



The ITRC is a **non-profit** organization established to **minimize risk** and **mitigate** the impact of **identity compromise**.

# *Safeguarding Your Identity: Essential Strategies for Staying Safe*

*Michael DiTurno*  
*Director of Operations*

**Your Life, Your Identity.**  
LET'S KEEP IT THAT WAY



© 2025 IDENTITY THEFT RESOURCE CENTER, ALL RIGHTS RESERVED | 888.400.5530 | [IDTHEFTCENTER.ORG](https://IDTHEFTCENTER.ORG)



# *The Identity Theft Resource Center*

- Nonprofit founded in 1999
- Free identity protection and recovery assistance for consumer
- Paid training and due diligence tools for business
- Largest data breach tracking database
- Ongoing research, analysis and education about identity crimes, their impact and current trends

A large, light blue fingerprint graphic is positioned in the upper left background of the slide.

# *What We Will Discuss*

- What is an identity?
- How thieves steal our identities
- How our identities are misused by the criminals
- Detecting and resolving misuse of our identities
- Protecting our data and devices



A large, light blue fingerprint graphic is visible in the background of the left side of the slide.

# *What Identifies Us?*



# IDENTITY

## CREDENTIALS

- + Social Security Number
- + Birth Certificate
- + Driver's License
- + Passports
- + Financial Accounts
- + Usernames & Passwords

## ATTRIBUTES

- + Name
- + Phone Numbers
- + Physical Address
- + Date of Birth
- + Employers

## BEHAVIORS

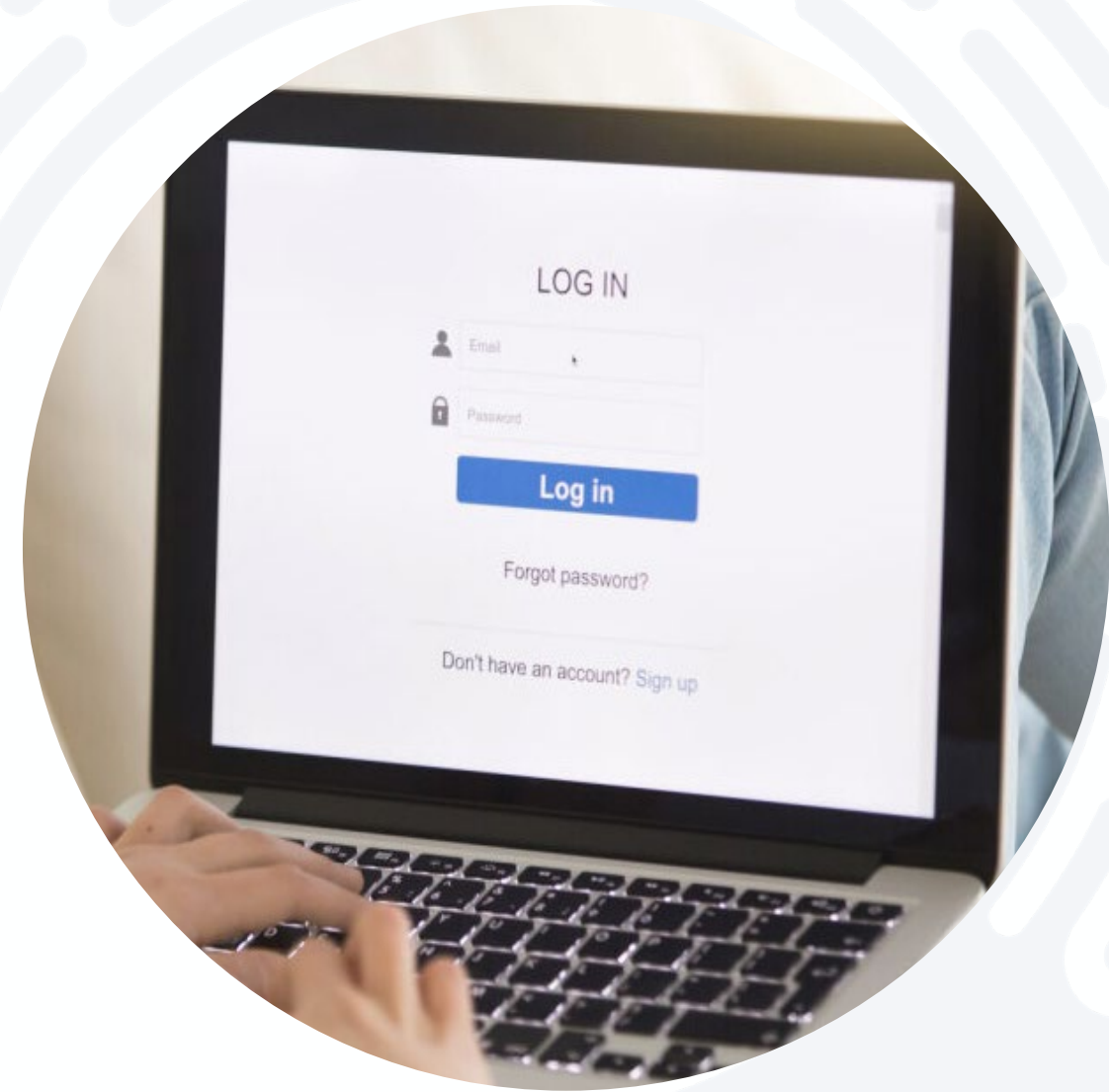
- + Downloading Apps
- + Browsing Activity
- + Travel Activity
- + Location
- + Online Quizzes
- + Device Use

## BIOMETRICS

- + Voice
- + Finger or thumb print
- + Face



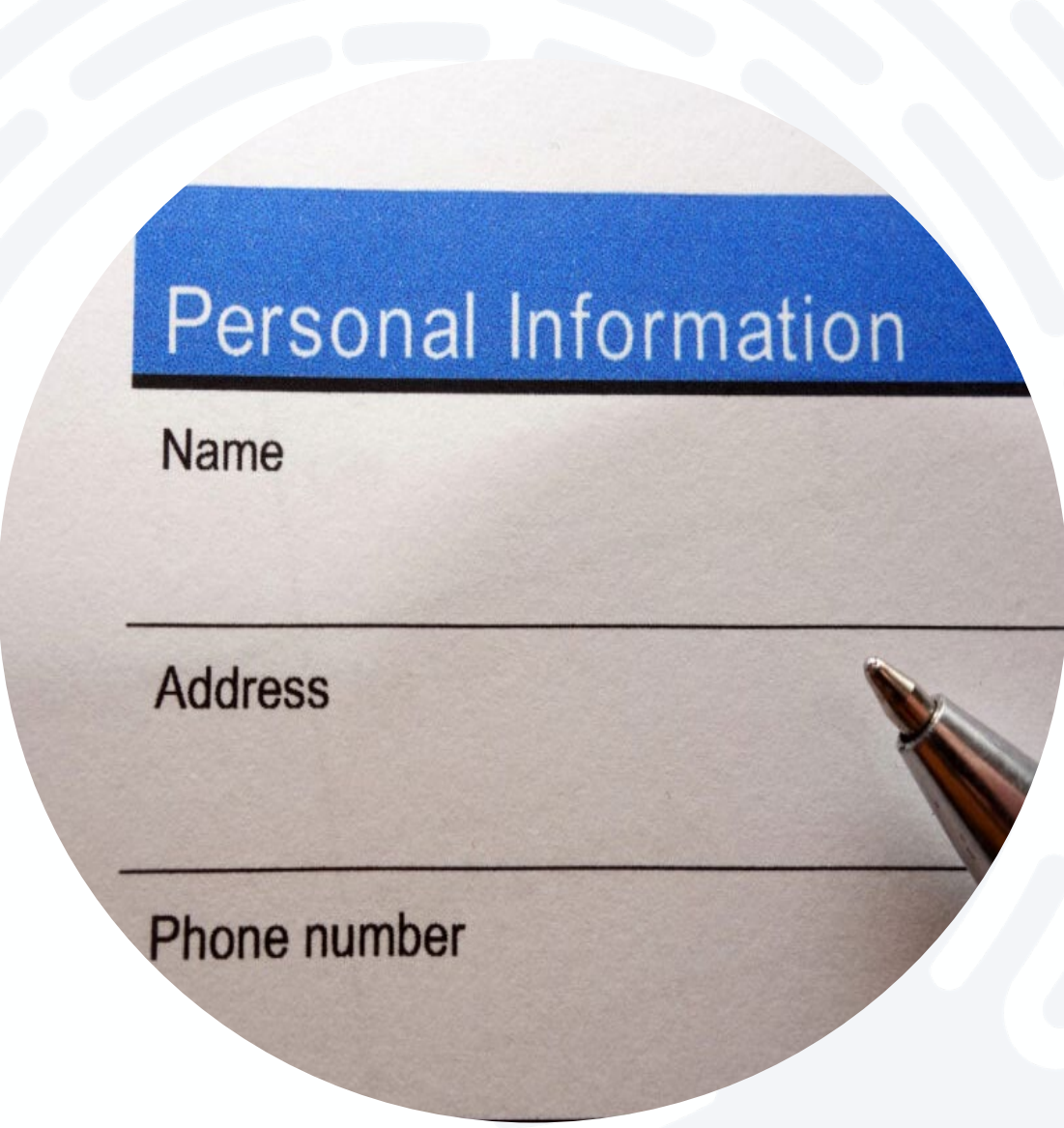
# CREDENTIALS ARE UNIQUE TO US



- Social Security number
- Birth certificate
- Passport
- Driver's license
- Financial accounts
- Username & password



# ATTRIBUTES ARE NOT UNIQUE TO US



## Personal Information

Name

Address

Phone number

- Name
- Address
- Date of birth
- Phone number
- Employer

# THINGS WE DO DEFINE BEHAVIORS

- Downloading Apps
- Browsing Activity
- Travel Activity
- Location
- Online Quizzes
- Device Use



# BIOMETRICS ARE PHYSICAL CHARACTERISTICS

- Voice characteristics
- Finger or thumb prints
- Facial features
- Unique to us as humans

# HOW THIEVES STEAL OUR IDENTITIES



# LOST OR STOLEN ITEMS

- Documents and devices
- Stolen items have greater risk of misuse



# DATA BREACH

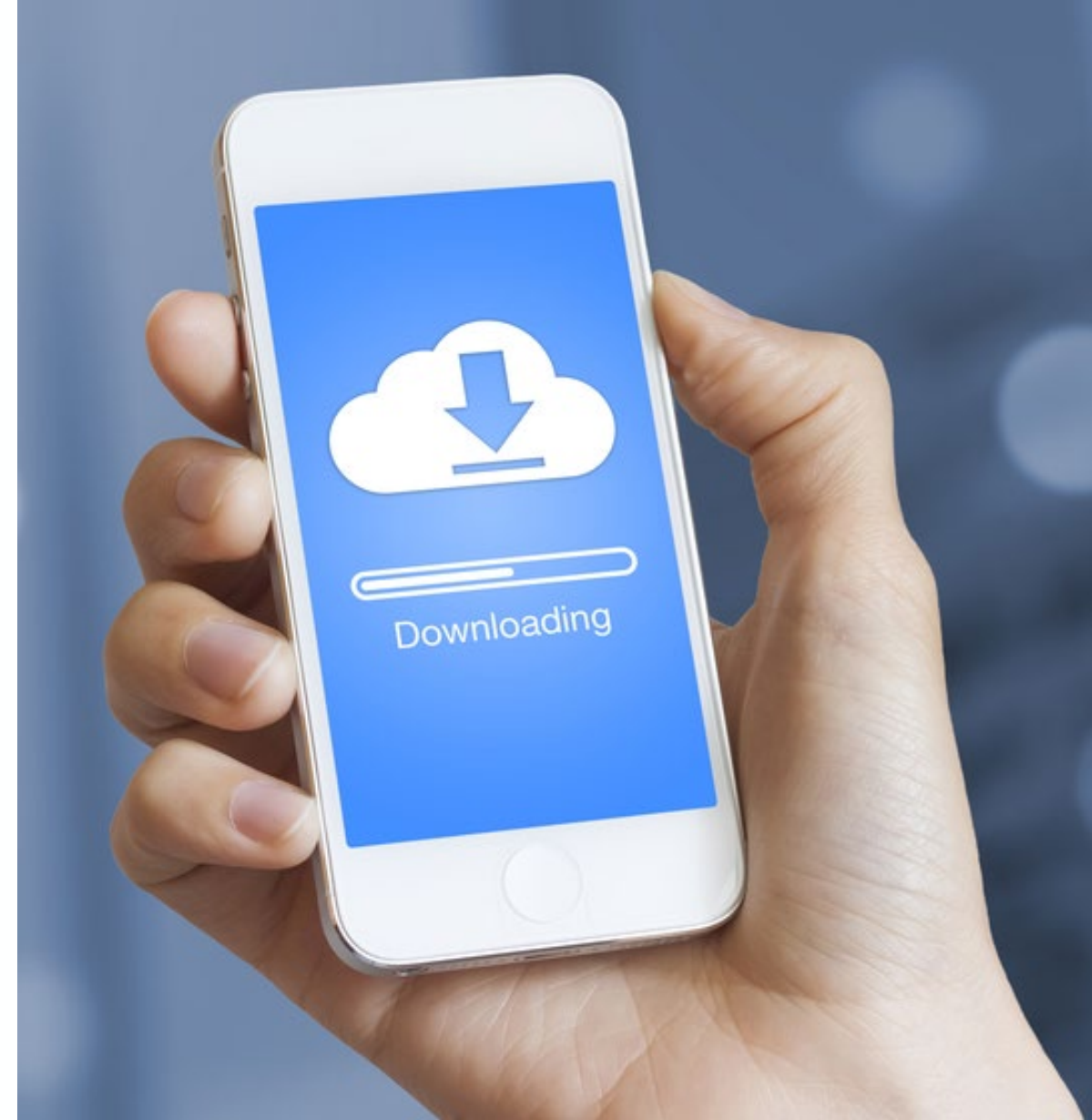
- Outside our control
- Theft of sensitive data in bulk
- Resold in smaller batches on Dark Web





# “HACKED” DEVICES

- Unauthorized activity continues despite changing credentials or accounts.
- Thieves have remote access to the device and are aware of every change.



# SCAMS COME IN MANY FORMS

- Romance
- Lottery
- Shipping
- Government official
- Retailer
- Shopping
- Work from home

All are rooted in impersonating another person, business, or entity

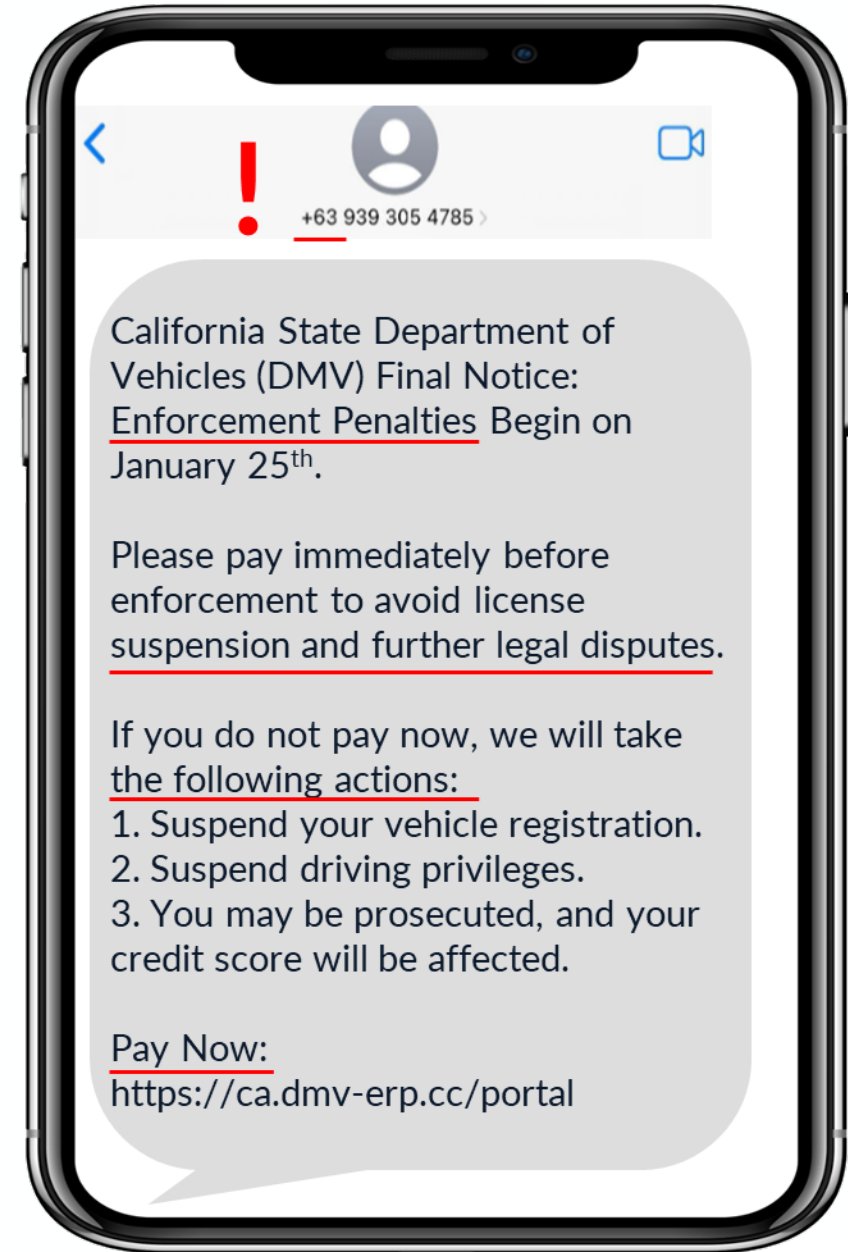


# SCAMMERS WILL SEND YOU TEXT MESSAGES IMPERSONATING OTHERS

!

!

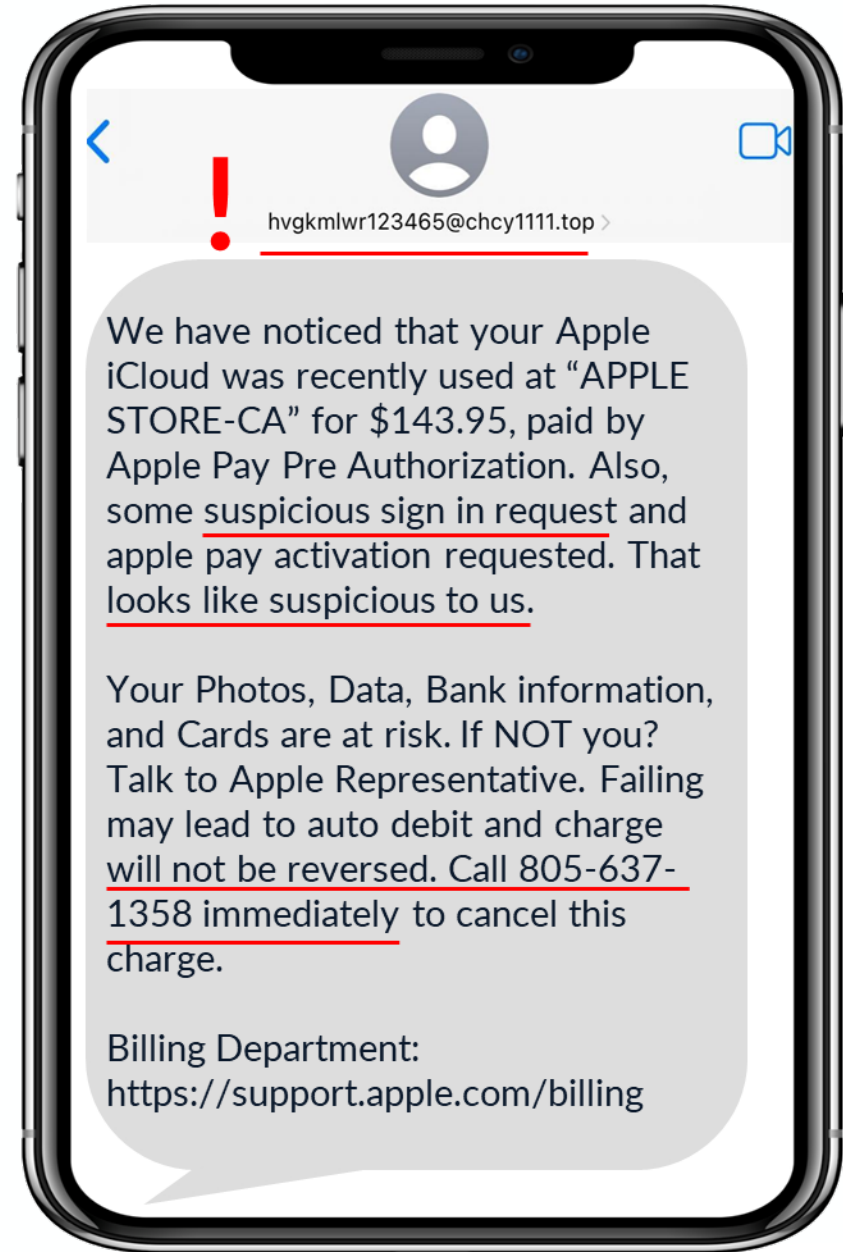
!



# SCAMMERS WILL SEND YOU TEXT MESSAGES TO GET YOU TO CALL THEM

!

!





SCAMMERS WILL ALSO  
USE EMAIL TO GET YOU  
TO CALL THEM

**RENEWAL Confirmation Geek Squad Premium 355924540403**

From: Geek.Squad43@hotmail.com

To: Mike



Order #355924540403

Membership 12JMZY44955ZO352

**Good morning**

Thank you for trusting Geek Squad to keep your digital life secure. As a reminder, your membership for Geek Squad Premium will renew on Mon, 18 Aug 2025 for \$ 299.00 for 2 Years.



**Your plan includes:**

**Premium Security** - Proactively blocks viruses and malware in real-time, 24/7

**Browser Guard** - Blocks ads, trackers, and scams

No action is required to renew your membership and continue your coverage without interruption. If you would like to opt out of auto-renewal, please contact +1 (802) 399-0510 into your account to update your membership settings. Learn more about managing your account.



# SCAMMERS WILL CALL YOU TOO

- Family emergency
- Bank alert
- Credit or loan
- Law Enforcement (FBI, DHS, etc.)
- Purchase confirmation

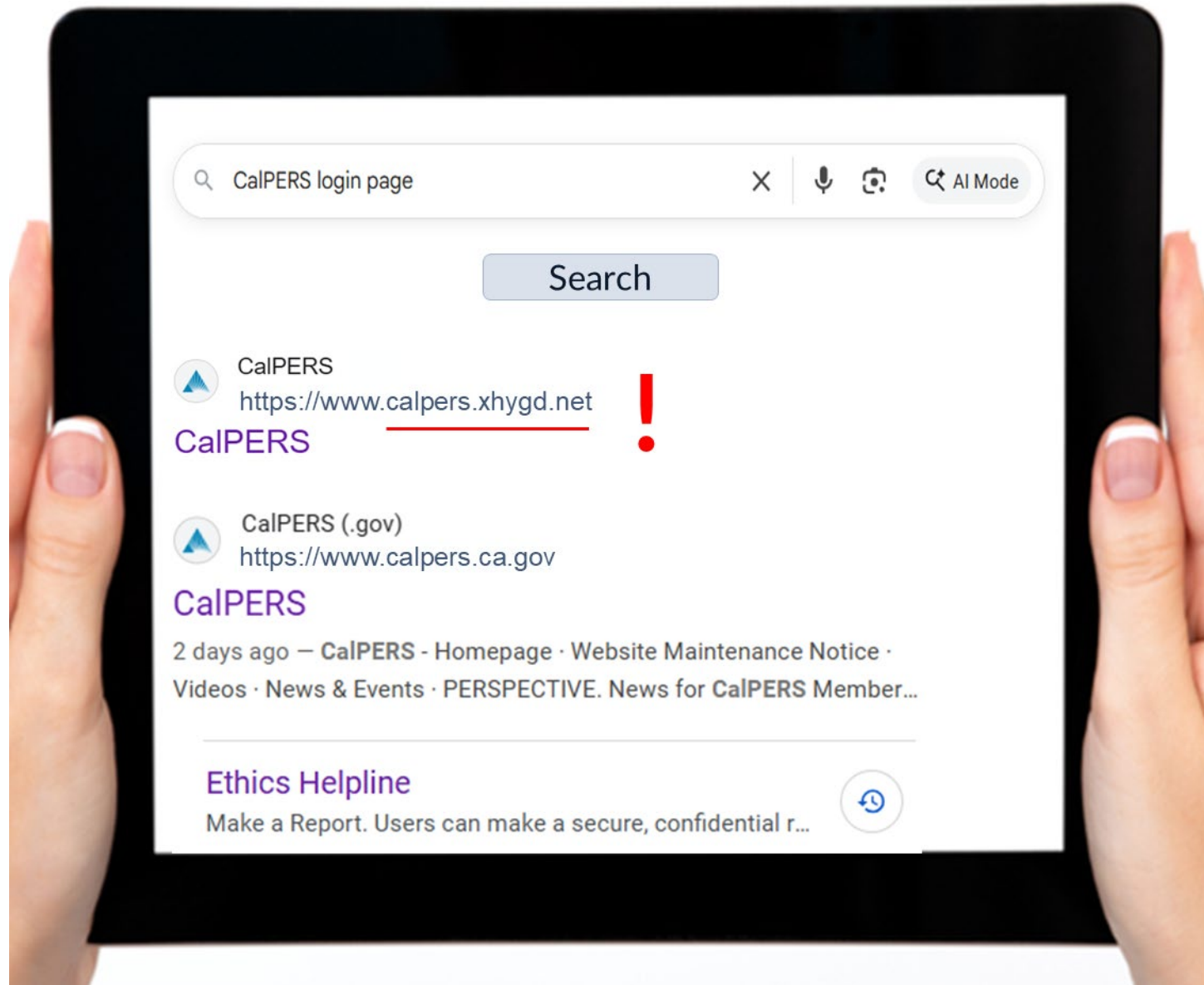


Actual Amazon Impersonation Call



# SEARCH ENGINE MANIPULATION

- Thieves pay to promote their fraudulent websites.
- The fraudulent sites are at the top of the list.
- Scan QR Code for more info:

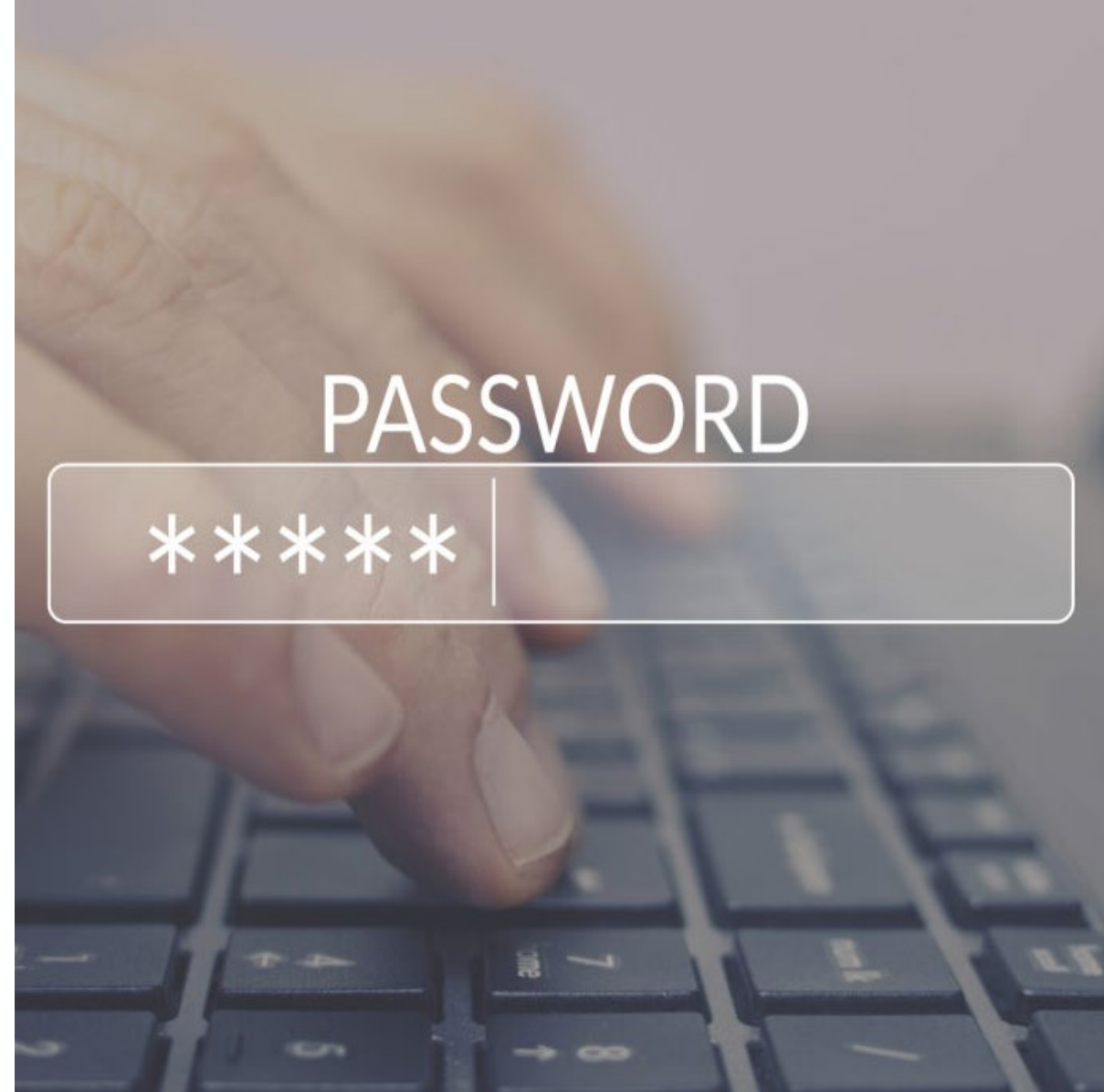


# HOW THIEVES MISUSE OUR IDENTITIES



# ACCOUNT TAKEOVER

- Can occur online or in person; in person includes by phone call
- Online takeover provides immediate access to information and assets
- In person only works where the victim is not known personally



# NEW ACCOUNT

- Credit accounts, loans, utilities, wireless carrier, and government benefit accounts
- Social media accounts are also popular to trick friends and relatives



# FRAUDULENT EMPLOYMENT

- Using someone else's identity to gain employment
- Identity of a minor is commonly used for employment





# FRAUDULENT TAX FILING

- Scammers collect fraudulent refunds by filing returns with someone else's identity
- Some use false W2's to show income for greater returns





# DETECTING AND RESOLVING MISUSE

# *Common Ways One Becomes Aware*

- Notified by CalPERS or other institution
- Suddenly unable to access online account
- Denied a job, benefit, product, or service
- Calls or letters from collection agencies
- Receive a breach notice

# VICTIMS ARE NOT ALONE

- There are people to help you if your identity is misused for unauthorized activity
- **CalPERS:** 888-225-7377
- **ITRC:** 888-400-5530

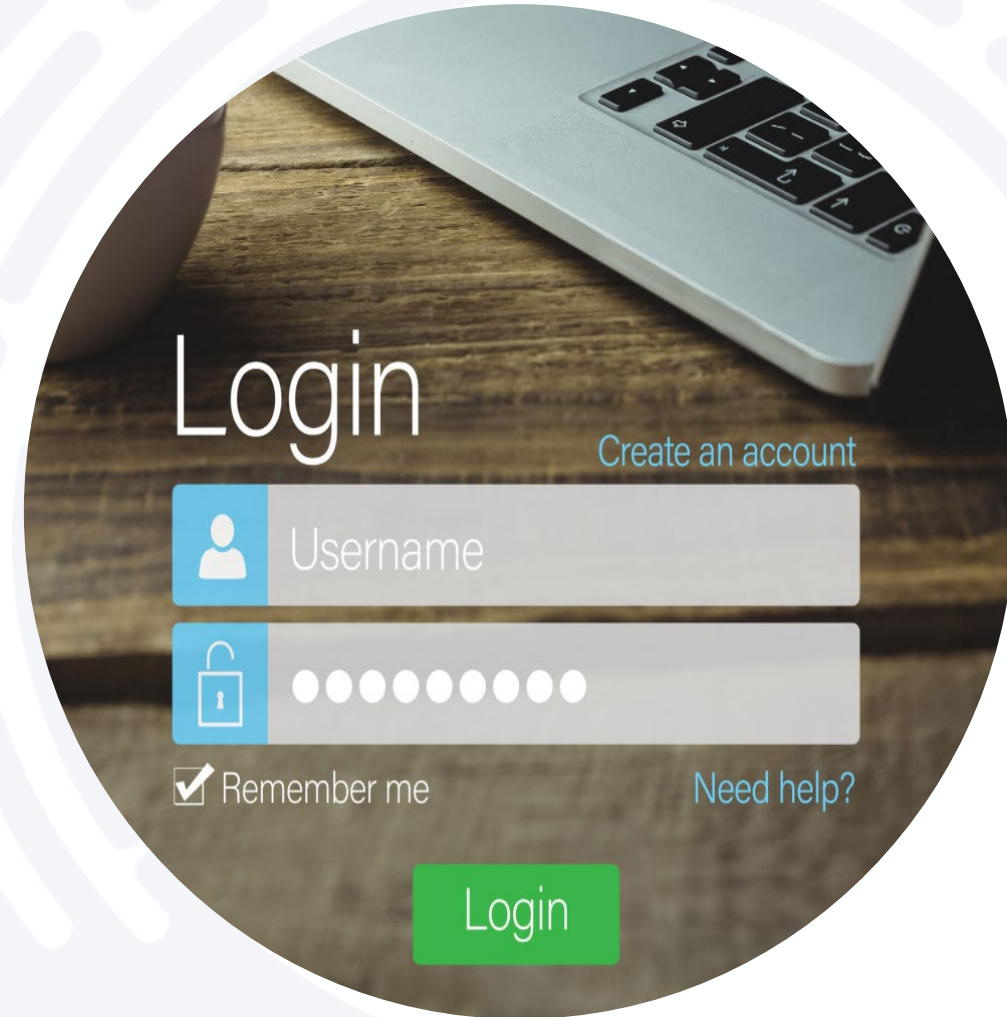


# HOW TO PROTECT YOURSELF



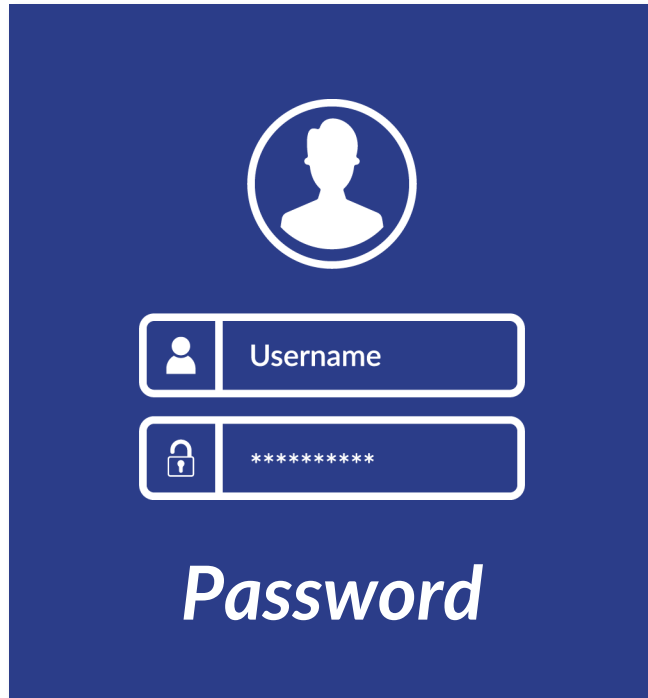
# UPGRADE YOUR PASSWORD

- One password per account
- Use a password manager
- Pick a book quote, song lyric or movie quote
- 16+ characters take longer to crack



# USE MULTI-FACTOR AUTHENTICATION

Send a code by text, call or email, or use an authentication app if available.



# CALPERS MFA DELIVERY METHODS



Reply HELP or call CalPERS for assistance.

Confirmation of account changes will come from

888-CalPERS or  
888-225-7377

**Text/SMS from  
749-43**



Email will include member name.

Do not reply; contact CalPERS for assistance if needed.

**Email from  
Noreply@calpers.ca.gov**



The call will automatically disconnect after the message is delivered.

**Call from  
916-795-7377**

# CREDIT FREEZES AND MONITORING

- Credit monitoring is just that ... monitoring
- If you received a breach notice you likely were offered monitoring
- Freezing your credit prevents misuse
- Consider freezing your child's credit file, too





# KEEP YOUR DOCUMENTS SAFE



*Secure  
Personal  
Information  
Documents*



*Use a Mailbox  
With a Lock*



*Don't Carry  
Blank Checks  
or Unnecessary  
Credentials*



*Shred  
Documents  
Containing PII*

# PROTECTING YOUR DEVICES

Recommendation	Computer	Smartphone
Keep all software up to date, especially antivirus and malware software.	✓	✓
Use caution with public Wi-Fi. Use a VPN if logging in to accounts.	✓	✓
Back up your data to a safe and protected location.	✓	✓
Lock your screen when not using your device.	✓	✓
Use only official app or software stores (Apple, Google, or Microsoft)	✓	✓
Use a biometric (fingerprint or face scan) to secure the lock screen.		✓
Enable “Find My iPad/iPhone” or Find My Device (Android).		✓
Set a SIM PIN with your carrier to prevent SIM Swapping attacks.		✓



# Questions?



CalPERS

1-888-225-7377



ITRC

1-888-400-5530

