Financial Transactions and Fraud Schemes

Computer and Internet Fraud
Computer Hacking

- *Hacking* refers to the use of technology to gain unauthorized access to sensitive information on a computer system.
Methods Used to Gain Unauthorized Access

- **Password Cracking**
  - An automated process by which an attacker attempts to guess a system user’s most likely passwords

- **Social Engineering**
  - An attacker deceives victims into disclosing personal information or convinces them to commit acts that facilitate the attacker’s intended scheme
Methods Used to Gain Unauthorized Access

- **Phishing**
  - Manipulates victims into providing sensitive information by falsely claiming to be from an actual business

- **SMiShing or Tishing**
  - Phishing by use of text messages

- **Pharming**
  - Malicious website that imitates a legitimate one

- **Piggybacking/Impersonation**
  - Physically (following behind someone), or
  - Electronically (sitting down at terminal)
Data Manipulation and Destruction

- Malware
- Wire Tapping
  - Tapping into a computer’s communication links to read info being transmitted
- Buffer Overflow Exploits
- Privilege Escalation Exploits
Malware

- *Malware* is an umbrella term for any kind of malicious software, including viruses, worms, Trojans, and spyware.

- Can come from:
  - Files downloaded from the Internet
  - Freeware and shareware
  - Email attachments
Types of Malware

- Viruses
- Worms
  - A worm is a self-replicating program that resides as a file on a system, executes an autonomous process, and deliberately moves from system to system
- Trojan Horses
  - A program or command procedure that gives the appearance that it is useful, but in fact contains hidden code that causes malicious damage
Types of Malware

- Spyware
  - A type of software that collects and reports information about a computer user without the user’s knowledge or consent

- Keyloggers
  - Monitor and log (or track) the keys pressed on a system’s keyboard

- Crimeware
Measures to Prevent Infection

- Use anti-malware software.
- Do not open email attachments unless they are from trusted sources.
- Regularly update operating system.
- Update with latest security patches.
- In a network environment, don’t place untested programs on the server.
- Don’t allow bootup from a removable device.
- Encourage employees to protect home systems.
Electronic Commerce

- *Electronic commerce*, or *e-commerce*, is the process of two or more parties making business transactions via computer and some type of network.

- Strives to provide its users with the following security goals:
  - Confidentiality
  - Integrity
  - Availability
Electronic Commerce

- Additional information security goals include:
  - *Authentication*: Entities want to make sure that they can determine with whom they (or their computers) are communicating.
  - *Non-repudiation*: Refers to the parties involved in an e-commerce transaction that cannot repudiate (deny) participation in that transaction. Entities need some way to recognize a “signature” between e-commerce parties, just as they rely on written signatures.
Insider Threats

The following are indicators of insider computer fraud:

- Access privileges are beyond those required to perform assigned job functions.
- Exception reports are not reviewed and resolved.
- Access logs are not reviewed.
- Production programs are run at unusual hours.
- Lack of separation of duties exists in the data center.
Computer Security

- Physical Access Controls
  - Locks and keys
  - Electronic access cards
  - Biometric systems

- Technical and Administrative Controls
  - Logical access controls
  - Network security
  - Operating system security
  - Encryption
Computer Security

• **Separation of Duties**
  • Program developers should be separated from program testers.
  • Computer operators should not perform computer programming.
  • End users should not have access to production data outside the scope of their normal job duties.
  • End users or system operators should not have direct access to program source code.
  • IT departments should be separated from information user departments.
Sample Prep Question

1. Which of the following is the definition of the computer manipulation technique known as a “Trojan horse”?
   
   A. Searching for valid access codes or trap doors
   B. Installation of a program or command procedure that gives the appearance that it is useful, but in fact contains hidden code that causes malicious damage
   C. Gaining information about a system using deception, such as someone else’s password
   D. Using several networks in a series in order to avoid detection
Correct Answer: B

- A *Trojan horse* is the installation of a program or command procedure that gives the appearance that it is useful, but in fact contains hidden code that causes malicious damage. This is the most common method used in computer-based frauds and sabotage.
Sample Prep Question

2. Which of the following is a measure that management can take to prevent an organization’s computers from being infected by malicious software?

A. Regularly update the organization’s operating systems.
B. Only allow systems to boot with removable storage devices.
C. Prevent employees from opening any emails with attachments.
D. Require that users re-use passwords for important accounts.
Correct Answer: A

The following are some measures can help avoid infection from a malicious program:

- Regularly update the operating system.
- Do not open email attachments unless they are from trusted sources.
- Consider preventing the system from booting with a removable storage device; this might prevent accidental infection.
- Regularly update with the latest security patches available for the operating system, software, browser, and email programs.
- Encourage employees to protect their home systems as well. Many malware infections result from employees bringing infected storage devices or files from home.
Sample Prep Question

3. Which of the following is a technical or administrative control for securing computer systems and communication networks?

A. Implementing logical access controls
B. Installing a network address prevention system
C. Using an intrusion admission system
D. Implementing privilege escalation
Correct Answer: A

- Common technical and administrative controls used to secure computer systems and communication networks include:
  - Logical access controls
  - Network security
  - Operating system security
  - Encryption
  - Application security
  - Separation of duties

- Privilege escalation is not a control, but is in fact a way hackers gain unauthorized access to a computer system.
Financial Transactions and Fraud Schemes

Bribery and Corruption
Corruption

- *Corruption* involves the wrongful use of influence to procure a benefit for the actor or another person, contrary to the duty or the rights of others.
Bribery Schemes

- *Kickbacks* are improper, undisclosed payments made to obtain favorable treatment without the employer’s knowledge and consent.

- Economic Extortion
  - Demand for a payment
  - “Pay up or else…”
Methods of Making Illegal Payments

- Gifts, travel, & entertainment
  - Wine and liquor
  - Clothes and jewelry
  - Sexual favors
  - Lavish entertainment
  - Paid vacations
  - Free luxury transportation
  - Free use of resort facilities
  - Gifts of the briber’s inventory or services

- Cash payments
- Checks & other financial instruments
- Hidden interests
- Loans
- Payment of credit card bills
- Transfers not at fair market value
- Promises of favorable treatment
Methods of Proving Corrupt Payments

- Three basic ways to prove illegal payments:
  - Turn an inside witness.
  - Conduct a covert or “sting” operation.
  - Identify and trace through audit steps.
Conflicts of Interest

- Occurs when an employee or agent—someone who is authorized to act on behalf of a principal—has an undisclosed personal or economic interest in a matter that could influence his professional role.

- Conflict of interest schemes generally constitute violations of the legal principle that a fiduciary, agent, or employee must act in good faith, with full disclosure, and in the best interest of the principal or employer.
1. Which of the following is TRUE regarding the methods typically used for making corrupt payments in bribery and corruption schemes?

A. Payers often make corrupt payments by selling property to recipients at prices lower than the property’s market value

B. Payers often make corrupt payments by paying off the recipient’s credit card debt

C. Payers often make corrupt payments by offering recipients loans on extremely favorable terms

D. All of the above
Correct Answer: D

- Often, corrupt payments occur in the form of loans. Three types of “loans” often turn up in fraud cases:
  - An outright payment that is falsely described as an innocent loan
  - A legitimate loan in which a third party—the corrupt payer—makes or guarantees the loan's payments
  - A legitimate loan made on favorable terms (e.g., an interest-free loan)

- A corrupt payment can also be in the form of payments toward a party’s credit card debt or transfers in which the corrupt payer might sell or lease property to the recipient at a price that is less than its market value.
Sample Prep Question

2. When an employee or official uses force or fear to demand money in exchange for making a particular business decision, he is engaging in:

A. Bribery
B. An illegal gratuity scheme
C. Economic extortion
D. A kickback scheme
Correct Answer: C

- *Extortion* is defined as the obtaining of property from another, with the other party’s consent induced by wrongful use of actual or threatened force or fear. Economic extortion is present when an employee or official, through the wrongful use of actual or threatened force or fear, demands money or some other consideration to make a particular business decision.
Sample Prep Question

3. Which of the following scenarios is an example of a conflict of interest?

A. An employee has an undisclosed personal relationship with a company that does business with his employer.

B. An employee for a phone installation company works as a fishing guide on weekends, but he does not tell the phone company about his other job.
Sample Prep Question

C. An employee for a pharmaceutical company has an economic interest in a company that does business with his employer and discloses it to his employer.

D. An employee is related to a party that works for one of his company’s vendors and informs his employer of the relationship.
Correct Answer: A

- A *conflict of interest* occurs when an employee or *agent*—someone who is authorized to act on behalf of a principal—has an undisclosed personal or economic interest in a matter that could influence his professional role. Thus, an employee with an undisclosed personal relationship with a company that does business with his employer is engaged in a conflict of interest.
Financial Transactions and Fraud Schemes: External Fraud

Contract and Procurement Fraud
Four Phases of the Contracting Process

- The presolicitation phase
- The solicitation phase
- The bid evaluation and award phase
- The post-award and administration phase
Phases of the Contracting Process

- Presolicitation Phase
  - Need recognition
  - Development of specifications
  - Determination of the method to use for acquiring the goods or services
  - Development of award criteria

- Solicitation Phase
  - Bid solicitation
  - Bid preparation
  - Bid submission
Phases of the Contracting Process

- Bid Evaluation and Award Phase
  - Procuring employees evaluate the bids or proposals
  - Award the contract

- Post-Award and Administration Phase
  - Contracting parties fulfill their respective duties through the performance of their contractual obligations
Collusion Among Contractors

- Complementary Bidding
  - Competitors submit token bids
- Bid Rotation
  - Take turns submitting the low bid
- Bid Suppression
  - Agree not to bid on certain jobs
- Market Division
  - Agree to only bid on jobs in a certain area
Red Flags of Collusion

- Industry has limited competition.
- Same contractors bid on each project.
- Qualified contractors do not submit bids.
- Winning bidder subcontracts work to one or more losing bidders.
- Some bids fail to conform to the essential requirements of the solicitation documents (i.e., some bids do not comply with bid specifications).
- Fewer competitors than usual submit bids on a project.
- When a new contractor enters the competition, the bid prices begin to fall.
Collusion Between Contractors and Employees

- Need Recognition Scheme
  - Employee receives a gratuity or kickback for recognizing a “need” for a particular product or service
  - Unusually high requirements for stock and inventory levels
  - Materials not reordered at optimal point
  - Writing off large numbers of surplus as scrap
  - Failure to develop a list of backup suppliers reveals strong attachment to one supplier
Bid Tailoring Schemes

- Employee with procurement responsibilities, often in collusion with a supplier or contractor, tailors bid specifications to give an unfair advantage to a certain contractor
  - Narrow specifications
  - Broad specifications
  - Vague specifications
Red Flags—Bid Tailoring Schemes

- One or just a few bidders respond to RFP
- Contract is not re-bid when minimum bids are not received
- Unusual or unreasonably narrow or broad specifications
- Requests for bid submissions do not provide clear bid submission information
- Unexplained changes in contract specifications from previous proposals
- High number of awards to one supplier
Bid Manipulation Schemes

- Altering bids
- Extending bid opening dates without justification
- Prematurely opening bids
- Discarding or losing a bid or proposal
- Disqualifying bids for improper reasons (e.g., voiding bids for alleged errors in specifications)
- Limiting the time for submitting bids so that only those with advance information have adequate time to prepare bids or proposals
Defective Pricing Schemes

- Negotiated contracts
- Defective pricing methods:
  - Using outdated cost schedules
  - Subcontracting to affiliated companies at inflated rates
  - Failing to disclose discounts and credits
Performance Schemes

- Non-Conforming Goods or Services
  - Product substitution, failure to meet specifications

- Detection
  - Examine contractor’s statements, claims, invoices, and supporting documents.
  - Segregate and identify the source of the suspect goods or materials.
  - Review the inspection and testing of reports.
  - Conduct routine, unannounced inspections.
  - Interview personnel about noncompliance.
Performance Schemes

- Change Order Abuse
- Cost Mischarging
  - Accounting mischarges
  - Material mischarges
  - Labor mischarges
- Accounting Mischarges
  - Knowingly charges unallowable costs to the buyer
  - Office supplies, personal trips, anything not allowed under the contract
Presolicitation Phase

- Need Recognition
- Bid Tailoring
  - Narrow Specifications
  - Broad Specifications
  - Vague Specifications
  - Change Order Abuse
Post Award and Administration

Product Substitution
- Inferior/substandard Material
- Untested or Falsified Testing
- Used/Surplus Parts
- Counterfeit

Cost Mischarging
- Accounting Mischarges
- Material Mischarges
- Labor Mischarges
Sample Prep Question

1. AD&N Railway solicits bids to lay several miles of new railroad track. Bob, who works for AD&N, writes the specifications for the project to provide that AD&N will only contract with companies that have more than 25 years of experience. Bob knows that only B&P Track Co., one of the prospective bidders, has more than 25 years of experience. What type of procurement fraud scheme has taken place?

A. Bid division
B. Bid tailoring by drafting narrow specifications
C. Bid tailoring by drafting broad specifications
D. Bid suppression
Correct Answer: B

- Bid tailoring schemes occur when an employee with procurement responsibilities, often in collusion with a supplier or contractor, tailors bid specifications to give an unfair advantage to a certain contractor. Individuals might tailor a bid by drafting narrow specifications. In these schemes, a corrupt employee tailors the bid specifications to accommodate a vendor’s capabilities and to eliminate other competitors so that the favored contractor is effectively guaranteed to win the contract.
Sample Prep Question

2. An unscrupulous contractor could engage in a cost mischarging scheme by taking which of the following actions?

A. Charging unallowable costs to the buyer
B. Misrepresenting the nature of unallowable costs to make them appear as allowable costs
C. Charging costs in a category where costs are limited to other cost categories that do not have such limits
D. All of the above
Correct Answer: D

- Cost mischarging schemes occur when a contractor charges the procuring entity for costs that are not allowable, not reasonable, or cannot be allocated to the contract directly or indirectly. Accounting mischarges occur when a contractor knowingly charges unallowable costs to the buyer by concealing or misrepresenting them as allowable costs, or by hiding them in accounts that are not usually closely audited. A variation of this type of scheme involves circumventing the limits for certain cost categories by charging those expenses to other cost categories that do not have such limits.
Sample Prep Question

3. Which of the following is NOT a red flag that might indicate the existence of a need recognition scheme?

A. The purchasing entity has unusually high requirements for stock and inventory levels.
B. The purchasing entity does not have a satisfactory list of backup suppliers.
C. The purchasing entity has large numbers of surplus items written off as scrap.
D. The purchasing entity’s materials are being ordered at the optimal reorder point.
Correct Answer: D

- Red flags that might indicate a need recognition scheme include:
  - An organization with unusually high requirements for stock and inventory levels
  - An organization’s materials are not being ordered at the optimal reorder point
  - An organization’s tendency to write off large numbers of surplus items as scrap
  - An organization’s failure to develop a satisfactory list of backup suppliers