Remain vigilant! Reported phishing and other business email compromise schemes targeting U.S. government employees and annuitants.

Please remain vigilant and immediately report phishing schemes and other business email compromise (BEC) attempts. USAID OIG's Office of Investigations recently undertook investigative steps to identify bad actors employing BEC tactics designed to redirect OIG employee paychecks to nonsanctioned bank accounts. In September 2023, USAID OIG posted a fraud alert on BECs, how to identify them, and how to mitigate them. Last week, the U.S. Department of State OIG posted a similar fraud alert on BECs targeting government employees and annuitants.

As a reminder, BEC **red flags** include:

- Requests to change bank account information through electronic communications
- Being pressed to act quickly to complete a transfer of funds/change account information
- Email from a known sender where the address appears similar to, but is different from, the actual email address
- Unusual or suspicious language used in the body of the email, such as spelling/grammar errors, or unfamiliar phrasing/terms
- Requests for unconventional payment methods (e.g., salary direct deposits to Green Dot or Western Union accounts)

We can all **mitigate** these fraud schemes through verification:

- Carefully examine all email addresses, URLs, and language
- Call the person or organization by telephone to verify bank account/payment changes or requests for other account information
- Do not click any links or download any attachments from unsolicited emails or text messages to update or verify account
- Do not call numbers provided by the unsolicited emails
- Strengthen protocols on funds transfers and payment procedures
- Maintain a robust IT security infrastructure and best practices with routine cybersecurity awareness training for all employees

If you think you've fallen victim to a BEC, please contact USAID OIG and your payroll office immediately. ***NOTE: All links in this alert are safe to click on.**