Identity Theft:
What You Need to Know
What is Identity Theft?
Identity Theft

Identity theft is a crime of stealing key pieces of someone’s identifying information, such as:

- name,
- address,
- Social Security number,
- birth date, and
- mother’s maiden name
Common Forms of Identity Theft

- Credit card fraud
- Communications services fraud
- Bank fraud
- Fraudulent loans
- Internet fraud
How Identity Theft Occurs

Identity thieves…

- steal wallets and purses containing your ID
- steal your mail
- complete false “change of address” forms
- rummage through trash ( “dumpster diving” )
- pose fraudulently as someone else to get your information
More Ways Identity Theft Occurs

Identity thieves...

- steal business or personnel records at your workplace.
- find personal info in your home.
- use info you put on the Internet.
- buy personal info from “inside sources.”
- “shoulder surf” at ATMs and telephones.
The National Privacy Principles

1 – Collection

- Must only collect personal information that is necessary for the purpose
- Collection of personal information must be fair and not intrusive
- Must take reasonable steps to ensure the person from whom personal information is

2 - Use and Disclosure

- Use and disclosure of personal information must only be for the purpose that it was
- intended for, or for strongly related secondary purposes, or for specified direct marketing,
3 – **Data Quality**

- Data quality must be good and reasonable steps must be taken to ensure personal information is accurate, complete and up to date when collected and used.

4 – **Data Security**

- Data must be kept safe from misuse, loss and unauthorized access. Personal information that is no longer needed must be destroyed or permanently de-identified.

5 – **Openness**

- A clear Privacy Policy statement must be available outlining the organization’s personal information handling practices. On request, reasonable steps must be made to let a person know what personal information it holds, for what purposes, how it collects, holds, uses and discloses that information.
6 – Access and Correction

- Access to and correction of personal information must be made available on request by
- the individual. A reasonable fee may be charged for providing access. Reasonable steps
- must be taken to correct information.

7 – Identifiers

- Commonwealth Government identifiers (such as TFN ‘s) cannot be adopted, used or
- disclosed.

8 – Anonymity

- Where lawful and practicable, individuals have a right not to identify themselves.
9 – Transborder Data Flows

- Transfer may only occur to a foreign country if the recipient is subject to a law similar to
- the NPP’s; or the individual has consented; or the transfer is necessary for the
- performance of the contract between the individual and the organization.

10 – Sensitive Information

- Sensitive information must not be collected unless the individual has consented or in some
- special circumstances as required by law such as public health and safety
Privacy of Medical Records

- The word 'privacy' means different things to different people. Your idea of privacy is likely to be different from the ideas of your family and friends.

- Electronic medical records ("EMRs") appear to present new threats to maintaining the privacy of patient-identifiable medical records.
The Issues

- The problem is that these techniques are expensive and no one is sure how well they work
- Most privacy proposals would give patients the right to correct inaccuracies in their records but not to delete material
The Managed Care Conflict

- A second reason for the increased concern over medical records privacy is the growth of managed care organizations.

- Technical steps being touted include unique patient and access identifiers.

- Special problems are created by employer-sponsored health plans.
Privacy Enhancing Technologies

- Goals
  - **data minimisation**: minimise the personal data collected and used by service providers and merchants
  - **data tracking**: allow users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions
  - facilitate the **use of their legal rights** of data inspection, correction and deletion
Existing PETs

- **Communication anonymizers**
- **Shared bogus online accounts.**

- **Access to personal data:** The service provider's infrastructure allows users to inspect, correct or delete all their data stored at the service provider.
Future PETs

- Wallets of multiple *virtual identities*; ideally unlinkable. Such wallets allow the efficient and easy creation, management and usage of virtual identities.

- Data transaction log.

- Anonymous credentials
Social Engineering

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information.
Organizations can get too focused on having all the latest technical controls but forget that people are typically one of their weakest links.
Some of The Types

- **Pretexting** is the act of creating and using an invented scenario (the pretext) to persuade a targeted victim to release information or perform an action and is typically done over the telephone.

- Phishing is a technique of fraudulently obtaining private information.

- This attack, the attacker leaves a malaria infected floppy disc, CD ROM, or USB flash drive in a location sure to be found.

- ETC
Assessing Threats

- Organizations must know how and where does information travel in and out of the organization and how this information trusted……
- And ensure that the people exposed are capable of identifying a threat and adhering to policies and practices established to mitigate them.