



Identity Theft

Harry W. Trombitas
Special Agent, FBI
614-744-2168
htrombitas@columbus.rr.com

Resources

- ❖ www.ftc.gov/idtheft
- ❖ www.fbi.gov
- ❖ www.ic3.gov
- ❖ www.fightidentitytheft.com
- ❖ www.usps.com/postalinspectors

ID Theft: Deter-Detect-Defend



What Is Identity Theft?



Identity Theft Defined

- ❖ Identity Theft Involves The Use Of A Victim's Personal Identity And/or Credit For Criminal Purposes.
 - ❖ Such identifying info includes a person's social security number, date of birth, mother's maiden name, account numbers, address
 - ❖ Almost always employed as a means to commit other crimes
 - ❖ Unique in that it is a component of many types of crimes and spans multiple investigative programs
 - ❖ Bank Fraud, Credit Card Fraud, Telemarketing Fraud, Internet Fraud, Bankruptcy Fraud, Insurance Fraud, Money Laundering, and Fugitive cases

Identity Fraud

- ❖ Identity Fraud Involves The Use Of A False Identity, Which Does Not Belong To Someone Else, For Criminal Purposes.

Warning Signs

- ❖ You Get A Call From A Financial Institution Concerning An Unusual Transaction
- ❖ You May See Unauthorized Charges On A Credit Card Or Checking Account Statement
- ❖ You May See An Account That You Did Not Open On Your Credit Report
- ❖ You May Get A Call From A Collection Agency Asking Why You Have Not Paid A Bill

What About The House?



How Your Identity Can Be Stolen

- ❖ Loss Or Theft Of Your Wallet, Purse, Or Credit Card
- ❖ Mail Theft
- ❖ Skimming Information From The Magnetic Strip On Your Credit Or Debit Card
- ❖ "Dumpster Diving" Through The Trash
- ❖ "Shoulder Surfing" : Looking Over Your Shoulder When You Are Entering PIN Or Password

I Love Computers



Other Ways

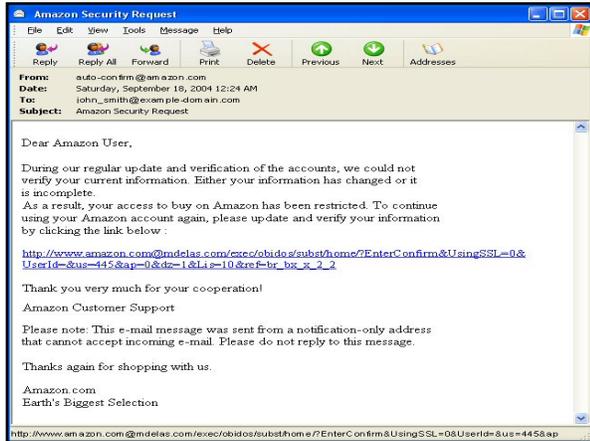
- ❖ Scam Phone Calls Where A Stranger Asks For Personal Or Financial Information
- ❖ Impersonation
- ❖ Computer Hacking
- ❖ "Phishing" Emails
- ❖ Spyware

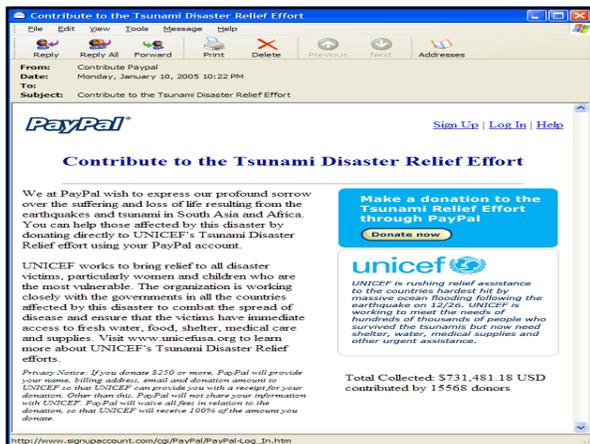
Outside Help



“Phishing”

- ❖ Uses Spam Or Junk Emails That:
 - ❖ Seek To Obtain Same Information That Any Identity Thief Would Want (Name; Address; SSN; DOB;PIN)
 - ❖ May Mimic:
 - ❖ Financial Institutions
 - ❖ Government Agencies
 - ❖ Legitimate Businesses
 - ❖ May Ask You To Go To A Website To Verify & Enter Your Personal Information
 - ❖ May Ask You To Follow A Link That Takes You To A Fictitious Site That Looks Authentic





What To Do If You Think You Responded To One By Accident?

- ❖ If You Responded To A “Phishing” Email And Provided Personal Information, Assume That You Will Become A Victim Of Identity Theft
- ❖ If You Provided Your Bank Account Or Credit Card Number, Cancel That Account And Open A New One Immediately

Skimming



Thieves use handheld magnetic card readers that can be bought on the Internet and elsewhere to glean personal information off the magnetic strip on credit and debit cards. Once info is stripped, the data can be transferred to other magnetic strips to make counterfeit credit & debit cards.





ATM Machines can be rigged to skim account information - and with a bank insider, your PIN # can be compromised

Skimming Device

What You Can Do To Protect Yourself

A cartoon illustration of a thief wearing a mask and a striped shirt, running away with a large bag of money. The thief is holding a stack of cash in one hand and a bag in the other. The background is a simple yellow circle.

Check Your Credit Report

- ❖ Check Your Credit Report At Least Once A Year
 - ❖ To See Whether Accounts Have Been Opened In Your Name Without Your Knowledge
 - ❖ To Spot Unexpected Delinquency On Established Accounts
 - ❖ To Review Your Credit Report Before Making A Major Purchase
- ❖ These Reports Can Be Free And Are Easy To Get
 - ❖ Contact : www.annualcreditreport.com

Steps To Catch Identity Thieves

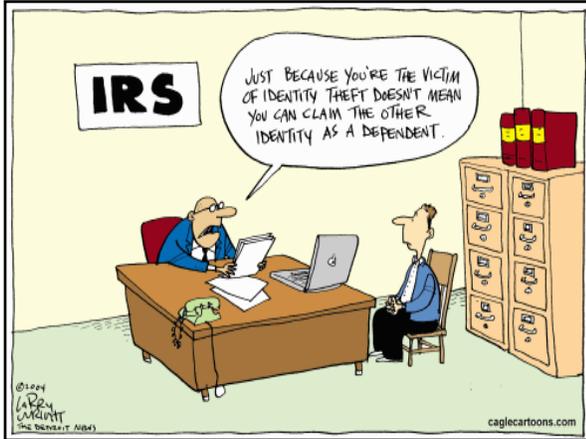
- ❖ Monitor Your Online Financial Accounts Frequently
- ❖ Promptly Review Your Other Bank & Credit Card Statements, As Well As Other Bills
- ❖ Quickly Call The Financial Institution Or Company If You See Anything Suspicious And Follow Up In Writing
- ❖ Sign Your New Credit & Debit Cards Promptly

Protect Your Information

- ❖ Shred Your Personal Records Effectively
- ❖ Never Give Anyone Your Personal Information Over The Phone Or Internet Unless You Initiated The Contact
- ❖ Banks & Credit Card Companies Already Have Your Account Information And Will Never Call Or Email To Ask You To Provide It
- ❖ Protect Your Mail – Quickly Pick Up Delivered Mail To Your Home And Place Mail To Be Sent Out In Secure Postal Box

Protect Your Social Security Number

- ❖ Do Not Carry Around Your Social Security Card
- ❖ Do Not Provide Your Number To Merchants Or Others Just Because They Say They Need It – Ask Why They Need It And How It Will Be Protected
- ❖ Remember, Financial Institutions Will Need Your Number For Tax Reporting And Other Identifying Purposes, But You Should Only Provide It To Someone Who You Are Sure Is An Employee With That Institution



On-line Safety

- ❖ Use Common Sense When On The Internet
 - ❖ Know The Web Address – Or URL – Of The Site You Wish To Visit
- ❖ Use A Firewall
- ❖ Never Walk Away From Your Computer Without Making Sure Others Won't Have Access To Your Information
- ❖ Make Sure Your Operating System And Software Are Updated With The Latest Security Patches
- ❖ Clean The Hard Drive Before Disposing Of Your Old Computer

**OPT OUT OF
PREAPPROVED/PRESCREENED CREDIT
CARD OFFERS**

1-888-5opt-out
1-888-567-8688
www.optoutprescreen.com

**What To Do If You Become A Victim
Of Identity Theft**

- ❖ Place A Fraud Alert On Your Credit Reports;
Review Your Credit Report; Correct Mistakes
 - ❖ Equifax: 1-800-525-6285
 - ❖ Experian: 1-888-Experian
 - ❖ TransUnion: 1-800-680-7289
- ❖ Close The Accounts That You Know Or Believe
Have Been Tampered With Or Opened
Fraudulently
- ❖ File A Police Report & Keep A Copy
- ❖ File A Complaint With The Federal Trade
Commission: www.consumer.gov/idtheft

Contact Your Financial Institution

- ❖ Most Financial Institutions Have Specially
Trained Agents To Help You
- ❖ They Will Investigate The Circumstances
- ❖ They Should Take The Suspect Charges Off
The Account, Pending Investigation
- ❖ They Will Reissue Cards, Close Accounts As
Necessary
- ❖ They Will Need A Written Report Of What You
Are Claiming

Tips For Organizing Your Case

- ❖ Keep Good Records Of Everything You Do, Everyone You Talk To, Including Dates
- ❖ Consider Using The FTC's Standard Affidavit & Sample Form Letters: www.consumer.gov/idtheft
- ❖ Keep Copies Of All Correspondence Or Forms You Send
- ❖ Keep The Originals Of All Supporting Documents
- ❖ File An Identity Theft Report To Insure That An Extended Alert Stays On Your Credit Report For Seven Years

Tips From The Postal Inspectors





Identity Theft

Harry W. Trombitas
Special Agent, FBI
614-744-2168
htrombitas@columbus.rr.com
