RECEIPT OF FRAUDULENT EMAIL

Email scams, such as phishing and spoofing, often target employees by making it seem as if the emails are coming from internal managers or other trusted persons. RAILS scam-detection systems provide some protection. However, such emails may still not be detected and reach an employee.

RAILS' Executive Director, or any other RAILS employee, will never request via email any employee to purchase anything on their behalf or to advance any employee's personal funds to an outside entity. In addition, the RAILS' Executive Director or any other RAILS employee will not make requests for any personal information (other than directly through Human Resources), particularly pertaining to banking or credit card account numbers.

If you receive a suspicious email, please do the following:

1. Do not respond to the email or unsubscribe to it. This tells the scammer that you have read the email and will only encourage additional solicitations.

2. Forward the email to the IT help desk, noting that it is a scam email, and then delete it from your mailbox.

3. If you have any doubt as to the email's authenticity, carefully view the sender's email address. It will often have the alleged sender's name in it but an address different from the sender's true email address (for example, a fraudulent email purporting to be from a RAILS employee but without an email address ending in @railslibraries.org). If you still have doubts, personally contact the alleged sender.