SCAM SQUAD

By Patti Teel, Deputy District Attorney Vicki Johnson & Richard Copelan, CEO/President of the BBB of the Tri-Counties

Beware of Work from Home Scams

Many companies are quickly making arrangements for employees to work from home, and others are fast tracking policies to meet the requirements of shelter-in-place orders issued by state officials. These actions are making it an even higher risk of people being targeted by scammers, especially through phishing emails or through an unsecured network connection.

Transitioning from an office setting to home, many may find themselves more vulnerable to tech support scams. With limited IT resources available, employees may attempt to solve technical issues themselves when confronted with pop-ups and virus alerts. BBB Scam Tracker received a report of a victim losing nearly $250 to a tech support scam. The report stated a pop-up window appeared when the user's computer froze. The instructions on the pop-up window said to contact a company claiming to be affiliated with Apple. After following the directions, the consumer paid for what they thought would fix the problem and never heard from the tech support company again.

Another concern for employees transitioning to a work-from-home environment is Business Email Compromise (BEC) scams. BEC scammers impersonate emails that appear to come directly from the boss. These fraudulent emails are often used to request large payments to "vendors" via wire transfer. While this is a common scheme, scammers may change their approach and use current events as a way to convince the recipient to take action. Compromised business emails may be used to request payments for things such as reimbursements, bogus invoice payments, or office equipment.

Advertised work from home opportunities aren't always what they seem, especially for people who have recently been furloughed or laid off. Employment scams are ranked the top riskiest scam in both the 2018 and 2019 Scam Tracker Risk Report. Common red flags are work from home ads offering a high hourly wage with minimal effort. As more employers practice social distancing and require employees to work from home, it will be crucial to differentiate between legitimate and fraudulent job opportunities.

While working from home and watching to see how the situation surrounding the COVID-19 outbreak develops, here are some tips from Better Business Bureau to avoid falling victim to scams:

● **Be aware of unusual procedures.** Job offers without interviews are a red flag of employment scams, as well as employers that overpay and ask newly hired employees to wire back the difference. Beware of companies that promise opportunities or high income if you pay them for training.

● **Check official job postings.** Scammers will often use emails, social media or online job boards. They are also known to use actual company names, addresses and human resource contacts found on the internet. If a job posting seems too good to be true, go directly to the company website and check their career page directly. If a website is charging you for information about a job opening, it is probably a scam.

● **Set up work-from-home IT policies.** When setting up remote employees, establish a plan to help them with technical problems they may face. Instruct them on who they should contact, and who to avoid, for tech support. A plan can protect employees, the business and your customers from having their personal and professional information compromised.

● **Maintain office billing policies at home.** One of the best ways to combat business email compromise scams is to set a policy requiring employees to confirm payment requests in person or over the phone, rather than through email. If the employees that handle billing are working from home, have them maintain these policies by calling to confirm any payment requests made by email.

● **Review safety practices with employees.** As employees are working remotely, remind them of the best practices to avoid scams. Practices such as avoiding clicking on pop-ups or links in unsolicited emails are encouraged and if they aren't sure of the origin of an email, have them contact a colleague or supervisor by phone. Make sure they know tech support professionals would never call them unless they had requested assistance first.

To report a scam, call the District Attorney's Fraud Hotline at 805-568-2442. The Better Business Bureau urges you to visit their Scam Tracker site at https://www.bbb.org/scamtracker/santa-barbara/reportscam or call them directly at 805-963-8657.

The District Attorney's office and Better Business Bureau of the Tri-Counties each have segments on the Young at Heart Radio Show, with host Patti Teel. It airs on KTMS Newstalk 990 on Saturdays at 5:30 pm and Sunday mornings at 8:30. During Scam Squad, Deputy District Attorney Vicki Johnson warns listeners about the latest scams and often interviews victims. This is followed by Your Moment of Trust, a segment by BBB of the Tri-Counties-- providing timely advice to businesses and individuals. After airing, they can be found at www.hubforpodcasting.com

###