PIRAEUS BANK

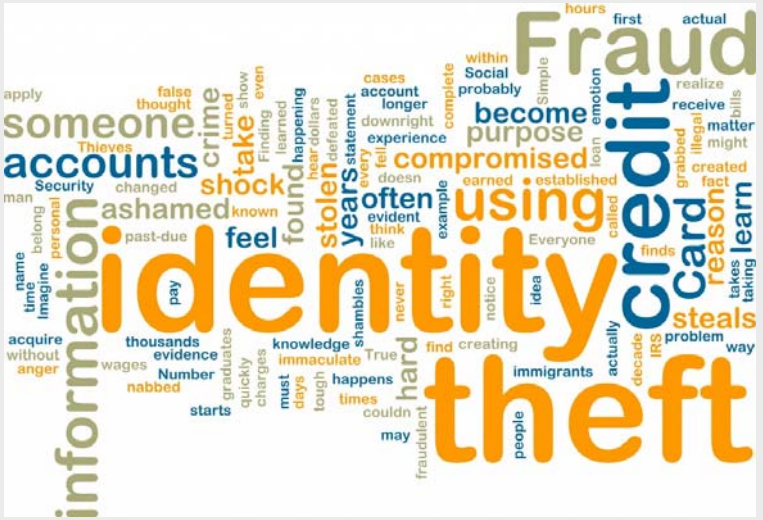
Identity Theft

CHRISTOS TOPAKAS

Head of Group IT Security and Control Office

Agenda

- Identity Theft – Threats and Techniques
- Identity Theft Definition and Facts
- Identity Theft & Financial Institutions
- Prevention / Recommendations
- Future Trends



Threats / Techniques for Identity Theft Crimes (1/2)

Cyberattack Threats and Techniques:

- Phishing
- Spam and Identity Theft
- Email Scam and Fake Web Sites
- Pharming
- Hacker
- Insider
- Spyware and Adware
- Malware / Ransomware
- Trojan Horse

Threats / Techniques for Identity Theft Crimes (2/2)

Other Threats and Techniques:

- Card Skimming
- Voice Phising – Vishing
- Social Engineering – Media
- Pick pocketing
- Garbage bins Theft
- Home Mail Box theft
- Theft of Utility Bills, Tax Revenue Bills and Social Security Information

Identity Theft - Definition

“Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner with the intent to make a false representation as to his identity in order to make a gain or acquire a benefit for himself or another or to cause loss to another or expose another to a risk of loss.”

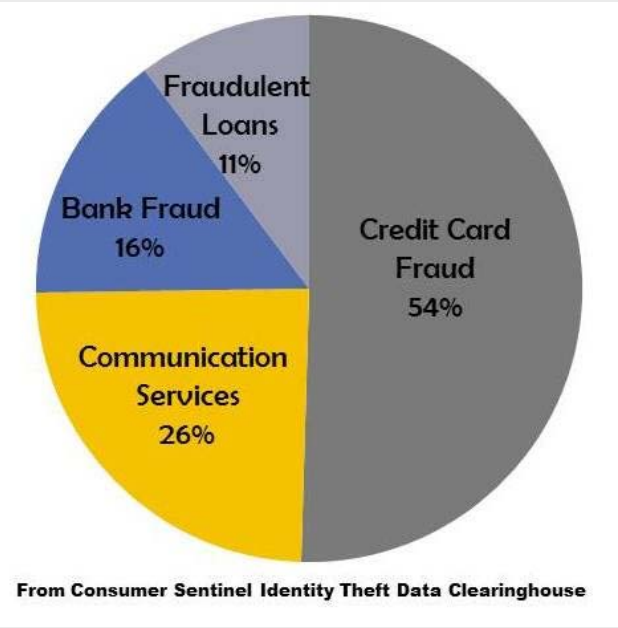
- Identity Theft has **Primary** (*the entity whose identity is abused*) and **Secondary** victims (*the third party who is defrauded*).

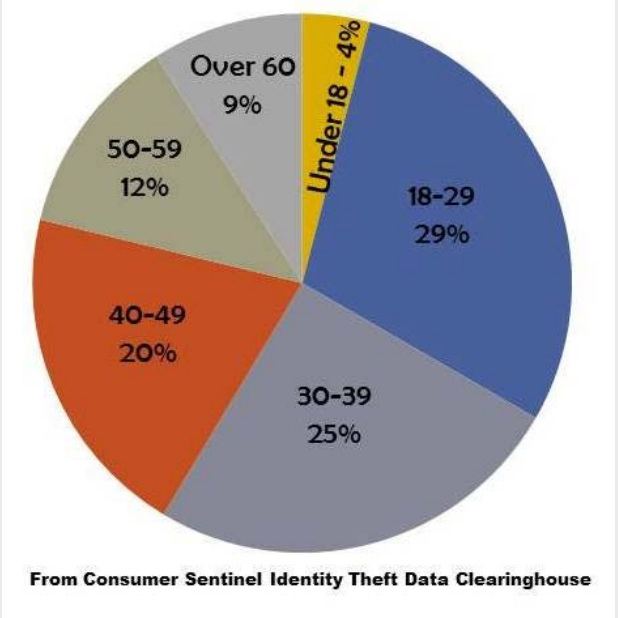
- The victim can be individuals, business corporations or other entities.

- Identity Information:
  - ✓name, mother’s maiden name
  - ✓passport number,
  - ✓biometrical data,
  - ✓credit card information,
  - ✓usernames and passwords,
  - ✓social security and tax data,
  - ✓utility bills data

Identity Theft – Some Facts (1/2)

- Drug trafficking has officially been replaced by identity theft as the number one crime.
- People between the ages of 18-29 are more likely to experience identity theft.
- The most common type of identity theft is linked to credit card fraud.



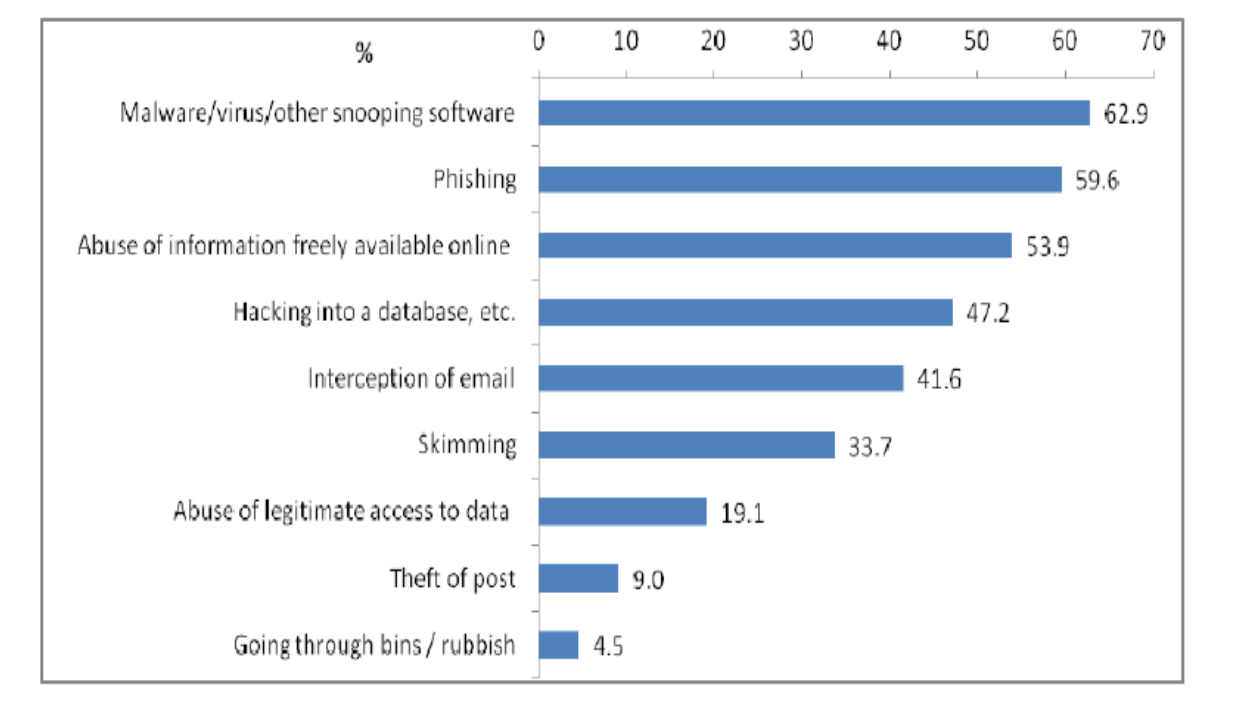


Source: Consumer Sentinel Identity Theft Data Clearinghouse

Identity Theft – Some Facts (2/2)

➢One third of all targeted attacks aimed at businesses with less than 250 employees (source: Symantec 2013).

➢Criminals still rely on non-technological methods to perform Identity Theft crimes (source: European commission 2012).



➢Stolen Identities Information can be used for a large period (Source: Consumer Sentinel Identity Theft Data Clearinghouse).

➢The emotional impact can be greater than the financial (source: US Department of Justice).

Non Financial Identity Theft Crimes

- Social Security Identity Theft
- Criminal Identity Theft
- Medical Identity Theft
- Driver's License Identity Theft
- Complete Identity Cloning
- Synthetic Identity Theft

Identity Theft and Financial Institutions

Fraudsters can use Identity Information to perform:

- Open bank account
- Clone Credit Cards for illegal purchases (individual) or fake transactions (merchant)
- Clone Debit cards for cash advances
- Check forgery
- Obtain loans
- Illegal money transfer

Prevention / Recommendations for Enterprises

- Enterprise that store sensitive data (credit card, bank account data, personal information) should protect their systems from outside and inside threats.

- No single layer of attack prevention is enough. Multiple layers must be employed. (eg account behavior monitoring across channels, secure browsing applications, etc)

- Establish Fraud management framework.

- Establish a stringent internal control framework to prevent insider threat (data classification, risk management framework, DLP, access controls, etc).

Prevention / Recommendations for Individuals

- Limit the information in purses, wallets, pockets, etc.
- Make online purchases from known companies only
- Do not click suspicious links in emails
- Download latest updates and fixes, use firewalls and install antivirus
- Protect your mobile device
- Memorize your passwords
- Shred documents at your home/office before disposal
- Clean IT assets before disposal

AWARENESS

illegal money transfer

malware

virus

ransomware

insider

email scam

hacker

trojan horse

adware

bill theft

spyware

attacks

phishing

social security theft

pay

compromised

security

mac attack

mail theft

Check forgery

spam

Credit card cloning

pick pocketing

mobile threats

identity cloning

vishing

Future Trends

- Growth of Social Networking:
  - ✓ Social media identity may be more valuable to cyber criminals than credit cards
  - ✓ New attack methods will go through the victim's social media "friends".

- Mobile devices (smartphone, tablet) is the new target:
  - ✓ BYOD – a new headache for enterprises
  - ✓ Mobile transactions – payments, purchases, email access, software access

- Fake technology tools are on the rise

- Mac Attacks – a new attack vector

Conclusion Points

- Identity Theft is on a rise
- Hackers are getting "smarter“
- E-commerce / e-Banking Services / Mobile Devices / e-tax - new fraud frontier
- Companies need to invest on stronger control framework and new technologies
- Focus should be given to outside and inside threats
- Users / individuals should…

be AWARE!

Questions and Answers