

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](#)

RIC NEW YORK STATE REGIONAL INFORMATION CENTERS
one DATA SECURITY PRACTICES FOR EDUCATORS

Educational agencies are experiencing more frequent cyberattacks. These attacks involve stealing data, holding information systems hostage, and causing disruptions in service. Follow these simple tips to help enhance your district's security posture.

HUMAN BEHAVIOR IS AT THE ROOT OF 95% OF ALL CYBER SECURITY INCIDENTS.

DATA PROTECTION REMINDERS

E-MAIL PRACTICES	Exercise caution before clicking on a link in an e-mail or opening an attachment.
WORKSTATION PRACTICES	Lock workstations when leaving them unattended.
PASSWORD PRACTICES	Establish strong passwords. Do not write down passwords and leave in an easily accessible location.
DATA HANDLING PRACTICES	Use appropriate tools when handling data. Never send sensitive information through unencrypted email.
PRIVACY PRACTICES	Do not establish accounts for students to access online resources without consulting with administration.

PHISHING EMAILS

Phishing e-mails are one of the most common, and effective, methods cyber attackers will use to gain access to secure information.

1. Exercise **CAUTION** before **SENDING SENSITIVE INFORMATION** through email.
2. Exercise **CAUTION** before **CLICKING ON A LINK** in an e-mail or **OPENING AN ATTACHMENT**.
3. **REPORT SUSPICIOUS EMAILS** to your IT Department.
4. If you fall victim, **REPORT INCIDENTS** to your IT Department immediately.