Republic of the Philippines
Department of Education
Region III
SCHOOLS DIVISION OF NUEVA ECIJA
Old Capitol Compound, Burgos Avenue, Cabanatuan City, 3100

DEP-ED-NUEVA ECIJA
RELEASED
JUN 16 2017
RECORDS SECTION

June 15, 2017

DIVISION MEMORANDUM
No. 108 s. 2017

PUBLIC WARNING REGARDING THE WANNACRY RANSOMWARE

TO: **Public Schools District Supervisors**
Principals / Teachers -in-Charge
Public Elementary and Secondary Schools
Unit Heads
All Other Division Employees

1. The month of June is celebrated as ICT Month. Part of this is the preparedness to face the unexpected incidents involving hardware and software attack. The Schools Division Office Officials, Personnel and Teachers should be aware of the current situation regarding the vulnerability of the Windows Operating System.

2. As of this moment, the National Security Agency warned Microsoft about the vulnerability in Windows after a hacker began to leak hacking tools used by the agency online. The vulnerability has been the center of attention in recent days, following the outbreak of the global "WannaCry" ransomware attack that crippled foreign government system and has spread to at least 150 countries. The ransomware is widely believed to be based on an alleged NSA hacking tool leaked by the group Shadow Brokers earlier this year.

3. Based on the analysis, the attack, "WannaCry", is initiated through an SMBv2 remote code execution in Microsoft Windows. This exploit (codenamed "EternalBlue") has been made available on the internet through the Shadowbrokers dump on April 14 2017 which allows to trick Windows into running any code they want by sending a special packet over the network. This is made possible by a bug in the Microsoft Server Message Block 1.0 (SMBv1) server, a service that is running by default on most Windows computers. According to the table released by Microsoft, "ETERNALBLUE" was fixed by MS17-010 released in March. However, the PC that is outdated is prone to this type of attack.

4. It is important to understand that while unpatched Windows computers exposing their SMB services can be remotely attacked with the "EternalBlue" exploit and infected by the WannaCry ransomware, the lack of existence of this vulnerability does not really prevent the ransomware component from working. Nevertheless, the presence of this vulnerability appears to be the most significant factor that caused the outbreak. **THUS, EVERYBODY IS ADVISED TO ALWAYS BACKUP THEIR FILES, TO UPDATE WINDOWS REGULARLY AND AVOID OPENING AND ACCESSING UNKNOWN SITES AND EMAIL PROMOS.**

5. Once infected, please isolate the computer from the network and contact Mr. Roderic S. Elegado, IT Officer. Remember that when the infection is severe there is no way to save the files. It is strongly advised not to pay any ransom money to recover files. To get rid of the infection, slowly format the hard drive and reinstall Windows OS.

6. Immediate dissemination of this Memorandum to all concerned is earnestly desired.

RONALDO A. POZON. Ph.D., CESO V
Schools Division Superintendent