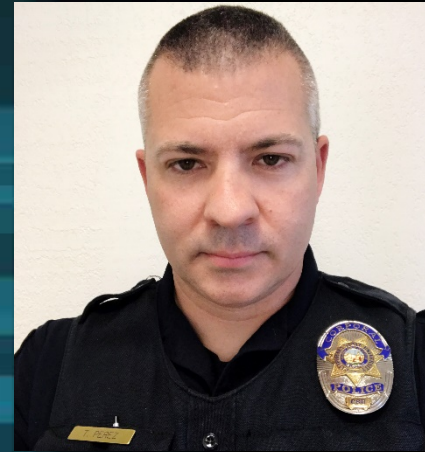


# IDENTITY THEFT





TOM PEREZ



# IDENTITY Theft

Presented by Corporal Tom Perez – CSUF P.D.



# IDENTITY Theft

## ABOUT ME

- Corporal with CSUF P.D.
- Police Officer 6 ½ years
- Community Services & Crime Prevention Unit
- Hi-tech Crime Certificate from CSULB



# IDENTITY Theft

**Every 2.5 seconds,  
someone in the U.S. is  
a victim of Identity  
Theft.**



\* According to California DOJ

# IDENTITY Theft

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





# IDENTITY Theft

TRUE of FALSE?

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



# IDENTITY Theft

## TRUE of FALSE?

**Seniors are the most targeted group for Identity Theft?**

**- FALSE -**

**Students age 18-25 (31%)**

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



# IDENTITY Theft

TRUE of FALSE?

**Identity Theft is easily  
resolved?**





# IDENTITY Theft

TRUE of FALSE?

Identity Theft is easily  
resolved?

- **FALSE** -

It takes an average of 6 months  
and 200+ hrs to recover from  
each I.T. incident



# IDENTITY Theft

TRUE of FALSE?

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



# IDENTITY Theft

## TRUE of 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 of FALSE?

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



# IDENTITY Theft

## TRUE of FALSE?

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

**- TRUE -**

**2008 survey, showed women more concerned on every I.T. question, & 4 out of 10 were very concerned.**





# IDENTITY Theft

## MY EXPERIENCE w/ I.T.

1. AOL
2. Landmark Steakhouse phone call
3. Recent U.S. Bank phone call
4. Arby's
5. Community Mailbox (331 Ave. 11)



# 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 2012

1. Target
2. Anthem Blue Cross
3. Chick-fil-A
4. Sony pictures (employees only)
5. United States Postal Service
6. Staples
7. Kmart
8. Home Depot
9. Yahoo



# 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.



# 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.



# 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.

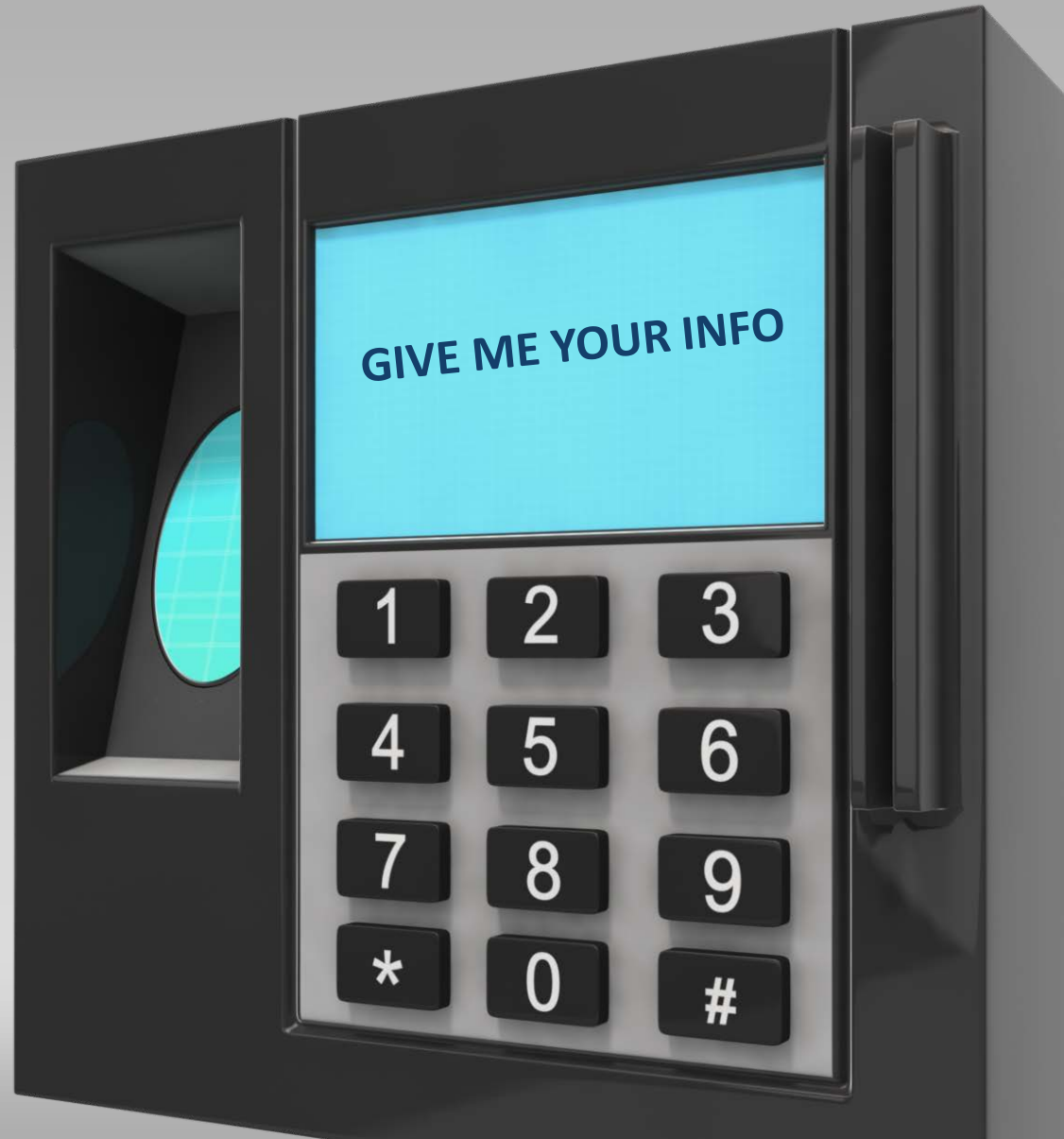


# IDENTITY THEFT

## 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.

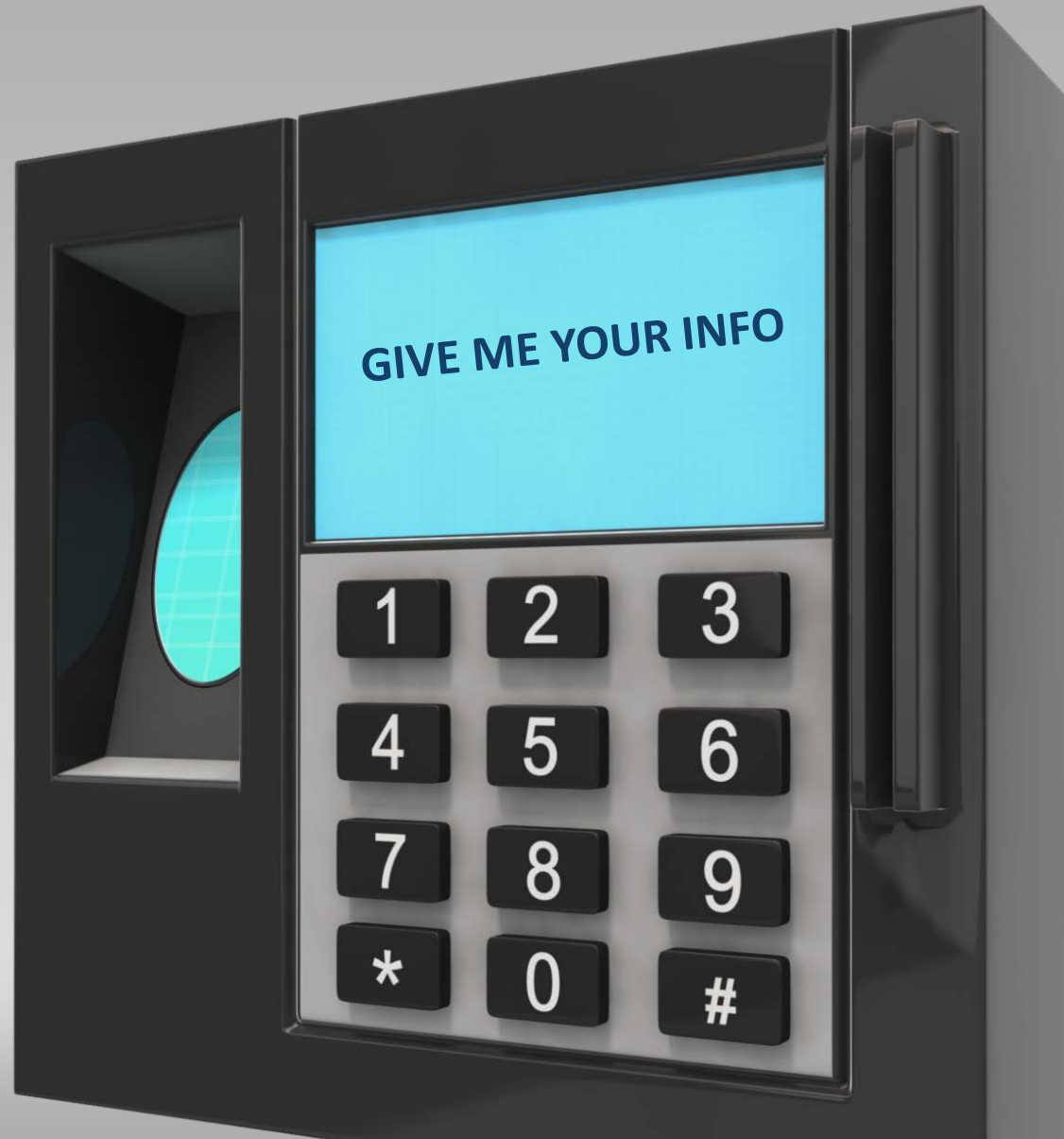
In the past 6 years,  
identity thieves have  
stolen over \$107 billion.



# 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

## TOP 5 STATES FOR I.T. CASES

1. District of Columbia
2. **CALIFORNIA**
3. Florida
4. Massachusetts
5. Nevada



# 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

## 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](http://www.ftc.gov). Go to the identity theft section.





# IDENTITY Theft

## WHAT IS PHISHING?

A computer window titled "Trusted Source" is shown, featuring a large red headline: **\*Information Update Required\***. A fishing hook is positioned as if catching the window. The form is divided into three tabs: "Personal Information", "Credit Card Information", and "Bank Account Information". The "Personal Information" tab is active and contains the following fields:

- Username:
- Old Password:
- New Password:
- Title:
- First Name:
- Last Name:
- Gender: Male  Female
- Birthday:
- Social Security Number:
- Company:
- Address 1:
- Address 3:
- City / Town:
- County:
- State / Province:
- ZIP / Postal Code:
- Country:

At the bottom right of the window are "OK" and "Cancel" buttons.

# 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.*

## 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.

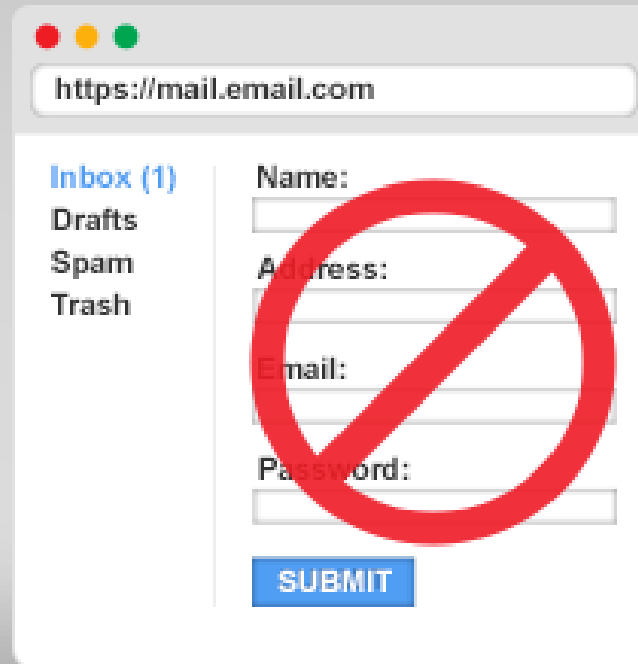




# IDENTITY Theft

## 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.



A simulated phishing email interface. The address bar shows "https://mail.email.com". On the left, there is a navigation menu with "Inbox (1)", "Drafts", "Spam", and "Trash". On the right, there are form fields for "Name:", "Address:", "Email:", and "Password:". A large red prohibition sign (a circle with a diagonal slash) is overlaid over the form fields, indicating that submitting information is prohibited. Below the form fields 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](mailto:fine@fbi.gov).



OK



MoneyPak

Where I can buy MoneyPak?



# 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 of electronics to overseas buyers





## 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

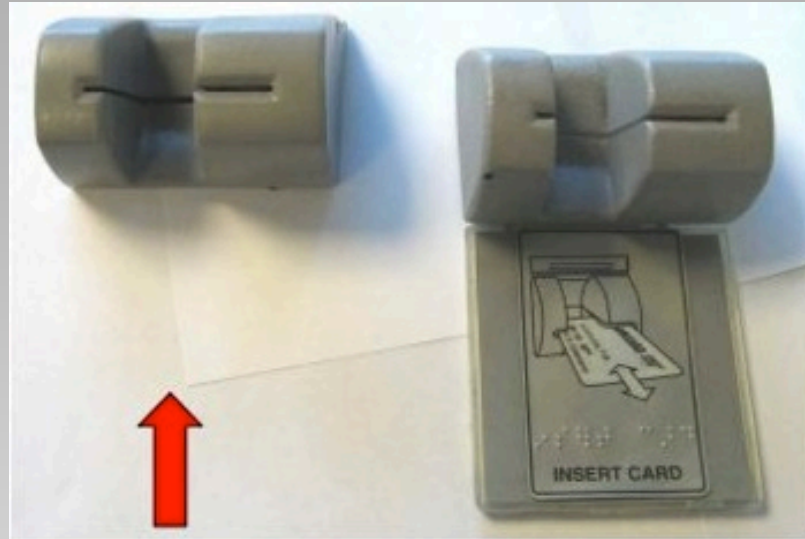
- Restaurant / Retail chain are also big target.
- Waiters hired and given skimming machine.
  - Do you know where your credit card is at all times? Is it always in your sight?
  - Many restaurants have gone to table side paying machines (i.e. Chili's)





# 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

## 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).



## 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.



## FRAUD AGAINST SENIORS


- Elderly victims 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

## 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

- Right to free credit report every 12 mo's
- To order:
  - [www.annualcreditreport.com](http://www.annualcreditreport.com)
  - 1(877) 322-8228
- Use free sites like CREDIT KARMA
- Only purchase online from TRUSTED companies websites.
- Avoid buying on overseas websites



# 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) -



# IDENTITY Theft

## REDUCE YOUR RISK

**Protect your computer.**

- Look your laptop
- Read privacy policies



# 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



## 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](http://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](http://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?

**Corporal Tom Perez**

**Community Services /**

**Crime Prevention**

**thperez@Fullerton.edu**



**Office Phone:**

**657-278-3423**

**University Police Department:**

**657-278-2515**

**Website:**

**<http://police.fullerton.edu>**

