Dear MCPS Colleagues,

As you probably are aware, last week a very serious cyber-attack known as the Wanna Decryptor 2.0, spread worldwide. This attack is the latest in a line of "ransomware" worm viruses that lock up files on a computer and use encryption to deny a legitimate user or file owner access to those files unless a fee (ransom) is paid to unlock them. This type of virus almost always enters an organization by a user clicking a link in the email or a link on a website. While we continue to enhance our systems and monitor the international, cyber security community's response to this attack, it is important to remember the following protective guidelines:

- Do not click a link in an email unless you are completely certain that it is safe to do so. Even though the web link may appear safe, the programming behind the link can often redirect you to an unsafe site once selected. When there is any doubt, do not click questionable links. You may delete the email immediately or send it to abuse@mcpsmd.org.

- Do not share your personal or financial information in an email.

- Do not respond to email solicitations for your information. This includes clicking on or visiting sites sent through email. Email solicitation is a very common method (phishing) of enticing users to share or automatically collect user access information.

- Enter your username and password only on known MCPS authorized applications.

- Ignore attachments that you were not expecting, especially if you do not know the sender. Many malicious attachments masquerade as Word documents or familiar file types. Contact the Help Desk (301) 517-5800 or report suspicious messages to abuse@mcpsmd.org.

- Do not open or interact with any email message from an organization or individual with whom you did not directly share your information.

- Do not respond to notices from financial institutions requesting that you change your personal information or your password. Financial institutions will never ask for these details through email. Contact your financial institution directly to verify that your account was not accessed or changed without your permission.

If you have any questions, please do not hesitate to contact the Help Desk at (301) 517-5800 with any questions. Thank you for your continued vigilance and cooperation.

Sincerely,

Andrew Zuckerman
Chief Operating Officer
Montgomery County Public Schools