Always THINK before you CLICK!

Don’t help others steal your information.

TARGETED EMAILS
From hackers will look legitimate at first glance.

Make sure the email is GENUINE before you click on Any links!

What to Check For

1. Look for grammatical errors.

2. Treat any email you did not expect to receive with suspicion.

3. Check for odd phrases and word choice based on your knowledge of the sender.

4. Hover over links to see if the web address is legitimate and relates to email’s content.

5. Verify any email that asks for person information by independently looking up the sender’s contact information.

Report To

Report all suspicious emails to the Department of Information Technology at:
CyberITsecurity@clevelandmetroschools.org