

# WHAT IS A RANSOMWARE ATTACK?

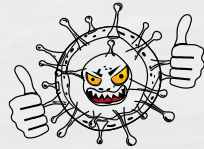
**Ransomware** is a global term for any computer virus used to deny access to a computer's system, data or files by the owner or authorized users. In exchange for its release, criminals typically ask for some form of payment or ransom, usually in bitcoin, which is untraceable.

## 5 Stages of a Ransomware Attack



### Installation

A victim opens a tainted email or link, unknowingly installing a ransomware virus into a computer or network.



### Confirmation

After installation but before the actual attack, the virus confirms execution with its criminal source code.



### Greeting

The virus and the criminal source server "shake hands," creating a key—the only thing that can unlock the locked files.



### Encryption

The virus starts the attack by encrypting files.



### Extortion

A demand is made for payment with the threat that the key will be destroyed and all files lost if not paid.

## IS THAT LINK LEGIT?

An employee clicks on a link in an email, releasing a virus that encrypts all files on the company's network, making them inaccessible. A demand appears for \$700 in bitcoin in return for the key to unlock the company's files.

Since the company has cyber insurance, they contact the incident response team provided by their insurance company. With the help of a forensic investigator, the team works with the company to remove the virus and restore the files from the company's last system back-up. Covered costs include system restoration and income lost due to network interruption.

## PROTECT YOUR BUSINESS

- ✦ Train employees to spot suspicious looking emails or websites
- ✦ Implement strong password protection rules
- ✦ Back up systems frequently
- ✦ Have a business continuity plan and test regularly
- ✦ Install and maintain updates for anti-malware software
- ✦ Maintain application and operating system updates
- ✦ Implement "least privileged" access
- ✦ Keep macros disabled
- ✦ Have a communication strategy in place to notify those affected

## INSURANCE TIPS

- ✦ Some policies only cover demands for money and not those related to social activism (like the Ashley Madison extortion).
- ✦ Demands are usually small. Consider a low deductible.
- ✦ Notice the "Notice Requirement." It may be a narrow reporting deadline.

## Cyber Insurance Education

- Fraudulent Funds Transfers
- Extortion / Ransomware**
- Social Engineering
- Business Interruption
- Data Breach/Privacy
- Network Security
- Website Media Liability

**ABA  
Insurance  
Services**

The loss prevention information presented is intended to provide guidance and is not intended as a legal interpretation of any federal, state or local laws, rules or regulations applicable to your business; it is intended only to assist policyholders in the management of potential loss producing conditions involving their operations based on generally accepted safe practices. The liability of Great American Insurance Company and its affiliated insurers is limited to the terms, limits and conditions of the insurance policies underwritten by any of them. The claims examples are provided for informational purposes only. No representation is made as to the truthfulness or accuracy of any fact, circumstance, allegation, or legal conclusion contained in or inferred from the examples presented above, nor is any representation made as to whether any claims example would constitute a "claim" or satisfy any other requirements for coverage under the applicable policy. Coverage for any claim is determined upon the specific facts presented, the terms and conditions of the policy and applicable law. ABA Insurance Services Inc. is an OH domiciled agency with its principal place of business at 3401 Tuttle Rd., Suite 300, Shaker Heights, OH 44122. © 2021 ABA Insurance Services Inc., dba Cabins Insurance Services in CA (License No. OG63200), ABA Insurance Services of Kentucky Inc. in KY, and ABA Insurance Agency Inc. in MI. 082021.SBM30