

Facebook Being Utilized to Victimize Families of U.S. Military Personnel Serving in Iraq

Facebook is a free-access global social networking website. Users can join networks organized by city, workplace, school and region to connect and interact with other people (see Figure 1).

Grandparents are being contacted through Facebook under the guise of being their grandson returning home on leave from Iraq. The "soldier" asks the grandparents to keep his presence secret so he can surprise his parents.

The "soldier" advises he is stranded because his buddy's car broke down enroute. He asks them to wire several thousand dollars to his buddy to cover the cost of car repairs.

Summary

It is opined that due to the alarming amount of personal data available through most Facebook accounts, scammers are utilizing social engineering to target relatives. These scammers exploit the trusting nature and limited contact that most grandparents have with their adult grandchildren. Community outreach organizations should advise all relatives to verify the identity of anyone who contacts them by asking specific questions known only to that person before wiring funds. Military members should provide family members with a codeword or phrase to verify their identity in the future, as well as assess their Facebook accounts for exploitable information.

This bulletin has been prepared by the Kansas City Division of the FBI. Comments and queries may be addressed to the Kansas City Field Intelligence Group at 816-512-8200.



(U) Figure 1.

Source: FBI Situational Intelligence Report - Kansas City Division