

# Spear Phishing Attacks Targeting Government Entities

Cybercriminals relentlessly try to infiltrate government agencies all over the world. Foreign adversaries, nation-states, and terrorists target our networks for espionage, financial gain, and to steal credentials and classified information. Attacks may also try to gain unauthorized access to military systems to cause physical damage, destruction, and disruption. Government agencies are frequently spoofed in phishing emails and fraudulent websites. Using social engineering techniques, phishers often impersonate senior officials requesting subordinates provide or review information. As the number of cyberattacks targeting our industry continues to increase, it is important to be aware of the latest threats.

The image shows a simulated email interface with several callouts pointing to specific parts of the email content:

- Callout 1:** "Do you recognize the sender?" points to the "From: admin@abcfed.net" header.
- Callout 2:** "Were you expecting this message?" points to the "Subject: Contract Number #DC244384066" header.
- Callout 3:** "Refers to a non-existent Government entity." points to the "U.S. Federal Financial Debt Department" header.
- Callout 4:** "Appeals to the emotions of fear." points to the text "As per agreed in 7.b of the loan contract, we are about to use our right of property expropriation." in the main body.
- Callout 5:** "Mentions a legitimate organization to try to establish credibility." points to the text "the sub-owner didn't have right for sub-lease the property until the end of the sub-lease agreement with the initial owner, which is HomeServices of America." in the main body.
- Callout 6:** "Do you know where this link leads?" points to the "Get Contract Details" link in the main body.

## REMEMBER:

- 1 Don't interact with unsolicited hyperlinks and attachments
- 2 Use extra caution on mobile devices
- 3 Encrypt email and files
- 4 Always verify