

ALERTS



SCAMS – You think it’s never going to happen to you – until it does.

RED FLAGS FOR PHONE AND EMAIL SCAMS

- Urgent or threatening language or a greeting that is too friendly
- Requests for personal information
- Requests to have access to your computer
- Link to a site that seems unrelated to the organization that contacted you
- Missing contact information in an email
- Payment via GIFT CARDS

STRATEGIES

- Call your **grandchildren** and establish a CODE WORD to verify identity
- GIFT CARDS: As soon as you hear these words, **HANG UP**.
- DO NOT BE POLITE. BE SMART. Hang up when you are unsure.
- DO NOT be pressured by urgent requests. **HANG UP**.
- CHECK CALLER ID: do NOT answer if you do not recognize the caller; legitimate callers will leave a message.
- EMAIL: Do not click on links from financial institutions. Call or go directly to the website and check there.
- DO NOT ALLOW ACCESS TO YOUR COMPUTER. **HANG UP**.
- Use the phone number from your bill or on your credit card if you need to contact a financial institution or vendor. If it’s a website, go directly to the website to find the number. DO NOT SEARCH (AKA Google) FOR THE NUMBER ONLINE.

VISIT [SCLHWATCH.ORG /SECURITY](https://www.sclhwatch.org/security) FOR ADDITIONAL INFORMATION

ALERTS PROGRAM COORDINATOR

Mary Cranston

916 434-5362

alerteditor@sclhwatch.org

NEIGHBORHOOD WATCH PUBLIC SAFETY LIAISON

Barry Johnson

916 434-6538

alerteditor@sclhwatch.org