We have recently noticed an increase of fraudulent activity and want to make you aware of one of the latest forms of fraudulent activity. The newest threat is posed as Executive Impersonation.

What is Executive Impersonation?

- The fraudster spoofs an executive's email account or pretends to be an executive on the phone.
- Spoofed emails may be targeted to individuals that can provide information or initiate payments.
- Fraudsters can perform a significant amount of research on the targets and the company to support their scheme beforehand.
- Types of scams include (but are not limited to): Requests to purchase gift cards, irregular wire transfer requests, and checks.

Tips to protect your School/Center:

- Carefully **scrutinize** all emails.
- Be wary of irregular emails that are sent from senior executives, as they are used to trick employees into acting with **urgency**.
- Review emails that request information/funds to determine if they are **out of the ordinary**. There are a few red flags you can look out for:
    - The email address contains a suspicious domain,
    - The sender name is vague, the content, contains poor grammar, or includes an irregular link (different from your organization's standard email address).
- If a caller claims to be an executive working for your organization, ask them politely for their internal phone number and say you'll call back.

More information

For additional ways to protect your school/center against fraud, check out the following information:

- **Payments Fraud Hits Record Highs**
  Check Fraud and Business Email Compromise (BEC) Scams Are on the Rise
  https://commercial.jpmorganchase.com/pages/commercial-banking/executive-connect/afp- infographic
- **Solutions That Protect Your Bottom Line**
  Our best-in-class security measures and industry-leading technology help keep your accounts and payments safe.
  https://commercial.jpmorganchase.com/pages/commercial-banking/services/ts-fraud- prevention