School Districts continue to be prime targets for the ransomers. Please also take your parents. Older folks are also primary targets of ransomers.
What we need to be aware of regarding ransomware:

- Ransomware is most often delivered through email, in an attachment, or through a link to a malicious website.
- Over the past week, our filters stopped over 12,500 emails from reaching CSH mailboxes. Many of these emails were Spam or Phishing attacks.
- Your email inbox is the preferred path into the district by hackers.
- Remember that all email sent by non-CSH users has "[EXTERNAL SENDER]" as the start of the subject line. So be suspicious of an email claiming to be from a CSH employee that.
    - Has [EXTERNAL SENDER]" in the subject line
    - The email address does not end in "@csh.k12.ny.us"
    - Is vague is the subject matter or states that XXXX is an urgent matter.
- If you ever suspect that an account has been compromised
    - For School – Contact Joe Monastero ASAP, and we will change the password.
    - A Personal account - Contact the vendor and change the password.

***Quick Tip* - Use the REPEL method to check your email for risk.**
R-REQUESTED - did you request this email? Is it relevant?
E- EMAIL ADDRESS - does the email of the sender look valid?
P- PERSONAL INFO - are you being asked for personal information or being requested to log in?
Beware of *Phishing!*
E-Errors- are there *obvious* grammatical or spelling errors in the copy?
L-LINKS - review the link; does it point to the claimed organization's website?
Additional Tips Below

Link to the Federal Trade Commission site on recognizing and Avoiding Phishing Scams