Chapter 5 summaries

Identity theft and fraud definitions and prevalence

- Fraud refers to the use of trickery for some gain, often financial.
- Identity theft refers to the use of someone else's documentation or personal information, again normally for financial gain.
- Fraud has many different types, and can target individuals, companies, public sector and not-for-profit groups.
- New technologies make it easier for fraudsters and identity thieves, but these types of offences are not new.
- Identity theft often involves the unauthorised use of some kind of 'trusted token', such as a password, account number, or other information or documentation.
- It is difficult to know exactly how much identity theft and fraud occurs, as there are several reasons why they may not be reported, including fear or embarrassment on the part of the victims, or a lack of awareness of who to report the offence to.
- However some organisations, such as the UK National Fraud Authority and the Anti-Phishing Working Group, publish regular updates on the extent of such problems.

Offline fraud schemes

- While online fraud is relatively new, offline fraud has existed for centuries.
- Offline fraud can take a variety of forms, including the selling of fake medicines, Ponzi schemes, pyramid schemes, employment fraud and lottery fraud.

Social networking site fraud, online dating fraud and conference fraud

- Social networking site fraud can involve a variety of techniques:

  - Potential identity thieves can gather personal information from profiles
  - Users can be persuaded to allow applications designed by fraudsters to have control of aspects of their accounts
  - Users can be persuaded to provide fraudsters with personal information in exchange for perceived benefits, such as the ability to see who has been viewing their profile
  - Social networking site fraud is often perpetrated by posting content and links to the victim's profile.
- Online dating fraud occurs when a criminal pretends to initiate a romantic relationship with a victim through an online dating site, only to later persuade the victim to send money to them.
- Conference frauds invite the email recipient to a seemingly important occasion or event, but indicate that they can only attend if they follow certain guidelines, such as by reserving a room at a specific hotel.

Phishing

- Phishing refers to emails that are directed at a user to obtain personal information, such as passwords and account details.
- Phishing scams often rely on the potential victim's fear or greed.
- Phishing which is distributed by text messaging is referred to as 'vishing'.
- Phishing which occurs using voice is referred to as 'smishing'.
- The redirection of an internet browser to a false website is often termed 'pharming'.
- 'Spear-phishing' occurs when phishing is targeted at specific individuals.
- 'Whaling' is a type of phishing that targets high level executives of companies.

Advance fee fraud

- Advance fee frauds are sometimes called '419 scams' or 'Nigerian scams'.
- In these scams the mark is persuaded to part with some money upfront (often allegedly for administrative costs), with the promise of a large return.
- There are many variations of advance fee fraud emails.

Other forms of attack

- Hardware or software keyloggers can be installed on a system to capture confidential information.
- Help-desk attacks involve a fraudster pretending to be a helpdesk, pretending to be a user in need of support or overhearing a call to a helpdesk.
- There are many variations of internet auction fraud, sometimes involving shill-bidding, or misrepresentation of items.
- Other forms of fraud include lottery fraud, pharma-fraud and charity and disaster relief frauds.

Human susceptibility to online fraud and identity theft

- There are several reasons why humans may be susceptible to seemingly obvious attempts at fraud.
- Many of these are based on the psychology of human decision making.
- The salience of certain cues in emails may make a user more likely to believe the sender is from a legitimate agency.
- Projected authority of the sender is a key factor in a decision whether or not to comply with a fraudulent email, particularly if the potential victim feels that the sender may be unhappy with a lack of cooperativeness.

 Back to top

- Advance fee fraud emails use a wide variety of tactics to engage the recipient, including serious tone, cordial greetings, typographical errors and 'foot in the door' techniques.
- Cognitive dissonance occurs when an individual holds simultaneous but conflicting views and seeks to eliminate one. This may explain why an individual who has already lost money during a fraud may continue to engage with the fraudster.
- Confirmation bias describes how individuals seek information that confirms a tentatively held hypothesis, and thus may explain why individuals do not notice cues that would disconfirm such a belief.

Effects on victims

- Identity theft and online fraud may have a variety of effects on victims – including both financial and psychological effects.
- Often banks or credit organisations cover losses relating to identity theft.
- Some authors and researchers have suggested that phishing and identity theft may have psychological effects on victims. These include embarrassment, depression and other maladaptive psychological and somatic symptoms.
- Some victims may also experience secondary victimisation.

Prevention methods

- Identity theft and online fraud has been enabled by the growing diversity of online behaviours.
- Several methods of preventing these crimes have been suggested. These include:
    - Improving public awareness of risks
    - Encouraging users to protect details of financial accounts
    - Encouraging users to choose strong passwords
    - Encouraging companies to inform their customers about risks

- Imposing more severe penalties for offenders
- Using newer technologies such as biometrics.