DLA CERT Fusion Cell

Date:
June 8, 2018

Malicious Actor Targeting Private Vendors Through GSA STARS II by E-Mail Spoofing

NOTICE

A fake solicitation purporting to be from Defense Logistics Agency (DLA) for a "REQUEST FOR QUOTATION" has been targeting GSA STARS II vendors in the public sector.

How to Spot the Fake E-Mails

The E-Mails are Not from DLA.MIL

The e-mail may appear to be from DLA on first glance; however, the "Reply-To" address of the fake e-mails ends with a "**@dla-mil.us**" extension. In some cases, "**stars2@americanconsultants.com**" has been identified to supposedly send messages on behalf of a DLA Contract Specialist – these are also fake.

Non-DoD Website Usage

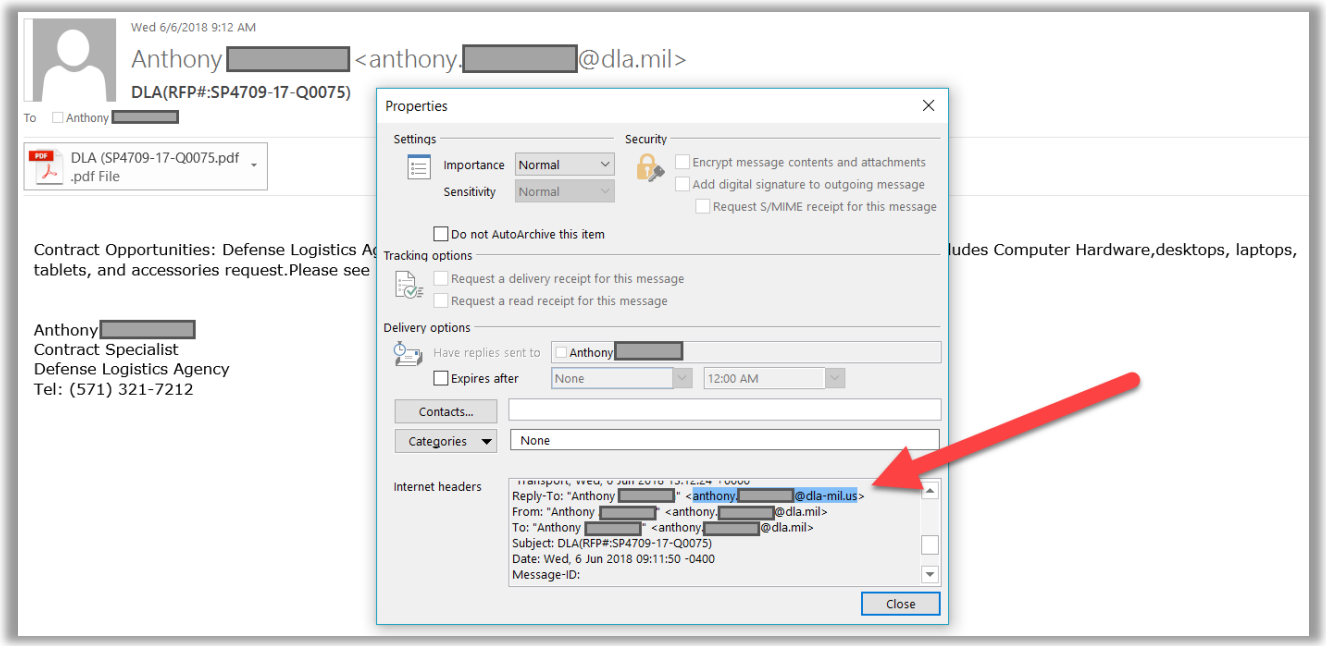
Some e-mails suggest the companies' use the "stars2" Google Group <https://groups.google.com/a/americanconsultants.com> for more information or to unsubscribe from the e-mail communication. The "stars2" group is *NOT* a DLA affiliated group.

Non-DoD PDF Attachment

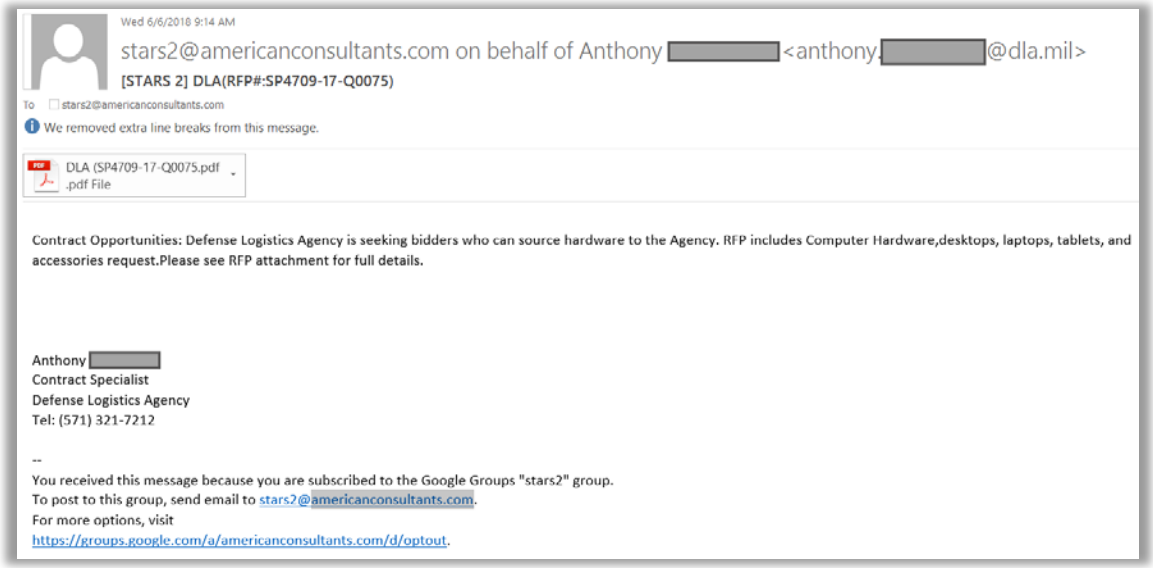
Example of the FAKE E-MAIL (#1) – "DLA(RFP#:SP4709-17-Q0075)"

FAKE E-MAIL (#1) uses a different "Reply-To" E-Mail Address

Only by looking at the "headers" of the e-mail address, or actually attempting to reply, would a user notice that the "Reply To" e-mail address (from the non-government domain **DLA-MIL.US**) is different than the sender's e-mail address.

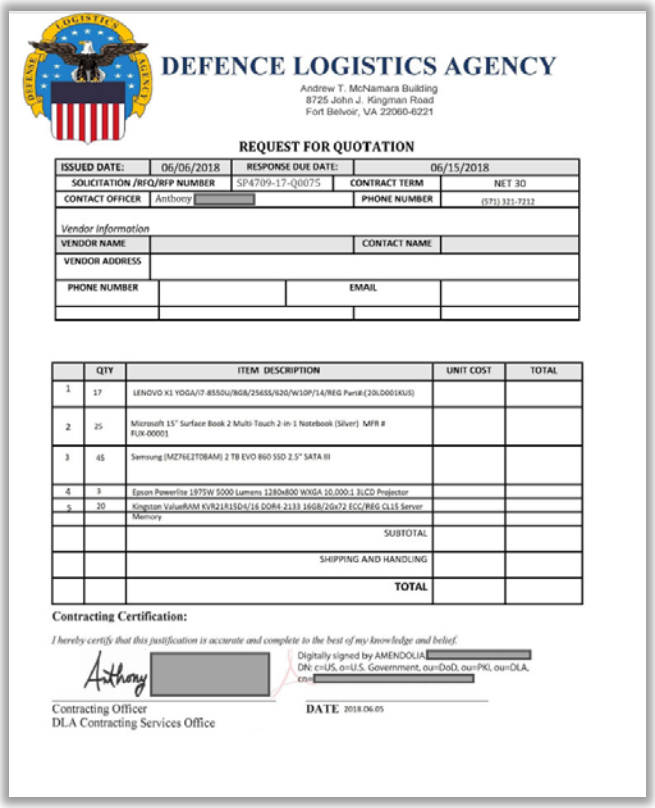


Example of another FAKE E-MAIL (#2) – "[STARS 2] DLA(RFP#:SP4709-17-Q0075)"



Non-DoD PDF Attachment

Example of the FAKE "REQUEST FOR QUOTATION"



DEFENCE LOGISTICS AGENCY

Andrew T. McNamara Building
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6221

REQUEST FOR QUOTATION

ISSUED DATE:	06/06/2018	RESPONSE DUE DATE:	06/15/2018
SOLICITATION /RFQ/RFP NUMBER	SP4709-17-Q0075	CONTRACT TERM	NET 30
CONTACT OFFICER	Anthony [redacted]	PHONE NUMBER	(571) 321-7212

Vendor information

VENDOR NAME		CONTACT NAME	
VENDOR ADDRESS			
PHONE NUMBER		EMAIL	

	QTY	ITEM DESCRIPTION	UNIT COST	TOTAL
1	17	LENOVO X1 YOGA/I7-8550U/8GB/256SS/620/W10P/14/REG Part#:(20LD001KUS)		
2	25	Microsoft 15" Surface Book 2 Multi Touch 2-in-1 Notebook (Silver) MFR # FUX-00001		
3	45	Samsung (MZ76E2T0BAM) 2 TB EVO 860 SSD 2.5" SATA III		
4	3	Epson Powerlite 1975W 5000 Lumens 1280x800 WXGA 10,000:1 3LCD Projector		
5	20	Kingston ValueRAM KVR21R15D4/16 DDR4-2133 16GB/2Gx72 ECC/REG CL15 Server Memory		
		SUBTOTAL		
		SHIPPING AND HANDLING		
		TOTAL		

Contracting Certification:

I hereby certify that this justification is accurate and complete to the best of my knowledge and belief.

Anthony [redacted]

Digitally signed by AMENDOLIA [redacted]
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OLA, cn=[redacted]

Contracting Officer
DLA Contracting Services Office

DATE 2018.06.05

In These Scams – Many Times You 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.

Non-DoD Form Usage and Phone Number

The telephone number (571) 321-7212 is *NOT* a Defense Logistics Agency (DLA) phone number. The shown "Request For Quotation" is not an official form, and the Common Access Card (CAC) Signature Block is flat and scanned in.

In Closing

Remain vigilant, and be cautious when opening attachments. This specific e-mail attachment was not identified to contain malware, but the financial risks are high if the scammer is able to get a company to send them a virtual grocery list of technical items. Be sure to contact your typical DoD point of contact when engaging in business to ensure the best possible communication and safety. Questions or comments can be directed to DLA CERT's Fusion Cell at: CERTFusionCell@DLA.MIL