DLA CERT Fusion Cell

Date:
Dec 10, 2018

Vendors are Frequent Targets of E-Mails and Scams from Spoofed E-Mails and Fake Domains

NOTICE

The Defense Logistics Agency's Cyber Emergency Response Team Fusion Cell has been made aware of multiple scams targeting DLA vendors and US corporations. These scams frequently are from non-governmental e-mail addresses and attempt to trick potential vendors into shipping products to locations and expecting payment from the government at a later date. Other scams may attempt to steal account credentials to governmental systems.

How to Identify Potential Fake E-Mails

The E-Mails are not from a .MIL or .GOV account

Some of the prime candidates for targeting of DLA vendors are users who may sell to DLA or use **FedMall**, **DIBBS**, **SAM**, **FedBizOpps**, **GSA STARS**, or **Login.GOV** websites.

Any e-mails received by vendors/companies regarding this services should undergo additional scrutiny as they have been key targets in 2018 of scammers, and will likely remain so for the foreseeable future.

E-Mails coming from domains/websites that do not end with .MIL or .GOV are highly suspicious!

If you receive an e-mail from an account at a domain that does not end in .MIL or .GOV, but claims to be a US government representative, it is probably a scam and could be malicious. If you receive an e-mail that appears to be from a government representative, but the "reply to" e-mail address is used that is not an e-mail address that ends in .MIL or .GOV, please be aware that the communication is a scam; if you use the Reply feature in your e-mail client, and the e-mail address that the e-mail supposedly came changes to one that is not the e-mail address it appeared to have been sent from, the e-mail is highly suspicious.

In These Scams – Many Times the Scam Targets Are Not in the "To" Line

Always remain cautious of e-mails that arrive in your inbox that are not explicitly sent to you. Sometimes scammers attempt to hide their actions by addressing their targets in the BCC (Blind Carbon Copy) Line. In these scams we have seen variations that are both "From" and "To" a supposed government employee.

Use Caution with Attachments and Links

Do Not Open Attachments from Suspicious Addresses

Do not open attachments or visit websites suggested by suspicious e-mail addresses. Malicious actors could potentially embed malware into an attachment or on a webpage in order to compromise a corporate network.

Links may look similar to an official website, but may be dangerously different

Typically if a password needs to be reset, a user should go directly to the site and follow the instructions on the official website. Malicious actors may send e-mails that encourage a user to take immediate action at the potential of having their system access revoked or be fined; this is often done to invoke an emotional response rather than allowing your brain to process the information. Assess every e-mail to ensure that it is in fact from an official source.

Actors can spoof e-mail accounts and make an e-mail address appear to be from a different domain. Contact your company's IT department or Help Desk if you are unsure of the authenticity of an e-mail.

In Closing

If you are a DLA vendor and are targeted by an actor pretending to be a DLA Employee, please reach out to the Fusion Cell via our official e-mail at: CERTFusionCell@DLA.MIL