ACCORDING TO THE FEDERAL BUREAU OF INVESTIGATION,
MORE THAN 4,000 RANSOMWARE ATTACKS HAVE OCCURRED DAILY SINCE JANUARY 1, 2016.

WHAT IS RANSOMWARE?

Ransomware is a form of malware that targets critical data and systems for the purpose of extortion. Currently, there are two primary types of ransomware:

- Lockscreen: shows a full-screen message that prevents users from accessing their PC or files
- Encryption: changes files so they can't be opened

HOW DOES IT WORK?

Ransomware directs a user to click a link to pay a ransom to the cybercriminal in order to regain access to their system or files.

HOW DID RANSOMWARE GET ON THE PC?

Ransomware can be inadvertently downloaded when a user visits a malicious website or a website that's been hacked. Links to these malicious sites and other malware can also be delivered by email (which can often seem as though it's coming from a trusted source), infected removable drives or bundled in other software.

HOW DO I PROTECT AGAINST RANSOMWARE?

- Implement awareness and training programs to educate staff about the threat and delivery methods
- Schedule frequent, automatic back-up of your entire system to a secure storage system
- Verify the integrity of backups and test the restoration process
- Enable automatic security updates from operating systems, applications and devices
- Set web browser security level to detect unauthorized downloads
- Enable web browser pop-up-blocker

WHAT SHOULD I DO IF SOMEONE IS INFECTED WITH RANSOMWARE?

- Isolate and power-off all infected computers then remove from network immediately
- Secure back-up data or systems by taking them offline
- Contact local law enforcement, a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service to report a ransomware event and request assistance

SHOULD I PAY THE RANSOM?

There is no one-size-fits-all response for victims. The payment link provided may be malicious and could lead to additional malware infections and there is no guarantee that paying the fine or following the ransomware instructions will restore access. Deciding whether or not to pay the ransom requires serious evaluation of all options to protect customers, employees, and business. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup versus payment of the ransom.

Proactive prevention is the best defense; businesses with appropriate security measures in place may be able to eliminate the need to pay a ransom to recover data.

Community Title Agency, LLC
9211 Forest Hill Avenue, Suite 100
Richmond, VA 23235
O: 804-320-4185 | F: 804-320-2200
www.communitytitlerva.com

Community Title Agency

AN INDEPENDENT POLICY-ISSUING AGENT OF FIRST AMERICAN TITLE INSURANCE COMPANY