PretiFlaherty

BEST PRACTICES FOR AVOIDING CYBER-FRAUD ON CONSTRUCTION PROJECTS

No industry is safe from the threat of cyber-fraud, and the construction industry is no exception. Criminals know that large construction projects often require significant payments, which occur regularly. It is fairly easy to identify the contractors involved in these projects, and criminals can then use that information to steal progress payments.

The scam typically works as follows. The criminal discovers an ongoing construction project and determines the identity of the contractor from media reports, job signage, or otherwise. The criminal then creates a false e-mail account that "spoofs" the actual e-mail address of the construction company using a similar domain. Accordingly, if the contractor's name is AAA Builders, and their correct e-mail suffix is @aaabuilders.com, the criminal may create and register a domain of @aaa-builders.com from which to send the e-mail.

The criminal then sends the e-mail with the spoofed address (usually using a name that the owner will recognize from the project) to the owner, requesting changes to the payment method. The e-mail often requests that future payments be wired to a specific account number, which is actually the criminal's account. The e-mail may include a phone number, which is actually the criminal's number, to answer any questions. When the owner then wires progress or other payments to the designated account, the criminal immediately removes the funds. At that point, the criminal has the owner's money, while the owner remains liable to the contractor for the applicable payment or payments that it wired to the fraudulent account. When these scams succeed, losses are usually significant and irreversible.

To protect yourself from this type of scam, we recommend that you take the following precautions, which include the suggestions contained in FBI Alert No. I-050517-PSA, along with a few additional recommendations. Always assume that any unsolicited e-mail concerning payment processing may be a fraud, and verify that the request is genuine. Closely examine the domain and e-mail address to confirm that it matches the correct domain of the contractor. Hover your mouse over any links in the e-mail to see the address before clicking. This may help you to identify a fraud but it is not enough, as there have been instances where hackers have been able to access legitimate e-mail accounts. Accordingly, it is essential that you also call someone at the contractor's office whose voice you know and verify the request. Do not use the telephone number included in the e-mail you received unless it is a number you have called before. Forward suspicious e-mails to your organization's IT department. You may also report suspected fraud to the FBI's Internet Crime Complaint Center at www.IC3.gov.

Following these protocols does not necessarily prevent all frauds. However, adhering to this approach should reduce the chances that a cyber fraud will succeed on this project, or any future project that you may undertake.