FRAUD Insights

CHICAGO TITLE®

BLACKMAIL

The week started out just like any other week with phone calls and emails coming in from customers — until one alarming email arrived:

"I won't reveal you just what exactly I'm aware of, I've got all the information along with me. To demonstrate this, allow myself reveal you that one of your security passwords is definitely ticor1. Pay me $9000 via BITCOIN to the address 1PXxPLWGsNsZcCPQi6TWKN4FjnXH2H7xES within the next 44 hours. I would like to make one thing obvious, that I will mess up your life fully if I do not get the payment. In case I do get the payment, I will erase every last information I've with me, and I will disappear for good and you will never hear a thing from me. This is actually the first and also last e mail from me as well as the offer is non negotiable, therefore do not answer this e–mail."

There was nothing attached, nor was there any link included within the email, but the escrow officer knew right away this was a scam and hit the Report Phishing button on the Microsoft® Outlook® Toolbar. This email was filled with threats, but nothing came of it.

This type of email is likely a phishing/sextortion scam. Although, this email did not include an attachment or link, it is clearly someone's attempt to extort money from the Company. Reporting it as a phishing attempt is the correct thing to do.

Many Information Technology (IT) specialists and the Federal Bureau Investigation's (FBI's) Cyber Division predict ransomware attempts will increase in the coming months. Ransomware attacks typically come in the form of an email with an attachment or link to something which appears legitimate.

An example of these types of emails includes an instruction to click a link to access the Closing Disclosure or closing statement, yet the email is coming from an outside source and no one is expecting it. These should be reported as phishing to IT right away.

In addition to the phishing/sextortion scam is the ransomware scam. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

Anyone who receives an email and does not know the sender or are not expecting the email, must proceed with caution. Once the attachment or link is opened a malicious ransomware code infects the computer and — in some instances — can infect a company's network with malicious software.

The software can encrypt and restrict a company's ability to access important data and can result in the loss of sensitive or proprietary information, the disruption of day–to–day business, financial losses and often a company's reputation.

Once the malware has successfully encrypted all of a company's data, they receive demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Our Company works hard each and every day to prevent the Company from becoming a victim, but all the firewalls and patches in the world do not account for the biggest weakness in security: human error.

Pay close attention to any email received. Note the email address and be sure not to open any attachments or links which may be suspicious. Are you unsure? Call the sender at a known trusted phone number to verify whether or not they sent the email. Report suspicious emails by selecting the Report Phishing button.

Reporting suspicious emails assists the Company in identifying the latest tricks the hackers are using. Always proceed with caution when clicking on links or opening attachments.

Article provided by contributing author: Diana Hoffman, Corporate Escrow Administrator, Fidelity National Title Group, National Escrow Administration