

# Protect Yourself from Fraud and Scams

Kue Lee

*Director of Targeted Outreach*

*Kue.Lee@dfpi.ca.gov*



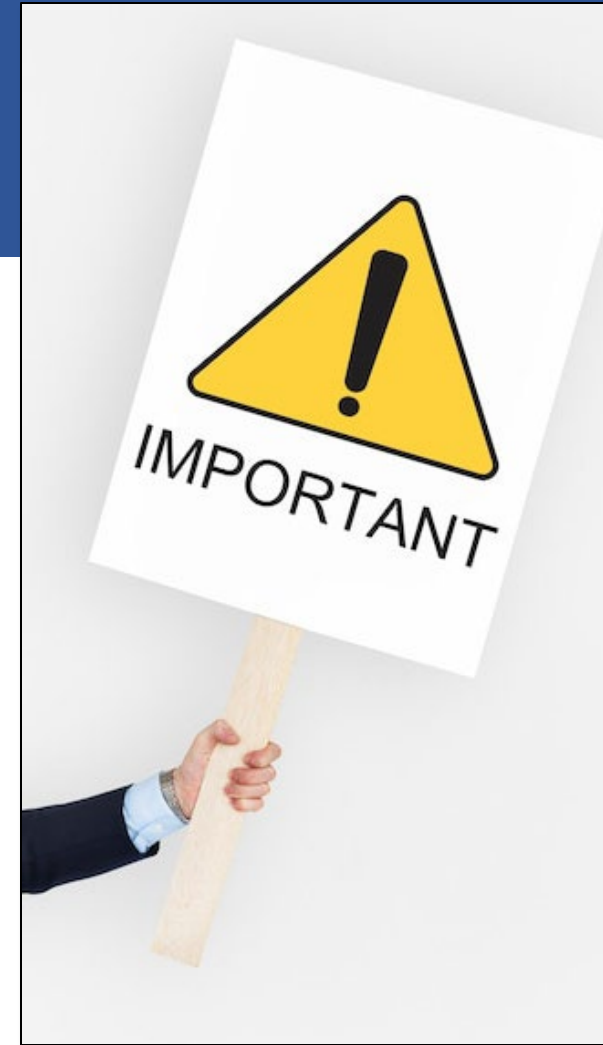
DEPARTMENT OF  
FINANCIAL PROTECTION  
& INNOVATION

**PROTECTING CONSUMERS**  
FOSTERING TRUST & INNOVATION

[www.DFPI.ca.gov](http://www.DFPI.ca.gov)

# Important Information about this Presentation

- The views and opinions expressed in this presentation are those of the presenter. They do not necessarily reflect the views or positions of the DFPI.
- This presentation is for educational and informational purposes only. **This is not financial advice** and does not replace independent or professional judgment.
- The DFPI does not assume responsibility for the completeness of the information presented in this presentation.
- For more information:
  - Visit: [dfpi.ca.gov](https://dfpi.ca.gov)
  - Email: [Outreach@dfpi.ca.gov](mailto:Outreach@dfpi.ca.gov)





# The Department of Financial Protection & Innovation

## Who Are We? What Is Our Role?

- The DFPI's central purpose is to maintain a fair, healthy, and trusted financial services marketplace for all Californians.
- The Department accomplishes its mission through regulation and enforcement of a variety of financial services, products, and professionals.
- Provide presentations throughout California to inform and protect consumers and to prevent them from falling prey to frauds and scams.
- Learn more at: [dfpi.ca.gov/consumers](https://dfpi.ca.gov/consumers)

# Access DFPI's No-Cost Online Financial Education

These courses are designed to meet you where you are, help build your money management skills and demystify the world of personal finance.

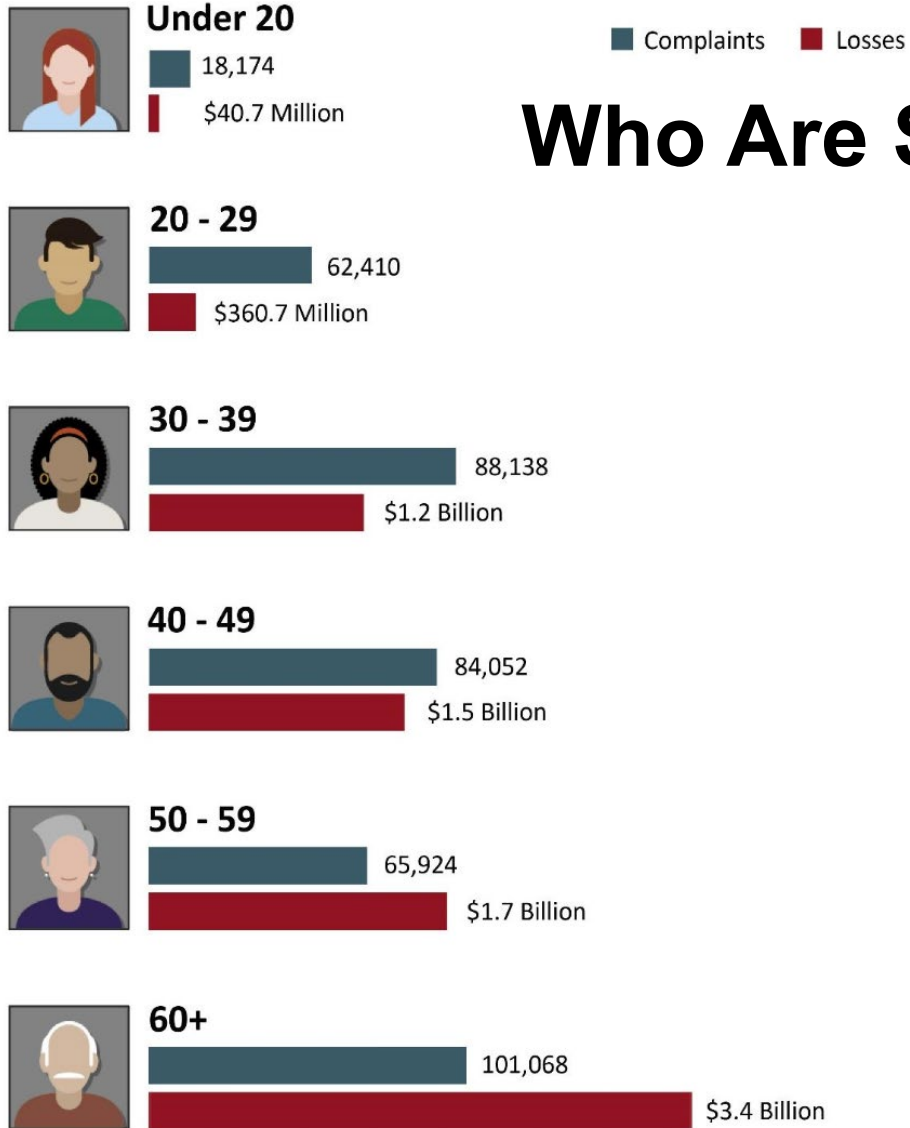
## Course topics include:

- Budgeting
- Investing education
- Retirement planning
- Paying for college
- Debt management
- and more!



➔ Get started at: [dfpi.ca.gov/learn](https://dfpi.ca.gov/learn)

# Who Are Scammers Targeting?



**YOU**

Source: [https://www.ic3.gov/Media/PDF/AnnualReport/2023\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf)

# Beware these Scams

- **Imposter Scams**

- Grandparent/Relative scams
- Debt collectors
- Government imposters:
  - IRS / Social Security
  - Utility company
  - Law enforcement
  - Financial institutions

- Investment scams

- Romance scams

- Tech support scams

- Payment app scams

- Student loan scams

- Employment scams



# Beware of **Precious Metal** Investment Scams

## Red Flags may include:

- **High-pressure sales tactics:** using fear or urgency to convince you to invest quickly.
- **Inflated prices** with precious metals being sold at higher prices than actual market value.
- **Promises of guaranteed returns** with claims of high profits with little risk.
- **Fake or low-quality metals.**
- **Hidden fees:** extra charges or fees associated with the purchase or storage of metals.



## To protect yourself from precious metal scams:

- Do your research: Learn about precious metals and their market prices.
- Verify the seller: Ensure the seller is reputable and licensed.
- Be wary of high-pressure sales tactics **and** don't invest based on fear or urgency.
- Get a second opinion: Consult with a financial advisor before making a significant investment.

If you believe you have been a victim of a precious metal scam, submit a complaint the California DFPI:  
[www.dfpi.ca.gov/submit-a-complaint](http://www.dfpi.ca.gov/submit-a-complaint).

# Example of a PHISHING Scam

Forward scam emails to:  
[reportphishing@apwg.org](mailto:reportphishing@apwg.org)

From: Bank of America <crvdgi@comcast.net>  
Subject: Notification Irregular Activity  
Date: September 23, 2014 3:44:42 PM PDT  
To: Undisclosed recipients: ;  
Reply-To: crvdgi@comcast.net

# Bank of America



## Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions ~~without interruption~~.

**Please sign in to** your account at <https://www.bankofamerica.com>

to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

<http://bit.do/ghsdfhgds>

If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error


© 2014 Bank of America Corporation. All rights reserved.



# Example of a PHISHING Scam

Forward scam emails to:  
[reportphishing@apwg.org](mailto:reportphishing@apwg.org)

**From:** QRCODE>>AUTHENTICATION\_NOTIFICATION <mstone@fpckerville.org>  
**Sent:** Thursday, September 28, 2023 7:15 PM  
**To:** [REDACTED]  
**Subject:** 2FA-Dfpi Compliance Mandate Required for your account. Qr600TF08202rtQ#.

 Microsoft  
**Security Authentication**



**Katie.carruesco**, due to recent security activities and updates.

You are being held responsible to review security update and requirement as of **28/09/2023**.

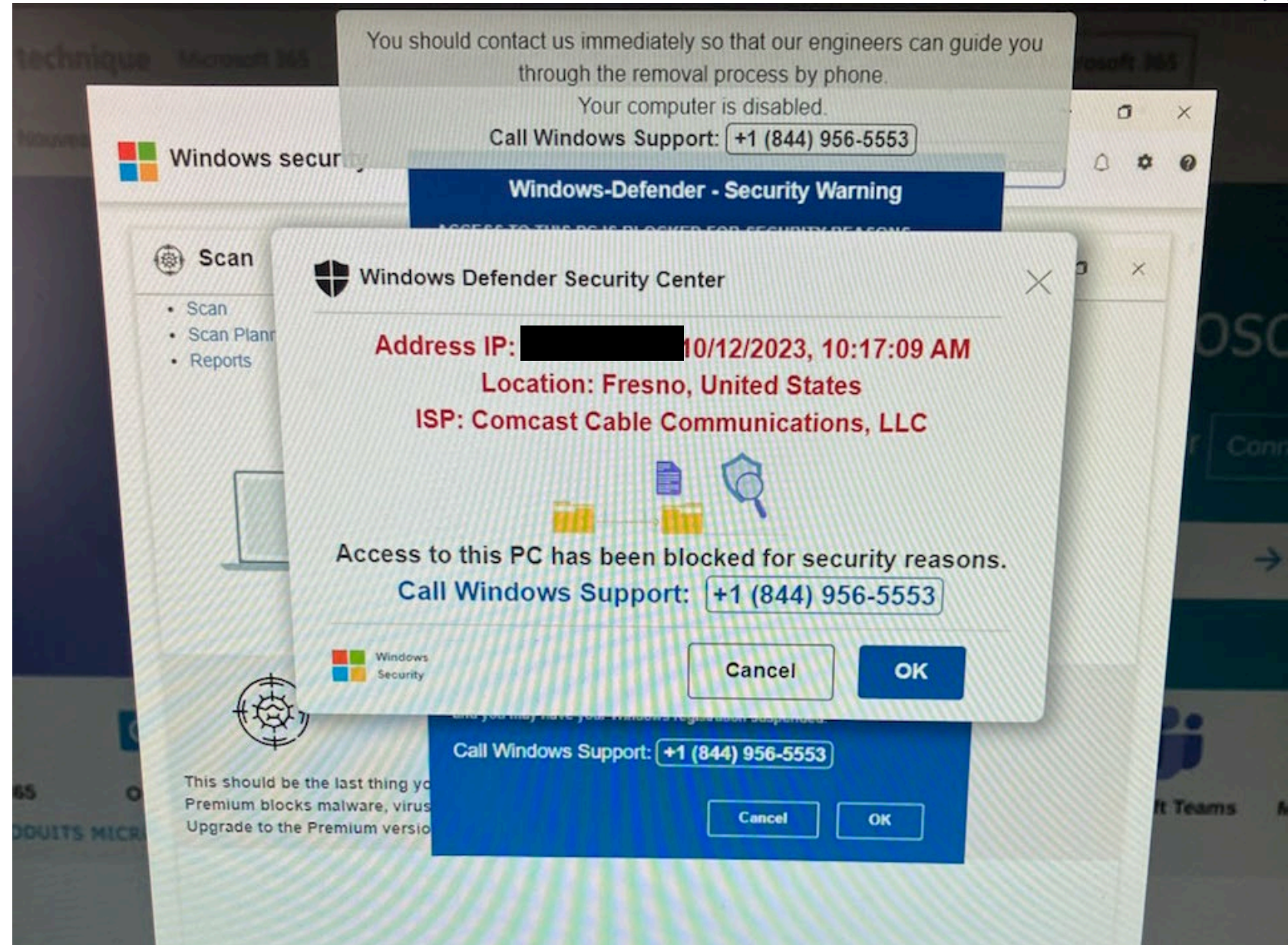
**Quickly scan above QR Code with your smartphone camera.**

Review security requirements within **3 days of the received date** by going to **Account manager** in the Security Center.

Dfpi© 2023 Microsoft Corporation. All rights reserved.

# Example of TECH SUPPORT Scams

Turn off or restart your  
computer!  
Run your antivirus  
program.



# Scammers are using Artificial Intelligence (AI)



# How Can You Protect Yourself?



# 1. Do Not Respond to Scammers



**Ignore anyone contacting you that you don't know.**

- Vishing** – Telephone
- Phishing** - Computer/Emails
- Smishing** - Text Messages
  - “Click here”
  - “Callback number”
  - “Reply back”



## 2. Do Your Research!

- Look for **red flags**:
  - Pay with cryptocurrency or gift cards
- Verify information.
- Check credentials.
- Go **directly** to the **official** source, company, or website.
- **Get Help**: ask an employee or professional **in person**.

## 3. Take Your Time

**Ignore** anyone who is:

- Threatening you
  - Giving you a limited-time offer
  - Telling you not to share this information with others
  - Asking for your personal or financial information
- ✓ **Do not** make any big financial decisions for at least 24 hours



## 4. Do Not Share Your Info

Limit what information you share on:

- Social media
- Websites, forums, communities
- Emails
- Sign-up forms
- Online shopping sites
- Phone apps
- Company or account profiles

\*\*\*When a company suffers a data breach, the more information you've shared, the more you are exposed.



## 5. Ask Someone You Trust

Ask and get help from a:

- Spouse
  - Friend
  - Children (18 years or older)
  - Community leader
  - Financial advisor or professional
- 
- Consider using a family *challenge and pass phrase*.





## 6. Report the Incident

Report this scam to:

- Local authorities
  - Police
  - District attorney's office
- State authorities
  - DFPI, DCA, AG
- Federal authorities
  - FBI – [www.ic3.gov](http://www.ic3.gov)
  - CFPB, SEC, FTC
  - [www.reportfraud.ftc.gov](http://www.reportfraud.ftc.gov)

# Protect Yourself Recap

1. Do not respond to scammers
2. Do your research
3. Take your time
4. Do not share your information
5. Ask someone you trust
6. Report the incident




# Credit Reports: What You Need to Know

- Three major credit reporting agencies
- **Credit Bureaus must:**
  1. Make sure that the information they collect about you is accurate.
  2. Give you a free copy of your report **once a week** (at your request).
  3. Provides you a chance to fix any mistakes.
- [Annualcreditreport.com](http://Annualcreditreport.com) or call 1-877-322-8228
- Reasons to access your free credit report:
  - Signs of identity theft
  - Freeze your credit
  - File a complaint



# Recovering from Identity Theft

An official website of the United States government [Here's how you know](#) ▾

 FEDERAL TRADE COMMISSION  
**IdentityTheft.gov**

Report identity theft and get a recovery plan

**Get Started** →

or browse recovery steps

[www.identitytheft.gov](http://www.identitytheft.gov)

- Hosted by the Federal Trade Commission (FTC)
- Step-by-step guide to recovering from identity theft
- You can also get help from your State Assemblymember or State Senator

## Additional Safety Tips:

### Protect Your Personal and Financial Information

- Official state and federal government agencies will not call, text, message or you directly. Expect a physical letter.
- Check a website's link before entering your username and password.
- Do not click on unknown links.
- Use a shredder for your mail and personal documents.
- **DO NOT** leave mail in mailboxes overnight or after pick-up hours.
- Deposit important mail directly to the post office.
- Use anti-theft gel pens for checks and other signature documents.
- Don't just close your Internet browser – be sure to log out of websites.

# Stay Connected to the DFPI!

- Subscribe to our newsletter: [dfpi.ca.gov/subscribe](https://dfpi.ca.gov/subscribe)
- Check out our other events: [dfpi.ca.gov/events](https://dfpi.ca.gov/events)
- Call: (866) 275-2677
- Email: [outreach@dfpi.ca.gov](mailto:outreach@dfpi.ca.gov)
- Web: [dfpi.ca.gov](https://dfpi.ca.gov)
- Social Media:
  - Facebook: [facebook.com/californiadfpi](https://facebook.com/californiadfpi)
  - LinkedIn: [linkedin.com/company/californiadfpi](https://linkedin.com/company/californiadfpi)
  - X: [x.com/californiadfpi](https://x.com/californiadfpi)
  - YouTube: [youtube.com/cadfpfi](https://youtube.com/cadfpfi)



THANK YOU