

# SCARE Membership Meeting

February 27, 2024

## Minutes

1. Speaker for the February membership meeting was Hana Aymar, Fraud Manager for Redwood Credit Union. Hana talked about the different ways scammers get to you and how you can protect yourself.
  - a. Impersonation Scams can come from any of those listed below. They mimic a local financial institution and ask that you click on the button provided to clear up a problem. DO NOT click on any link. Close out of the email. Call a trusted number to see if there is any problem with your account. If you get a pop up on your computer screen saying something like, “Your computer is infected, call tech support to solve”, immediately disconnect your computer. Have the computer cleaned by a professional to make sure the hacker has not left any programs behind to get into your computer later. If it happens on your phone, you can go to the Apple support app chat for help. Artificial intelligence has made it possible to duplicate a family member’s voice and image, so be careful if someone you know is calling for money to be sent.
    - i. Financial institutions
    - ii. Phantom Hacking
    - iii. Social Security
    - iv. Friends and family
    - v. Virus/Malware pop-up or email
    - vi. Tech companies
    - vii. Government Agencies
  - b. Romance Scammers. If someone is asking for money, walk away immediately. They often start small and build a relationship with you. They ask for more as time goes on. Scammers also try to get you to communicate outside of the dating app. That way they won’t be caught since dating apps do monitor the site for scams.
  - c. Social media scams – here they hack into your social media account and contact your family and friends for money to cover a broken leg or some other story. Limit your friends. Verify the account. Contact the relative or friend directly to see if they need help. Do not take financial advice from someone online!
  - d. Employment scams – be wary if someone contacts you with a job that is too good to be true. If there are asking for money, gift cards or other forms of payment, stop communication immediately.

- e. Don't purchase any gift cards and send the codes. Check gift cards when you purchase them to make sure they haven't been tampered with. Some are getting the codes and returning the gift card to the rack.
  - f. Crypto currency scams are hard to catch. Don't communicate with people you don't know. Don't friend people you don't know. Some scammers will text you asking if you know each other; ignore it.
  - g. Many scamming centers are staffed with people who are being trafficked. So they have no choice but to try to get your money for the scammers.
  - h. Don't give out your password, social security number, birthdate, or other identifying information.
  - i. Pay for a good credit monitoring service.
  - j. Check your credit report quarterly.
  - k. Use a password manager.
  - l. Hana Aymar can be reached at [haymar@redwoodcu.org](mailto:haymar@redwoodcu.org), 707-545-400 X30351
2. Paul gave the JLMBC report. He talked about the changes to insurance coverage and that the booklets should be sent out soon.
  3. Bill talked about SCCLO, NBLC, and ICPC. No current activity with SCCLO. NBLC – Ed Clites attended the successful COPE awards dinner on behalf of SCARE. He had the opportunity to talk with CA Senator Mike Maguire about the lack of COLAs for Sonoma County retirees. ICPC met in December. HRA benefits were discussed.
  4. Kathy reminded members that SCERA will be discussing the Negative Contingency Reserve and the Interest Fluctuation Reserve on Thursday, March 21, 9:00 AM. You may attend in person or by Zoom. A reminder will be sent out.

Respectfully submitted,

Kathy Young