Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 04, 2014

# AFRICAN CYBER CRIMINAL ENTERPRISE MEMBERS USING "SCHOOL IMPERSONATION" SCHEME TO DEFRAUD RETAILERS

Subjects posing as school officials are defrauding retailers by purchasing large volumes of merchandise using fraudulently obtained lines of credit. Originally this scheme affected mostly office suppliers and computer retailers; however, recent successful attempts lead subjects to use this scheme against other retailers for industrial equipment, pharmaceuticals, safety and medical equipment. This advisory informs readers how the scheme works, offers measures to help mitigate the threat, and advise how to report incidents to law enforcement.

How the Scheme Works

Step 1: A subject, posing as a school official, contacts a retailer's customer service call center by telephone or e-mail. Using social engineering tactics, the subject attempts to gather additional information about the purchasing account. The subject typically terminates the phone call or e-mail session once sufficient information is gathered to place an order. Subjects also obtain account information from the school's public website, if available.

Step 2: The subject makes a second contact with the target vendor, again representing himself as a school official and providing the account information obtained from step one. Billing to the school's line of credit, the subject makes large purchases (such as laptops, routers, hard drives, printer toner, printer ink, medical supplies, and industrial equipment) with some orders totaling more than $200,000.

Step 3: During the purchase, the subject provides the customer service representative with a U.S. shipping address, typically belonging to a victim of a "romance scam" or "work from home" fraud scheme. A subject contacts the online scam victim and directs the individual to re-ship the office supplies to an address in West Africa, typically Nigeria, the United Kingdom, or to a U.S.-based storage or warehouse facility. To facilitate the re-shipment, the individual receives a shipping label prior to receiving the merchandise.

In a more recent variation of the scheme, the subject provides the true shipping address of the school he is purporting to represent. The subject then contacts the school, posing as an employee of the vendor, claiming that the products were shipped to the school in error. The school, believing it is returning the products to their rightful owner, reships the items to a domestic address provided by the subject. Recruited individuals in the U.S. then re-ship the products overseas. What started with a small number of educational institutions has rapidly spread through copycatting and spoofing techniques to include some complaints reporting businesses instead of schools or universities being victimized.

E-mail Account Spoofing Techniques are used by subjects to place orders by establishing false school e-mail accounts, which appear similar to legitimate school e-mail addresses but lack the .edu extension. Below are variations of spoof email addresses:

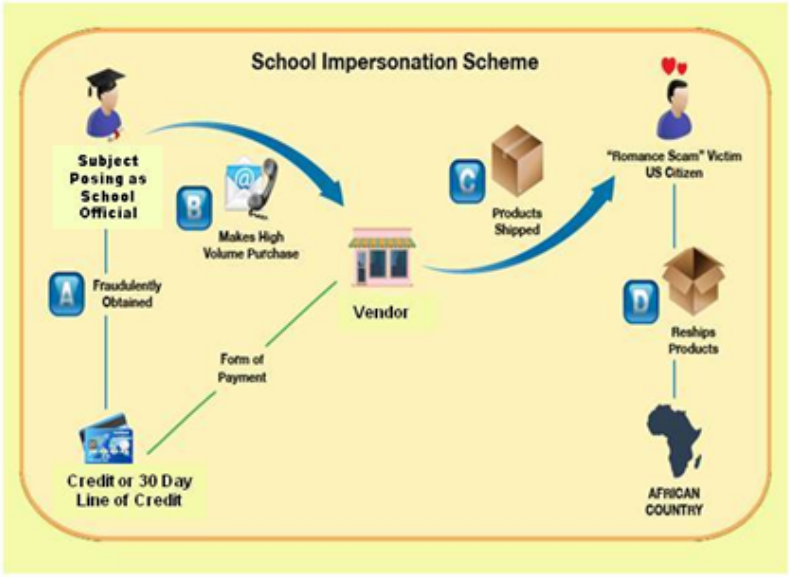
- purchasing@ucdavised.us
- purchasingdept@unlav-edu.org

- purchase@uchicagoed.us

Once the fraud is discovered, the retailer absorbs the financial losses without recourse to the school. See the graphic below for a depiction of a common variation of the school impersonation scheme.

A subject, posing as an employer or romantic interest, gains the trust of individuals searching for employment opportunities or a romantic relationship. After a period of social engineering, the individuals are convinced to serve as money remitters or re-shippers on behalf of the subject.

---




Visit

http://www.ic3.gov for more information.