Office of Inspector General

Committee for Purchase From People Who Are Blind or Severely Disabled (U.S. AbilityOne Commission)

Investigative Summary │20-32

Finding of a Policy Violation by a Senior Official for Sharing Access to the Official's Outlook Email System with Two Subordinates, Thereby Contributing to the Success of a Spoofing Attack

The Office of Inspector General with assistance from GSA OIG has completed an investigation on a spoofing attack that targeted the U.S. AbilityOne Commission. The attack concluded with a theft of $6,482.11 from the payroll of a Senior Agency Official (the "Official"), a breach of the Official's account at OPM's Employee Express system, and release of the Official's PII from government systems.

During the course of the investigation, AbilityOne employees expressed concern that the hacker appeared to use inside knowledge to succeed at the spoofing attack. AbilityOne OIG examined how the hacker may have gained access to the information necessary to spoof the Official's name and writing style, as well as how the hacker knew to target the attack at the contractor in charge of payroll. We also examined whether AbilityOne policies and actions of staff may have enabled the hacker's success.

AbilityOne written IT policies forbid the sharing of system access. With technical assistance from the IT office, the Official shared access to the Official's outlook email system with two assistants. Access included all sent and received emails, and the ability to send emails on behalf of the Official. The shared access was critical to the hacker's success, as the hacker deceived staff into using the Official's email account to reset an OPM Employee Express password and to forward the reset code from the Official's government email account to the hacker. The Official's violation of the IT policy contributed to the hacker's success.

Through the effort of AbilityOne and GSA, all payroll funds were recovered, leading to no loss for the Official or the Government. On learning that all funds had been recovered, and on learning that the hacker based his attack from a server located outside of the United States, we determined to bring the investigation into the hacker to a close.

We provided a report of investigation to the Commission for appropriate action.