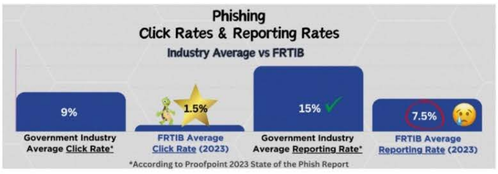
Are you looking for an easy New Year's resolution that will also protect FRTIB? We have just the thing. Commit to reporting suspicious emails! Reporting phishing emails is crucial to protect yourself and others from online threats and contributes to the identification and mitigation of phishing attacks. This helps in preventing potential financial losses, unauthorized access to personal information, and the spread of malicious activities. Additionally, reporting phishing emails assists in raising awareness and allows cybersecurity experts to analyze emerging trends, enhancing overall online security measures. According to Proofpoint's 2023 State of the Phish report, FRTIB is way below the government industry average in regard to our click rate but there is definitely room for improvement in our reporting!



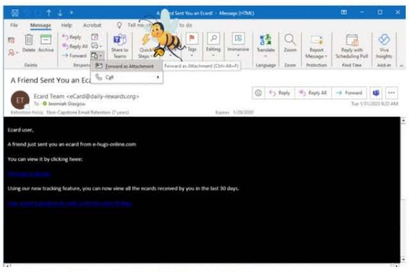
When examining emails for potential phishing attempts, watch out for:

- Sender information: Review the sender information to verify the email address is legitimate.
- Mismatched URLs: Check if the email links direct you to legitimate websites. Hover over links to preview the destination.
- Spelling and Grammar: Phishing emails often contain spelling mistakes and grammatical errors although this is becoming less common with the increasing use of AI.
- Urgency or Threats: Phishing emails often create a sense of urgency or use threats to manipulate recipients into taking immediate action.
- Attachments or Links in Unsolicited Emails: Avoid opening attachments or clicking on links in emails from unknown or unexpected sources.

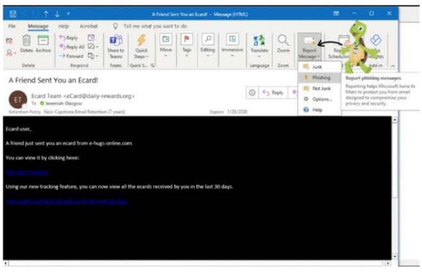
How to report a suspicious email:

You have 2 options:

1. Forward the email to **ReportPhishing@frtib.gov**



2. Use the **Report Message** tool on the ribbon in Outlook



For additional information, visit: Security Education, Training and Awareness (sharepoint.com)

JPMorgan Chase Confronts Unprecedented Cybersecurity Challenge

In a staggering revelation, JPMorgan Chase finds itself at the epicenter of an escalating cybersecurity battle, contending with a relentless barrage of 45 billion hacking attempts daily. This alarming figure marks a doubling from the previous year, highlighting the intensification of cyber threats faced by the financial giant.

To counter this unprecedented onslaught, JPMorgan has committed a substantial $15 billion annual investment in cybersecurity measures. The enormity of the task at hand is reflected in JPMorgan's formidable technologist workforce, numbering 62,000 strong.

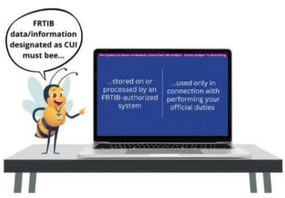
Moreover, the deployment of artificial intelligence (AI) has emerged as a critical component in JPMorgan's defense against cyber threats. As adversaries leverage AI to enhance the sophistication of their attacks, the bank's technologists employ cutting-edge AI tools to stay one step ahead. The dynamic nature of the cybersecurity landscape requires continuous innovation, and JPMorgan's commitment to maintaining a robust technological infrastructure is evident in its ongoing efforts.

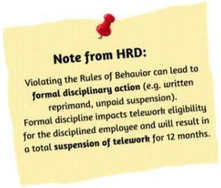
Read the full article here: https://www.cnbctv18.com/technology/davos-wef-jpmorgan-battles-45-billion-daily-hacking-attempts-amid-rising-cyber-threats-18833651.htm

Reminder: FRTIB Data/Information: To Send or Not to Send!

In case you missed our communication in December on this subject, here is a recap:

Recently, the Threat Detection & Response Branch (TDRB) and Insider Threat team have identified numerous events involving employees and contractors forwarding official documents to personal and/or corporate accounts without approval. While some documents are safe for you to send to a non-FRTIB email address, others are prohibited. Please review the information below to avoid violating Agency policy.



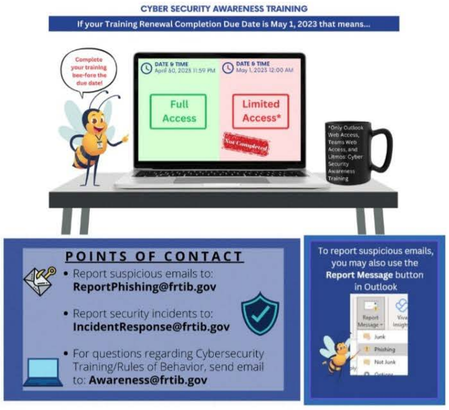


All users are required to review and accept the Rules of Behavior (RoB) before being granted access to the network on first login and annually thereafter. As a refresher, we highly encourage you to review the full Rules of Behavior, which can be found in the SETA Site Reading Room or by clicking the link here: FRTIB Rules of Behavior.pdf

Important updates to this communication:

1. Do not send any FRTIB data/information to your personal or corporate email address unless Agency approved (see FRTIB Rules of Behavior, Item 28 for exception list) or approved by your Office Director.
2. Please reach out to the CUI Program Manager for guidance on this topic, cui@frtib.gov.

Reminders:



For additional information and resources, please visit the SETA Site on the FRTIB Town Center under Offices > OTS > IT Security Management Division > Security Education, Training, and Awareness (SETA) .

Stay safe. Stay Secure.

Regards,
The SETA Team