District Attorney's Office ▪ 18th Judicial District
George H. Brauchler, District Attorney ▪ Arapahoe, Douglas, Elbert & Lincoln Counties

Consumer Advisory

Lessons Learned from the '*WannaCry*' Ransomware Attack

By now, almost everyone has heard of the ransomware virus that recently infected thousands of computers worldwide. The assault, known as *WannaCry,* locked up computers and threatened to erase all stored information unless a ransom was paid to the extortionists to decrypt the files. Several Microsoft operating systems were hit, primarily networks that had not yet installed a security patch that was issued last March when the vulnerability was first detected. Also hit were Asian and European hospitals and organizations operating on Microsoft Windows XP, an older program that Microsoft terminated its support of in 2014. Most revealing, victims had not backed up their data to an external drive. This ultimately led to their attack.

Although ransomware viruses have been around for some time, the *WannaCry* attack has been the most widespread to date. This frightening event that shut down hospitals and emergency systems should nevertheless serve as a wake-up call – one that has revealed valuable lessons that if practiced, will provide important protections against a particularly nasty cybercrime that is expected to proliferate:

- **Make a habit of backing up critical data stored on the computer.** It is the most effective preventative measure against a ransomware attack. Back-up options include storing to the cloud, or to an external hard drive.
- Upgrade or run computer operating systems that are actively supported by the manufacturer. Outdated systems are at greatest risk of infection in spite of installed firewall/antivirus systems.
- Keep security software updated. Settings should be turned on to allow for automatic updates.
- Do not use unregistered or unlicensed (pirated) software. Updates cannot be installed on unlicensed software systems.
- Visit (or open) only trusted websites and familiar emails. When in doubt, don't open.
- Never pay the ransom (in ***Bitcoin**, or otherwise), if taken in a ransomware attack. Criminals can't be trusted and often don't unlock computers, even if paid. Instead, take the computer off-line so as to not infect other computers that may be on the network, and then engage a professional to fix the problem and to check for possible undetected viruses and other defects. Note that this isn't likely to restore any deleted files on the computer taken in a ransomware hit.

  For information on how Bitcoin, and other internet currencies work, click on Bitcoin
- Shut the computer down, or take the computer off-line when not in use.
- Take special precautions when using a public Wi-Fi. Choose settings that indicate you are on a public site. Doing so automatically blocks possible unsafe pathways to outside ports.
- If you are uncomfortable with computer knowledge or have difficulty keeping up with constantly evolving computer technology and 'language', consider making a trusted and knowledgeable friend or family member an administrator of your computer.

18th Judicial Consumer Fraud Protection Line: 720-874-8547 **5/18/2017**