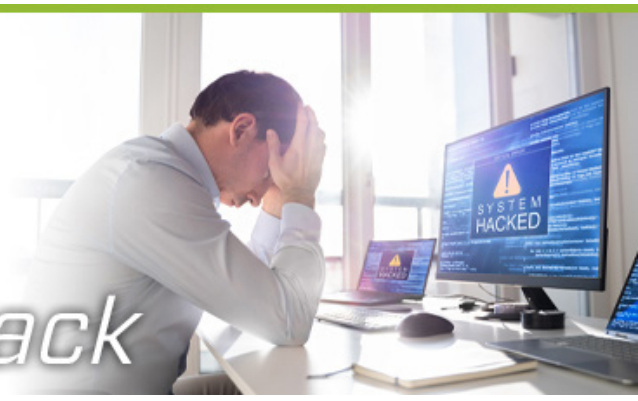
FRAUD Insights

CHICAGO TITLE®

WHAT to do in a ransomware cyberattack



The Cybersecurity and Infrastructure Security Agency (CISA) has put together a comprehensive website which contains tools for victims. One of these tools is a Ransomware Guide which includes a comprehensive checklist for victims. It is available on their website https://www.cisa.gov/stopransomware/ransomware-guide.
(Important: FNF employees should report any cyberattacks to our Security Operations Center for handling.)

Management also needs to consider whether they should enlist assistance from outside cybersecurity resources and/or report the attack to law enforcement. There are plenty of private firms who offer forensic, incident response and recovery services. In addition, the Federal Government has set up resources that companies can contact voluntarily for assistance. These resources offer two types of assistance.

The first type of assistance is technical in nature. CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are agencies which have extensive knowledge of the tactics and variants criminals use to infiltrate their victims' computers and networks. They may be able to provide technical details on the attack and recommend mitigation strategies and actions. The agencies can be contacted directly for assistance.

The FBI and U.S. Secret Service are the agencies to contact to initiate a criminal investigation. They will investigate with the goal to bring the perpetrators to justice, but their investigation will include efforts to investigate links to other attacks and threats to our national security. Ransomware complaints can be filed directly with the FBI at https://www.ic3.gov/Home/Ransomware or with the Secret Service https://www.secretservice.gov/contact/field-offices/.

Last, the victim must decide whether they should pay the ransom or not. The federal government does not support the payment of ransom in response to a ransomware attack. Paying the ransom does not guarantee the criminal will deliver the decryption software/keys or restore the stolen data. Paying the ransom can also encourage the criminals to carry out more attacks and can attract new criminals looking to make a quick buck. It can also fund illicit activities or parties, in violation of the law. If the victim does not remediate the original vulnerability, the criminal may carry out the same ransomware attack again. More recently, in a twist on the typical ransomware scheme, criminals have exfiltrated sensitive data, threatening to sell or release the data on the black market unless a ransom is paid.

Whether a victim pays a ransom or not, the government still encourages victims to report the attack. This enables the government to track ransomware activity and link possible syndicates to other successful attacks. It also allows the government agencies to share the information with the private sector that may be helpful to prevent future attacks. Next month's article will discuss the type of payment the criminals demand and why. Tune in.

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