

CRIMINAL JUSTICE and the **MEDIA:**

FBI'S RANSOMWARE VIRUS

Beginning just a few years ago, Internet users across the United States were startled when their computers froze up and a message popped up stating that they had been caught either downloading music or viewing illegal pornography. The message claimed to come from the FBI and stipulated that the computer would remain frozen until the user purchased a \$200 MoneyPak card (similar to a gift card) and entered the card number into the computer. These cards are untraceable but allow those with the card numbers to use them as if they were cash. The message on the computer also threatened criminal prosecution if the computer user did not enter a MoneyPak card number.

What was actually happening was that the computer had become infected with a type of *ransomware*. In some cases, the virus even turned on the computer's webcam and showed a video of the user on the screen. This really made it seem as if the computer user was being watched by someone.

Criminal justice officials offer the following advice to guard against ransomware:

- **Backup, backup, backup.** Regularly backup your files and keep these backups in an offline location that is not connected to the Internet.
- **Be careful what you click.** Be careful about e-mail attachments that you open and the links you click. As a rule, you should never open an unsolicited e-mail from a source you do not recognize.
- **Use anti-virus software.** Install anti-virus software and keep it up to date.
- **Stay on top of software updates.** Keep your operating system and other software up to date with the newest patches.

Adapted from Schuette, B. (n.d.). Consumer alert: Computer ransomware. Retrieved from http://www.michigan.gov/ag/0,4534,7-164-17337_20942-324685-,00.html