3351 Michelson Drive, Suite 100
Irvine, CA 92612-0697

6 April 2020

Dear Valued Ingram Micro Partner,

Please be aware and take action: Fraudulent sales orders are on the rise. As a channel, we have a responsibility to do everything we can to mitigate this behavior to protect ourselves, our companies, and our clients.

Please pay closer attention to details, watch for suspicious activity, and let's work together to keep our teams informed and empowered to take the extra step to verify legitimate deals. We're seeing instances of fraud for our partners from their long-term customers (who have had their email breached) as well as from 'new customers' that are 100% fraudulent.

To help teams identify and stop what may be fraud, our Ingram Micro sales teams offer up this great advice.

For New Customers
If an order comes in from a new customer, is unsolicited, and seems too good to be true, then it probably is. Other potential fraud signals that we've seen from the frontlines include:

- If the new customer is pressed for time and okay with any price you give them.
- If the customer is ordering something that is not your core area of focus (memory, laptops, tablets).
- If the new customer wants you to overnight a large order with no concern for cost.

If you suspect a fraudulent order from a new customer, what should you do?

- As a best practice, perform an internet search on the company name and check their email address against the known company domain.
- Google Earth any address given to you as a "ship-to" and see the locations and its surroundings. Warehouses in desolate areas or non-descript office parks and freight forwarder addresses are all common ship-to addresses for scammers.
- Check all addresses for that company on the internet and confirm if the address they are having you ship to is one of them. Be warned – scammers have been known to transpose street numbers or zip code numbers on their ship-to location to look very similar to actual end user addresses.

For Existing Customers:
Your existing customers can be and are being breached as well. The bad guys are getting into their email systems and creating PO's on company letterhead which can look perfectly legitimate – especially when it is sent directly from a valid email address from a known customer. And watch for abnormal purchases. Is your managed security client with 50 employees, sending you a PO for 150 laptops?

If you suspect a fraudulent order from an existing customer what should you do?

- Check the email address sent to you for the request carefully. A common trick is when an email address has one character off from the actual company or entity domain name or will use a .net instead of .com or .org.
- Check if the ship-to location is different than the location you usually ship to (ex: a different state, a completely different address or an unlikely address for that company or entity).
- Perform an internet search on the company and check the domain website against the domain email address.
- Pick up the phone – and call your client to verify.
- Take a quick inventory. If the existing customer is buying unusual product than what they typically purchase AND are buying in fairly extraordinary quantities, STOP and call them via the phone number YOU have on file for them, not the one in the email sent to you with the request.

Fraud isn't as easy to spot as it used to be. Scammers are getting better and more sophisticated. At Ingram Micro we are continually training our team to spot potential fraud and to contact you directly to confirm if there is any doubt.

Let's work together to eliminate fraudulent orders.

Warmest Regards,

Eric

Eric Kohl
Vice President, Advanced Solutions
Ingram Micro Inc.