



Social Engineering

SCENARIO

A property manager was having a particularly busy Friday when he received an email that appeared to be from the community association's president of the board. The email advised that the contractor that had recently renovated the association's pool needed to paid the next contract installment by the end of the day or the association would incur a penalty. The email explained that the money should be wired to the contractor's new account rather than the one that the PM had on file. The email also stated that the president was about to board a plane and would be unable to communicate further with the PM before the payment was due. The PM followed the directions in the email and sent the \$35,000 payment, via wire transfer, to the new account as indicated in the email. The next week, at a board meeting, the PM mentioned the payment to the president. The president did not know what the PM was talking about, so the PM forwarded the email to the president. It was determined that the email was not from the president, but from a criminal who had hacked the president's email account, and that the \$35,000 had been diverted to the criminal. The funds had been withdrawn and the account closed by the criminal by the time the scheme was discovered.

RISK CONTROL TIP

Provide social engineering training to employees and board members to reduce the likelihood they

will fall prey to social engineering schemes. Learn to recognize some of the common signs of social engineering attacks, including to be suspicious of: (1) urgent requests for money that 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, (3) requests by an unknown person claiming to work for a trusted person, made in circumstances which discourage the recipient from seeking confirmation, and/or (4) requesting that a payment or money transfer be made to an unverified account or using unusual procedures. Confirm all money transfers and requests to change vendor and customer account information by a direct call to the vendor or customer using only an authenticated phone number previously provided by the vendor before the transfer or change request was received. Ensure that important vendors, including Property Managers, receive similar training in recognizing social engineering attacks and are under instructions to confirm any unusual requests for payment. Consider using simulations and other means to ensure that employees and the board understand cyber risks as well as their obligation to protect the organization's computer systems and assets. Implement multifactor authentication to protect computer systems from remote attacks by providing an additional layer of security.



info@ihginsurance.com | 800.621.2324 | ihginsurance.com

Underwritten by:



Administered by:



In Step with
Community
Associations



The purpose of this material is to provide information, rather than advice or opinion. The information it contains is accurate to the best of the author's knowledge as of the date it was written, but it does not constitute and cannot substitute for the advice of a retained legal professional. Only your own attorney can provide you with assurances that the information contained herein is applicable or appropriate to your particular situation. Accordingly, you should not rely upon (or act upon, or refrain from acting upon) the material herein without first seeking legal advice from a lawyer admitted to practice in the relevant jurisdiction.

These examples are not those of any actual claim tendered to the CNA companies, and any resemblance to actual persons, insureds, and/or claims is purely accidental. The examples described herein are for illustrative purposes only. They are not intended to constitute a contract, to establish any duties or standards of care, or to acknowledge or imply that any given factual situation would be covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

Ian H. Graham Insurance is the brand name for the brokerage and program administration operations of Affinity Insurance Services, Inc., a licensed producer in all states (TX 13695); (AR 100106022); in CA & MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.

X-14905-0725