United States Secret Service Cybercrime Investigations

COVID-19 Vaccine Fraud

On December 11, 2020, the U.S. Food and Drug Administration (FDA) issued the first emergency use authorization for a COVID-19 vaccine in the United States. The U.S. Secret Service reminds the public that criminal elements will attempt to exploit this for profit.

Sale of Unapproved or Counterfeit Vaccines | *A fraudster offers unapproved vaccines or counterfeit vaccines that appear to be from an FDA approved manufacturer.*

Non-Delivery of Vaccines | *A cyber actor elicits an advance payment for vaccines, but never delivers them.*

Phishing and Smishing | *A cyber actor sends an email or text message offering access to vaccines, then requests credit card information and personally identifiable information (PII) with the intention of using the information in other fraudulent activity.*

Employment Offers and Money Laundering | *A cyber actor offers an employment opportunity to make quick and easy money by receiving and sending funds from vaccine sales.*

PROTECT YOURSELF FROM COVID-19 VACCINE FRAUD

Never trust an unknown source for medical goods.

Never respond to an email or text message from an unknown source.

Never click on a link or open an attachment from an unknown source.

Never share your bank/credit account information or PII with unknown individuals.

Always independently verify where a request for sensitive information originates.

Always read the entire email message and look out for suspicious indicators, such as poor grammar or email addresses disguised to appear legitimate.

Always mark an email from an unknown source as spam.

Always read the entire text message and look out for suspicious indicators, such as poor grammar.

Never respond "Stop" or "No" to prevent future text messages, delete the text instead.

Never open a joint account with unknown individuals.

Never respond to an offer to earn quick and easy money.

Never agree to receive and send money on behalf of others, money laundering is a crime.

Remember: Government agencies or legitimate businesses will never solicit personal information by sending you an email, text message, or calling you.

Protect Your Information

- ✓ ***Ensure that all your electronic devices have the latest software updates and active anti-virus protection.***
- ✓ ***Create strong passwords, change them appropriately, and avoid utilizing the same password across multiple apps.***
- ✓ ***Use multi-factor authentication to avoid unauthorized access to your accounts.***
- ✓ ***Regularly back up data stored on your devices.***