Dr. Juliette Pennyman, Superintendent of Schools

The following message is being sent on behalf of Hudson City School District Superintendent Dr. Juliette Pennyman, Manager of Instructional Technology Cheryl Rabinowitz and the Instructional Technology Department to Hudson City School District families, faculty and staff members.*

May 15, 2024

Good morning, Hudson City School District Families, Faculty and Staff!

The Hudson City School District has a high level of network security, anti-virus, and monitoring systems in place, but nothing is 100% foolproof. The best defense is our staff and students (technology users), who we ask to continue to be conscientious and report emails that may be suspicious, or emails that may not look suspicious, but they have questions about.

Recently, we addressed a phishing email that appeared to come from a staff member but was not sent by the staff member. The email went to some of our students and staff members throughout the District.

The email contained a link to a Google Form that requested information from the recipient. Some users who received these emails opened the email and entered personal information, such as their name, address, and phone number. Then, they were sent a text message that asked for their bank account information. We understand that is where users became suspicious and reported it.

When this type of data is entered through a phishing email, it's considered a data incident. As the Data Privacy Officer for an educational agency, it is reported to NYSED.

We want to thank the students and staff who brought the phishing email to the attention of the Hudson City School District Instructional Technology Department, which was immediately able to retract it from any user who received it. The IT Department isolated the device from which the email was sent, temporarily disabled the staff member's account, and changed the password.

Unfortunately, schools are becoming more and more targets of cyber attacks, such as phishing, viruses, scams, and other types of cybersecurity threats. We ask that you continue to be hyper-vigilant in reporting concerns when they arise, whether they be an email, an advertisement, or a link that you may have clicked on. It is very important that we address it immediately. We also want to remind technology users not to enter any personal information that is requested. Always question the source. It is best NOT

to respond to the email with the question but either contact the person by phone, in person, or through a separate email inquiring if they sent you an email to confirm the legitimacy.

For reporting the emails, we ask that you do not forward the email but report it as "phishing" in the email system and notify the District's IT Department immediately so it can be reviewed and addressed if it is a phishing email. To report a phishing email in the email system, you will notice when an email message is open, there are 3 dots in the top right corner (see screenshots below). Click on the 3 dots and choose, "Report phishing."

Besides emails, people may be targeted through their cell phones, and we suggest you follow these protocols on your personal devices to protect your information and block the user who is sending you text messages.

In the next two weeks, the District will roll out Multi-Factor Authentication to all staff. We currently have it for our district administrators, the IT department, and other district office staff. It is another layer of security that will continue to enhance our protocols.

We will also continue with Cyber Security Awareness Training for our staff, which we have implemented in the past. In the near future, staff will be receiving more information about MFA and Cyber Security Awareness Training.

We ask that staff and families continue to review the importance with the students for reporting emails that may be found suspicious to their teacher and their family, who should report it to the District's IT Department through the District's Helpdesk System, Incident IQ for staff and families by contacting the IT Department at 518-828-4360 ext. 2118.

Working together, we can continue to keep all technology users safe from these cybersecurity threats.

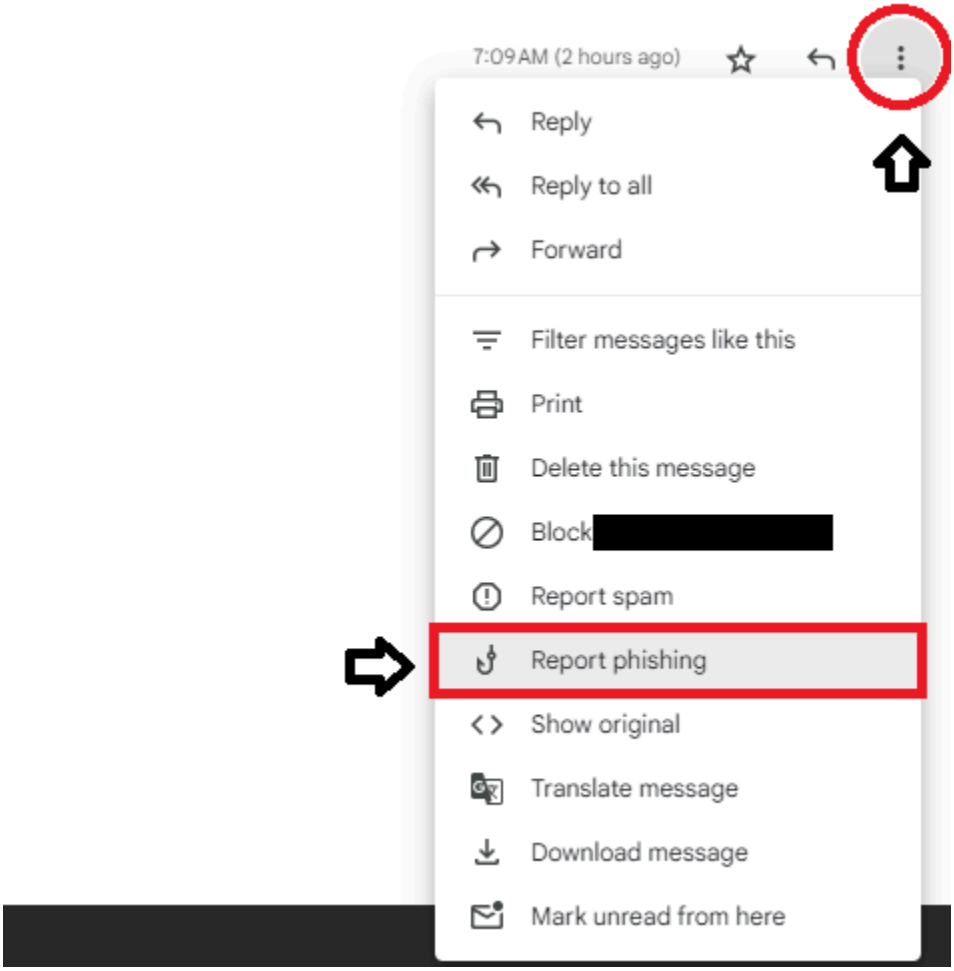
As always, if you have any questions or concerns about the phishing email/data incident, please do not hesitate to contact Cheryl Rabinowitz,Manager of Instructional Technology and Data Privacy Officer at rabinowitzc@hudsoncsd.org or at 518-828-4360 ext. 2119.

Thank you for your continued support.

Have a great day!

HUDSON
CITY SCHOOL DISTRICT

Directions for Reporting Phishing through the Email System



Sincerely,

Dr. Juliette Pennyman
Superintendent of Schools
Hudson City School District
#HudsonTogetherWeCan!

Cheryl Rabinowitz
Manager of Instructional Technology
Hudson City School District