



# Identity Theft

A consumer's guide to protecting your personal identity and finances

Offered by the Michigan State Police



## *Definition*

**Identity Theft-** Identity theft occurs when information of a living or deceased person, or business entity, is used for any unlawful purpose. **Most often used for financial gain.** May also be used to hide from authorities and/or establish bogus residency.

➤ **Now includes an array of criminal acts.**



# *Why commit identity theft?*

- **Take over financial accounts**
- **Establish new bank accounts**
- **Apply for loans**
- **Apply for credit cards**
- **Apply for Social Security benefits**
- **Purchase or lease property**
- **Property rental**
- **Establish services (phone, utilities, etc.)**
- **Manufacture/counterfeit checks**
- **To fund organized criminal enterprises**



## *Methods of obtaining your personal information*

- Theft of wallets/purses/computers
- Mail theft and/or diversion of mail
- Dumpster diving
- Shoulder surfing
- Dishonest employees
- Phishing
- Vishing
- Skimming devices
- Scams



## *Cause for concern?*

- **Can strike anyone at any time.**
- **Can destroy a person's credit standing.**
- **Can cause adverse employment actions.**
- **Can result in wrongful criminal convictions.**
- **Creates difficulty with restoring credit.**
- **Causes heavy fraud losses to honest businesses, escalating consumer prices.**

# Phishing

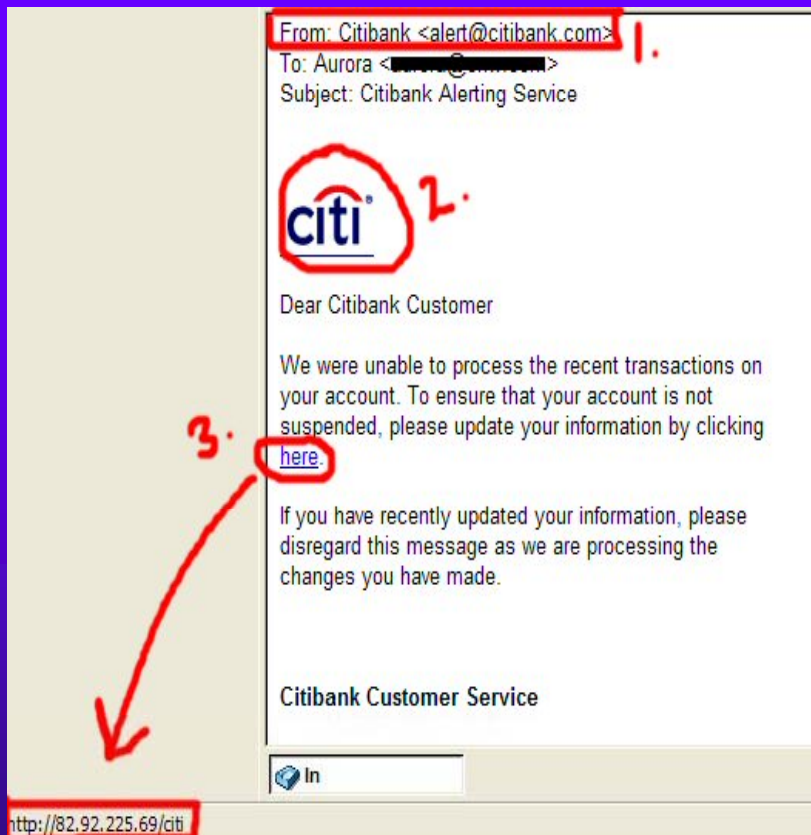
**Phishing** – High tech scam that most often uses spam or pop-up messages to deceive consumers into disclosing the following information:

- **Bank account information**
- **Credit card numbers**
- **Social security numbers**
- **Passwords, etc...**
- **In addition, “Social Engineering” – children’s names, ages, name of pets, etc...**

**\*May also be carried out in person or over the phone.**



# Example



1. The “From Field” appears to be from a legitimate company. Field is very simple to change.
2. The e-mail will usually contain logos or images that have been taken from the web site of the company.
3. The e-mail will contain a clickable link with text suggesting you use the inserted link to validate your information. May also state “Log into Citibank”

**\*Notice the actual website, in the lower left corner.**

# Skimming



- **The use of electronic devices to copy the magnetic codes from the back of the card.**
  - **Your credit information, once copied, can be used on other existing credit cards using simple electronic equipment**
  - **Report unusual handling of credit cards, by clerks, waitresses or agents, to loss prevention or management**

# *Skimming Devices*



- ◆ Can be built from commercially available parts.
- ◆ Be aware of how your card is handled.

# *ATM Skimming Device*





## *Vishing*

- ◆ Subjects use Voice over Internet Protocol (VoIP) phones.
- ◆ Victims receive recorded message informing them of a breach.
- ◆ Message instructs victim to call the designated phone number.
- ◆ Then instructs them to enter their 16 digit account number, for verification purposes.
- ◆ The VoIP phone recognizes the victims telephone keystrokes.
- ◆ The rest is academic.



## Scams

- Often times, you make the decision to participate in various types of fraud/scams.
- **SOLUTION:** Hang up the phone, do not respond to shady emails, pop-ups or mailings.
- **REMEMBER** – *If it looks or sounds too good to be true, it probably is!!*

[www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com)



## *Types of scams*

- ◆ **Nigerian**
- ◆ **Foreign Lottery**
- ◆ **Re-shipping**
- ◆ **Western Union**

# *Is Cyberspace Safe ?*

- ◆ **Individual enterprises vary greatly in the protections they provide the consumer**
  - **Contrary to popular belief identities are not stolen in cyberspace; but rather from the files of the business.**



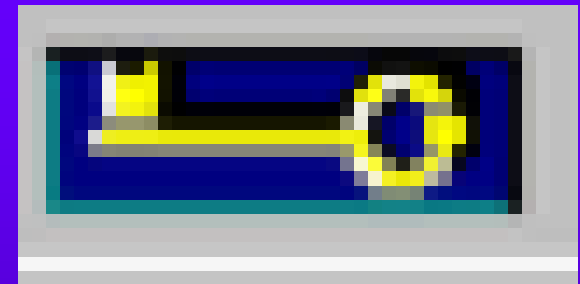
# Secure Shopping Sites

- Contain the letter “s” in their web address prefix code

**Example:**

[https //www.nocyberpests.com](https://www.nocyberpests.com)

- **Additionally:**
  - A lock or key will be displayed in the lower, right hand corner of your screen





## *Security on the internet*

- **Shopping online offers many benefits that you will not find in a store or by mail.**
  - **Open 24hrs/day, 7 days a week.**
  - **Bargains**
  - **No less safe than shopping in a store or by mail.**



## *Online shopping tips*

- **Use a secure browser (software used to navigate the internet.)**
- **Shop with companies you are familiar with.**
  - **If not familiar, ask for a catalog or brochure**
  - **Determine refund and return policies before order is placed.**
  - **Keep your passwords private. Be creative with them. Use combination of letters/symbols.**



## *Shopping tips, continued*

- Pay by a designated credit card. Protected by the Fair Credit Billing Act, which allows you to dispute charges. Liable for max of \$50.00.
- Keep a record. Print a copy of your purchase order and confirmation number.
- Pay your bills online. Many companies will offer this service. Prior to doing so, evaluate how the company secures your information.



## *Tips for preventing ID theft*

- ◆ Never give out personal info in response to unsolicited offers by phone, mail, internet, or in person unless you initiate the contact.
- ◆ Order and review your credit report yearly.
- ◆ Review financial statements carefully.
- ◆ Cross-shred paperwork containing personal information.
- ◆ Remove mail from your mailbox a.s.a.p.
- ◆ Be aware of where your personal identification information is kept – at work and home.



## *Tips for preventing ID theft*

- ◆ Do not leave your purse/wallet unattended at any time.
- ◆ Do not carry your social security card in your wallet!
- ◆ Do not carry your credit card PIN # in your purse/wallet.
- ◆ Do not leave trash on curbside overnight.
- ◆ Be aware of missed bills, which could indicate an account takeover.



## *Federal Trade Commission*

- **Federal agency which acts as a resource center for identity theft and additional fraud related incidents.**
- **Do not have enforcement authority.**
- **Investigative tool for law enforcement.**



## *Victim action steps*

- Contact all three credit bureaus and place a fraud alert on your credit report. Order a copy of your report from each agency at [freecreditreport.com](http://freecreditreport.com) or [annualcreditreport.com](http://annualcreditreport.com)
- Dispute and close all accounts that were opened fraudulently.
  - Ask the company to send you the necessary forms.
  - Fair Credit Billing Act requires you to dispute the matter, in writing, within 60 days from receipt of the erroneous information.
  - Send dispute letter by certified mail.
  - Creditor must acknowledge your complaint, in writing, within 30 days.
  - Dispute must be resolved within two billing cycles.



## *Victim action steps, continued*

- Place an alert on accounts not yet affected. Inform creditor that you would like to be contacted prior to any changes being made to your account.
- Contact collection agencies, if applicable.
- Keep detailed notes/timeline of information.
- If possible, retain original related documents.
- Contact Secretary of State and U.S. Dept of State (passports), if applicable.
- File a complaint with the FTC.
- File a report with your local law enforcement agency. Do not take no for an answer.
- Provide detailed information and necessary documentation to law enforcement agency.



## *Police reports*

### ◆ *MCL 780.754a*

- To facilitate compliance with 15 USC 1681g, a bona fide victim of identity theft is entitled to file a police report with a law enforcement agency in a jurisdiction where the alleged violation of identity theft may be prosecuted as provided by section 10c of chapter II of the code of criminal procedure, 1927 PA 175, MCL 762.10C, and to obtain a copy of the report from that law enforcement agency. (2) as used in this section, “Identity Theft” means that term as defined in section 3 of the Identity Theft Protection Act.
- The police agency with jurisdiction where the incident is reported must take the original report.



# *Telemarketers*

## **PHONE**

- **Consumers who have not already registered their phone numbers may do so at [www.donotcall.gov](http://www.donotcall.gov) or by calling 1-888-382-1222.**

## **MAIL**

- **Mail Preference Service  
POB 9008  
Farmingdale, NY 11735**



## *Pre-approved credit card offers*

Three methods of opting out include:

- **Calling 1-888-5-OPTOUT**
- **OptOutPreScreen.com**
- **Contacting individual credit bureaus**



## *Credit bureau contact information*

- **Equifax Inc**  
**PO Box 740123**  
**Atlanta, GA 30374-0123**
- **TransUnion**  
**P.O. Box 505**  
**Woodlyn, PA 19094**
- **Experian**  
**901 West Bond**  
**Lincoln, NE 68521**  
**Attn: Consumer Services Department**

*Michigan State Police*  
*resources*



*Toll free hotline:*  
**(877)MI-ID THEFT**

*Website:*  
**[www.michigan.gov/identity-theft](http://www.michigan.gov/identity-theft)**



# *MSP website information*

## FORMS

- CIS-10** Affidavit of fraud and forgery
- DD-008** Certification of records
- DD-009** ID theft witness statement
- DD-014** ID theft victim information

## RESOURCES

- Cybersecurity website
- ID theft legislative link
- ID theft victim assistance information
- Letter to collection agencies
- Letter to credit grantors
- Letter to flag accounts