PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 002-2019 January 11, 2019

# FEDERAL SHUTDOWN SCAMS

The Pennsylvania State Police (PSP) is reminding residents to be alert for scams that may attempt to take advantage of the current government shutdown. These scams may appear as email solicitations, email links or attachments, phone solicitations, or pop-up Internet pages. Residents should note that due to the shutdown the Federal Trade Commission customer complaint system is non-operational, leaving a gap between victim reporting and consumer alerts.[1] Some of the known scams include:

- Contacting people over the phone or by email and claiming to be from a government office and implying that the victim's federal benefits such as their Medicare direct deposits will stop unless personal bank information is received for verification.[2] The scammer may spoof their phone number so it looks like it came from a local area code when in reality, they could be calling from anywhere and it may be impossible to trace.[3]
- Calling and offering pre-approved loans or grants in exchange for the victim's banking information, claiming the scammer needs it so they know where to send the money.[4]
- Furloughed workers should also be aware of the side job offers. There are a lot of fake postings that require an application fee.[5]
- Cybercriminals often send fake emails that look like they came from banks so people will open them. The emails may not specifically be related to the shutdown, but they might be good enough to fool someone who is under financial stress. These emails contain links leading to websites that will download malware, or have attachments containing malware.[6]

## RECOMMENDATIONS

The PSP reminds residents to remain vigilant and follow the below recommendations. If something does not seem right, report the suspicious incident to your local police department. Additional tips to avoid falling victim to scams include:

- Never provide anyone with personal information such as your social security number, date of birth, credit card number, bank account, or address.
- If you receive an email from a financial institution that looks suspicious, do not open links or attachments.[7] For example, if the email uses poor grammar and spelling, does not use your name or other personal identifying information, or goes to an email address not linked to the company or agency it pretends to be sent from, it is probably not legitimate.[8] Delete it and sign on to your account using the web address you know belongs to that agency or your bank.
- Government agencies will rarely call you unless you have been in touch with them first. If someone calls you claiming to be from a government agency and you were not expecting a call, hang up and call the agency back either at their customer-service number (available on the agency's website, which ends in .gov), or at another number for that agency that you may use, such as the number for a local office.[9] Government agencies will never ask for your personal information over the phone or through email.
- If you have questions about your government benefits or the government shut down, visit or call your elected representative for the most up to date information.
- Above all, use common sense. If something does not seem right, it probably is not right.

**If you become the victim of a scam, notify your financial institution and local law enforcement agency immediately!**

[1] First Orion. (2019, January 4). Scam alert: Government shutdown scam. *First Orion*. Retrieved on 1/9/19 from https://firstorion.com/scam-alert-government-shutdown-scam/.
[2] Seamen's Bank. (n.d.). Banks report seniors targeted in shutdown-related scam. *Seamen's Bank.* Retrieved on 1/9/19 from https://www.seamensbank.com/banks-report-seniors-targeted-in-shutdown-related-scam/.
[3] Federal Communications Commission. (n.d.). Caller ID spoofing. *Federal Communications Commission*. Retrieved 1/10/19 from https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.
[4] First Orion. (2019, January 4). Scam alert: Government shutdown scam. *First Orion*. Retrieved on 1/9/19 from https://firstorion.com/scam-alert-government-shutdown-scam/.
[5] Shone, C. (2019, January 9). Scammers targeting federal workers impacted by govt. shutdown. *KOB4.* Retrieved on 1/10/19 from https://www.kob.com/investigative-news/scammers-targeting-federal-works-impacted-by-govt-shutdown/5204357/.
[6] Palmer, D. (2017, September 28). Watch out: These phishing emails claiming to be a 'secure message' from your bank. *ZDNet.com* Retrieved on 1/10/19 from https://www.zdnet.com/article/watch-out-these-phishing-emails-claiming-to-be-a-secure-message-from-your-bank/.
[7] Palmer, D. (2017, September 28). Watch out: These phishing emails claiming to be a 'secure message' from your bank. *ZDNet.com* Retrieved on 1/10/19 from https://www.zdnet.com/article/watch-out-these-phishing-emails-claiming-to-be-a-secure-message-from-your-bank/.
[8] Broida, R. (2017, September 5). How to spot a phishing email. *CNet.com*. Retrieved on 1/11/19 from https://www.cnet.com/news/galaxy-s10-launch-date-confirmed-feb-20-at-samsungs-unpacked-event-in-san-francisco/.
[9] AARP. (n.d.). Social Security scams. *AARP.* Retrieved 1/10/19 from https://www.aarp.org/money/scams-fraud/info-2019/social-security.html?intcmp=AE-FWN-LIB3-POS5.