Scam Alert –No. 1 Email Domain Typosquatting

Issue: Schemes in which a scammer will represent itself to be a company employee and place an order with a vendor/supplier on the company's account. Also schemes in which a scammer will represent itself as being a company customer and place an order with the company.

Description: In these schemes, the scammer creates an email address and represents itself to be an employee of a company looking to purchase an item or items. The email address domain often includes a slight misspelling of a company's actual email domain. In some cases, the difference can be just one letter. The scammer may also use an email domain that someone could reasonably expect to be a legitimate email domain.

The scammer may request a pricing quote for loosely controlled export items that cannot be legitimately purchased through other means (3M masks, fluke meters, flir cameras, Enerpac items, etc.). The scammer then creates a fake Purchase Order with an illegitimate "ship to" address and sends to the seller. Frequently, the order needs to be rushed, drop shipped, etc. in an attempt to get the seller to order and ship without processing any red flags that might be present. The scammer will also request frequent updates on shipping information so the package can be tracked and, possibly, re-routed. Often the material is ordered and shipped across multiple states in order to convolute the process and complicate any investigation.

Law enforcement personnel believe it is common for the scammers to contact the shipping party and advise them that the material will be picked up at the shipping facility to avoid it ever reaching the address in question. In other cases, individuals who stay at home, and want to make extra money, will receive the product, unbox and repackage the material to be shipped elsewhere (often overseas). These handlers may not have any knowledge of the item's origin or that the material was part of a scam. Once it leaves the U.S., the items are impossible to recover.

As for the phone numbers used by the scammer, a common practice is to use something like the MAGIC JACK computer based VOIP phone system, which allows the scammer to create a temporary number from any legitimate address.

Red Flags: Below are key red flag fraud indicators:
* Email address does not match the company's valid email domain.
* The shipping address on a purchase order does not match a valid business location, but maybe a residence or self-storage facility.
* 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. Numbers that are not answered by a live person. If a phone call is answered, often the person answering has a foreign accent and could not provide any information to validate the legitimacy of the order.
* Orders for unusually large quantities of merchandise with a request to ship priority or overnight. Sense of urgency for the seller to act quickly.
* Frequent requests for updates on shipping info, tracking, etc.

Conclusion: Look for red flags. If something doesn't seem right, it probably isn't, so it's worth the time to investigate. If you haven't transacted with the individual or business before, take the extra steps necessary to validate the order. Consider having someone else review to determine legitimacy. Use the resources available to research – company websites, location information, Google Maps/Google Earth search, etc. If the order seems too good to be true, it might be.