

CYBER AWARENESS ADVISORY

DIGITAL INVESTIGATIONS BUREAU - CYBER INVESTIGATIVE GROUP



JANUARY 2024



Phone Calls or Emails from **FAKE** Law Enforcement or Government Officials

The Cyber Investigative Group (CIG) of the Las Vegas Metropolitan Police Department has been made aware of an increase in phone calls, texts and emails impersonating law enforcement officers and government officials.

What Is An Impersonation Scam?


An impersonation scam is a type of phone or email scam where cybercriminals attempt to extort money from victims by claiming to be a legitimate law enforcement officer or an agent from a Federal agency like the FBI, DEA and IRS.

The victims are told they have warrants for failing to appear in court and are threatened with arrest, instilling a sense of fear. These scammers often want money but some have forcibly convinced victims to show their private parts or perform an intimate act on video.

How To Protect Yourself

- Do **NOT** send cash, wire transfer, mail gift cards or go to a cryptocurrency ATM to anyone saying they are from a law enforcement agency or a government entity.
- Do **NOT** trust the caller ID. Phone numbers and identities can be spoofed or tricked. Be skeptical and verify by calling the main phone line or non-emergency number.
- Do **NOT** give or confirm your personal identifiable information (PII) with unsolicited phone calls, text messages and emails.

If you get a suspicious phone call, immediately hang up. If you get a questionable email or text message, just delete it. And do the following:

- File a complaint with the Internet Crime Complaint Center  www.IC3.gov, the FBI-managed reporting mechanism for suspected Internet-facilitated crimes.
- If you have sent money by any method, nude pictures or divulged PII, and you feel that you were a victim of a crime, go to your local substation and file a police report.