Prevention Is the Best Cure:
Defensive Tactics against Ransomware

Submitted by Judy Hart, Chair of Informative and Protective Services

Attorney Ben Rossen of the Federal Trade Commission's Division of Privacy and Identity Protection, identifies "ransomware . . . as the most serious online threats . . . and the most profitable form of malware criminals use. Hackers hold your files 'hostage' by encrypting them and demanding payment, typically in bitcoins, for you to get them back." Nevertheless, there are some preventative steps you can take:

1. The breach occurred because of a security hole in the Windows server's software (Wood). It can be closed by an update from Microsoft. Keep your anti-virus software updated. The most effective step is to set your computer's anti-virus software to update automatically on your computers. Mobile devices may require that you manually update them. Keeping everything up-to-date gives you the most security. Install all security patches when they become available.
2. Avoid "clicking on links or downloading attachments and apps." Do not click on web pop-ups or unfamiliar e-mails. Ninety-one "percent of ransomware is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads" (Rossen). A phishing scam is not a virus. It is simply a hacker attempting to trick you and other people via emails with fraudulent websites that look legitimate (Kipter). The website is the bait. They snag you into looking for a good deal and ultimately into revealing financial data so that they can steal your identity. Once they lure you to the fake website, they seek your passwords and definitely your credit card numbers. If you have been phished, cancel your credit cards immediately.
3. Always back up your important files—all those files that would make you sick to lose them. When you have completed your task, routinely log out of the cloud, unplug external hard drives, and turn the computer off. If your computer routinely runs a security check at 2:00 a.m., for example, do not turn it off. Simply close the lid of your laptop or turn off the screen light on your desktop. Your computer will enter the sleep mode.

What if your defense has been breached?

1. You can sometimes contain an attack by disconnecting the infected devise from your network to keep ransomware from spreading. Otherwise, the ransomware attack spreads from your computer to your cellphone to your I-pads, etc.

2. If you have backed up your files and removed the malware, you may be able to restore your computer. Follow the instructions from your operating system to re-boot your computer, if possible. Unfortunately many of us rely on our

children and grandchildren to help us with our computer’s restoration. Since many of us have been in education for a lifetime, it is ironic that we balk at being educated about electronic devices.

3. You may want to go against the norm and choose an alternate operating system. C. Mitchell Shaw in his article “Foiling Foul Hackers” writes “installing or using Windows requires accepting Microsoft’s End User License Agreement (EULA) — which states, *`Finally, we will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary.’”* Shaw has taken exception to having his personal data compromised because Microsoft wants to use it as a marketing tool and sell it to others. He has opted for another operating system—Ubuntu, which has no EULA. And it’s free.” Furthermore, most of the applications available for Ubuntu are free, as well. It comes with LibreOffice (an open-source office suite comparable in function features to Microsoft Office) preinstalled, and there are open-source alternatives to almost any proprietary program. In fact, Shaw does all of his work on a laptop running Ubuntu 16.10 and has no proprietary software apps installed at all.

4. If you should experience a ransomware attack, report it to the Internet Crime Complaint Center of an FBI field office. You will need to include the contact information of the criminal such as the email address or payment demand information. For example, to what Bitcoin wallet number did he or she tell you to deposit? This information may prove helpful to investigators.

Crooks are a crooked and smarmy sort. If you pay the ransom, they may realize that your files are not backed up. Their next step may be to increase the ransom. After you pay the higher ransom, they may take pleasure in deleting your files. Or they may corrupt your files and give them back still encrypted. There is no guarantee that you can open the files if they return them (Mozure, Scott, and Goel.

Kipter, Barbara Ann and Robert L. Chapman. *Dictionary of American Slang.* Harper Collings. 2007.

Mozure, Paul, Mark Scott, and Vindu Goel. “Victims Call Hackers’ Bluff as Ransomware Deadline Nears.” *Business Day.* May 19, 2017. www.nytimes.com.

Rossen, Ben. “How to Defend against Ransomware.” FTC. Nov. 2016.

Shaw, C. Mitchel. “Foiling Foul Hackers.” *New American. April 14, 2017. www.thenewamerican.com.*

Wood, Nat. “WannaCry Worries? Update Now.” FTC Consumer Protection. May 15, 2017.

Informative and Protective Services Committee
Judy Hart, chair, District 16
Dr. Amy Jo Baker, District 20
Ron Gawryszewski, District 12
Jose Lugo, District 1
Dr. Thalia Matherson, District 10