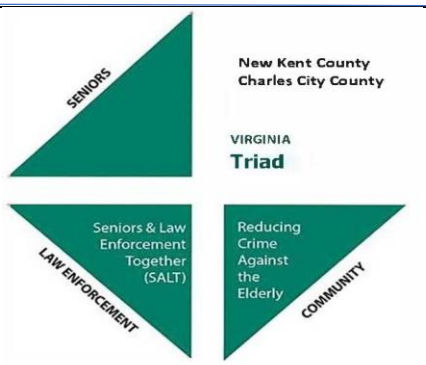

Chickahominy Area Triad

Scam/Fraud Alert Bulletin #18

Be Aware, Be Smart, Stay Protected

Serving the Counties of New Kent and Charles City, VA.

Type	Synopsis of Reported Incidents
Fraud: Scam:	The victim advised that they had received an email from someone posing as a subcontractor which they frequently conduct business with regularly. The email came with an invoice and new banking information to make payment. Luckily, the victim's bank found this to be fishy and alerted the victim and flagged the payment.
Fraud: SCAM	The victim was scammed by someone on Facebook Market Place. He reached out to a "Mike Martin", who claimed to be living in Alabama and selling a Ranger Bass Boat cover for $300.00. The victim paid Mike $150 via PayPal to an email of SpenceEugen123@jujjk.com. The victim began questioning things because "Mike" wanted him to send a screenshot of the payment to confirm he had sent it. After the victim began asking questions, "Mike" then stopped all communications.
Fraud: SCAM	The victim received phone calls on April 3rd, 4th and 5th claiming she paid too much for a Geek Squad account. The victim told the caller that she didn't have a Geek Squad account and they convinced her to create an account and provide them with all her information. In the three days of calls, the scammer convinced the victim to purchase gift cards that totaled $21, 200.00 and provided the scammers with the numbers on the back of the cards.
Fraud: SCAM	The victim received a phone call for a male claiming to be from PayPal fraud support. The individual claimed that her account was compromised and was showing a pending and approved transaction for $499.00 in her account. The victim was given instructions over the phone to provide PID

	information, which was used by the scammer to gain access to her digital financial accounts. The caller signed into the victim's PayPal account, and through that, accessed her Wells Farge Bank account.
Fraud: SCAM	The victim said that on April 12, 2024, at approximately 5:28pm, she was contacted by phone number 888-842-6320 with the caller ID "Nave FCU" notifying her that there were multiple fraudulent transactions on her account. The caller was impersonating a Navy Federal Credit Union Fraud investigator who informed the victim that they were going to fix the fraudulent transactions and told her what she needed to do. The victim was instructed by the scammer to make a single $5,000 transaction and a $4,000 deposit to a "Tyshana A. Alexander". The victim later received an email from Navy FCU saying that she was approved for a $9,000 loan and that she is to pay $298.34 on the 23rd of every month. The victim realized this had been a scam and contacted Navy Federal Credit Union only to discover that "Tyshanna Alexander" had been added as a 3rd Party to her account.
Fraud: SCAM	Victim applied for jobs on Indeed for work from home. Victim later I received an email asking to submit her my resume, which was forwarded. They later provided her with a link to download for an interview. The victim was contacted and interviewed was conducted by a "Haley Watson." After the interview she was notified that I was hired. They sent a welcome aboard letter along with background check form and four (4) additional forms. She completed the forms and sent them back. The scammer then informed the victim that they would send her a startup check to purchase materials. They sent the victim a fraudulent $2,500 check via email and requested the victim use her mobile banking to deposit in her account, which she did.
Fraud: SCAM	The victim was offering a job by text, which referred the victim to a trainer who could reach on WhatsApp and provide victim in on the details. The job was being a "Data Generator" by completing daily tasks that paid exponentially for consistent daily attendance and completion of the online

	tasks. The trainer guided the victim every step of the way while having me take and forward screen shots of every step. The profits and commissions looked great on the Mamba page but were not accessible for a 72-hour period, which then grew longer. Moving forward required payment of a "negative balance' due to being "lucky" by getting multiple products bringing potentially larger commissions. Victim bought into the scheme four times for about $1,400.00 loss.
Fraud: SCAM	The scammer contacted the victim by phone and said that victim had won the Publisher's Clearing House Sweepstakes. The victim had indeed entered the sweepstakes months earlier ago. They knew all of the victim's personal information and all about the sweepstakes prize. The victim believed that Publisher's Clearing House was a legitimate sweepstakes. The scammer told the victim that he had to pay a small portion of the taxes with a Green Dot card, and everything would be on its way from Cleveland, TN. After purchasing two cards totaling $485, they wanted another $250. I told them I didn't have any more money and they wanted me to open a new bank account and write a bad check to get a new card. The scammer became irritated when I said no. The victim told the scammer no. The victim did not have any more contact with the scammer until the next day. The victim was given a number to call to get his money. The scammer then offered the victim a receipt that could be used to purchase green dot gift cards. It was explained that it was necessary to purchase a Green Dot card to collect his prize money that the Lord wanted me to have that money. The victim contacted Green Dot through their email on the back of the card to dispute the transaction and they also asked for a picture of the receipts and then said they could not refund my money.
Fraud: SCAM	The scammer called and victim and informed the victim that he had been approved for a loan of $5,000. The victim decided to accept the loan. Conversations between the scammer and victim when back and forth between the two at least six (6) times. Each time the scammer used a different telephone number. After the last call, the victim learned his

	Google account had been hacked and his banking bank account drained.

NOTE: The reported occurrences depicted in this bulletin are true. **They did not occur within the Counties of New Kent or Charles City, Virginia.** However, they were reported to a Northern Virginia Sheriff's Department or the Better Business Bureau (BBB) within the past month. Stay alert, don't become a victim, as you can see it can be costly and don't think that it couldn't happen to you.

Meta: Chickahominy Area Triad Scam Warriors
www.chickahominytriad.org

Meta: Chickahominy Area Triad