DEPARTMENT OF PUBLIC SAFETY

DAVID Y. IGE
GOVERNOR

NOLAN P. ESPINDA
DIRECTOR

FOR IMMEDIATE RELEASE
Apr. 22, 2020

SHERIFF IMPERSONATORS, PHONE TEXT EXTORTION SCAM ALERT

HONOLULU – A recent Sheriff impersonator scam incident has prompted the Department of Public Safety Sheriff Division to put out a warning. On Monday, an individual called the Sheriff Division to report that he was contacted via text by someone claiming to be a “Sergeant Anderson” with the Sheriff Division Internet Crimes Task Force. The impersonator stated that the man would be arrested for inappropriate internet use unless he paid an undisclosed amount of money.

The public is reminded that Sheriffs do not call, text or email people asking for personal information or to solicit payment electronically or by phone. Hawaii residents are also advised not to provide credit card numbers or other personal information to callers claiming to represent a law enforcement agency.

If you receive a call matching this scam please alert the Sheriff Division by calling 586-1352.

The FBI recently put out a warning to the public about an increase in similar online extortion scams during the current “stay at home” orders due to the COVID-19 crisis.

According to the FBI public service announcement: online extortion schemes vary, but there are a few common indicators of the scam.

- The online extortion attempt comes as an e-mail from an unknown party and, many times, will be written in broken English with grammatical errors.
- The recipient's personal information is noted in the e-mail or letter to add a higher degree of intimidation to the scam. For example, the recipient's user name or password is provided at the beginning of the e-mail or letter.
- The recipient is accused of visiting adult websites, cheating on a spouse, or being involved in other compromising situations.
- The e-mail or letter includes a statement like, "I had a serious spyware and adware infect your computer," or "I have a recorded video of you" as an explanation of how the information was allegedly gathered.
- The e-mail or letter threatens to send a video or other compromising information to family, friends, coworkers, or social network contacts if a ransom is not paid.

- The recipient is instructed to pay the ransom in Bitcoin, a virtual currency that provides a high degree of anonymity to the transactions.

FBI's TIPS TO PROTECT YOURSELF:

- Do not open e-mails or attachments from unknown individuals.
- Do not communicate with unsolicited e-mail senders.
- Do not store sensitive or embarrassing photos or information online or on your mobile devices.
- Use strong passwords and do not use the same password for multiple websites.
- Never provide personal information of any sort via e-mail. Be aware that many e-mails requesting your personal information appear to be legitimate.
- Ensure security settings for social media accounts are activated and set at the highest level of protection.

The FBI's public service announcement can be found here:
https://www.ic3.gov/media/2020/200420.aspx
Questions regarding the FBI PSA should be directed to the local **FBI Field Office**.
Local Field Office Locations: www.fbi.gov/contact-us/field

###

Media Contact:
Toni Schwartz
Public Information Officer
Hawaii Department of Public Safety
Office: 808-587-1358
Cell: 808-683-5507
Toni.E.Schwartz@hawaii.gov
http://hawaii.gov/psd/