

IDENTITY Theft & Fraud

Presented by
Officer Tom Perez
Menifee Police Dept



IDENTITY Theft

ABOUT ME

- Police Officer 10 years
- Currently with Menifee P.D.
- Prev. w/ CSUF P.D. for 9 years
- 4th time giving presentation to OLLI



IDENTITY Theft

OBJECTIVES

1. Define Identity Theft
2. Discuss why you should worry about it
3. Examine how Identity Theft occurs
4. Look at how Identity Theft has emerged
5. Discuss what is being done about I.T.
6. Look at ways to protect yourself.



IDENTITY Theft

**Every 2 seconds,
someone in the U.S. is
a victim of Identity
Theft.**



* According to California DOJ



IDENTITY Theft

By the end of this presentation, 4500 people in the U.S. will become victims of Identity Theft (9000 secs / 2 secs)



* According to California DOJ

IDENTITY Theft

Most Recent Company Data

Breaches:



IDENTITY Theft

Most Recent Company Data

Breaches:

California DMV

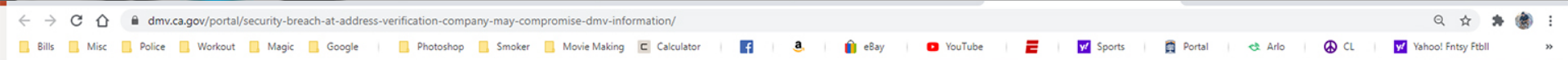
Press release 2/17/21

[CLICK HERE](#)

(to be taken do dmv.ca.gov website)



IDENTITY Theft



Online Services Translate MyDMV

- Vehicle Registration
- Driver's License & ID Cards
- Vehicle Industry Services
- Driver Education & Safety
- Appointments
- Locations

Home Security Breach At Address Verification Company May Compromise DMV Information

SECURITY BREACH AT ADDRESS VERIFICATION COMPANY MAY COMPROMISE DMV INFORMATION

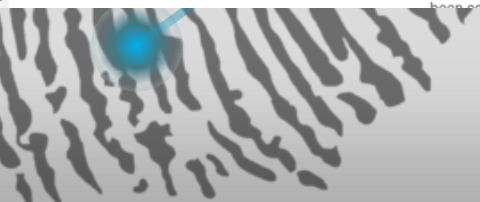
Contact: Office of Public Affairs
2415 First Avenue
Sacramento, CA 95818
(916) 657-6437 | dmvpublicaffairs@dmv.ca.gov

FOR IMMEDIATE RELEASE
February 17, 2021

Potentially impacts vehicle registration records, no driver's license information
DMV working with law enforcement and assessing additional privacy protections

Sacramento – The California Department of Motor Vehicles (DMV), out of an abundance of caution, is notifying customers that a company it uses to verify vehicle registration addresses has had a security breach. DMV systems have not been compromised and it is unknown if DMV data shared with the company has been compromised. An investigation is under way.

Ask DMV



IDENTITY Theft

Most Recent Company Data

Breaches:





IDENTITY Theft

Most Recent Company Data

Breaches:

**Kaiser Foundation
Hospitals, Northern
California**

Press release 2/23/21

IDENTITY Theft

Most Recent Company Data

Breaches:





IDENTITY Theft

Most Recent Company Data

Breaches:

JPMorgan Chase Bank

Press release 12/23/20

IDENTITY Theft

Most Recent Company Data

Breaches:



IDENTITY Theft

Most Recent Company Data

Breaches:

U.S. Bank / Sam's Club / Valley Presbyterian Hospital
/ Dickey's BBQ Pit / GenRx Pharmacy / Aetna /
Canon U.S.A. Inc. / University of California, San
Fran / San Diego Union H.S. district / California
Physicians' Services doing business as Blue Shield
Of California / Rady's Children's Hospital – San
Diego / Trinity Health / City of Torrance / Carnival
Corporation / Bosley Inc. / Syracuse University

(** from State of California Department of Justice website. Search
“data security breaches”)



IDENTITY Theft

As of February 2019, more than 740 million accounts stolen from 24 different websites were found up for sale in online markets (sellers ask for \$14,000 - \$20,000 in bitcoin)



* According to Bleeping Computer

IDENTITY Theft

2019 worst data breaches:

1. Fortnite – 200 million users compromised
2. MyFitnessPal (owned by Under Armour) – 150 million accounts stolen from hackers
3. MyHeritage – 92 million accounts
4. Dunkin Donuts – twice in three months were hacked.

* According to Bleeping Computer



IDENTITY Theft

**How many people in
this room have been a
victim of Identity Theft?**



IDENTITY Theft

If you have a social security number &/or a credit card, your info is the wrong hands of someone.



IDENTITY Theft

- **1936: SS# first used by U.S. Government. Was supposed to be limited to SS programs.**
- **Today it's the most frequently used recordkeeping number in the U.S.**



IDENTITY Theft

- Social Security #'s are **NOT** issued sequentially.
- First 3 #'s represent the state in which you applied for SS card (area code)
- Second 3 are group #'s
- Last 4#'s are serial numbers



IDENTITY Theft

TRUE or FALSE?

**You can get a different SS# if
you are the victim of Identity
Theft?**



IDENTITY Theft

TRUE or FALSE?

You can get a different SS# if you are the victim of Identity Theft?

- TRUE -

But it is very difficult, time consuming, & all resources to fix problems from misuse would have to be exhausted



IDENTITY Theft

TRUE or FALSE?

Seniors (age 65 +) are the most targeted group for Identity Theft?



IDENTITY Theft

TRUE or FALSE?

Seniors are the most targeted group for Identity Theft?

- **FALSE** -

Student's age 18-25 (31%)

***(Why? Because it takes them
3 times longer to find out)***



IDENTITY Theft

TRUE or FALSE?

**Identity Theft is easily
resolved?**



IDENTITY Theft

TRUE or FALSE?

Identity Theft is easily
resolved?

- **FALSE** -

It takes an average of 6 months
and 250+ hrs to recover from
each I.T. incident



IDENTITY Theft

TRUE or FALSE?

**The best way to prevent
Identity Theft is NOT to shop
online?**



IDENTITY Theft

TRUE or FALSE?

The best way to prevent
Identity Theft is NOT to shop
online?

- FALSE -

More than half of all Identity
Theft happens OFFLINE.



IDENTITY Theft

TRUE or FALSE?

**Women are more concerned
about Identity Theft than men?**



IDENTITY Theft

TRUE or FALSE?

Women are more concerned about Identity Theft than men?

- TRUE -

2011 survey, showed women more concerned on every I.T. question, & 4 out of 10 were very concerned.



IDENTITY Theft

TRUE or FALSE?

**The most common type of
Identity Theft is Credit Card
Fraud?**





IDENTITY Theft

TRUE or FALSE?

The most common type of Identity Theft is Credit Card Fraud?

- **TRUE** -

54% of Identity Theft is CC Fraud (due to ease of applying)

IDENTITY Theft

TRUE or FALSE?

Drug trafficking has officially been replaced by Identity Theft as the number one crime?



IDENTITY Theft

TRUE or FALSE?

Drug trafficking has officially
been replaced by Identity Theft
as the number one crime?

- **TRUE** -

**40 million cases reported in
2016**



IDENTITY Theft

TRUE or FALSE?

Minorities are more often victims of Identity Theft?



IDENTITY Theft

TRUE or FALSE?

Minorities are more often victims of Identity Theft?

- FALSE -

White, non-Hispanic's make up 38% of all I.T. cases.



IDENTITY Theft

TRUE or FALSE?

**13% of the World's White
Collar Crime is perpetrated in
California?**



IDENTITY Theft

TRUE or FALSE?

**13% of the World's White
Collar Crime is perpetrated in
California?**

- TRUE -

**A good portion out of Newport
Beach. NY is close at 11%**



IDENTITY Theft

#1 scam in America right now
is the Covid Vaccine scam

Rep calls you on the phone to
let you know the vaccine is
available in your area right now
and you can get vaccinated for
only \$299. So get out the credit
card!!!





IDENTITY Theft

#2 scam in America right now tax scam

The “I.R.S.” calls you up to let you know you have unresolved tax issues and owe thousands of dollars in back taxes. If you don’t want to go to jail, you better pay with gift cards



IDENTITY Theft

When you receive a legitimate gift card as a present, use it!

Scammers often have BOTs that steal the gift card balance.

Hackers use a bot called “GiftGhostBot” to run a store’s online gift card balance check system looking for a match

IDENTITY Theft

MY EXPERIENCE w/ I.T.

1. AOL
2. Landmark Steakhouse phone call
3. Recent U.S. Bank phishing phone call
4. Arby's & El Pollo Loco Skimmer
5. Community Mailbox (331 Ave. 11)
6. Vehicle break-in in driveway
7. AZ left dayplanner w/ CCs on ATM
8. Microsoft calling my dad (Jan 2020)

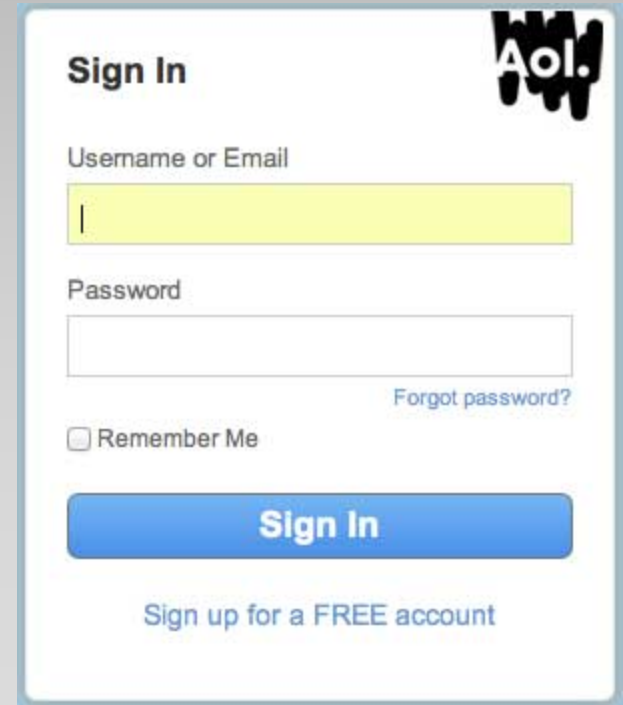


IDENTITY Theft

AOL LOG-IN SCREEN

1999 received an email from “AOL” saying I needed to log-in. After trying it 3 times, nothing happened.

Next day 10k+, spam emails sent & my account suspended.



The image shows a screenshot of the AOL sign-in interface. At the top left, it says "Sign In" and at the top right is the AOL logo. Below the logo, there are two input fields: "Username or Email" and "Password". The "Username or Email" field is highlighted in yellow. Below the "Password" field, there is a link that says "Forgot password?". At the bottom left, there is a checkbox labeled "Remember Me". At the bottom center, there is a blue button labeled "Sign In". At the bottom right, there is a link that says "Sign up for a FREE account".



IDENTITY Theft

LANDMARK STEAKHOUSE

2010 – Video Relay Service (VRS) or Deaf Relay Service.

- Relay Service call taker ordered 2k in food.
- Wanted me to pay driver cash



IDENTITY Theft

U.S. BANK PHISHING CALL

- Caller from “U.S. Bank” asked me if I recently made a purchase from Best Buy in Nashville, TN for \$2700. When I said No, caller asked if card still in my possession. Asked for CC# to verify.



IDENTITY Theft

MAILBOX BREAK-IN

Seven times broken into. Prior year stole tax returns.



IDENTITY Theft

VEHICLE BREAK-IN

Broke into my wife's vehicle after seeing her purse on the front seat.

Used both of our credit cards at two Walmart's, two Gas Stations, fast food in under 90 minutes.



IDENTITY Theft

Dayplanner / ATM in AZ

Used ATM at BofA – Tempe, AZ. Left my day planner with all my credit cards on top of it. Discover Card constantly calling.





IDENTITY Theft

Microsoft Tech Support calling my dad

My dad received a phone call from “Microsoft” saying they detected viruses and they computer has been hacked & they need remote access to get rid of it immediately. They gave him a website to type in so they could gain access and “fix” his computer.

IDENTITY Theft

Common pop-up you might see on your computer. This is the opposite of the call you receive, here, you actually call them.

The screenshot displays a browser window with several overlapping alerts and a support banner. At the top left, there is a navigation bar with 'Microsoft', 'Office', 'Windows', and 'Surf'. Below this, a red banner reads 'HARD DRIVE ERROR WARNING CRIT' and 'Critical internal error codexxXX00296H Reboot your device now call support'. A white dialog box in the center is titled 'VIRUS ALERT FROM MICROSOFT' and states 'This computer is BLOCKED'. It lists reasons for the block: 'Your computer's registration key is Blocked', 'Why we blocked your computer? The window's registration key is illegal. This window is using pirated software. This window is sending virus over the internet. This window is hacked or used from undefined location. We block this computer for your security.' To the right, another red banner asks to 'Enter Windows registration key to unblock' with an 'ENTER KEY:' field and a 'Submit' button. At the bottom, a blue banner features the Microsoft logo and the text 'Windows Support Alert Your System Detected Some Unusual Activity. It might harm your computer data and track your financial activities. Please report this activity to 1-800- 297-5426'. Two buttons, 'Ignore Alert' and 'Chat Now', are at the bottom.

Microsoft Office Windows Surf

HARD DRIVE ERROR WARNING CRIT
Critical internal error codexxXX00296H
Reboot your device now
call support
Microsoft Security Tollfree:
+1(800) 297-5426

Prevent this page from creating additional dialogues.

VIRUS ALERT FROM MICROSOFT
This computer is **BLOCKED**

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.
We block this computer for your security.
Contact microsoft helpline to reactivate your computer.

Enter Windows registration key to unblock.
ENTER KEY:

Windows Support Alert
Your System Detected Some Unusual Activity.
It might harm your computer data and track your financial activities.
Please report this activity to 1-800- 297-5426

IDENTITY Theft

MAJOR COMPANIES BREACHED SINCE 2012

Breach of Target customer data

Target says about 40 million credit and debit card accounts may be affected by a data breach. Cards that were swiped during purchases at Target stores in the U.S. between Nov. 27 and Dec. 15 may have been compromised.



Target says the breach affected store purchases and not online transactions. The stolen data includes:

- **Credit/debit card number**
- **Expiration date**
- **Name**
- **Three-digit security code on back of card**

The store advised customers to:

Check statements carefully

Report suspicious charges to credit card company and call Target at 866-852-8680

Report cases of identity theft to law enforcement or the Federal Trade Commission

IDENTITY Theft

MAJOR COMPANIES BREACHED SINCE 2013

2017 – EQUIFAX (143 million)

2016 – Adult FriendFinder (412.2 million)

2015 – Anthem Insurance (78.8 million)

2014 – ebay (145 million)

2014 – CHASE bank (76 million)

2014 – Home Depot (56 million)

2013 – YAHOO (3 billion!!!)

2013 – Target (110 million)



IDENTITY Theft

EQUIFAX BREACH

Hackers stole half of the U.S. populations
SS# and Driver's License #.

Go to: www.equifaxsecurity2017.com to see
if your information has been compromised.



IDENTITY Theft

MAJOR COMPANIES BREACHED SINCE 2011

Chick-fil-A

Sony pictures (employees only)

United States Postal Service

Staples

Kmart

US Office of Personal Management

Sony Play Station Network

RSA Security



IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO

Genealogy websites contain massive amounts of data about people.

(ancestry.com / 23andme /
FamilyTreenow.com)


- Ancestry.com no longer shares SS#'s from those deceased less than 10 years.

However, many people still claim SScards can be access on the site.



IDENTITY Theft

2019 / 2020 New Scams



Airbnb Rentals – fake ads for non-existent property where user pays the scamster directly

Home Improvement – especially for older adults. Door to door salesman trying to sell home improvements. Make you pay up front then don't show up for the service.

Netflix – scam usually deals with a “payment declined” email or phone call. User should log in to Netflix account to verify.

IDENTITY Theft

2019 / 2020 New Scams

Amazon– order cancellation fake email.

Goal is trick victim into downloading malware (spoofing) or redirect them to a fake Amazon website that asks for username and password.

Veterans – phony phone call solicitations for charity contributions or pension buyouts.

Make sure to independently verify. Go to their website.,



IDENTITY Theft


2019 / 2020 New Scams

Charging cable scam – be careful to charge your cell phone in public (i.e. airport, Starbucks). Huge increase in L.A. county. AKA “Juice Jacking” where you plug in and your cellphone data is downloaded to a remote server



IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO



FamilyTreeNow.com contains a remarkable amount of personal information including age, home address (current and past), name of family members, copies of birth certificates, marriage certificates, death certificates.

Removal process is cumbersome, and in some cases does not work at all.

IDENTITY Theft



bat
@mzbat

Follow

The @familytreenow site is a nightmare. They dox you & your family with a total disregard for safety. The "Opt Out" option doesn't work.



Your opt out request could not be processed due to an error. Please try again by refreshing your browser, or go back and click optout button again. If that doesn't work, please submit your request manually to customer service using our contact us form.

4:45 PM - 10 Jan 2017



IDENTITY Theft

ALWAYS BE ON LOOKOUT FOR NATURAL DISASTER SCAMS

Government disaster assistance agencies do not call or text asking for financial account information and there is NEVER a fee required to apply for or get disaster assistance from FEMA of the Small Business Administration.

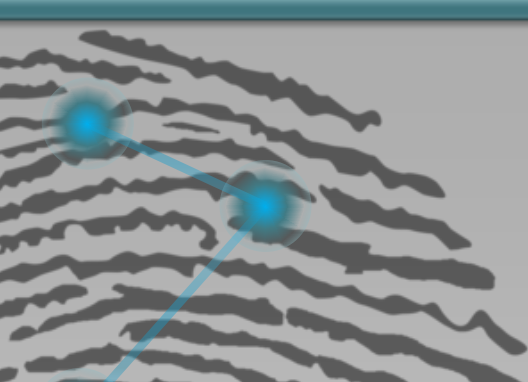
IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO

Spokeo.com

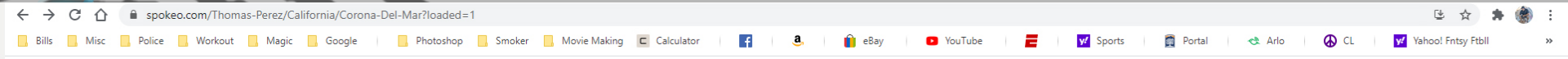
Intelius.com





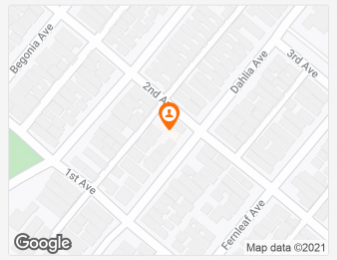
IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO



Thomas Perez

ABOUT LOGIN SIGN UP



People Search > Perez > Thomas Perez > California > Corona Del Mar

Thomas Perez in Corona Del Mar, CA

Thomas Perez may also have lived outside of Corona Del Mar, such as Costa Mesa, Lake Elsinore and 2 other cities in California.

Refine Your Search Results

Sort by Relevance

All Filters 2

Thomas Raymond Perez, 47

RESIDES IN COSTA MESA, CA

Lived In Quail Valley CA, Scottsdale AZ, Freeport NY, Corona Del Mar CA

Related To Ricardo Perez, Raymond Perez, Margaret Perez, Pamela Perez, Kristin Perez

Also known as Perez Ray, Tom Perez, Perez Thomas

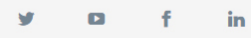
Includes Address(15) Phone(12) Email(7)

SEE RESULTS

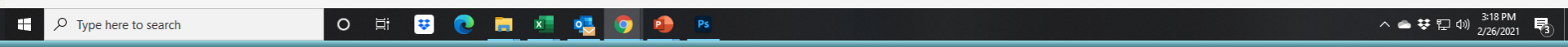
Email Lookup | Area Code: 2 3 4 5 6 7 8 9 | Name: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

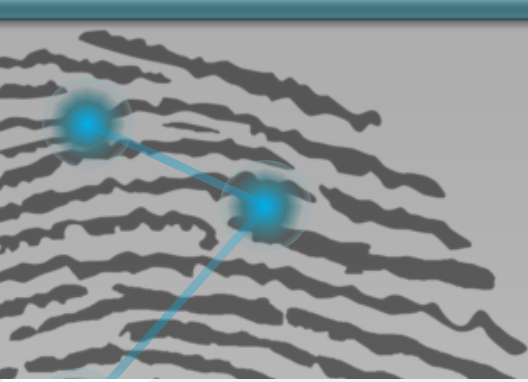
About Terms Privacy Contact Careers Help Blog Affiliates

Spokeo is not a consumer reporting agency as defined by the Fair Credit Reporting Act (FCRA). Do not use this site to make decisions about employment, tenant screening, or any purpose covered by the FCRA.



Copyright © 2006-2021 Spokeo, Inc.





IDENTITY Theft


HOW EASY IS IT TO GET YOUR INFO

spokeo.com/Thomas-Perez/California/Costa-Mesa/p30079197101

Bills Misc Police Workout Magic Google Photoshop Smoker Movie Making Calculator f a eBay YouTube Sports Portal Arlo CL Yahoo! Fntsy Ftball

SPOKEO Thomas Perez ABOUT LOGIN SIGN UP

People Search > Perez > Thomas Perez > California > Costa Mesa > **Thomas Raymond Perez**



Thomas Raymond Perez, Age 47

aka Perez Ray, Tom Perez, Perez Thomas




- ✓ **Current Address:** Oriole Dr, Costa Mesa, CA
- ✓ **Past Addresses:** Quail Valley CA, Scottsdale AZ +12 more
- ✓ **Phone Number:** (928) 486- +11 phones
- ✓ **Email Address:** c @aol.com +6 emails

UNLOCK PROFILE

● **Contacts (19)** ● **Locations (15)** ● **Family (28)** ● **Social (147)** ● **Court (125)** ● **And More**

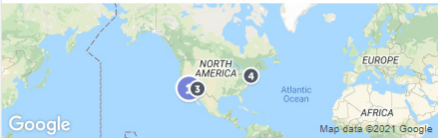
PHONE & EMAIL (19)

We found 19 phone numbers and email addresses.
See Thomas' contact info now >

-  (928) 486- Lake Havasu City, AZ • Sprint
-  (949) 285- Anaheim, CA • Verizon Wireless
-  c @aol.com aol

ADDRESS HISTORY (15)

We found 15 addresses for Thomas.
See where Thomas has lived >




Address information for Thomas may include:

- ✓ Current Address
- ✓ Past Addresses
- ✓ Property Owner
- ✓ Home Value

FAMILY MEMBERS (28)

We found 28 relatives for Thomas.
See Thomas' family members >



Family member details may include:

- ✓ Name & Age
- ✓ Contact Info
- ✓ Demographics
- ✓ Location

Type here to search

3:22 PM 2/26/2021



IDENTITY Theft

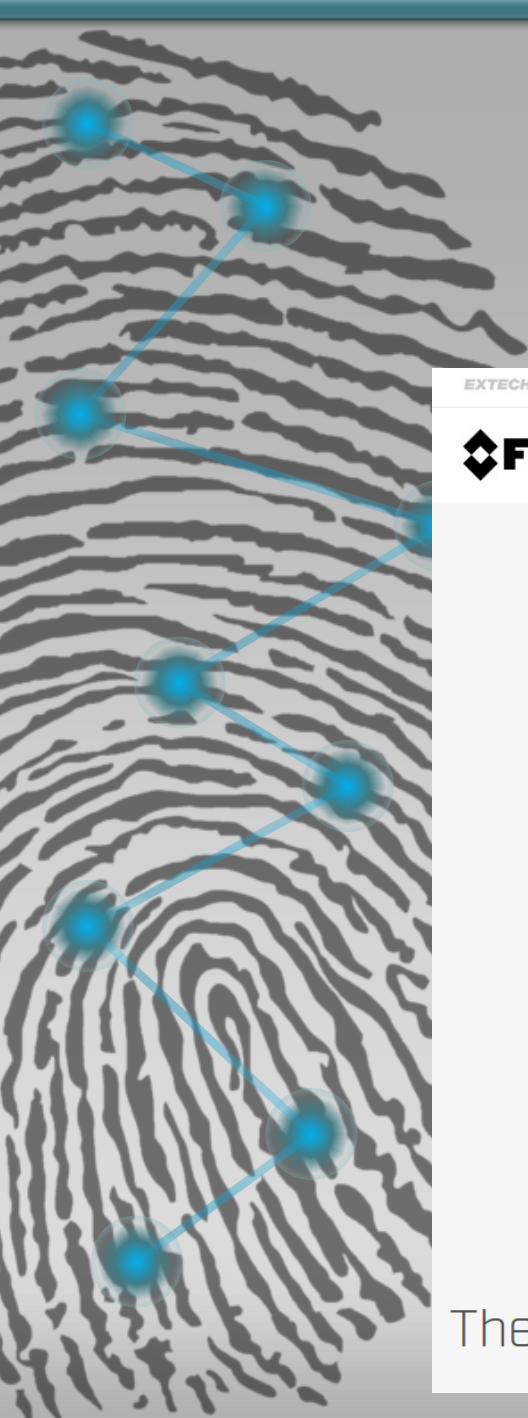
EMERGING SCAM

Text message from “Mexican Cartel” saying they are going to kill your family if you don’t pay \$2500. Send graphic pictures and have real names of relatives and the cities they live in.

Pay your fine so you don't involve your family in your problems pay the fine and nobody will get hurt

IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO



EXTECH | Raymarine | itc

FLIR

APPLICATIONS PRODUCTS DISCOVER SUPPORT NEWS ABOUT

THERMAL CAMERA FOR SMART PHONES

FLIR ONE Gen 3

MODEL: FLIR ONE GEN 3 - ANDROID (USB-C)

[Go to Support Page »](#)

There's an invisible world right next to the one you see every day, just waiting for you to explore it with the FLIR ONE. Whether you're seeing the world in a whole new way or just finding problems around the house, FLIR ONE's thermal camera gives you a new view of your everyday world. Discover what's been around you all the time, with FLIR ONE. The FLIR ONE app requires sign in, which enables automatic warranty registration and access to all the latest updates from FLIR.

PRODUCT VARIATIONS:

FLIR ONE Gen 3 - Android (USB-C)

\$199.99

[BUY NOW](#) [REQUEST INFO](#)

Thermal Imaging Camera Attachment

IDENTITY Theft

HOW EASY IS IT TO GET YOUR INFO

Flir.com – thermal camera that displays infrared which allows you to see the temperature of things up to 15 mins

Latest technique on how to steal an ATM pin number

Written by [Odipo Riaga](#) ✓



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

The 3 layers of the WWW:

Surface web vs

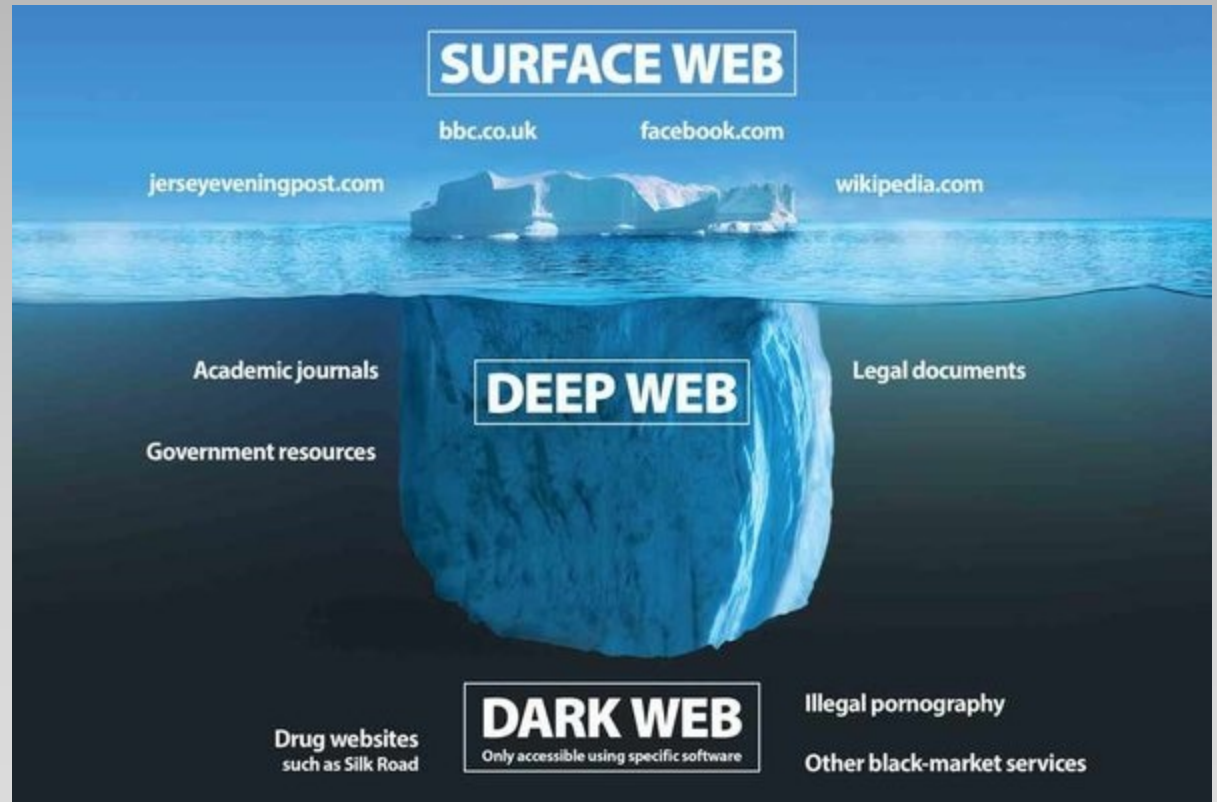
Deep Web vs

Dark Web



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

SURFACE or OPEN WEB – what most people use. Includes news articles, blog posts, social media, google searches, general info. Facebook, Tik Tok, Google, Yahoo, ESPN, etc. Only 4% of the use of the WWW is done on the Surface Web





IDENTITY Theft

WHAT DO THEY DO WITH YOUR INFO?

DEEP WEB – this is not the Dark web which it is often confused with and used interchangeably. These are outside the reach of search engines. Only accessible through certain browsers, and is often the basis for criminal activity since users can remain anonymous. Basically they are unindexed web databases a search engine can't reach.

IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

DEEP WEB – except for law enforcement and the intelligence community, most organizations have no interest in gathering data from this part of the web. And it's mostly not censored or regulated. (ex. Medical records, financial records, govnmnt resources, legal docs, scientific reports)



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

DEEP WEB – Gold mine of info, but access usually goes through some sort of login. Deep web, while less accessible, is potentially more valuable for businesses and organizations since it's hundred of times larger than the surface web and the content it serves up is often a more authoritative source of info.



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

DARK WEB – an encrypted online content that is not indexed by conventional search engines. Very secure and very private. Identities are almost always concealed. Hotspot for criminal activity. Used to keep internet activity hidden. (ex. Wikileaks, Russian anonymous marketplace, hidden wiki, dream market)



IDENTITY Theft

WHAT DO THEY DO WITH YOU INFO?

DARK WEB – tons of child porn.

Terrorist activity. Human trafficking.

Murder for hire. Identity theft (fake birth certificates, real cc numbers, fake citizenship papers, fake IDs, real bank account numbers). These can all be purchased with bitcoin (cryptocurrency – a computer file stored in a digital wallet)



WHAT IS IDENTITY THEFT?





IDENTITY Theft

IDENTITY THEFT IS:

- One person, using personal information gathered from some source, takes on the identity of another person *without permission* and conducts a variety of activities using that identity.
- The intent is to use that identity for personal gain, generally with the intent to defraud others.

IDENTITY Theft

IDENTITY THEFT IS:

- California Penal Code 530.5(a) is the primary law addressing criminal Identity Theft.

“Every person who willfully obtains personal identifying information, of another person, and uses that information for any unlawful purpose, including to obtain credit, goods, services, real property, or medical information without the consent of that person...”



IDENTITY Theft

IDENTITY THEFT PENALTY:

- California Penal Code 530.5 is a wobbler (can be charged as a misdemeanor or a felony).
- Usually depends on the monetary value of damages.





IDENTITY Theft

TRUE or FALSE?

Identity theft is easy to prosecute?



IDENTITY Theft

TRUE or FALSE?

Identity theft is easy to prosecute?

- FALSE -

The majority of Identity theft cases are never prosecuted or solved.

WHY WORRY ABOUT I.T.?



IDENTITY Theft

WHY WORRY ABOUT I.T.?

- One in 33 households discovered at least one type of identity theft during the previous 12 months.
- Households with the highest incomes and those headed by persons ages 18–25 were the most likely victims.
- One in five victimized households spent about two months resolving problems resulting from identity theft.
- Identity theft is of greater concern to adults with older children at home (45%) than those with younger children at home (27%).



IDENTITY Theft

WHY WORRY ABOUT I.T.?

Victims of Identity Theft and those who know victims, are far more likely to be concerned about this issue than those who have not been victims.

- Concern among victims, 60%; versus among non-victims, 31%
- Concern among those who know a victim, 45%; versus concern among those who do not know a victim, 32%



IDENTITY Theft

WHY WORRY ABOUT I.T.?

Deterrence and apprehension are not yet effective. **PREVENTION** is the best defense.

There are jurisdictional problems concerning where the crime occurs.

It is an attractive crime to criminals because of its low risk and high return.

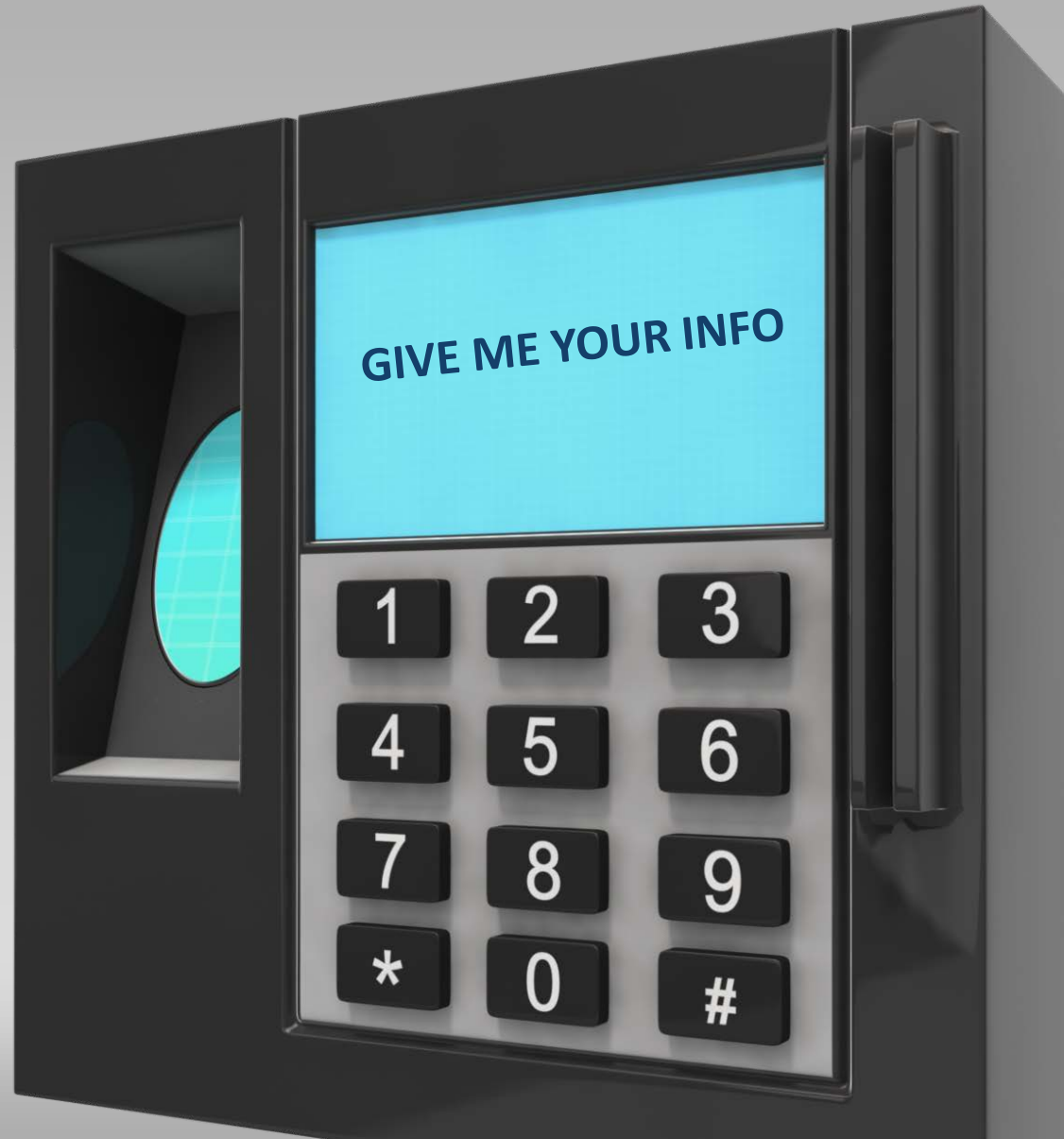


IDENTITY THEFT

IS IT A PROBLEM?

2017 Identity Theft study
by Javelin Strategy &
Research, found that over
\$16 billion was stolen
from 15.4 million U.S.
consumers in 2016 alone.

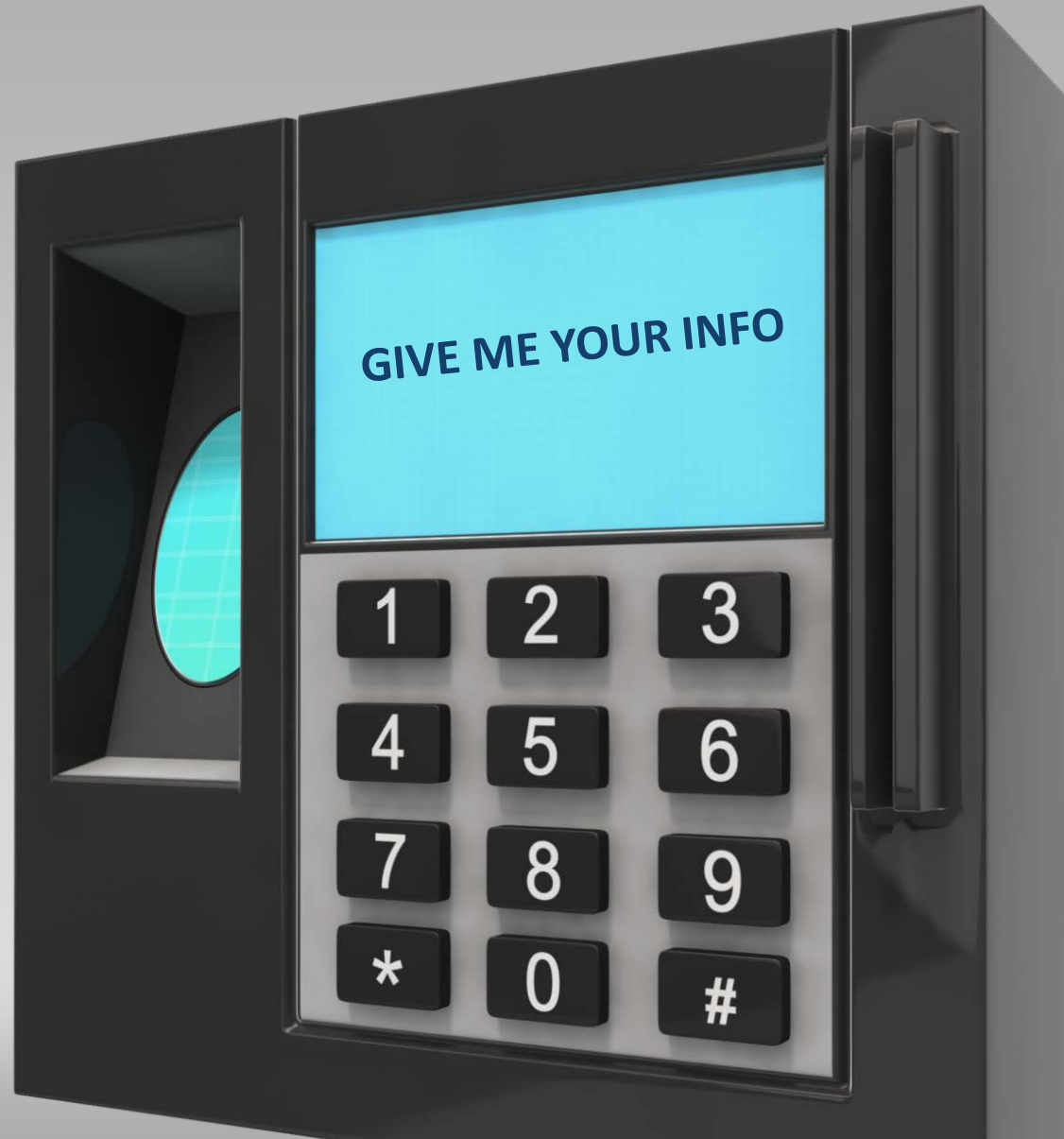
In the past 6 years,
identity thieves have
stolen over \$107 billion.



IDENTITY THEFT

IS IT A PROBLEM?

- The good news is most people are taken for less than \$100 (most times they are reimbursed by banks).
- Only 14% of I.T. victims lose their money.
- Only 2% of I.T. victims lose more than \$1000.



IDENTITY Theft

HOW VICTIM'S INFO WAS MISUSED IN 2015

PERCENT

Government documents or benefits fraud	49.2%
Credit Card Fraud	15.8%
Phone or utilities fraud	9.9%
Bank fraud	5.9%
Attempted Identity Theft	3.7%
Loan Fraud	3.5%
Employment related fraud	3.3%
Other Identity Theft	19.2%





IDENTITY Theft

TRUE or FALSE?

The national average loss for credit card fraud is nearly \$3,000?

- TRUE -

The avg loss when someone uses your C.C. is \$2,935



IDENTITY Theft

TOP 5 STATES FOR I.T. CASES

- 
1. Nevada
 2. **CALIFORNIA**
 3. Florida
 4. Massachusetts
 5. New Mexico

IDENTITY Theft

TOP 5 STATES FOR I.T. CASES

1. Nevada
2. **CALIFORNIA**
3. Florida
4. New Mexico
5. Texas



HOW DOES I.T. HAPPEN?



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 1: Getting the Identity

- Thieves look for information in a number of ways.
 - Discarded documents in the trash.
 - Receipts from purchases.
 - Lost or stolen wallets / purses.
 - Online “phishing”
 - Stolen mail from mailboxes
 - New, inventive ways daily



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 1: Getting the Identity (cont.)

- Some thieves obtain lists of personal information through computer hacking, theft, or bribery.
- The information may be resold to other crooks or used numerous times by the original thief or thieves.
- Profits may be used to support additional criminal activities, such as drug use and terrorism.



IDENTITY Theft



What are some important numbers associated with a person that thieves might want to steal or gain access to?

IDENTITY Theft

8 NUMBERS IDENTITY THIEVES WANT TO STEAL FROM YOU:

- Phone #'s
- Dates & Zips
- PIN Codes
- Social Security #'s
- Bank Account #'s
- Driver's License # & Passport #
- Health Insurance account #'s
- I.P. Addresses



IDENTITY Theft

WHAT OTHER INFORMATION DO IDENTITY THIEVE'S OBTAIN?

Email addresses, full name, online passwords, mother's maiden name, 4 digit code on back of you cc card, PIN's, what city you were born



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 2: Exploiting the Identity

With the information available, the thief may have false ID cards made.

- State driver's license with the thief's picture & victim's name
- State identification card
- Social Security card
- Employer identification card
- Credit cards



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 2: Exploiting the Identity

The thief may simply begin leveraging one piece of information to obtain or establish other information or assets.

These may include

- New credit card accounts
- State or local licenses
- Accounts with utility companies, apartment leases, or even home mortgages



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 3: Discovering the Theft

- The thief continues to build a “persona” using the victim’s name, good credit, and even good character references. The thief never pays the bills, but the victim is left with a bad name and ruined credit.
- Eventually, the victim tries to get a new credit account and is turned down, or gets a bill for a credit card he or she never owned, or starts getting calls from bill collectors.



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 3: Discovering the Theft

- The thief might abandon the victim's identity because he or she has "spoiled" the name of the victim (e.g., with a criminal offense or bankruptcy).
- When the crime or ruined credit is discovered, the victim is left to clean up the mess.
- On average it takes 132 days before Identity Theft is discovered.



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 4: Reporting & Restoring

- The victim reports the theft to the local police & to nation's 3 credit bureaus.
- The victim asks the credit bureaus to note the identity theft crime on his or her credit report.
- The victim may need to consult with a local victims' assistance agency or an attorney to obtain information on the necessary, specific steps in a given state.



IDENTITY Theft

HOW IDENTITY THEFT WORKS

STEP 4: Reporting & Restoring

- The victim can also file an online report and affidavit with the Federal Trade Commission registry at www.ftc.gov. Go to the identity theft section.



IDENTITY Theft

WHAT IS PHISHING?



IDENTITY Theft

WHAT IS PHISHING?

The fraudulent practice of sending electronic communication (emails, social media, etc) purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords, user names, & credit card #'s.



IDENTITY Theft

Your Barclays Bank Account Has Been Blocked(Verification Required)

Inbox x



Barclays Bank PLC <ibankingservice@barclays.co.uk>

to me ▾



Dear Valued Customer,

For your security, Barclays Bank has safeguard your account when there is a possibility that someone other than you is attempting to Access your account from an unidentified location. You now need to verify your **Identity**.

To verify your **identity**, kindly follow the reference below and instantly re-activate your account.

<https://bank.barclays.co.uk/olb/auth/verification/>

Thank you for helping us to protect you.

Security Advisor

Barclays Bank PLC .

Registered in England. Registered no. 1026167. Barclays Insurance Services Company Limited. Registered in England. Registered no. 973765. Registered office for both: 1 Churchill Place, London E14 5HP. 'The Woolwich' and 'Woolwich' are trademarks and trading names of Barclays Bank PLC. Barclays Business is a trading name of Barclays Bank PLC.



IDENTITY Theft



HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

1. Be wary of emails asking for **CONFIDENTIAL INFORMATION**, especially when it comes to finances. When in doubt, contact the merchant directly.
2. Don't get pressured into providing sensitive information. Phishers like to use scare tactics, and often threaten to disable an account or delay services until you update the information they are asking for.



HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

3. Make sure you familiarize yourself with a website's privacy policy. The majority of commercial websites have a privacy policy, usually accessible at the foot of the page. Look at that to see if it is the company's policy on selling their mail list.

***Most of the spam you receive on a daily basis is coming to you because a site you have signed up to has sold your email address to another company.*



HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

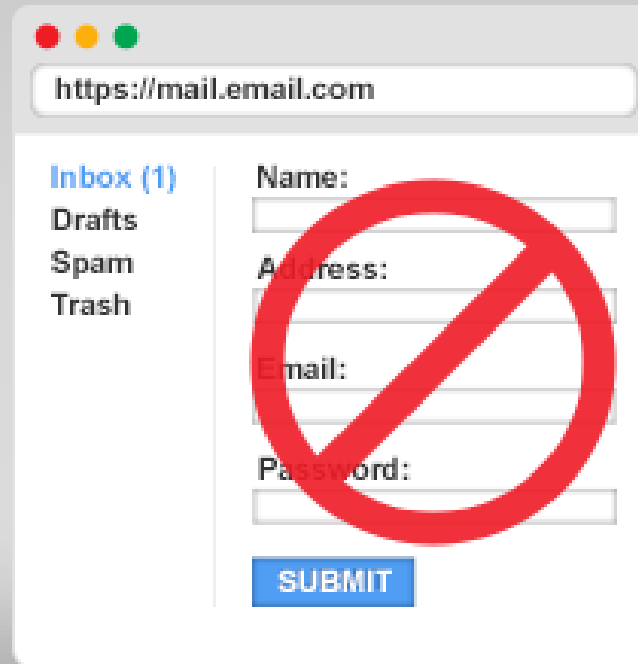
4. Watch out for generic looking requests for information. Fraudulent emails are often not personalized, while authentic emails from your bank often reference an account you have with them. Many phishing emails begin with “Dear Sir/Maam” and some come from a bank with which you do not have an account. Many of the emails also tend to have grammatical errors in them.



IDENTITY Theft

HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

5. Never submit confidential information via FORMS embedded within email messages. Senders are often able to track all information needed.



The image shows a simulated phishing email interface. At the top, there is a browser address bar containing the URL "https://mail.email.com". Below the address bar, there is a navigation menu with the following items: "Inbox (1)", "Drafts", "Spam", and "Trash". To the right of the navigation menu, there is a form with the following fields: "Name:" with an input box, "Address:" with an input box, "Email:" with an input box, and "Password:" with an input box. A large red prohibition sign (a circle with a diagonal slash) is overlaid on the form fields, indicating that submitting information is prohibited. At the bottom of the form, there is a blue "SUBMIT" button.

HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

6. Never use links in an email to connect to a website unless you are absolutely sure they are authentic. Instead, open a new browser window and type the URL directly into the address bar. Often a phishing website will look identical to the original (look at the address bar to make sure this is the case).



IDENTITY Theft

HOW TO PROTECT YOURSELF FROM PHISHING SCAMS?

7. Make sure you maintain effective virus software to combat Phishing.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:

To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.



OK



MoneyPak

Where I can buy MoneyPak?

Walmart * Walgreens



IDENTITY Theft

WHAT IDENTITY THEFT DO WE SEE ON CAMPUS?

1. Skimmers (in person or atm/gas station)
2. Nigerian Scam (When General Motumboo Bumboo emails you because there's a trunk of money waiting from a dead relative)
3. Online selling off electronics to overseas buyers (Overnight a check to you for 3 times amount of item)



SKIMMING / SKIMMERS

- Identity thieves steal your credit card or debit card information by using a device that affixes to a card reader on something like an ATM machine or a gas station pump. It blends in with existing equipment well enough that unsuspecting customers never notice it.
- Can occur almost anywhere.



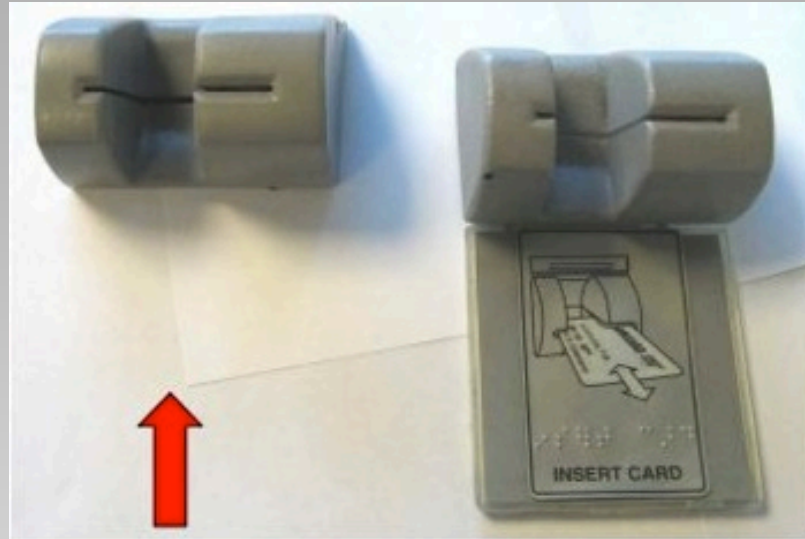
SKIMMING / SKIMMERS

- Restaurant / Retail chain are also big target.
- Waiters hired and given skimming machine.
 - Do you know where your credit card is at all times? Is it always in your site?
 - Many restaurants have gone to table side paying machines (i.e. Chili's)



IDENTITY Theft

SKIMMING / SKIMMERS



The real card reader slot.

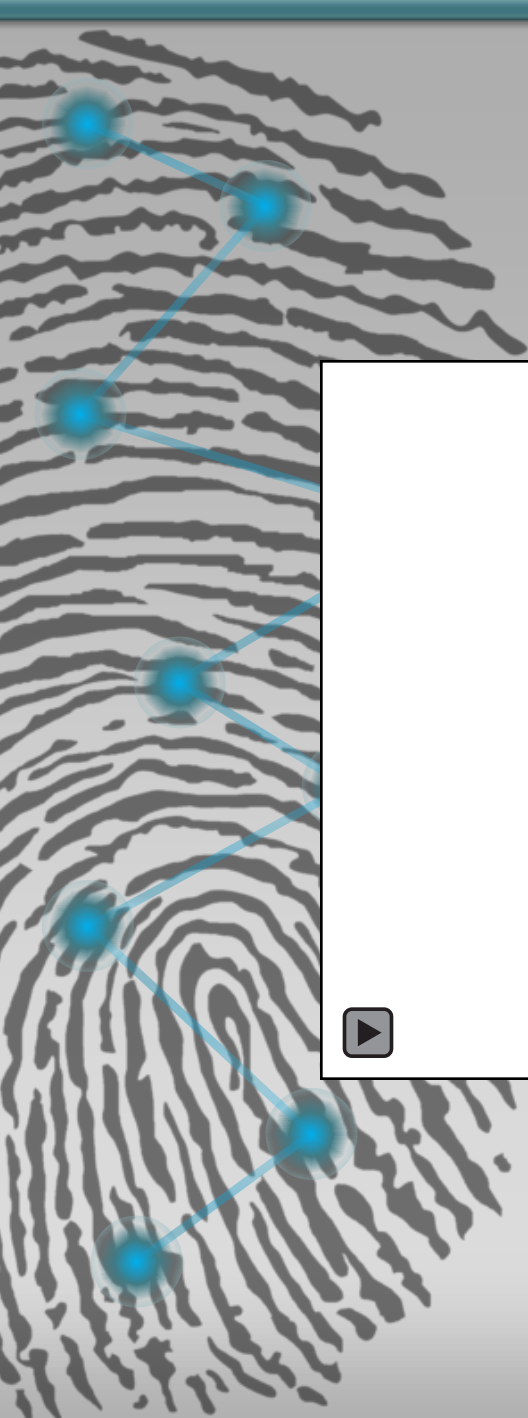
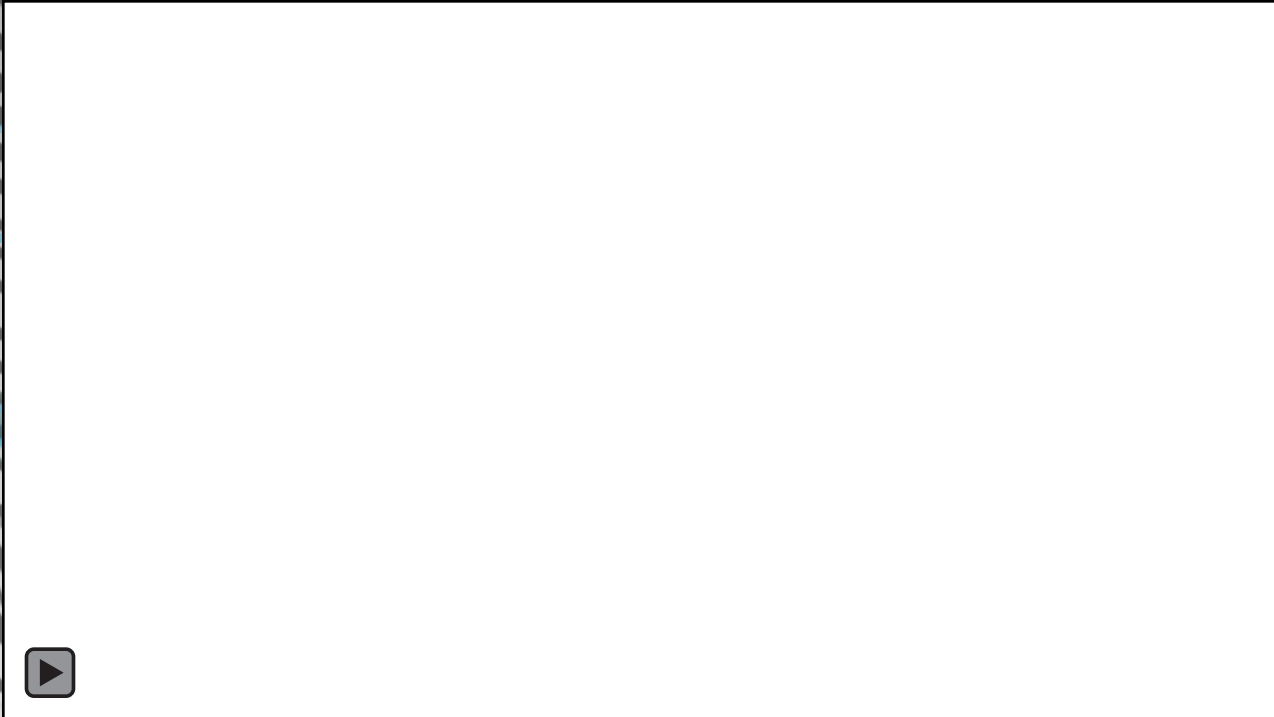
The capture device



The side cut out is not visible when on the ATM.

IDENTITY Theft

SKIMMING / SKIMMERS



IDENTITY Theft

WAYS TO PREVENT SKIMMING

- Look at card reader (give it a tug).
- Some cards can be turned on and off via online app. (i.e. Turn off online purchases, or atm withdrawals).
- Have credit card company set limits to card (i.e. GPS limits to card when outside geographical area, or phone tracking to where purchase is being made).
- Only use cards w/ Chip in it (more secure).



IDENTITY Theft

ARE WRITING CHECKS SAFE?

- Older adults are often hesitant about paying bills online.
- Think safer to write a check.



Parts of a Check

1 Chandler Bing
123 Main 52
Anywhere US 101111

6 DATE 03/11/2018

11 790

12 MON73

2 PAY TO THE ORDER OF Central Perk coffee house \$ 50~

3 Fifty Dollars

4 ABC Savings and Loan
321 Avenue
Anytown US 001111

5 MEMO Coffee w/ Friends

7 Chandler Bing

9 123400056

10 98765432

11 0790

the balance

IDENTITY Theft

ARE WRITING CHECKS SAFE?

- Checks give people access to your money.
- They contain valuable info (name, address, bank name, bank account #, routing #).
- Easy to alter / forge
- Someone can add themselves as a joint account holder



FRAUD AGAINST SENIORS

- Senior citizens are most likely to have a “nest egg,” to own their home, and/or to have excellent credit—all of which make them attractive to con artists.
- Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed.



IDENTITY Theft


FRAUD AGAINST SENIORS

- Victims age 70+ may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.



IDENTITY Theft

TELEMARKETING FRAUD FOR SENIORS



If you are age 60 or older—and especially if you are an older woman living alone—you may be a special target of people who sell bogus products and services by telephone. Telemarketing scams often involve offers of free prizes, low-cost vitamins and health care products, and inexpensive vacations.

If it's too good to be true, it probably is!

HOW HAS I.T. EMERGED?



IDENTITY Theft

WHY IS IDENTITY THEFT ON THE RISE?

- Computers have made record keeping faster. Automation also removes human analysis, making it easier for someone to steal an identity or pose as another person.
- More and more transactions are being handled electronically, a trend that is continuing to increase dramatically.
- More computer hackers now go for monetary returns, not for the thrill of conquering another computer.



IDENTITY Theft

WHY IS IDENTITY THEFT ON THE RISE?

- Mobility means that many of us shop in stores all over our communities, regions, or the country, so we are more anonymous than ever.
- Many find it hard to believe I.T. could happen to us, even though millions are victims each year.



WHAT IS BEING DONE ABOUT I.T.?



WHAT IS BEING DONE?

- Increased reporting, resulting in more criminals being caught.
- Increased consumer education and awareness of fraud tactics.
- Creditors are using fraud prevention tools effectively.
- Constant security upgrades to web browsers / better filters / spyware

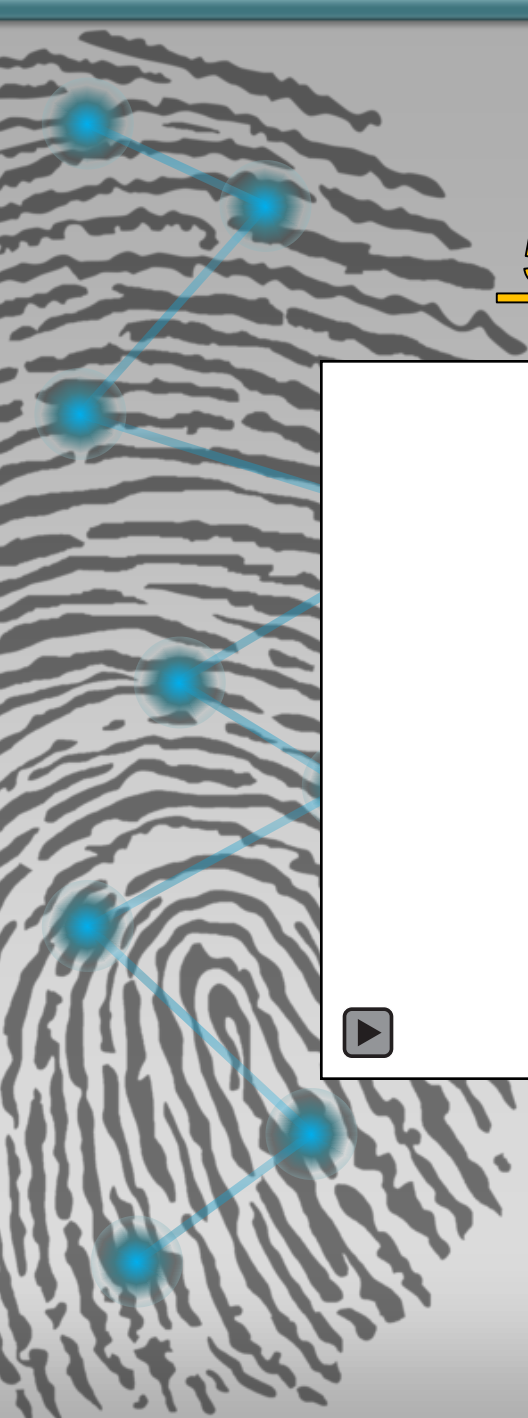


HOW TO PROTECT YOURSELF



IDENTITY Theft

5WAYS TO PROTECT YOURSELF



IDENTITY Theft

KNOW THE WARNING SIGNS

- Mistakes on accounts and/or your “Explanation of Medical benefits”
- Regular bills go missing
- Calls from debt collectors for debts that are not yours
- Notice from the I.R.S.
- Calls or mail about accounts in your minor child’s/grandchild’s name



IDENTITY Theft

REDUCE YOUR RISK

Identity protection means treating your personal information with care.

Make it a habit.

- Like buckling your seatbelt or
- Locking the doors at night



IDENTITY Theft

REDUCE YOUR RISK

- Secure your Social Security number .
- Don't carry your SS card in wallet.
- Only give out number when necessary.



IDENTITY Theft

REDUCE YOUR RISK



IDENTITY Theft

TRUE or FALSE

1 in 4 people have MAJOR errors on their credit report?



IDENTITY Theft

TRUE or FALSE

1 in 4 people have MAJOR errors on their credit report?

- **TRUE** -

A 2013 study by the Federal Trade Commission found that 25% of consumers had errors on at least one of their credit reports



IDENTITY Theft

REDUCE YOUR RISK

- Under Federal Law, right to free copy of credit report every 12 mo's from all 3 reporting agencies (Experian, Equifax, Transunion)
- To order:
 - www.annualcreditreport.com
 - 1(877) 322-8228 (FACTACT)
- Get Experian Credit Report free every 30 days



IDENTITY Theft

REDUCE YOUR RISK

- Use free sites like CREDIT KARMA (Get a full credit report from TransUnion once a week)
- Other FREE credit checking sites:
 - Credit Sesame,
 - Credit.com
- 96% of free credit reports go unclaimed each year. Most people check only when they are applying for something



IDENTITY Theft

REDUCE YOUR RISK

- Only purchase online from TRUSTED companies websites.
- Avoid buying on overseas websites



REDUCE YOUR RISK

- Best credit monitoring companies:
 1. Identity Force (monitor all 3 CC bureaus, New credit reports, bank/CC cards, 24/7 help, 2 factor authentication) *(\$19.95 / month)*
 2. LifeLock *(\$26.99 / month – Ultimate Plus)*
 3. Identity Guard *(\$22.99 / month - Premier)*
 4. ID Shield
 5. Experian
 6. Equifax

IDENTITY Theft

REDUCE YOUR RISK

Be alert to online impersonators

- Do you know who is getting your personal information?
- Be alert for bills that don't arrive when you expect them.
- Follow up if you get account statements you don't expect.



REDUCE YOUR RISK

Protect your computer.

- Use anti-virus software, anti-spyware software, and a firewall.
- Create strong passwords.
- Keep your computer's operating system, browser, and security up to date.

- (cont) -



REDUCE YOUR RISK

Protect your computer.

- Lock your laptop
- Read privacy policies
- Don't use obvious passwords
(birthdates, addresses, 12345, etc.)
- Passwords of 8 characters can now be
“cracked” in less than 2 ½ hrs (use at
least 9 digits/characters)



IDENTITY Theft

WHAT DO YOU DO IF SOMEONE HAS STOLEN YOUR IDENTITY?

- Act fast to limit the damage.
- Take steps immediately.



IF YOUR IDENTITY IS STOLEN...

Step 1: Place an initial fraud alert on your credit report.

- Contact any one of the three nationwide credit reporting companies:
 - ***Equifax*** 1(800) 525-6285
 - ***Experian*** 1(888) 397-3742
 - ***TransUnion*** 1(800) 680-7289



IDENTITY Theft

IF YOUR IDENTITY IS STOLEN...

Step 2: Order your credit reports.

- Contact each of the three credit reporting agencies.
- ID theft victims get a copy of their reports for free.
- Read your reports carefully and correct any errors.



IDENTITY Theft

IF YOUR IDENTITY IS STOLEN...

Step 3: Create an Identity Theft report.

- Gives you rights that help you to recover more quickly.
- File a complaint with
 - Ftc.gov/complaint or 1-877-438-4338
 - This will become your FTC affidavit
- File a police report.



IDENTITY Theft

IF YOUR IDENTITY IS STOLEN...

Step 3: Create an Identity Theft report.

- Gives you rights that help you to recover more quickly.
- File a complaint with
 - Ftc.gov/complaint or 1-877-438-4338
 - This will become your FTC affidavit
- File a police report.



IDENTITY Theft



**IDENTITY
THEFT
AFFIDAVIT**



+
**POLICE
REPORT**



=
**IDENTITY
THEFT
REPORT**

Questions? More Information?

Tom Perez

Police Officer

tperez@menifeepolice.org



Office Phone:

951-746-7149

