1

Beware of certain banks

Green Dot and GoBank are legitimate banks, and many people use them. Governments should pay attention to transactions with these banks because most of the losses reported to our Office have used one of them.

2

"Kindly" look for certain language

Many scam requests ask you to "kindly" respond or "kindly" make the change. This word, in particular, as well as generally overly formal language, seems to be a telltale sign of a fraudulent request.

3

Double-check the check

Look for obvious flaws in the check included with the request, such as incorrect payee info, banking/routing numbers in the wrong location, unusual font or format; or signatures and "void" notations using a machine-generated script font.

Change Payment Requests:

SIX SIGNS of a SCAM

4

Show some love to that @gov email address

Watch for spoofed email addresses, which look close to the real deal but may be a character or two off. You should also be wary of employee emails coming from non-work addresses.

5

Question new requests submitted in new ways

If you require employees to make changes in person or through an online portal, closely scrutinize any requests coming through email. Similarly, look for requests sent through a different department, which scammers typically do in an effort to avoid scrutiny.

6

Obey the speed limit

Don't rush to process a request that's close the payment date or instills a sense of urgency. Scammers often use this pressure tactic hoping you will act before closely evaluating the request's legitimacy, or that you will bypass established verification procedures.

Go to **www.sao.wa.gov/improving-government/preventing-fraud** for more resources