. Ensure that the individual is who they say they are by using an independent means other than the contact information provided by the individual. Consider providing, in advance, a code specific to the vendor that must be provided to effectuate money transfers or account changes.[vii]
5. To be certain that email senders are who they purport to be, type the name of the recipient of an email instead of hitting "reply." Be skeptical of last-minute changes in wiring instructions or recipient account information.
6. Consider using a spam filter to detect and divert suspicious emails.[viii]

[i] https://edenredpay.com/protecting-hoas-from-cyber-attacks-and-payment-fraud/

[ii] https://www.cna.com/from-the-experts/authorbio/blogdetails/jeff-portis/as-social-engineering-fraud-spreads-take-steps-to-protect-your-business

[iii] https://cybersecurity.yale.edu/newsletter/summer2023/bee-active

[iv] https://blogs.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks

[v] https://www.social-engineer.org/social-engineering/four-ways-to-stay-safe-online/

[vi] https://www.mtb.com/library/article/what-you-need-to-know-about-social-engineering#:~:text=Educate%20your%20team:%20Train%20employees,the%20response%20to%20fraud%20attempts.

[vii] https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

[viii] https://blogs.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks

Underwritten by:

CNA

Administered by:

ihg In Step with Community Associations

NATIONAL CORPORATE MEMBER OF community ASSOCIATIONS INSTITUTE

X-14990-0326