Save Computers from Hackers Attacks

- **The Computer Emergency Response Team** (CERT), based at Carnegie Mellon University, was established in 1988 in response to the Internet Worm
- The experts of CERT helped system administrators investigate and protect against intrusions
- The CERT reported newly discovered security flaws:

i) to government agencies

ii) to the public and

iii) to the defenses

Save Computers from Hackers Attacks

- CERT offers:
- i) **Security advice**
- ii) **Provides immediate security warnings to business subscribers** and
- iii) **Planned to develop a system to certify the security of business computer networks**
- Although CERT itself was the victim of a denial-of-service attack in 2001, bogging down its Web sites for 30 hours

Save Computers from Hackers Attacks

- The **Financial Services Information Sharing and Analysis Center** was formed by large banks to provide early warnings of computer attacks
- **Attrition.org** provides subscribers with quick information about hacking incidents (e.g. FBI is a subscriber)
- Many law-enforcement agencies established special units to deal with computer crime (e.g. FBI's National Computer Crime Squad)

Save Computers from Hackers Attacks

- The FBI formed the **National Infrastructure Protection Center (NIPC)** to protect against hackers
- The **NIPC** participated in the investigations of the Melissa virus and mafiaboy's denial-of-service attacks on major Web sites
- However, **the NIPC was strongly criticized by**:

1. Congress' investigative agency
2. The General Accounting Office
3. Industry group and others for failing to warn companies under attack by hackers for weeks or months after the NIPC knew of the attacks

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Credit Cards, Identity Theft, Cell Phones

1. Credit Cards
2. Automated Teller Machine (ATM)
3. Telephone Calling Cards and
4. Cell Phones use computer technology to give us convenience but expose us to risks we did not have before

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Most of the people would not casually carry around hundreds or thousands of dollar in cash but
- a credit card, ATM card or calling card gives the holder access to large sums

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Credit Card Fraud:
- Loses from credit-card fraud are estimated to be several billion dollars each year
- (Some security and law-enforcement officials believe it is higher than what is reported by the industry)
- There are many varieties of credit-card fraud.

o Account numbers are stolen by store clerks and by thieves who search the trash near stores for receipts or

o Just call people and ask for them with some pretext (e.g., telling the person he or she own a prize but the card number is needed)

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Cards are stolen by large, well-organized theft and by individual purse-snatchers
- Several dozen people were convicted in one case where Northwest Airlines employees stole new cards from the mail transported on Northwest's airplanes.
- The employees used some of the cards themselves and sold others.
- As estimated $7.5 million was charged on the stolen cards
- On the Web, credit card numbers can be stolen in transmission and from stored files, if secure servers are not used

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- An e-commerce security service provider calls credit-card fraud on the Web “electronic shoplifting”
- Most fraudulent charges are made with stolen cards or account numbers
- In some cases, a customer charges expensive items on his or her own card, then claims not to have ordered or received the goods.

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Identity Theft
- In our modern world, where most of us live in large communities, cash checks at stores where

o we are not personally known and borrow money from strangers

o Our identity has become a series of numbers:

1. Social Security Number
2. Driver’s License Number
3. Account Numbers

o Computer files:

1. Credit history
2. Driving record

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- Identity theft, where a criminal assumes the identity of the victim and runs up large credit-card charges or cashes bad checks, is a growing problem
- It might cost the victim little in direct monetary loses, but much in anguish, disruption of his or her life and legal fees

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- For example:
- **A man applied for numerous credit cards** in the names of real people who had good credit records; the people whose names were used did not know the accounts existed
- The man lived well for two years, took several trips to Europe, and **fraudulently charged more than USD500000** before being caught and sent to prison.
- A part-time English teacher at a California junior college used the Social Security Numbers of some of her students, provided on her class lists, to open fraudulent credit-card accounts.

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- ATM Fraud:
- A few cases illustrate how automated teller machine (ATM) frauds work. The first is an insider case:
  - o A man who worked for a company that installed ATM machines had access to the machines, using the installer's password.
  - o He wrote software to capture the account numbers and PINs (Personal Identification Number) used by customer, then made fake cards, encoded to mimic the real ones.

Fraud Embezzlement, Sabotage, Information Theft and Forgery

- It is very easy for thieves to get account numbers and PIN numbers of ATM cards.
- They use **binoculars, telescopes and video cameras** to spy on **customers and PINs**
- Then they collect **discarded receipts** which contained **account numbers**.
- The location of the **ATMs often in public places**, **made the spying easily**.

BIOMETRICS

- There are many situations where it is important **to identify a person accurately**. **For example:**
- When someone is using:

1. a credit card in a store or
2. online or
3. when someone logs on to a computer system
4. Credits cards can be counterfeited; password can be stolen or guessed
5. Is there any "**foolproof**" way to identify someone?

BIOMETRICS

- Biometrics are biological characteristics that are unique to an individual.
- They include:

1. Fingerprints
2. Voiceprints
3. The face
4. Hand geometry
5. Retina scans and
6. DNA (deoxyribo nucleic acid) which is found in the nucleus cell.

- Biometric technology for identification applications is rapidly developing worldwide

BIOMETRICS

- DNA matching has freed numerous innocent people who had been mistakenly convicted of such serious crimes as rape and murder in the last few years.
- The main application of Biometrics is to ensure security and prevent fraud
- Some computer systems require a thumbprint match to log on to a computer, **physically or over Net**, reducing access by hackers
- To reduce the risks of terrorism several airports use fingerprint identification systems to ensure that only employees enter restricted areas

BIOMETRICS

- Some states use a face scanner and digital image matching to make sure a person does not for extra driver's licenses or welfare benefits with different names.
- You can use biometrics information to open your door by touching a scanner with your finger avoiding keys to loss, forget, or drop while carrying packages.