Identity Theft

Wiam Younes
Training and Awareness Coordinator

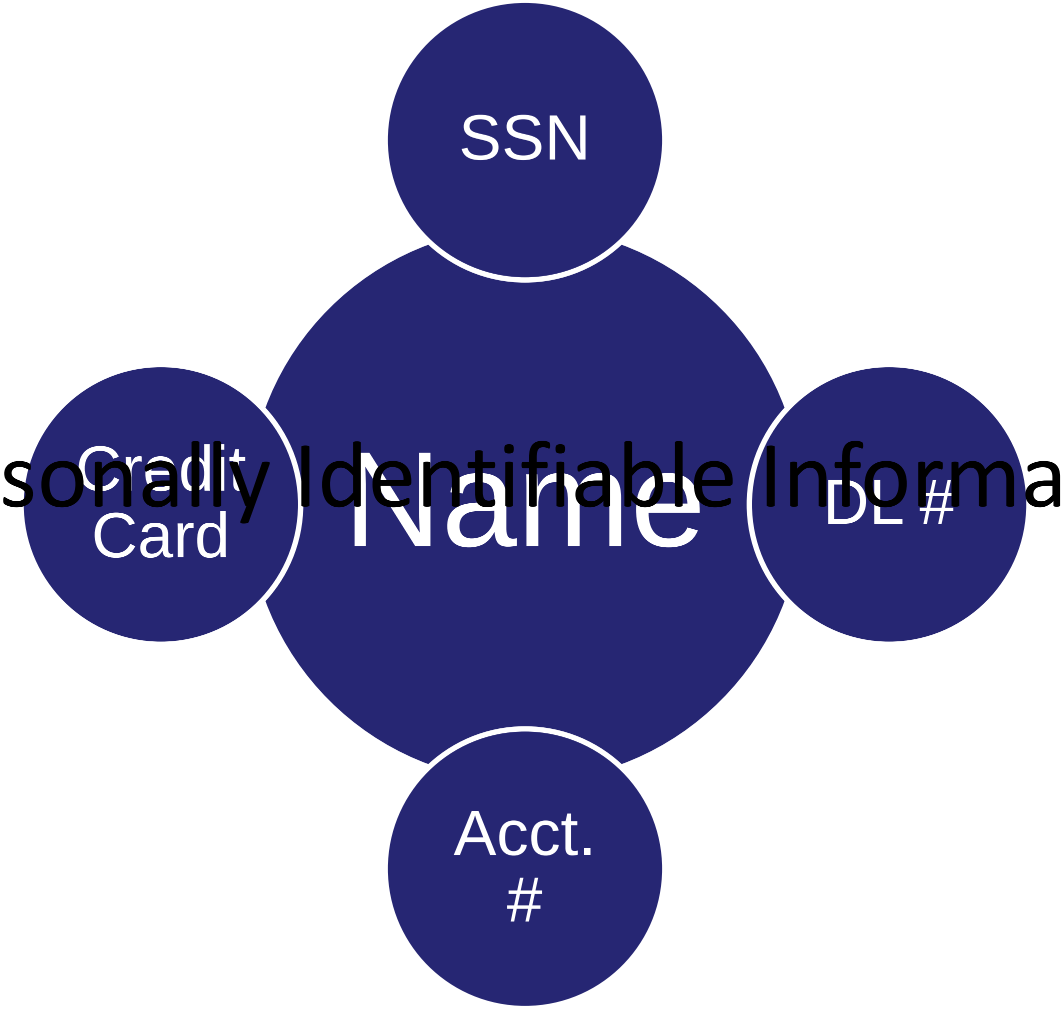
Information Security Office(ISO)
www.cmu.edu/iso
Computing Services
www.cmu.edu/computing

What is Identity Theft?

Identity Theft is a crime in which an impostor obtains key pieces of personal Identifying Information (PII) such as Social Security Numbers and driver's license numbers and uses them for their own personal gain.

Your name + key information = PII

Carnegie Mellon



PII – “Personally Identifiable Information”

How does it happen?

- Stolen wallet
  - Driver license ID
  - Credit cards
  - Debit cards
  - Bank accounts checks; last withdrawal banking statement
  - Health insurance
  - Auto registration and insurance card
  - Frequent flyer card
- Pilfered mail
- Computer virus
- Phishing and Social Engineering
  - Links to fraudulent web sites
  - Email
  - Phone call
  - Mail
- Social Networking account
- License plate
- Health records
- Financial Data

Identity Theft related crimes include

- Check fraud
- Credit card fraud
- Financial Identity Theft
- Criminal identity theft
- Governmental identity theft
- License plate number identity theft
- Mortgage fraud

Good and bad news

2003

2007

US Adult Identity Fraud

10.1 m

8.4 m

2006

One year fraud amount

55.7 b

49.3 b

The mean per fraud victim

6,278

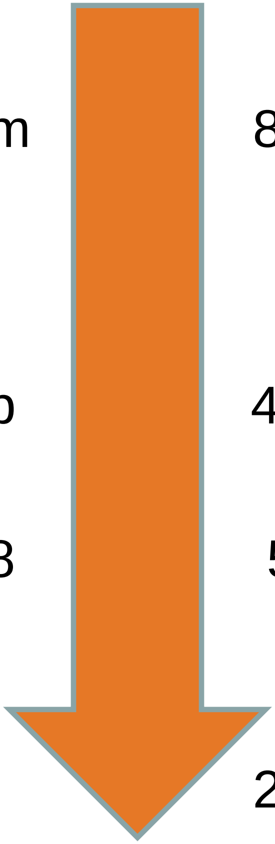
5,720

The mean for the resolution

Time per victim

40 hr

25 hr

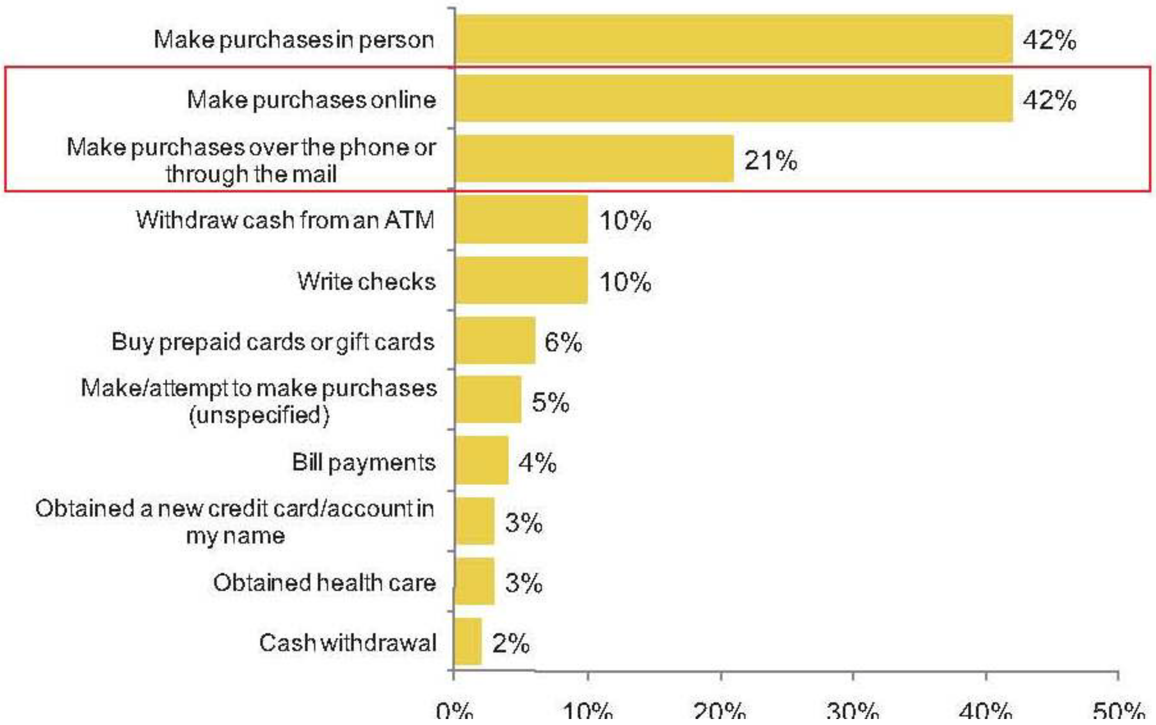


Identity Report 2010

The Javelin Strategy and Research 2010 report on identity fraud

https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf

Figure 3: What Are the Most Common Methods of Fraud?

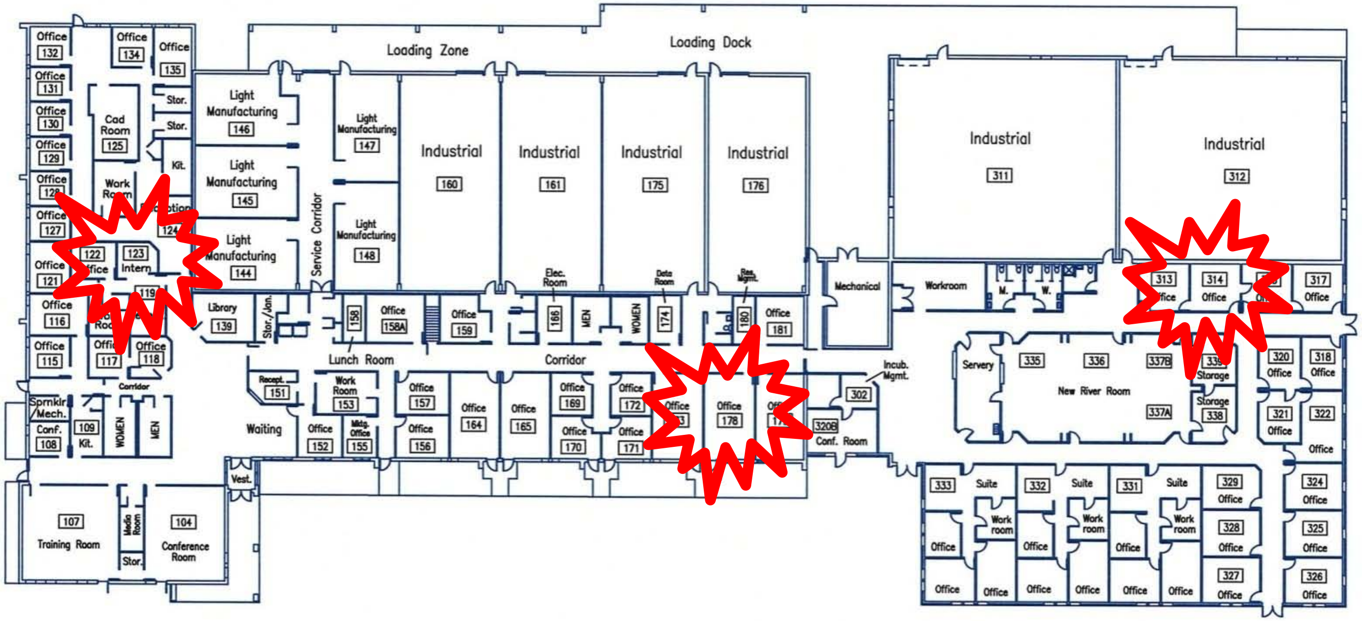


Information Security Office(ISO)

The threat of identity theft hits close to home

This is my street.
1 out of every 33 people means someone on my street will have their identity stolen this year.

Translating statistics to campus



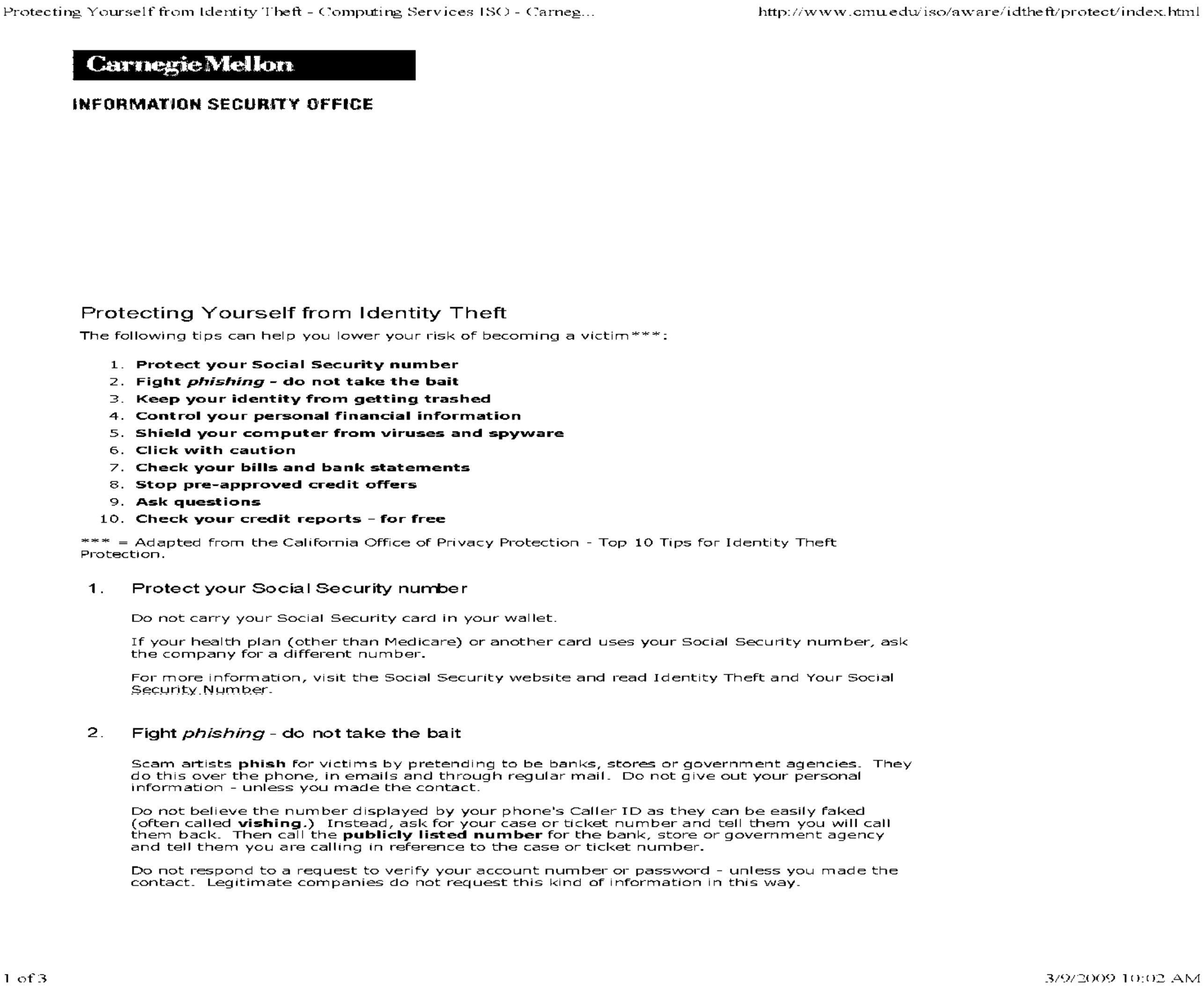
Standard office floor

1 out of every 37 people will be a victim this year.

At least 3 people will be hit this year.

Protect yourself from Identity Theft

Carnegie Mellon



Protecting Yourself from Identity Theft - Computing Services ISO - Carneg...   http://www.cmu.edu/iso/aware/idtheft/protect/index.html

Carnegie Mellon

INFORMATION SECURITY OFFICE

Protecting Yourself from Identity Theft

The following tips can help you lower your risk of becoming a victim***:

1. **Protect your Social Security number**
2. **Fight *phishing* - do not take the bait**
3. **Keep your identity from getting trashed**
4. **Control your personal financial information**
5. **Shield your computer from viruses and spyware**
6. **Click with caution**
7. **Check your bills and bank statements**
8. **Stop pre-approved credit offers**
9. **Ask questions**
10. **Check your credit reports - for free**

*** = Adapted from the California Office of Privacy Protection - Top 10 Tips for Identity Theft Protection.

1. Protect your Social Security number

Do not carry your Social Security card in your wallet.

If your health plan (other than Medicare) or another card uses your Social Security number, ask the company for a different number.

For more information, visit the Social Security website and read Identity Theft and Your Social Security Number.

2. Fight *phishing* - do not take the bait

Scam artists **phish** for victims by pretending to be banks, stores or government agencies. They do this over the phone, in emails and through regular mail. Do not give out your personal information - unless you made the contact.

Do not believe the number displayed by your phone's Caller ID as they can be easily faked (often called **vishing.**) Instead, ask for your case or ticket number and tell them you will call them back. Then call the **publicly listed number** for the bank, store or government agency and tell them you are calling in reference to the case or ticket number.

Do not respond to a request to verify your account number or password - unless you made the contact. Legitimate companies do not request this kind of information in this way.

1 of 3   3/9/2009 10:02 AM

Stolen Identity

If you suspect that you are a victim of identity theft;

http://www.cmu.edu/iso/aware/idtheft/notify/index.html

1. Report identity theft to your local police department
2. Contact the fraud hotline at the Social Security Administration (SSA), if your social security was stolen
3. Contact the fraud department of the three major credit bureaus

   - Equifax

   - Experian

   - Trans Union
4. Contact your creditors or bank when suspecting that your credit card, debit card or bank account is compromised.

How to keep your data safe

Carnegie Mellon

1. Secure Your Computer
2. Know What You Have
3. Delete or Secure Regularly
4. Transfer Securely

5. Physically Store Securely
6. Proper Disposal
7. Evaluate Workflow
8. Remain Vigilant

Information Security Office(ISO)
www.cmu.edu/iso

What About Everyone Else?

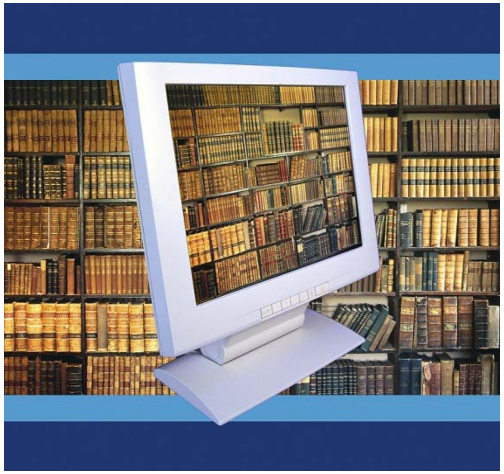
1. We can help keep others safe from identity theft!

2. What happens when we don't?
   - PA Breach of Personal Information Notification Act
   - What To Do If You Suspect A Breach
   - ISO Breach Handling Process

3. Proper Handling of Sensitive Data – How To Avoid Breaches

Common CMU Sources of Identity Data

- Old Class and Grade rosters
- Old Salary files
- Any Excel export file from central systems (e.g. HRIS, SIS, etc.)
- Shadow systems (e.g. local financial aid, admission applications, etc.)
- Research datasets
- Locally stored email
- Old backups & media



PA Breach of Personal Information Notification Act 1/2

- Effective June 20, 2006
- Triggered when computerized “Personal Information” is compromised
- Notification must be made “without unreasonable delay”

PA Breach of Personal Information Notification Act 2/2

- “Personal Information” = First name (or first initial) and Last name linked with one or more of:
  - Social Security Number
  - Driver’s License Number
  - Financial Account Number or Credit or Debit Card Number with any required access code or password in un-encrypted or un-redacted form

- Or if encrypted and the encryption is breached/involves a person with access to the encryption key

What To Do If You Suspect A Breach

Responding to a Compromised/Stolen Computer
http://www.cmu.edu/iso/governance/procedures/compromised-computer.html

Compromised - Reasonable suspicion of unauthorized interactive access

1. Disconnect From Network
2. Do NOT Turn Off
3. Do NOT Use/Modify
4. Contact ISO & Dept Admin
5. Preserve External Backups/Logs
6. Produce Backups/Logs/Machine ASAP For Investigation

Also report stolen computers

ISO Breach Handling Process

The ISO:

1. Confirm compromise, notifiable data, and likelihood of data breach (stolen laptop = data breach)
2. If data breach – proceed to notification

The ISO, the organization, & General Counsel's Office:

3. Identify population and locate current contact info via alumni records
4. Draft & send notification letter and interface w/ law enforcement and consumer reporting agencies as required
5. Operate call center and respond to legal action

Proper Handling of Sensitive Data 1/5

1. Know what data is stored on your personal computer

Run identityfinder

http://www.cmu.edu/computing/doc/security/identity/intro.html

Training video and material

http://www.cmu.edu/iso/aware/id-finder/index.html

Proper Handling of Sensitive Data 2/5

2. Delete or redact what you don’t absolutely need.

Identity Finder for Windows (Commercial)

http://www.cmu.edu/computing/doc/security/identity/index.html

Tools Matrix for Windows, Mac Unix

http://www.cmu.edu/computing/security/secure/tools/data-sanitization-tools.html

Proper Handling of Sensitive Data 3/5

3. Don’t store it on your personal computer especially not on your laptop or home computer.

   If you must store sensitive data, check with your departmental computing administrator about options to store it on a secured file server, one with robust access control mechanisms and encrypted transfer services.

Proper Handling of Sensitive Data 4/5

Carnegie Mellon

4. If you must store it on your personal computer
   A. Follow the “Securing your Computer guidelines” http://www.cmu.edu/computing/documentation/secure_general/secure_general.html
   B. Password protect the file if possible
   C. Encrypt the file (Identity Finder’s Secure Zip, Computing Services,PGP Desktop or TrueCrypt)
   http://www.cmu.edu/computing/doc/security/encrypt/overview.html
   http://www.pgp.com/products/desktop_home/index.html
   http://www.truecrypt.org/

Proper Handling of Sensitive Data 5/5

4. If you must store it on your personal computer (cont.)

   D. Only transmit via encrypted protocols (NOT Telnet, FTP, or Windows File Shares – instead use SCP and SFTP)

   E. Reformat and/or destroy your hard drive before disposal or giving your computer to someone else http://www.cmu.edu/iso/governance/guidelines/data-sanitization.html

   F. Secure delete it as soon as feasible

      http://www.cmu.edu/computing/security/secure/tools/data-sanitization-tools.html

   G. Secure your backups and media

Thank you, and stay safe!

Carnegie Mellon

Questions, Concerns, Feedback?

iso@andrew.cmu.edu

Practice Safe Computing

http://www.cmu.edu/iso/aware/pledge/index.html

Information Security Office(ISO)
www.cmu.edu/iso