



Santa Clara County

Scam Awareness



COUNTY OF SANTA CLARA
PRIVACY OFFICE
privacy.sccgov.org

What You Will Learn



How to spot a scam



Common scam types



How to protect yourself



What to do if you are scammed



Where to learn more



✓ How to Spot a Scam

- Scam types quickly evolve but share the following techniques:
 - There is a sense of urgency; usually emotionally based
 - Payment is required; gift card or other instant transfer mechanism
 - There is a promise or threat
 - The request is unexpected
 - The request does not “feel right”

Scams Are Increasing

- Americans lost \$2.7 billion to scams originating on social media between January 2021 and June 2023
 - \$700 million more than website scams
 - \$1.8 billion more than email scams
- Fraud victims are generally 18 – 19 years of age
- Most common social media scam is fake advertisements
 - Second most common is financial “experts”
- Be vigilant
 - If it is too good to be true; it is most likely a scam
 - Never answer messages from someone you do not know
 - Limit who can see your social media postings



Common Scams Types

- Tax/IRS
- Debt collection
- Counterfeit check
- Advance fee
- Windfall
- Recovery/refund
- Charity
- Pyramid / Ponzi schemes
- Affinity fraud
- Sales
- Tech support
- False health claims
- Romance
- Blackmail
- Tech Support

Targeted Scam Populations and Types

Seniors

- Medicare / Social Security Administration
- Home equity loans
- Grandparent
- Funeral / burial

Veterans

- Charity
- Military benefits schemes
- VA records / assistance
- GI bills
- VA Phishing attempts

Immigrants

- Immigration assistance schemes
- Deportation

Students

- Tuition
- Advance fee
- Online textbooks
- Check-cashing

Phishing

Can be delivered by email, phone, text message, or social media

- Impersonation (false identity)
- Urgency
- Spoofing
- Malware and ransomware
- Don't get hooked

All phishing attempts use impersonation to fool their targets

- Impersonate a legitimate business or government
- Instills a sense of urgency



Crypto Investing: 'Pig Butchering'

- Term refers to an unsuspecting victim being *manipulated* by the scammers to invest in crypto currency
- Scam starts out as a random text message, "Hi, how are you today?"
- Over time, scammers build a relationship
 - Suggests crypto investment
 - Encourages investment; represents prior profits
- Provided a fictitious financial statement showing substantial return (fattening the pig)
 - Encourages more investments
 - Disappears when you try to get your money



Quishing

- A newer trick to steal identities and money
- Scammers place fake QR codes, which direct you to websites that appear to be legitimate
 - Commonly found on parking meters
- Look for signs of tampering on signs with QR codes
- Check the website URL after scanning the code





How to Protect Yourself

1. Be vigilant
2. Have a healthy skepticism
3. Beware of urgency
4. Guard your money and data
5. Do your due diligence
6. Consult with someone you trust
7. Pay with a credit card

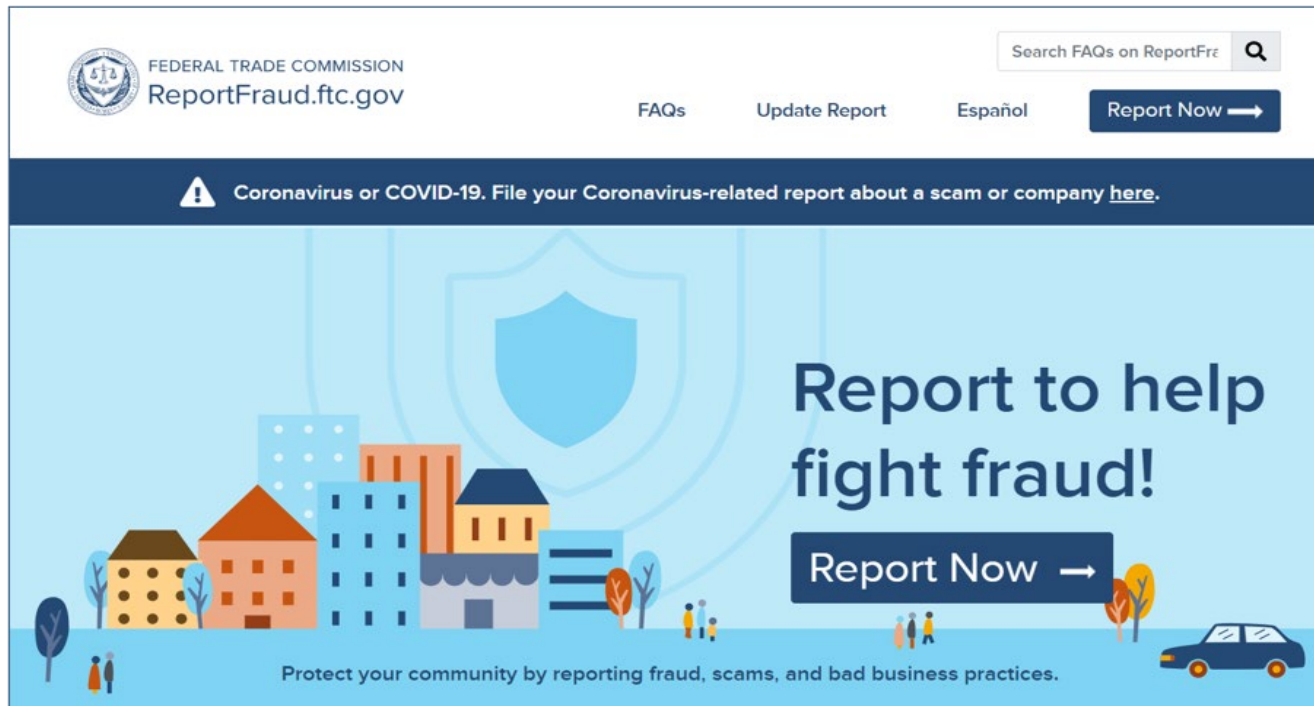
Search Online to Avoid Scams

- Conduct an online search to identify and avoid scams
 - Research a company or individual
 - Confirm a website address or contact number
 - Check reviews
 - Compare prices



What to do if You Are Scammed

- Report it! Your report matters
- Where to report depends on the type of scam
- Federal Trade Commission



English:

ReportFraud.ftc.gov

Spanish:

ReporteFraude.ftc.gov

Where to Learn More: County Privacy Office Webpage

Privacy Home Page:

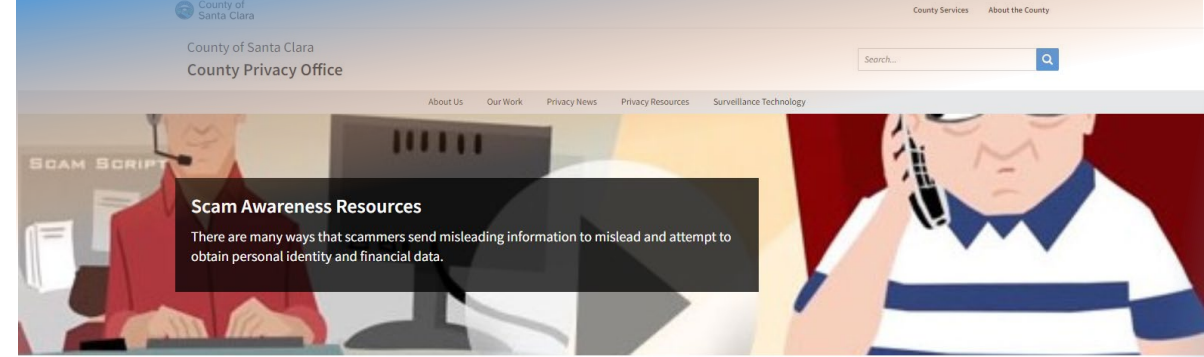
<https://privacy.sccgov.org/>

Scam Awareness Page:

<https://privacy.sccgov.org/scam-awareness-resources>

Email:

PrivacyOffice@ceo.sccgov.org



News and Updates about different scams

News about different scams from the trusted sources such as the Federal Trade Commission



Medical and Insurance Scams

The FTC Warns of various techniques scammers use to steal medical and financial information from medical and insurance sites.



Fake Emergency Scam

Someone calls or contacts you saying they're a family member or close friend. They say they need money to get out of trouble. Not so fast. Is there really an emergency? Is that really your family or friend calling? It could be a scammer.



Scam Awareness Resources

Use these resources to learn best practices for avoiding scams, report potential fraud, and download consumer brochures

Articles

Source	Article/Website Name
Consumer Action	When a Collector Calls
Federal Trade Commission	Fake and Abusive Debt Collectors
Federal Trade Commission	Consumer Advice Page
Federal Trade Commission	How To Spot, Avoid, and Report Fake Check Scams
Federal Trade Commission	What to Know About Advance-Fee Loans
Federal Trade Commission	Fake Prize, Sweepstakes, and Lottery Scams
Federal Trade Commission	Romance Scams
Food and Drug Administration	Health Fraud Scams
Housing and Urban Development	Home Equity Loan Scams
Internal Revenue Service	IRS Tax Scam Awareness

Funeral and Burial Scams

Source	Article/Website Name
--------	----------------------

Homework: What You Can Do to Protect Your Identity

- Freeze Your Credit Report
 - Equifax equifax.com/personal/help/place-lift-remove-security-freeze/
 - Experian experian.com/freeze/center.html
 - Transunion transunion.com/credit-freeze
- Monitor Your Credit Report
 - annualcreditreport.com/index.action
- Opt-Out of Pre-Screened Credit Offers
 - OptOutPrescreen.com
- Set up USPS Informed Delivery notifications
 - usps.com/manage/informed-delivery.htm
- Establish charge alerts with financial institutions
- Shred any document containing your information
- Set up an alternative email for shopping or non-critical communications
- Stay vigilant