

logo not found or type unknown

Puerto Rican Government Agency Lost \$2.6 Million to an Email Phishing Similar to the One That Cost WAPA a Similar Amount

Government / **Published On February 14, 2020 05:30 AM /**

Robert Moore **February 14, 2020**

Image not found or type unknown



Puerto Rico Flag By. RICARDO ARDUENGO/AP

Much like the V.I. Water and Power Authority (WAPA), the Puerto Rican government industrial development agency lost more than \$2.6 million after falling for an email phishing scam, the Associated Press reported Thursday.

The AP cited a complaint filed with police by Ruben Rivera, the finance director of the Puerto Rico's Industrial Development Company. Rivera told authorities that the agency transferred the money back in January after receiving an email that alleged a change to a banking account tied to remittance payments, the AP reported. Officials told the AP that the incident was discovered

earlier this week and was immediately reported to the FBI.

In 2018, [WAPA twice paid invoices](#) it believed to be from a real vendor, paying a total of \$2.17 million, according to statement the power authority issued in June 2019. The FBI was also investigating the so-called “Business Email Compromise” scam.

Digital thieves targeted companies that conduct wire transfers, like WAPA. Publicly known email addresses of employees that conduct financial transactions are compromised by phishing or other digital attacks to carry out fraudulent money transfers.

WAPA has since provided cybersecurity training for its staff, and training on how to recognize phishing emails.

In neighboring Puerto Rico, Industrial Development Company officials declined to say how officials found out about the scam, whether anyone has been dismissed or how the company’s operations have been affected by the missing funds, according to the Associated Press.

“This is a very serious situation, extremely serious,” said Manuel Labor, executive director of the agency. “We want it to be investigated until the last consequences.”

Similarities in the two phishing scams are striking, but it is unknown whether the two cases are related.