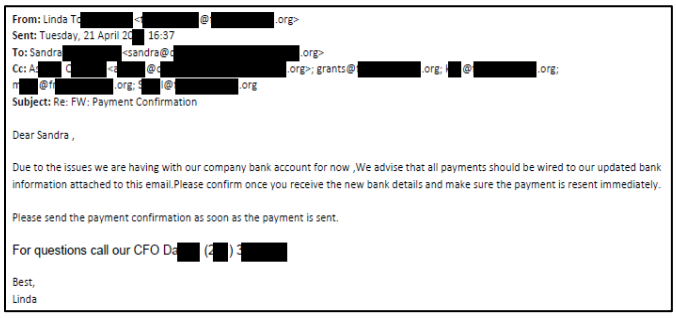
USAID Office of Inspector General
Office of Investigations
Fraud Alert – Sept 2023

Business Email Compromise Scheme Alert

USAID's Office of Inspector General (USAID OIG) investigates allegations of fraud and corruption in U.S.-funded foreign assistance programs. This document highlights an ongoing fraud scheme and identifies mitigation steps for preventing future attempts to compromise USAID's programming worldwide.

Business Email Compromise Schemes

Business email compromise (BEC) is a sophisticated yet common scam. It is often perpetrated by international organized crime syndicates that target individuals, businesses, and organizations that make routine wire transfer payments to vendors or suppliers. These schemes rely on compromised email accounts, typically gained from cyber intrusion or social engineering techniques, to trick an organization's employee to unwittingly transfer funds to bank accounts belonging to the scammers.



From: Linda T[redacted]
Sent: Tuesday, 21 April 20[redacted] 16:37
To: Sandra [redacted]
Cc: A[redacted]
Subject: Re: FW: Payment Confirmation

Dear Sandra ,

Due to the issues we are having with our company bank account for now ,We advise that all payments should be wired to our updated bank information attached to this email.Please confirm once you receive the new bank details and make sure the payment is resent immediately.

Please send the payment confirmation as soon as the payment is sent.

For questions call our CFO D[redacted]

Best,
Linda

Figure 1. Actual BEC email sent to a USAID awardee.

Detection

USAID offices, awardees, and program beneficiaries are particularly vulnerable to BEC scams due to the international nature of their work, the significant electronic monetary transactions, and the availability of information online about awardees, projects, and employees. USAID OIG has identified and investigated allegations regarding successful and attempted BEC scams affecting USAID programming around the globe.

BECs are easy to detect and, with simple due diligence, can be mitigated, saving billions of dollars annually. The red flags listed below outline BEC efforts USAID OIG has recently identified. Figure 1 provides an actual example received by a USAID awardee. Allegations received to date include:

- Under a government-to-government award, USAID received an email message from an alleged host government agency to transfer project funds to a new scammer-controlled bank account based in a third country.
- Beneficiaries received fictitious emails from individuals impersonating USAID staff, alleging that they had been selected to receive hundreds of thousands of dollars in COVID-relief funds. The emails contained a link to the official USAID website and contact information for an alleged USAID employee. However, upon closer examination, it became clear the emails had originated from a Gmail account unrelated to USAID.
- Beneficiaries received text and WhatsApp messages from individuals impersonating U.S. government officials attempting to acquire personal identifying information.
- A U.S.-based awardee was defrauded after receiving a spoofed email from a scammer pretending to be its subgrantee overseas. The scammer then tricked the employee into transferring funds to a new bank account.
- An awardee's executive unwittingly fell victim to a malware attack; their official email was compromised, and fraudsters used their real email address to instruct the awardee's financial team to change its SAM.gov information. As a result, USAID deposited funds into the scammer's bank account rather than the awardee's.

Red Flags

- Requests to change bank account information through electronic communications.
- You are pressed to act quickly to complete a transfer of funds – especially if there is also a change in payment 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 (i.e., cryptocurrency, gift cards).

Mitigation Efforts

- **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 information.
- **Do not call numbers** provided by the unsolicited emails.
- **Carefully examine** all email addresses, URLs, and language.
- 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.

To report suspected fraud, corruption, or other serious misconduct go to:
https://oigportal.ains.com/eCasePortal/Forms/Complaints.aspx?templateName=Hotline