Department of Energy
Office of Inspector General

February 9, 2018

FRAUD ALERT

False Government Purchase Order Scheme

The OIG is alerting vendors throughout the United States of a false purchase order scheme. The scheme consists of conspirators submitting false purchase orders to vendors through the use of fictitious email addresses made to resemble authentic Government email addresses. Specifically, conspirators misrepresent themselves and Department contractor employees to vendors and submit false purchase orders to vendors for products such as hard drives, computers, and toner cartridges. Shipments are routed out of the country, as vendors await payment.

Businesses can take proper precautions to minimize risks of becoming potential victims of the false purchase order scheme. Below are some potential fraud indicators.

- Incorrect domain names on websites, e-mails, and purchase orders are used by conspirators. As example, a ".com" or ".org" is used by conspirators to communicate, rather than a ".gov" address.
- The shipping address on a purchase order is not the same as the business location, as per the Department contractor website.
- Purchase orders request immediate shipment of goods on 30 day credit, pending Government payment.
- The delivery address is a personal residence or private-storage facility.
- E-mail are poorly written and correspondence contains grammatical errors, suggesting messages were not written by fluent English speakers.
- Phone numbers used and provided are not associated with Department contractors.
- Calls to phone numbers provided by conspirators are not answered.
- Purchase orders for unusually large quantities of merchandise are requested to ship priority or overnight.

If you believe your business has been victimized by this scheme, please report the incident immediately to local authorities, the DOE OIG Hotline, and/or the FBI. Early notification can help authorities locate and stop shipments before merchandise is shipped out of the country. Early notification may increase the likelihood for items to be located, seized, and returned. The DOE OIG Hotline may be contacted by telephone at (800) 541-1625 or by email at ighotline@hq.doe.gov. The FBI has an Internet Crime Complaint Center (IC3) that allows businesses and private parties to report such matters. The website can be accessed at https://www.ic3.gov/default.aspx.

October 27, 2014

Cyber Crime

Purchase Order Scam Leaves a Trail of Victims

Nigerian criminals behind purchase order frauds use fake or stolen e-mail addresses to deceive retailers. They also dupe individuals who are the victims of online romance or work from home scams to re-ship merchandise out of the country, as seen above.

What began as a scheme to defraud office supply stores has evolved into more ambitious crimes that have cost retailers around the country millions of dollars—and the Nigerian cyber criminals behind the fraud have also turned at-home Internet users into unsuspecting accomplices.

FBI investigators are calling it purchase order fraud, and the perpetrators are extremely skillful. Through online and telephone social engineering techniques, the fraudsters trick retailers into believing they are from legitimate businesses and academic institutions and want to order merchandise. The retailers believe they are filling requests for

established customers, but the goods end up being shipped elsewhere—often to the unsuspecting at-home Internet users, who are then duped into re-shipping the merchandise to Nigeria.

"They order large quantities of items such as laptops and hard drives," said Special Agent Joanne Altenburg, who has been investigating the cyber criminals since 2012 out of our Washington Field Office. "They have also ordered expensive and very specialized equipment, such as centrifuges and other medical and pharmaceutical items."

Our investigators have found more than 85 companies and universities nationwide whose identities were used to perpetrate the scheme. Approximately 400 actual or attempted incidents have targeted some 250 vendors, and nearly $5 million has been lost so far.

The scam has several variations, but basically it works like this:

- The criminals set up fake websites with domain names almost identical to those of real businesses or universities. They do the same for e-mail accounts and also use telephone spoofing techniques to make calls appear to be from the right area codes.
- Next, the fraudsters—posing as school or business officials—contact a retailer's customer service center and use social engineering tactics to gather information about the organization's purchasing account.
- The criminals then contact the target business and request a quote for products. They use forged documents, complete with letterhead and sometimes even the name of the organization's actual product manager. They request that the shipments be made on a 30-day credit—and since the real institution often has good credit, vendors usually agree.
- The criminals provide a U.S. shipping address that might be a warehouse, self-storage facility, or the residence of a victim of an online romance or work-from-home scam (see sidebar). Those at-home victims are directed to re-ship the merchandise to Nigeria and are provided with shipping labels to make the job easy.
- The vendor eventually bills the real institution and discovers the fraud. By then, the items have been re-shipped overseas, and the retailer must absorb the financial loss.

"Once the merchandise has been shipped to Nigeria, it is nearly impossible to get it back," Altenburg said. "Small and mid-size businesses and universities are being targeted all over the country."

Although the cyber criminals are practiced at deception, there are ways to spot the fraud, according to Special Agent Paula Ebersole in our Washington Field Office. "The most important thing is to independently verify shipping addresses," she said, "no matter how legitimate a website or e-mail looks."

Businesses should also be on the lookout for e-mails that contain unusual phrases or spellings, indicating that messages were not written by a fluent English speaker. And bogus phone numbers provided by the fraudsters are rarely answered by a live person. "That should raise a red flag," Ebersole said.

"If your business has been scammed," she added, "time is of the essence. If you report the theft to local authorities or the FBI before the merchandise is shipped out of the country, there is a chance the items can be located and returned."

In addition to investigating these crimes, Ebersole and Altenburg are also getting the word out to the business community about purchase order fraud through the Domestic Security Alliance Council, a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security, and the private sector. "We want to make everyone aware of this potential threat," Ebersole said.

At-Home Victims

E-mail and Internet ads offering lucrative work-from-home jobs are everywhere online, and so are match-making websites. But many online offers of employment and romance are scams—and those who fall for them might end up helping African cyber criminals carry out purchase order fraud.

"These criminals are experts at posing as an employer or romantic interest online," said Special Agent Joanne Altenburg. "They gain the trust of individuals looking for work or a romantic relationship, and after a period of social engineering, those individuals are convinced to serve as re-shippers on behalf of the subject. They almost never suspect they are doing anything illegal."

These secondary victims agree to accept packages sent directly to them and then re-ship them overseas, thinking it is either part of their job or they are doing a favor for their romantic interest. "A lot of these people don't believe it when I tell them they are being scammed," Altenburg said. "The criminals are very good at what they do."

Indicators of Fraud

Businesses can avoid becoming victims of purchase order fraud by being aware of several fraud indicators:

- Incorrect domain names on websites, e-mails, and purchase orders. The scammers use nearly identical domain names of legitimate organizations, but in the case of a university, for example, if the URL does not end in .edu, it is likely fraudulent.
- The shipping address on a purchase order is not the same as the business location. Likewise, if the delivery address is a residence or self-storage facility, it should raise red flags.
- Poorly written e-mail correspondence that contains grammatical errors, suggesting that the message was not written by a fluent English speaker.
- Phone numbers not associated with the company or university, and numbers that are not answered by a live person.
- Orders for unusually large quantities of merchandise, with a request to ship priority or overnight.

If you are the victim of purchase order fraud, it's important to contact local law enforcement and the FBI. You should also report the crime to the Internet Complaint Center (IC3). If the fraud is discovered before the goods are shipped to Nigeria, there is a good chance the merchandise can be recovered. More than $1 million worth of merchandise has been recovered, thanks to businesses quickly discovering the fraud. More on IC3 (https://www.ic3.gov/default.aspx).

Resources:

- Press release (https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/african-cyber-criminal-enterprise-members-using-school-impersonation-

scheme-to-defraud-retailers)
- More about African cyber criminal enterprises
(https://www.fbi.gov/news/stories/understanding-school-impersonation-fraud)
- Domestic Security Alliance Council (https://www.dsac.gov/)