SCAM ALERT!!

By: Kimberly A. Pendo & Rachel C. Steiner

Cybersecurity is a paramount concern for not-for-profit (and for-profit) businesses alike. Methods of attack are more sophisticated than ever. Associations have legal obligations to take reasonable steps to safeguard funds and protect information. Educating leadership and staff about cybercrime activities is an organization's first line of defense against cyber intrusions and theft.

Recent scams highlight how an individual can unwittingly facilitate an institutional network breach. The FBI warns of a widespread business email compromise ("BEC") scam with five main variations: (i) a purported supplier requests that a business pay an invoice; (ii) a purported association officer/director/executive asks an employee or other officer/director or financial institution to transfer funds; (iii) a purported employee asks a vendor to pay an invoice; (iv) a purported lawyer seeks an urgent or secret funds transfer from a business executive; and (v) a purported business executive requests data, such as tax forms or other personally identifiable information, from a department responsible for handling such information.

BEC schemes generally involve email hacking or spoofing as well as social engineering to impersonate an officer/director/employee. The cybercriminal studies the targeted business victim to identify the correct officers/directors/employees to contact, applicable procedures to follow, appropriate language to use, and customary dollar amounts to request so as to accomplish a wire transfer at that particular association. Sometimes another cyber fraud event may precede the BEC to obtain information necessary to execute the scam. For example, victims may receive phishing emails that try to elicit relevant information about the association or individual officer/director/employee, such as name and travel schedule. Victims also may experience Scareware or Ransomware intrusions that allow the perpetrator access to relevant data, such as passwords and financial account information.

Specific tactics may vary, but the goal remains the same: Steal money by effectuating a transfer of funds or obtaining valuable data. Victims range from small to large companies and from public to private sector entities, including not-for-profits. The FBI offers various security tips:

1. Do not use free web-based email accounts.

2. Limit company information available online: Do not post, for example, job descriptions, organizational structure, and out-of-office schedules.

3. Be skeptical of urgent or secret requests.

4. Implement additional security procedures: For example, have a two-step verification process to authorize financial transactions; use digital signatures; report spam emails; forward, rather than reply to, an email to guarantee the correct recipient; and require multi-factor authentication to access email accounts.

5. Note any change in a business contact's usual practice or habit, and verify directly that you are not dealing with an impostor.

6. Set up system rules to identify emails with extensions similar to the association's email.

7. Register domain names that are similar to your association's name.

In the event of a cyber attack, contact your attorney. If funds were transferred, immediately alert your bank, and ask the bank to contact the receiving institution. Depending on the nature of the scam, file a complaint with the FBI Internet Crime Complaint Center, contact the IRS and state tax agencies, and/or report suspicious activity to your Attorney General's Office.