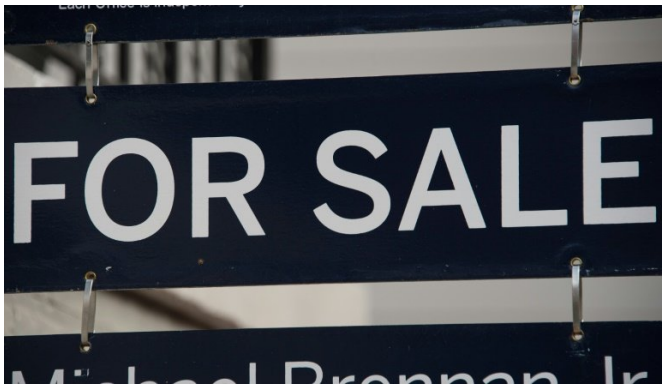
Hackers target real estate deals, with devastating impact

23 September 2018, by Rob Lever



Real estate agents and others involved in home transactions have become increasing targets for hackers

James and Candace Butcher were ready to finalize the purchase of their dream retirement home, and at closing time wired $272,000 from their bank following instructions they received by email.

Within hours, the money had vanished.

Unbeknownst to the Colorado couple, the email account for the real estate settlement company had been hacked, and fraudsters had altered the wiring instruction to make off with the hefty sum representing a big chunk of the Butchers' life savings, according to a lawsuit filed in state court.

A report by the FBI's Internet Crime Complaint Center said the number of victims of email fraud involving real estate transactions rose 1,110 percent between 2015 to 2017 and losses rose nearly 2,200 percent.

Nearly 10,000 people reported being victims of this kind of fraud in 2017 with losses over $56 million, the FBI report said.

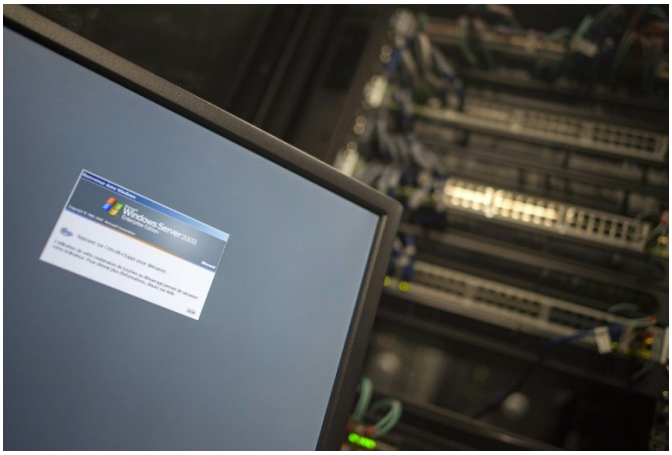
The Butchers, forced to move into their son's basement instead of their dream home, eventually reached a confidential settlement in a lawsuit against their real estate agent, bank and settlement company, according to their lawyer Ian Hicks.

The problem is growing as hackers take advantage of lax security in the chain of businesses involved in real estate and a potential for a large payoff.

"In these cases, the fraudster knows all of the particulars of the transaction, things that are completely confidential, things they should not know," said Hicks, who is involved in more than a dozen similar cases across the United States.

Email insecurity

Numerous cases have been filed in courts around the country seeking restitution from various parties. One couple in the US capital Washington claimed to have lost $1.5 million in a similar fraud scheme.



Hackers have been stepping up attacks on real estate transactions, sometimes stealing large down payments and purchase amounts by falsifying wiring instructions

Real estate is just one segment of what the FBI

calls "business email compromise" fraud which has resulted in some $12 billion in losses over the past five years. But for home buyers, the fraud can be particularly catastrophic.

"In these cases, the loss can be devastating and life-altering," Hicks said.

Real estate transactions have become a lucrative target for hackers "because they handle a lot of money and because they have employees who are not the most technically savvy," said Sherrod DeGrippo, director of threat research for the security firm Proofpoint.

Additionally, hackers often do their homework and "sometimes they know more about the business than the employees do," she said.

Consumers may also be less cautious when they are feeling positive about a new home, making it easy to fall prey to scammers, DeGrippo said.

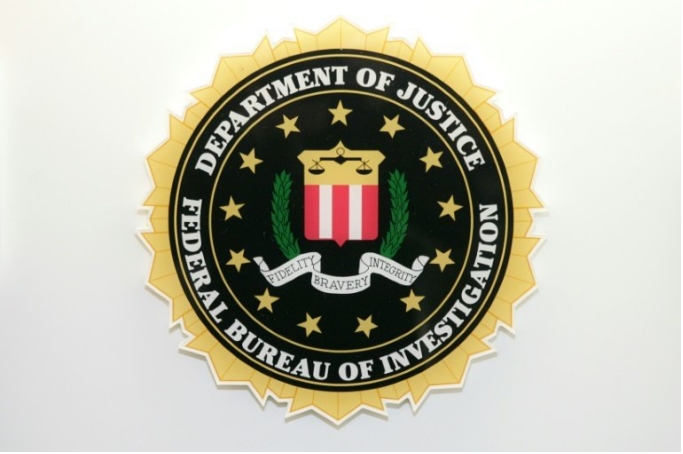
"These social engineering tactics rely on a heightened emotional state, and people can be in that state when it comes to purchase their dream home," she added.

DeGrippo said the schemes appear to originate from overseas, possibly from Russia or Africa, using a variety of techniques to stay ahead of law enforcement.

"They employ a lot of money 'mules,'" she said. "They move the cash from bank to bank to bank."

Banks have been working to counter what is seen as a growing fraud problem but are often unable to prevent scams stemming from hacked emails, said Paul Benda, senior vice president for risk and cybersecurity at the American Bankers Association.

"Banks have very strong controls in place," he said. "But when they are given wiring instructions from a customer they have a responsibility to send it where it was instructed."



The FBI issued a warning this year about increased efforts by hackers to target those involvedin real estate transactions

Benda said that customers need to know a wire transfer is "just like cash" and may be impossible to recover, especially if it ends up overseas.

Who's to blame?

Lawsuits from consumers often target real estate agents, attorneys, escrow agents, banks and settlement companies that prepare documents for deals.

"There are a lot of people involved, and (fraudsters) can hack into any one of these parties," said Finley Maxson, senior counsel at the National Association of Realtors.

"These emails have become much more sophisticated, they are much harder to catch."

Maxson said the Realtors and other associations are moving aggressively to educate all parties involved about the potential for fraud and the need for better security.

"We're telling people they should never give these (wiring) instructions by email," he said.

It may be difficult to establish liability, but Hicks said that "consumers are not going to be careless with their life savings" and that the real estate

professionals have a responsibility to ensure the security of their systems, and to give customers adequate information.

The lawsuit filed by Hicks for the Butchers said that "the scam that befell the Butchers was well-known in the real estate industry and easily preventable."

Earlier this year, a Kansas court assigned 85 percent of the liability to a hacked real estate agent and awarded a homebuyer defrauded by fake wiring instructions $167,129.

Hicks said that in these cases, "there is a lot of blame to go around," but argued that "unless companies have to pay money they won't do what's necessary to protect the consumer."