







### **Protecting Yourself, Yourself**





APCUG Security
Virtual Technology Conference
October 17. 2015

Judy Taylour, Chair APCUG Board of Advisors Jtaylour (at) apcug.org



# The problem is.... they are out to get you

Identity theft is a crime of stealing key pieces of someone's identifying information

### Why?

It beats working and with the internet they don't have to get dressed

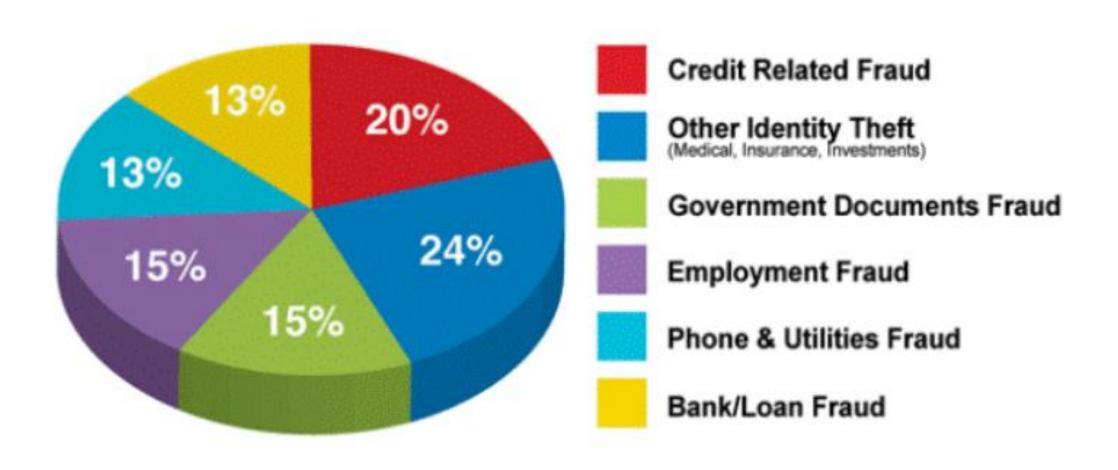
### FTC Top Consumer Complaints - 2015

- ▶ 15<sup>th</sup> year ID theft complaints topped list
- Nearly 25% of ID theft complaints related to tax or wagerelated fraud
- ▶ 50+ = 30% of ID theft / single largest demographic of ID theft victims
- Company data breaches more frequent
- Phishing e-mails = all-time high
- Military consumers
  - ID theft was #1 complaint category

# FTC - Top 10 ID Theft States 2014



### FTC – Types of ID Theft



### Time to Fix

- ▶ Average estimate 40 hours
  - Over 5% reported 1,200 hours
- ▶ 56% did not discover new account fraud until after 1<sup>st</sup> month
- > 24% took more than 6 months
- ▶ Nearly 1/3 unable to repair compromised identities

# What do they need to steal your ID?

- Name
- Address
- Birth date
- Social Security Number
- Drivers' License Number
- Mother's maiden name

They now have every thing they need!

#### **Stolen Wallet**

- Have access to information they need to steal your ID
- Low-tech but still a major source of identity theft





#### Mail theft

- Steal from unlocked mailboxes at your front door
- Postal trucks
- Locked community mailboxes
- Mail theft is a felony



### **Change of address**

- Collect addresses through phone book (real phone book or online white pages, etc.)
- ▶ Complete change of address form online or at Post Office
- Reroutes all your mail
- ▶ 2010 #1 way thieves took over existing accounts

### **Shoulder Surfing**

- Protect your pin numbers by shielding them at check stands
- Be aware of who is around you when giving personal information over the phone
- Smartphones can snap pictures of your credit cards, credit applications, or record conversations



#### **Card Skimmers**

- Now inside gas station pumps
- Make sure pump door is securely closed
- Sometimes tape across pump door
- Pay inside
- Pay by credit card
- Using debit card? Run it as a credit card



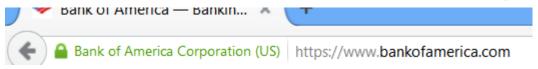
### **Prevent ATM Scam**

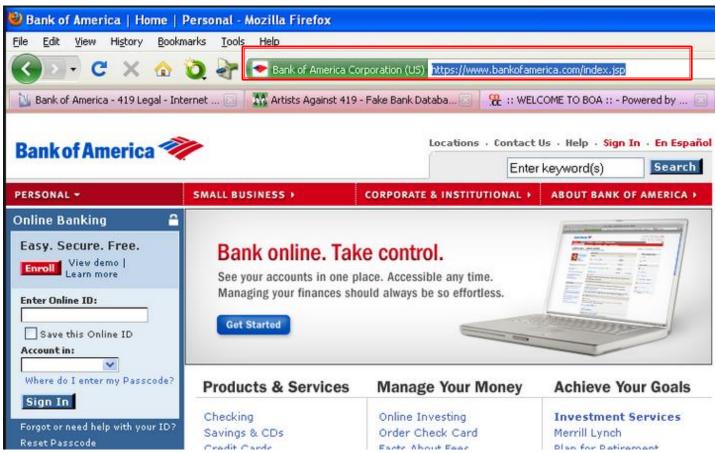
- Cover your PIN number
- Don't leave ATM machine too early
- Use ATM machines inside banks
- ▶ LAPD suggests using ATM inside a police station
- Monitor your account activity



### **Phishing**

- ▶ E-mail attempts from....
- Banks
- UPS / Fed Ex / Post Office delivery
- Social websites
- Directed to fake website that closely resemble legitimate website





# Red flags of phishing

### **Do Not Hurry**

- Your friend in Nigeria
- ▶ The email is full of promises to reward you
- You won the lottery in Ireland
- Your friend has lost his/her passport, the embassy is closed and needs money NOW to get home

# Red flags of phishing

- E-mails that direct you to a Website to "validate" or "update" info
- ▶ E-mails warning your accounts will be closed
- Banks never ask for account info, especially in an e-mail
- References to latest disaster, income tax refund / need to pay or go to jail
- Want your opinion

# Red flags of phishing

- Words Like "Urgent" and "Important"
- Grammatical errors and typos
- Don't click on any links in suspicious e-mails
- Report suspicious e-mails to companies
- ▶ S-P-A-M / D-E-L-E-T-E

### Vishing via the phone

- Automated message = nothing wrong with your credit card, bank account but.... (our friend Rachel)
- Need to verify information
- Your cousin / nephew / grandson is in (wherever) and needs money NOW
- Something wrong with your computer
- You're going to jail unless you respond

### **Online Shopping**

- Shop at duplicated websites
- Goal to get you to believe you are on the real site
- Thieves can capture all of your information when you check out
- ▶ Hover over URL (website address) to see the complete address

### **Online Shopping**

- Check spelling / grammar, etc.
- Is there a brick & mortar address
- Is there a phone number
- Give them a call before placing an order

- Steal business or personnel records at your workplace / MD's office
- Find personal info in your home
- Use info you put on the Internet
- Buy personal info from "inside sources"



#### **Online Presence**

- ▶ I Googled my name and got about 10K hits -- everything except that I like Diet Pepsi with lemon
- With your birthday and where you were born they can get your birth certificate

About 10,100 results (0.37 seconds)

# How do I protect myself?

### **A Little Paranoia Helps**

- Give out as little information as possible
- Ask why they need the information
- Don't be in a hurry...slow is better
- Check them out
  - i.e. Better Business Bureau



# How do I protect myself?

#### **Social Media**

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn

- Customize privacy options
- Only friend people you know
- Phishing is the same as with e-mail
- Don't put any information in social media accounts that you won't put on your front door – Abby Stokes
- Same goes for e-mail, etc.

Stay Safe Online Tips http://bit.ly/1xkcH7a

- Make sure program extensions are turned on
- Update all programs
- Run security program scan at least weekly
- Deep scan monthly
- Additional malware program Malwarebytes
- Strong passwords
  - Different password for each account
  - 10 characters (lower case / upper case letters, at least 1 number and a symbol)

- Different password for each account
- 10 characters (lower case / upper case letters, at least 1 number and a symbol)
- No words or numbers or alpha characters in order
- Check out password strength at Microsoft's password check website: bit.ly/1NM1lhe

Password:

Strength:

Not rated

Type a password into the box.

- Use a passphrase
- Infamous Edward Snowdon recommends using passphrases to be more secure
- John Oliver interviews Snowden re passphrases http://bit.ly/1GPve2D

- SCvccmts2ndWdnsdayofmnth!
- Steve Gibson's Password Checker
- www.grc.com/haystack.htm

# How Big is Your Haystack?

... and how well hidden is YOUR needle?

▶ Every password you use can be thought of as a needle hiding in a haystack. After all searches of common passwords and dictionaries have failed, an attacker must resort to a "brute force" search—ultimately trying every possible combination of letters, numbers and then symbols until the combination you chose, is discovered.



Enter and edit your test passwords in the field above while viewing the analysis below.

#### Brute Force Search Space Analysis:

26+26+10+33 = <b>95</b>	Search Space Depth (Alphabet):
25 characters	Search Space Length (Characters):
28,034,052,602,738, 549,436,590,497,089,977, 609,984,418,179,126,495	Exact Search Space Size (Count):  (count of all possible passwords with this alphabet size and up to this password's length)

#### Time Required to Exhaustively Search this Password's Space:

8.91 trillion trillion trillion centuries	Online Attack Scenario: (Assuming one thousand guesses per second)
	Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)
89.14 trillion trillion centuries	Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Use a password manager





- Do you have a home network?
- Does your router have a strong password?
- Do you make sure all of the machines connected to the network are free of malware?
- Make sure security programs are up-to-date on all machines
- Malwarebytes on all machines

NEVER click on unsolicited pop-up ads



#### YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit. Sirefef. Spy and Trojan. Fake AV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

High Priority Virus Removal Call Line)

Your IP Address: 216.37.72.238 | Generated on 03-11-2014 | Priority: Urgent

- Avoid putting your e-mail address on public Web pages (can be harvested by spammers)
- Name (at) blah.org or change address into a graphic
- Don't unsubscribe to unwanted e-mails
  - Verified address brings more \$\$ to spammers
- Have an alternate to your family/friends address
- Don't use "good" e-mail address when registering software / subscribing to anything

- Don't "Click Here" in an e-mail...
- ▶ Hovering over "Click Here" shows the URL's destination probably not your bank, irs.gov, etc.
- Set up an account at irs.gov before fraudsters do and steal your info & tax data
- Never forward chain letters & virus warnings
- **Bcc:**

## How ID thieves use your information

- Open new credit card accounts
- Establish phone or wireless service in your name
- Open new bank accounts and write bad checks
- File for bankruptcy under your name
- Counterfeit checks or debit cards

## How ID thieves use your information

- Buy and take out car loans in your name
- Seek medical treatment in your name
- Don't pay the bills
- In other words, trash your identity and your credit



- More than 2.3M adult Americans or close family members became victims during or before 2014
- Extremely difficult to untangle fraudulent bills and ruined medical records
- Office visits / ER / Prescriptions
- Scarey....

- May go unnoticed for months even years
- Rarely informed about medical ID theft by healthcare provider
- Because of privacy laws protecting release of health information, fixing problem is difficult
- Very difficult to prove you're not the one who received TX

Average cost to victim \$13,500

- Monitor "Explanation of Benefits" sent by health insurer
- Request copies of medical files from health care provider
- If you are a victim FILE A POLICE REPORT
- Correct erroneous and false information
- · Keep an eye on your credit report
- Request and accounting of disclosures



## Reducing the risk of ID theft

- Treat your trash and mail carefully
- Destroy credit card applications, receipts, bank, and billing statements SHRED/SHRED/SHRED





## Reducing the risk of ID theft

- Opt out prescreened credit offers: 1-800-567-8688
- Put passwords on credit card, bank, and phone accounts
- Use two-factor authentication



## Reducing the risk of ID theft

- Opening a new account?
  - Password vs. mother's maiden name
- Avoid giving your SSN unless it's absolutely necessary use other identifiers
- Carry as little identification information as possible
- Limit the number of credit cards you carry

## More ways to reduce ID theft

- Don't give personal identification on the phone unless you initiate the call
- Be cautious with personal info in your home
- Check on who has access to your personal info at work

# Still more ways to reduce ID theft

- Never carry your Social Security card
- Save ATM and credit card receipts to check against statements
- Be informed about your financial institutions' policies of sharing information
- Make sure your credit reports are accurate

## How do you find out they did it

### Credit report

 Guard the report -- it has all the information needed to clean you out before you can find out

### Free Reports

Monitor and review your credit report every 4 months



### How do you find out they did it

- Free annual credit reports www.annualcreditreport.com
- Go to one of three companies at a time
- Get 3 reports per year free

### Your ID has been stolen

### Now what do you do?

- Initial fraud alert call the toll free fraud numbers of each of the three credit report companies
  - Equifax: 1-800-525-6285
  - Experian: 1-888-397-3742
  - TransUnion: 1-800-680-7289

### Your ID has been stolen

- Write everything down so your reports are consistent
- Contact creditors or financial institutions for any accounts that have been tampered with
- File a report with your local police and police where the theft took place

## **Security Freeze**

- Usually FREE for those over 65 or ID theft victims
- Businesses can't see your credit report
  - Won't approve new account
- Other consumers charged \$10+ / credit reporting company
  - X 3 companies



### **Fraud Alerts**

- Always free
- Less secure than a freeze
- Potential creditors must contact you
- May not prevent the misuse of existing accounts

## Safeguards

### **Lock your accounts**

- ▶ For \$10.00 each lock your accounts:
  - No new loans
  - No credit cards can be opened and no change of address made until you unlock them

### AAA

#### Free ID Theft Protection benefit

- ProtectMyID® Essential, a \$79 value
- ▶ FREE to members
- Monitors your Experian Credit Report
- ▶ E-mail alerts
- Fraud Resolution Support
- Lost Wallet Assistance





ProtectMyID®, Exclusively for AAA Members



Our Product About ID Theft FAQ

Member Log In

#### Dear Judy Taylour,

Customer Number: 1

All month long, ProtectMyID has been working behind the scenes to monitor for possible identity theft. You are receiving this email because we have not detected any Credit Alerts in the last calendar month.

#### Rest easy knowing that our powerful tools are:

- . Checking for address changes involving your name.
- . Monitoring new accounts, collections, and public records as well as checking 50 other leading indicators of identity theft on your credit reports.
- . More protection, plus your Experian credit score Upgrade now!
- . Prepared to help you if identity theft is detected. Our team of dedicated U.S.-based Identity Theft Resolution Agents are here to assist you in resolving identity theft incidents.

Always Stay Vigilant

### **IRS Account**

### Sign up for an IRS account before the crooks do it for you

http://1.usa.gov/1F163W7

https://sa.www4.irs.gov/eauth/pub/login.jsp



#### First Time Users

Create a Login to:

- Verify your identity for access to your personal tax information.
- Create a user ID and password to save time on future visits.
- Lock or Disable access to your online account.

Information you need to verify your identity



### **SSA Account**

### my Social Security - Sign In Or Create An Account

http://www.ssa.gov/myaccount/

- Keep track of your earnings and verify them every year;
- Get an estimate of your future benefits if you are still working;
- · Get a letter with proof of your benefits if you currently receive them; and
- Manage your benefits:
  - Change your address;
  - Start or change your direct deposit;
  - Get a replacement Medicare card; and
  - Get a replacement SSA-1099 or SSA-1042S for tax season.

- We really don't like to talk about this but....
- The year after somebody passes is one of the most vulnerable times for identity theft.
- It's a really terrible crime but, because death is public record, criminals comb through recently deceased records and create a fake identity.
- The deceased don't check email so they don't get the mail.

I, personally, don't want a thief to become me and rack up a lot of charges, open new accounts, etc. and trash my identity





























- E-mail accounts
- Website domain names
- Online banking accounts
- Automatic bill pay
- Credit Cards
- Cell phone
- Cloud storage
- Photo storage

- Facebook
- Twitter
- LinkedIn
- Frequent Flyer
- Loyalty programs
- Computer(s)
- External hard drive(s)
- Flash Drives
- And on and on

- Designate a 'digital executor' in your will, living trust, etc.
- Password program?
- Password list on an encrypted flash drive?
- Although we are told not to give our master password to anyone, you can give your master password to your Digital Asset Executor, put it in a lock box, etc. for when it is needed.
- http://www.safehousesoftware.com/



Of course, we need to remember to keep our account numbers
 & passwords up-to-date wherever we are saving them

### **Credit Bureaus**

- Equifax: 1-800-525-6285 (Atlanta, GA)
  - www.equifax.com
- Experian: 1-888-397-3742 (Costa Mesa, CA)
  - www.experian.com
- TransUnion: 1-800-680-7289 (Chicago, IL)
  - www.transunion.com

Good educational information

http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html ---

http://bit.ly/uESBk

What to do if it happens to you

http://www.privacyrights.org/fs/fs17a.htm

http://bit.ly/598iuB

- www.ftc.gov/complaint
- www.ftc.gov/idtheft
- Where to go to learn what to do if your identity is stolen
  - http://www.onguardonline.gov/

### http://www.consumer.ftc.gov/

- File a consumer complaint
- Register for Do Not Call
- Report Identity Theft
- Get Your Free Credit Report
- Order Free Resources
- ▶ IRS ID Theft Hot Line 800-908-4490

- Free encryption program
  - http://www.safehousesoftware.com/
- John Oliver Snowdon interview
  - http://bit.ly/1GPve2D
- ▶ IRS Account Brian Krebs Article
  - http://bit.ly/1G8iFiv
  - Set up Account http://1.usa.gov/1LsnJOB
- http://www.safehousesoftware.com/

- http://www.safehousesoftware.com/
- Social Security myAccount
  - http://www.ssa.gov/myaccount/
- Steve Gibson's Password Checker
  - www.grc.com/haystack.htm

### Take an ID Theft Test

https://www.privacyrights.org/itrc-quiz1.htm http://bitly.com/AqeBnX

## Questions???

Judy Taylour
APCUG Chair
Board of Advisors
Jtaylour (at) apcug.org



