TitleNews Online Archive

How Wire Fraud Starts

July 25, 2017

Criminals begin the wire fraud process way before the attempted theft occurs. Most often, they begin with a common social engineering technique called phishing. This can take the form of email messages, website forms or phone calls to fraudulently obtain private information. Through seemingly innocuous communication, criminals trick users into inputting their information or clicking a link that allows hackers to steal login and password information.

Phishing emails might appear to come from a legitimate business or recognized user. Spear phishing is

a more targeted email attack sent to a select number of users, while a whaling attack, also known as Business Email Compromise (BEC), is a more targeted variation of spear phishing aimed at high-profile executives or personnel who manage wire transfers. According to the latest Association for Financial Professionals' Payments Fraud and Control Survey, a majority of finance professionals (64 percent) reports that their organizations were exposed to BEC in 2015. The FBI's Internet Crime Complaint Center reports that "the BEC scam continues to grow, evolve and target businesses of all sizes." Since January 2015, there has been a 1,300 percent increase in identified losses, now totaling over $3 billion.

The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone. Don't rely on email alone.

Martin Licciardo, a special agent in the FBI's Washington Field Office, said the best way to avoid getting ripped off is to verify the authenticity of requests by speaking to people directly.

"The ability of these criminal groups to compromise legitimate business e-mail accounts is staggering," he said. "They are experts at deception."

It is disconcerting that, in spite of safeguards being implemented, criminals are still making headway with BEC scams. The significant increase in wire fraud also suggests that BEC fraud may be more difficult to prevent than was previously believed.

Once hackers gain access to an email account, they will monitor messages to find someone in the process of buying a home. Hacks can come from various parties involved in a transaction, including real estate agents, title companies, attorneys or consumers. Criminals then use the stolen information to email fraudulent wire transfer instructions dressed up to appear as if they came from the victim. To this end, criminals will use either the victim's actual email account (which they may actually control) or create a fake email account resembling the victim's email.

“We all want to avoid the scenario where the buyer’s funds are sent to a fake account and are unrecoverable,” said Bill Burding, a member of ALTA’s Information Security Committee and general counsel for Orange Coast Title Co. “One of the key indications of any wire fraud scam is the sense of urgency. These tend to come from someone of authority to the person who is responsible for wiring funds within the organization. This is when it’s imperative to slow down and make sure policies for handling wire instructions are followed to a T.”

Over the past few years, there’s been a lot of discussion and training over the past few years about preventing outbound wires from being intercepted. According to Christopher Hacker, chief product officer at ShortTrack, criminals are now targeting the “inbound wire” of cash to close sent by the buyer.

“Unfortunately, again and again, we hear leaders of title agencies say they’re handling all of the wire diversion and fraud issues with the controls for outbound wires,” Hacker said. “The bad actor sits and waits for the wire instructions to show up in the buyer’s inbox, downloads them, deletes the message with the accurate document and resends updated wire instructions either from a spoofed account of the title company or from the compromised account of the real estate agent.”

Contact ALTA at 202-296-3671 or ***communications@alta.org****.*