Identity Theft Presentation Outline
Detective Jackelyn Weibel

I. Identity theft
   a. Definitions
   b. Examples
   c. FTC Statistics
II. Protecting business and personal identifying information
   a. Business information
      i. Businesses' identifying information
      ii. Clients' identifying information
         1. The law
         2. Ethical considerations
   b. Personal identifying information
   c. Importance of monitoring individual and business credit reports reguarly
III. Types of identity theft
   a. Medical
   b. Child
   c. Elderly
   d. Government
   e. Financial
      i. Identity theft schemes
         1. Skimming
         2. Phishing
         3. Pharming
         4. Spyware
IV. Consumer rights for use of credit and debit cards
V. Corporate responsibilities
   a. The law
   b. Ethical considerations
VI. Business precautions
VII. Safeguarding information
   a. Identifying information
   b. Client information
VIII. What to do if you or your business becomes a victim of identity theft

IDENTITY THEFT

Detective Jackelyn Weibel, CFE
Allegheny County District Attorney's Office

- Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

-U.S. Department of Justice

- For the 12th year in a row, identity theft was the #1 consumer complaint to the FTC.
- In 2011, approximately 7% of adults in the United States were affected by identity theft.
- Each instance resulted in an average loss of $3,500.
- Each instance averaged 25 hrs to fix. For many, it takes years to repair the damage.

- In 2011, over 15 million U.S. residents had their identities used fraudulently with financial losses upwards of $50 billion.
- Close to 10 million additional Americans have had their personal identifying information placed at risk when records maintained by government or corporate databases are lost or stolen.

Discovery

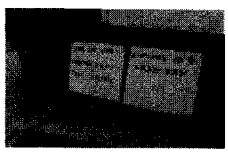
- 38-48% of victims discover their identity has been stolen within three months.
- 9-18% of victims do not discover their identity has been stolen for 4 or more years.
- Over 50 million Americans (businesses) are utilizing a credit monitoring service.
- 44% of consumers view their credit reports using AnnualCreditReport.com.

Personal Information is Everywhere!

No way to protect personal information 100%
Individual information v. client information
Actual laws v. ethical responsibilities

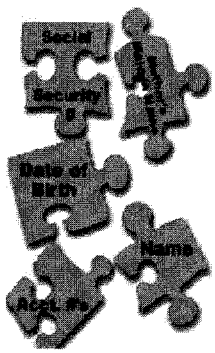
At Work...

- Businesses and places of employment.
- Co-workers and visitors have easy access to information.
- Employee training.



Types of Identity Theft

- Medical identity theft
- Child identity theft
- Senior identity theft
- Government identity theft
- Financial identity theft



Medical Identity Theft

- 25,000 Americans are victims of medical identity theft each year.
- The most difficult identity theft to detect.
- Thieves steal identities for the purpose of receiving free medical care and as a result create a false medical record for the victim.
- Consequences include:
  - ✓Incorrect treatment for victims;
  - ✓False health insurance claims filed;
  - ✓Denial of legitimate medical claims.

Child Identity Theft

- Perpetrator may be family member or someone known to the family.
- Targets children because of the length of time it takes to discover the theft.
- Children were targeted by scammers 35 times more often than adults, with 15% of the victims under the age of five.

Senior Identity Theft

- In 2010, reports of identity theft targeting people 50 and older represented about 28 percent of the total 236,765 cases.

  Senior Citizens more susceptible to acts of deception and manipulation.

- They have worked diligently their whole life to achieve good credit.

  They rarely check their credit reports.

Government Identity Theft

- Stealing personal information to obtain government assistance such as:
  - Social Security retirement or disability
  - Medical insurance or welfare benefits.

- Stealing personal information to fraudulent income tax returns to receive refundable credits such as earned income or child tax credits. (Always paid by debit card.)
- Billions of taxpayer dollars are wasted each year on fraudulent tax refunds!

Financial Identity Theft

- Individuals or businesses can be affected.
- Personal identifying information everywhere!
- Billion dollar business.
- Most common form of identity theft!

WHO IS STEALING YOUR IDENTITY?

- Retail Merchants and Their Employees
- Restaurant Employees
- Bank Employees
- Drug Abusers
- Terrorist Groups
- Organized Crime Members
- Illegal Immigrants
- Your Family Members
- Your Co-Workers
- Your Employees
- Neighbors

WHERE IS YOUR IDENTITY STOLEN?

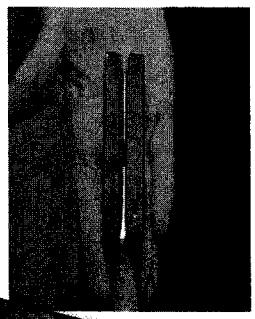
- Your mailbox
- Retailers
- Restaurants
- Hospital or health care facilities
- Discarded/stolen computers
- Internet
- Your motor vehicle
- ATM machines
- On the telephone

- Your place of employment
  - Certifications or licenses on walls
  - Personal information in desk / cubicle
  - By employees acting as accomplices

WHY IS YOUR IDENTITY STOLEN?

- Financial gain.
  - Money
  - Assets
  - Good credit rating
- Obtain a better life, history or job
  - Hide from criminal past
  - Stay in country
  - Desire for better social status-keep up with Joneses
- Revenge, cause malicious harm.
- Domestic reasons.
- Addictions to vice.

HOW IS YOUR IDENTITY STOLEN?



- Theft of your trash ("Dumpster Diving")
- Purse or wallet theft
- Dishonest employees
- Public Records
- Shoulder surfing
- "Pharming"
- "Phishing"
- Skimming devises
- Counterfeit documents
- EBay & Craigslist scams

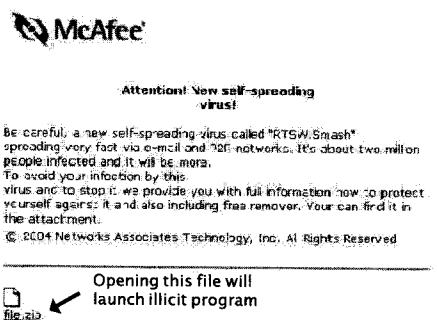
Identity Theft Schemes

- Database Hacking
- Social Engineering
- Dumpster Diving
- Skimming
- "Spam"- Spyware
- Dishonest Employee
- Pharming
- Phising
- Counterfeit Cards/Checks

UNKNOWN EMAILS

- Also known as "SPAM".
- Could launch hackers software (Spyware).
- Could cause victim to respond to fraud scheme (i.e. "Phishing").
- Could cause victim to give up personal info when making a "purchase".
- Best practice is to delete unknown or suspicious looking emails.

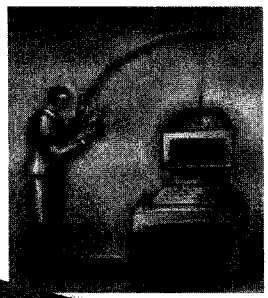
Example of an Unknown Email



"PHARMING"

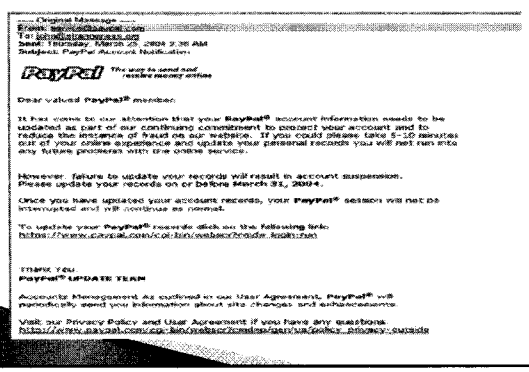
- Computer hacker using a malicious code acquires domain or host name information for a legitimate website and then redirects traffic to another identical looking (bogus) website.
- Usually banking or retail websites.
- Most often used to steal passwords, PIN numbers or bank information.

"PHISHING"



- The theft of personal information using emails that look legitimate.
- 75-150 million phishing e-mails are sent *EVERY DAY* with losses total more than $1 billion dollars a year.
- Email will reference a link which will take the victim to an authentic looking web site for a major company. When victim provides personal information, it is used by the thief to commit identity theft.

Example of a "Phishing" Email



Original Message
From: [redacted]
To: [redacted]
Sent: Thursday, March 25, 2004 2:36 AM
Subject: PayPal Account Notification

PayPal The way to send and receive money online

Dear valued PayPal® member,

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before March 31, 2004.

Once you have updated your account records, your PayPal® session will not be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Thank you.
PayPal® UPDATE TEAM

Accounts Management As outlined in our User Agreement, PayPal® will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside

Step by step "phishing" scenario...

Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below.

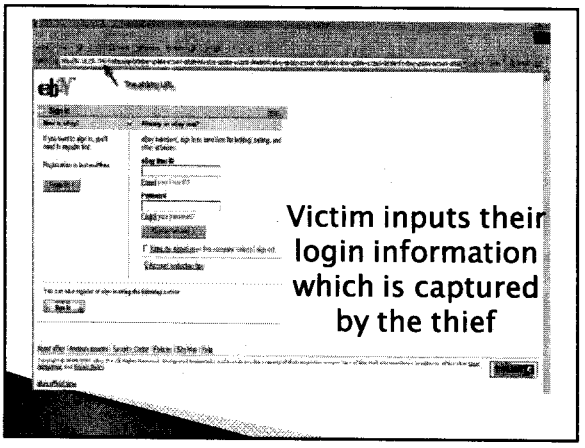
http://cgi1.ebay.com/aw-cgi/eboyISAPI.dll?MfcISAPICommand=SignInWelcome&siteid=0&co_partnerid=2&ru=http%3A%2F%2Fcgi1.ebay.com%2Faw-cgi%2Febayisapi.dll%3FMyeBay%26gbh%3D1

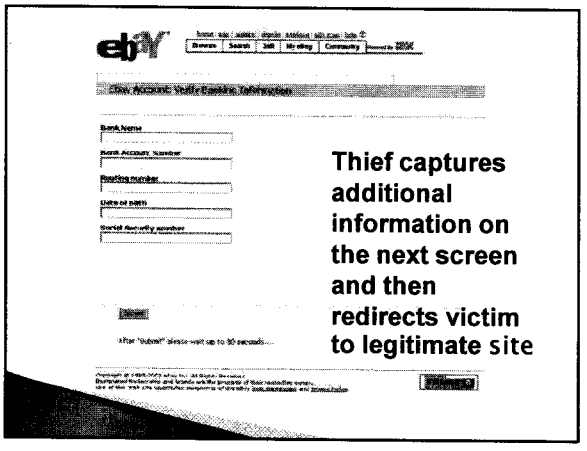
If your account information is not updated within **48 hours** then your ability to sell or bid on eBay will become restricted.

Kenneth Favot,

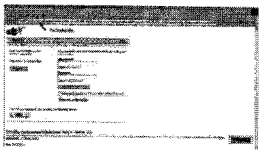
eBay Safe Harbour Dpt.

Victim receives an e-mail allegedly from "eBay" and clicks on the link...





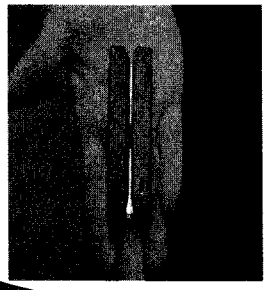
eBay is shutting down 30 phishing sites per day!



← Fake eBay site

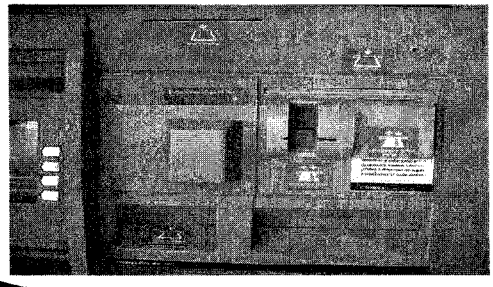
Real eBay site →

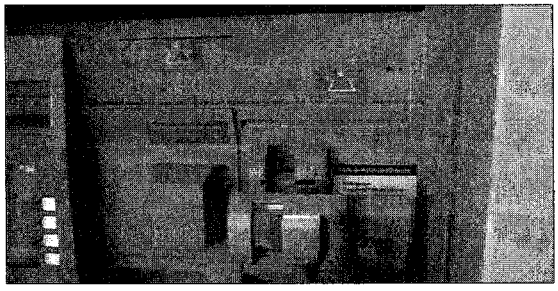
SKIMMING



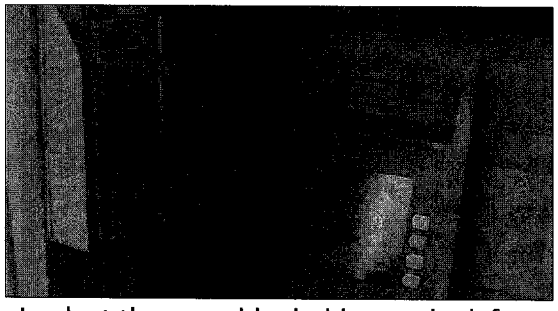
- Suspect uses a "wedge" to store information. contained on credit card strip.
- Downloads info later to computer.
- Uses info to create counterfeit cards with your personal information.

Standard ATM machine?

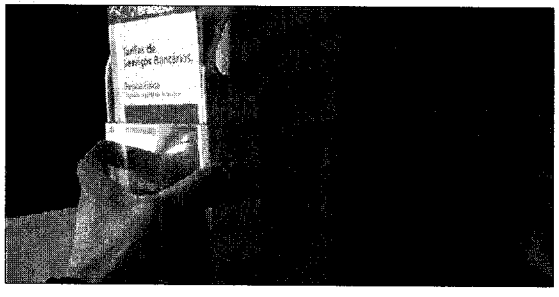




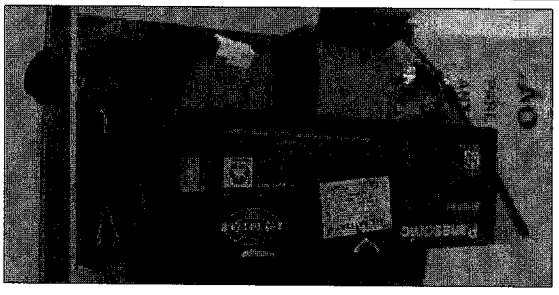
False front is attached to ATM with card reader »
to copy magnetic strip info on your card



Look at the pamphlet holder on the left »



Note the hole in the side »



Camera/transmitter housed inside »