



EMS Information Bulletin 2017-08

DATE: May 30, 2017

SUBJECT: WannaCry ransomware cyber attack

TO: Pennsylvania EMS Agencies

FROM: Aaron M. Rhone, EMS Program Manager

A handwritten signature in blue ink, appearing to read "AMR", located to the right of the "FROM:" line.

In the wake of the recent WannaCry Ransomware cyber-attack, the Department of Health, Bureau of EMS would like to remind EMS agencies of the importance of cyber security.

The U.S. Department of Health and Human Services stressed that email attachments are a way for ransomware to spread and the following suggestions are recommended:

- Only open email attachments from people you know and from whom you are expecting information from. An attacker may impersonate the sender or the person you know may have an infected computer system without their knowledge.
- Do not click on links in emails if you weren't expecting them. Cyber-attacks can be camouflaged in seemingly harmless links.
- Keep your computer and antivirus software up to date. Software vendors are continually adding patches to their programs to help fight viruses.
- Software and technology companies like Microsoft and Apple will not call you and request access to your device or network, these are typically malicious actors trying to take advantage of the current situation. Access or information should not be provided to these individuals.

The Bureau of EMS recommends EMS agencies follow the above best practice recommendations. Questions regarding technical support for your agency's devices, including mobile devices, should be referenced to your technology provider.

Source:

HealthITSecurity. (2017). HHS Urges Caution in Wake of WannaCry Ransomware Attack. Retrieved May 25, 2017, from <http://healthitsecurity.com/news/hhs-urges-caution-in-wake-of-wannacry-ransomware-attackv>