Fraud Alert: Fraudsters are Targeting Cisco Channel Partners

Cisco Brand Protection

April 21, 2021
There is currently a known fraud scheme targeting resellers of technology products, including Cisco Channel Partners. The fraudsters are buying internet domain names similar to real end users and are then, via email, posing as that end user to purchase a large volume of Cisco products on credit from the reseller. The reseller supplies the requested products on credit, but no payment is received.

Here are some tips to protect your company from being a victim of this fraud scheme.

Verify the email company name (e.g., xyz.com and xyzco.com) and domain (.gov, .edu, etc). Domains can be checked through free websites like https://www.whois.com or https://whois.icann.org/en. The following are red flags for bogus domains:

- Domain is recently registered.
- Website has no information or is “under construction.”
- Domain lacks information that allows one to verify ownership.

Verify the shipping address. Red flags include:

- Address not used previously by company
- PO Box
- Residential address
- Shipping/logistics company or freight forwarder
- Public storage facility

Conduct due diligence on the individual or company to ensure that they are legitimate and are in fact part of the company they represent.

- Check the telephone number and email address.
- Check other websites regarding the person and/or company (e.g., LinkedIn).
- Telephone a company-verified telephone number to check the status of domain name, individual, shipment address, and/or telephone number.

Please contact Cisco's Brand Protection team at brandprotection@cisco.com if you think you may be a victim of this fraud scheme. This information will help Cisco:

1. validate that a fraudulent transaction has in fact occurred; and
2. identify information that may be of use to law enforcement in their investigation.

If you have already determined you are a victim of this fraud scheme and the fraud is in the United States or one of its territories, we also recommend reporting the case to the FBI at the Internet Crime Complaint Center (IC3) website: https://www.ic3.gov/.