Identity Theft & Prevention: The inside story

A public service by:

San Mateo County District Attorney's Office

Vishal Jangla, Deputy District Attorney
vjangla@smcgov.org 650-363-4784

There's a victim of identity theft every 2 seconds

CNN Money, Feb 6 2014

What does "identity" mean?

Any personal identifying information (PII) that could be used to commit fraud or inflict harm

Name, address, date of birth, phone number, insurance number, tax id, social security, driver's license number, employee id number, place of employment, mother's maiden name, banking information, PIN, usernames, passwords, passport number, fingerprint, facial scan identifiers, voiceprint, retina/iris image, credit card information…

Overview

- How identity theft happens
- The journey of PII
- Protect yourself

How it happens

Theft:

Mailbox &
Dumpster divers

Stolen wallets,
purses &
briefcases

ATM skimmers

Credit cards skimmers

Using public WiFi to access unsecured internet services

Rogue employee at an insurance/medical/tax/mortgage service provider.

Hacking

Breaking into the computer systems of a retailer/service provider/employer/government

Social Engineering

The use of deception to manipulate individuals into divulging PII

Social Engineering

- *Phishing emails*
- *"Enter to win" forms*
- *Pretend to be owner/CEO*
- *Spoofed calls/email*

Trojan horse

- *Someone you know preys on you*
- *Knows majority of your PII*
- *Able to re-set security Qs*

Compromised Email Accounts

Harvesting PII from hacked email accounts

What's at risk?

- *Financial accounts:*
  - *Unauthorized transactions*
  - *Unauthorized accounts/loans*
- *Credit rating*
- *Taxes*
- *Loyalty program accounts*
- *Stored value accounts*
- *Gift cards*
- *Internet services (Netflix, Amazon, Google)*

The Journey of PII

Low-level criminals

Obtain & use PII to:

- *Open new accounts (all forms of credit)*
- *Use your credit card info*
- *File taxes*
- *Sell your information*

Aggregators/resellers

Acquire information from others to:

- *Manufacture IDs & credit cards*
- *Perform larger scale fraud*

Organized crime

- *Sophisticated criminals*
- *Conduct large scale hacks and compromises*
- *Sell information on Darknet for use by aggregators/resellers*

Your identity used against you

Compromised username/passwords from one site and used against popular sites across the Internet

(Credentials from Netflix used on Amazon, Bank of America, Virgin Atlantic, etc.)

Consolidation of PII – a complete person?

- *Name and credit card # from skimmer*
- *Address from a billing statement*
- *Email & date of birth from a hacked website*
- *Social Security from hacked employer*
- *Security Qs from Yahoo*

Protect yourself

Disclaimer:

Commercial products in this presentation are not endorsed by the County of San Mateo or the District Attorney's Office.

On the front end

- *Physical mail:*
  - *Opt for electronic communications/statements*
  - *Don't use road-side mailboxes*
  - *Video surveillance (real or fake) to deter*
  - *Shred sensitive PII*
    - *Opt-out of pre-screened offers: http://www.optoutprescreen.com*

- *Connecting to the Internet:*
  - *Use a firewall and anti-virus software*
    - *ISPs now give them away for free. Comcast does. Check your ISP.*
  - *Use a web browser with the least security concerns*
    - *Firefox or Chrome are good options*
  - *Do not download files from websites you don't know or trust*

- *Online:*
  - *<u>NEVER</u> use simple passwords*
    - *Have upper case, lower case, numbers, and special characters (!, @, %, $)*
  - *Avoid re-using passwords across websites*
    - *Use an app to help you track your username/passwords*

<u>mSecure – secure PII storage</u>

- *Go to www.msecure.com or search for msecure in the App Store*

- *Email:*
  - *NEVER open attachments from a stranger*
  - *BE WARY of opening attachments you aren't expecting from people you know.*
  - *When clicking on links, look at the address that shows up in the address bar. Does it look right?*
    - *Is it www.bank0famerica.com?*

- *2-factor authentication:*
  - What is it?
    - Also called "2-step" verification
    - First factor: username/password combination
    - Second factor:
      - Code texted to the email/cell phone on the account
      - Authenticator apps (Google authenticator)

- Advantages?
  - Even if your username/password compromised, intruder cannot access your account
  - You get notified of access from an unusual location
  - Lets you know your credentials are compromised
- Disadvantage?
  - You need access to your phone/email
- Who offers it?
  - Many well-known internet companies, banks and others
  - Loyal programs (hotels/airlines) noticeably absent

  Does your service provider have "2-factor" authentication?
  Visit http://*www.twofactorauth.org*

- *Online:*
  - Avoid using debit cards online. Use a credit card
    - FTC limits loss on credit cards to $50
    - Debit cards have less protection
  - Do not provide your bank account and routing number unless you absolutely

trust a company

- Exceptions: banking institutions and payment services

Even if you do everything to prevent loss of PII, you can't control compromises of banks, utility companies, government agencies, employers, retailers, professional service providers, mortgage lenders, and others.

On the back end

- *Monitor your finances*
  - *Set up alerts with your banks*
  - *Regularly log into your accounts for a checkup*
  - *Check your statements*
- *Get a complete picture with great tools:*

  www.mint.com
  Apps for iPhone & Android
  *(search for **mint** in the app store)*
  Free!

- *Monitor your credit reports*
  - *Three credit reporting bureaus – Experian, Equifax, TransUnion*
  - *New inquiries, accounts, debts or use of existing accounts reported*
- *Once a year:*
  - *Free credit reports from all 3 agencies*
  - *Go to http://www.annualcreditreport.com*

- *On-going monitoring*
  - ***Credit Karma***
    - *TransUnion & Equifax*
    - *Instant alerts*
    - *Weekly updates to credit scores & reports*
    - *iPhone & Android apps*
    - *Free!*
    - *Go to http://www.creditkarma.com*
  - ***Experian app***
    - *Instant alerts for inquiries or new accounts*
    - *Monthly updates to reports only*
    - *iPhone & Android apps*
    - *Free!*
    - *Not on their website – need to download the app. Search for* ***Experian*** *in the app store*

Victim?

- *Place a **freeze** on your credit reports*
  - *Restricts access to reports*
  - *Only prevents new inquiries or accounts*
  - *Does not prevent continued use of your compromised financial information*
  - *Does not affect your credit score*
  - *You'll need to lift the freeze temporarily if you need a credit check*
  - *Nominal charges*

Don't want a freeze?

- *Place a **fraud alert** on your credit files*
- *Puts creditors on notice of potential fraud*
- *You may require a verification call*
  - *Initial Fraud Alert – lost wallet, but not victim yet - lasts 90 days*
  - *Extended Fraud Alert – victim – lasts 7 years*
  - *Active Duty Military Alert – lasts 1 year*
- *Free*

Freeze & Fraud Alerts

Additional info:
Go to
http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
Or
Google ***FTC credit freeze***

Monitor your points and miles

- *On-going tracking & monitoring*
- *AwardWallet*
- *Online at https://www.awardwallet.com*
- *iPhone & Android apps (search **awardwallet** in the app store)*
- *Basic monitoring free*
- *Upgraded tracking for a yearly fee*