PENNSYLVANIA STATE POLICE

COMMUNITY AWARENESS BULLETIN

CAB 001-20 March 13, 2020

CORONAVIRUS RELATED SCAMS

The Pennsylvania State Police (PSP) reminds Pennsylvania residents to remain vigilant against scams attempting to take advantage of the coronavirus (COVID-19) pandemic. Criminals often use current events to gain the victim's sympathy and trust to make their scams seem more legitimate. Below are examples of some of the scams that are circulating.

- Fraudulent fundraising campaigns that claim to collect for the CDC or WHO, or for victims through a crowdfunding site, such as GoFundMe.
- Price gouging on household supplies such as bathroom tissue, hand sanitizer, and bleach. Pennsylvania law defines gouging as charging a price over 20% of the price charged before the emergency started. Report gouging to the Attorney General's office at https://www.attorneygeneral.gov.
- Advertisements for supplies that take your money and fail to deliver what was promised.
- Advertisements on social or other media claiming to sell vaccines, cures, or tests for COVID-19. Some of these "treatments" are dangerous, but all are worthless. ***There is currently no known cure or vaccine for COVID-19 and tests must be obtained through a physician or hospital.***
- Investment "opportunities" that promise high returns for low risk, or that claim to be a hedge against a volatile market. For more information, visit https://www.media.pa.gov/pages/banking_details.aspx?newsid=309.
- Phishing emails that use fear of COVID-19 to get you to download malware to your computer. These emails claim to be from the Centers for Disease Control (CDC) or the World Health Organization (WHO) and may have an attachment claiming to be a list of cures.
- Malicious websites mirroring legitimate sources of information. Currently, a malicious website is masquerading as the Johns Hopkins University of Medicine coronavirus COVID -19 Global Cases map. Visiting the malicious website infects the user with the AZORult trojan, an information stealing program which can exfiltrate a variety of sensitive data.

RECOMMENDATIONS

- Make sure your computer has the latest updates, and make sure it has an antivirus program. Delete any email from people you do not recognize or has attachments you are not expecting.
- Verify charities through https://www.charities.pa.gov and do not contribute to a crowdfunding campaign unless you know the people who are collecting the money or who are benefiting from the collecting.
- Avoid purchasing supplies from unfamiliar companies. Stick to companies and stores you know. If you must buy supplies from an unfamiliar source, use a credit card.
- Check unknown or suspicious files and URLs for malware. Individuals can check files and links by scanning them using https://www.virustotal.com.

For the most up-to-date and accurate information about coronavirus and COVID-19 in Pennsylvania, visit https://www.health.pa.gov/topics/disease/Pages/Coronavirus.aspx.

The PSP reminds residents, if you fall victim to a scam, call your local police department.