Informatics Ethics and Law

Prof. Dr. Eşref ADALI

Cybercrime

3

Cyber Attacks and Frauds

Attacks and frauds against information systems are classified from different angles:

- Active and Passive attacks and frauds
- Internal and External attacks and frauds
- Purposeful attacks and frauds

Classificaton of Cyber Attacks

Cybercrime is a crime in which a computer is the object of the crime or is used as a tool to commit an offense.

Active Attacks

Aim to

- Read information
- Change data
- Clear data
- Interrupt activities
- Give damage to the system resources

Passive Attacks

Aim to

- Read information

Internal and External Attacks

Internal Attacks and Frauds

Internal fraud make by member of staff against the organization.

- Payment
- Procurement
- Travel and subsistence
- Personnel management
- Exploiting assets and information
- Receipt

Internal fraud can range from compromising customer or payroll data to inflating expenses to straightforward theft.

Sometimes it is an attack purely for personal financial gain.

External Attacks and Frauds

A person or a group or an organization make attack for:

- Read information
- Change data
- Clear data
- Interrupt activities
- Give damage to the system resources
- Blocking of operations
- Financial gain

External attacks aim to financial gain or make damage to system.

Classificaton of Cyber Attacks

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society

Internal Attacks

- Salami slice
- External expert
- Virtual time bomb
- Information theft

Salami Slice

- Transferring the small quantity that emerge at the end of the interest calculations to the private account in the bank, resetting them in the customer account.
- In the car rental company, the vehicle fuel tanks are defined larger and more money is received from the customers and this money is transferred to the special account.

Legal Review

The programmer, who made changes to the program used to calculate interest rates on client accounts, stole money from the accounts of customers and the bank. It is therefore guilty in terms of law.

Evaluation in Terms of Ethics

The programmer, who added the salami slice program to the banking software, broke the ethical rules of his organization. As a result of violating the ethical rules, the organization suffered a loss of respectability.

It violated the ethical rules of the programmer organization that made the salami slice addition to make the vehicles' fuel tanks larger than its real. As a result of violating the ethical rules of the organization he worked for, the organization suffered a loss of respectability.

External Expert

The malicious use of the username and password given to the external specialist to maintain the mainframe computer.

Legal Review

The external expert can change, delete or take action that will benefit him or others by using the right of access provided to him and whose removal is permitted. It is guilty in terms of law in exchange for these actions.

The authority of the organization, which authorizes access to the external expert and acts in a way that is revoked, is also erroneous.

Evaluation in Terms of Ethics

He knows that the right to access the external expert information system is granted to him for certain actions. In addition, these rights were granted because he was trusted. It is against ethical values to use the access authority other than its purpose.

Virtual Time Bomb

Adding a program into the software that will corrupt programs and data when the time comes.

Evaluation in Terms of Ethics

Someone who works as a programmer in an organization cannot act in a way that will harm the organization. Therefore, he / she has no right to embed bomb-type programs in the information system.

Ethical rules of every trade have been formed. Organizations that produce and sell software must comply with these ethical rules. In this context, for whatever reason, there is no right to place a bomb program in the software it sells.

Legal Review

The programmer who prepared the bomb program is guilty for aiming to damage the organization's information system in a conscious and planned manner. He is also guilty of putting this program on the computer using the authority provided to him / her. Therefore, his punishment will be heavy.

In the incident at the bank in our country, it was impossible to find the dismissed programmer guilty because the bomb program could not be detected, but it is known that the bank learned lessons from this incident.

When the license or maintenance agreement expires, it is a crime to sell a bomb program that will corrupt the software or data, embedded in the software. When the license agreement expires, the organization cannot take advantage of updates and patches if it continues to use this software. Maintenance support is not provided to the organization whose maintenance agreement has ended.

Information Theft

- It is seen that the information regarding the valuable customers of the bank branch is transferred to the neighboring bank. The person making this transfer starts to work at the neighboring bank.
- The news of an executive who sold all the technical information of a rifle produced by the organization he was in, to a competitor, was published in the press.
- It is known that citizenship information in the MERNIS database is published on foreign websites.

Legal Review

- It is a wrong behavior for someone working at the bank to transfer customer information to another bank in return for benefit. However, this action is unlikely to be proved and the person found guilty.
- It is a crime in terms of law to sell the technical information about the production of rifle for a benefit. If the rifle produced especially has the feature of being a national rifle, it is punished with a second penalty for selling the national secrets.
- It is unacceptable to transfer the records in the MERNIS database out of the institution. How this leak occurred has not been precisely determined. Therefore, it is not clear whether it was done consciously or unconsciously.

Evaluation in Terms of Ethics

- An official working in an organization such as a bank must know the bank's code of ethics. These ethical rules tell customer information to remain confidential within the bank. Therefore, transferring customer information to another bank or organization cannot be considered an ethical behavior.
- The behavior of the top manager of the rifle-producing organization is not acceptable. The organization is against ethical rules. It is also against national values.
- If we assume that the data about citizens at MERNIS are unconsciously taken out, we can say that those who do this sloppy behavior violate the ethical rules.

External Attacks

- Stealing information from the information system
- Changing the information
- Deleting information
- Interrupting or stopping the operation of the computer

Steal, Change or Delete Information

The act of entering, stealing, changing or deleting an information system without the right to access it

Legal Review

- Entering an unauthorized information system can be compared to entering a residence or office without permission. It is a crime regardless of its purpose by trying to fit the key in the lock or entering the house through a door or window without security measures. To say that he made this entrance to reveal the security vulnerability of the house does not alleviate the crime.
- Stealing, changing or deleting information in the system after entering into an information system without permission is a criminal offense.
- Entering the information system without permission, stealing data, changing and deleting data is defined as a crime in our criminal laws.

Evaluation in Terms of Ethics

Entering an information system without permission, stealing, changing or deleting data are wrong behaviors according to general ethical rules.

Prevention of Information System Operation

The act of causing disruption in the services provided by occupying an information system.

Legal Review

- Preventing, disrupting or stopping the operation of an information system is defined as a crime in our laws. However, it is not easy to identify the manager of the blocking with robot computers. Even if it is detected, it is difficult to catch it outside the country. There is not much that can be done, especially if the administrator conducting such attacks is supported by another country.
- Such behaviors are mostly carried out by certain groups or intelligence agencies of a country.

Evaluation in Terms of Ethics

To render the computers of a country that is considered as a competitor or an enemy in an over-busy state cannot be interpreted with ethical values.

Internet Banking Fraud

Key loger: It is very difficult to learn the bank account number and password of a customer by entering the computers of the bank. The communication between the client's computer and the bank's server is encrypted, so the line cannot be obtained by listening. This information can be obtained with a spy program is placed on the customer's computer.

Screen Shoter: Banks switched to virtual keypad application to close the security gap noticed by the emergence of key loger programs. In response to this application, which is thought to close the security vulnerability in the first stage, the programs that took and sent the copy of computer screen were used by Screen Copy robbers.

One-Time Password: One of the methods developed for hiding the customer password when logging into Internet bank is the One-Time Password (OTP) method. In the OTP method, a program given to the customer or a hardware (smart key) with which this program runs produces a password in accordance with a certain algorithm.

Credit Card Fraud

Issuer						Unique number of card									E
4	4	1	1	0	5	1	2	3	4	5	6	7	8	9	7
4x2=8	4	1x2=2	1	0x2=0	5	1x2=2	2	3x2=6	4	5x2=10	6	7x2=14	8	9x2=18	7
8	4	2	1	0	5	2	2	6	4	10-9=1	6	14-9=5	8	18-9=9	7
8	4	2	1	0	5	2	2	6	4	1	6	5	8	9	7

Methods of robberies with credit card are:

- Making extra copies
- Using real credit card information
- Changing the information on the card

Known but Crimes Committed Through Informatics

Encourage to Suicide: People who encourage or even provoke people with mental health to commit suicide are seen in Internet. It is heard that these people form teams and are working to commit suicide to the person they choose. There are many examples on this subject in Internet.

Facilitating the Use of Drugs or Stimulants: Communities formed on Internet encourage the use of drugs or stimulants and can provide guidance for the provision of such substances. It is also witnessed that drugs or stimulants are marketed by e-commerce method. Facilitating drug delivery through e-commerce made it necessary to take measures in this direction.

Providing Hazardous Substances for Health: Actions similar to drugs are also seen for substances that are dangerous to health.

Providing Space and Opportunity for Gambling: Gambling is prohibited in some countries and is free in some countries. Countries where gambling is prohibited want to apply their laws on this issue on Internet. However, gamblers are located in countries where gambling is free and they can continue their business. Countries banning gambling can only work to prevent money traffic in combating gambling.

Known but Crimes Committed Through Informatics

Obscenity: Obscenity is considered as a concept that varies from society to society. In addition, according to one view, interest in obscene objects can be considered as the preference of the person. For this reason, each country defines obscenity according to its tradition, customs and moral understanding.

Prostitution: Being an easily and cheaply accessible environment in Internet sharing and announcing information also provides opportunities for prostitution actions. Also, it is not easily understandable whether the action was with consent or money. The subject can be evaluated differently according to the customs and traditions of the countries.

Sexual Abuse of Children: The only issue that the whole world consensus about crimes committed in the informatics environment is the sexual abuse of children. The problem experienced in this regard appears in the **definition of the child**. There is no consensus on whether the child will be evaluated by age or body development.

In the laws of our country, it is considered a crime to produce pornographic images for child abuse, to make distribution and even to have them on a person's computer.

Crimes Against Private Life

Learning and spreading the information about the personal information of the people is an opposite to the general morality. We also know that this issue is given importance in the **United Nations Universal Declaration of Human Rights**. These basic principles are also included in the Constitution of Turkey.

People have the freedom to communicate, and it is forbidden to listen, record and publish the communication. Listening can only be made with a decision made by the judge when deemed necessary.

Information about the private life of the person cannot be published. This type of information is protected by law. However, this law is interpreted more flexibly for people who are closely watched by the society and whose lives are in the press.

Today, data about a person is kept in different informatics environments. When these data are collected individually or together, they provide important information about the person. Since the information formed may affect the life and future of the person, it should be protected.

Personal data is defined as any information about a person. In this context, the most basic identity information of the **personal information**, as well as his **race, ethnicity, political thought, philosophical belief, religious, sect** or other **beliefs, disguise** and **outfit, association, foundation or union membership, health, sexual life, criminal conviction and security measures. related information** and **biometric** data are also included.

Crimes Against Assets

Stealing a person's Money or property using information systems is called qualified theft. Internet banking robberies and credit card robberies are evaluated within the scope of qualified theft and fraud.

It is becoming increasingly common to carry out financial transactions over Internet and its use is easily foreseen. The reason for this is obvious. It is easy for a bank customer to perform banking transactions from the place where he lives, with the ease provided by the Internet environment. Internet banking also greatly reduces the costs of banks. Therefore, Internet banking is a profitable practice for both the customer and the bank and will become more and more widespread.

Lost or Stolen Card: It is the most common fraud to make robbery by getting cards that have been forgotten somehow or by using the cards they have stolen.

Identity Theft: Identity theft method is a robbery method applied only for cards with magnetic stripe. It is done by changing the information in the magnetic stripe of the credit card.

Types of Attacks

Virus attacks: The purpose of those who produced viruses that disrupt programs or data in computers was considered as recognition and personal satisfaction. However, it has been witnessed that they aim at increasingly bad goals.

- It is a shame to harm people by producing a virus program and to ignore ethical values.
- Legal action can be taken against them by looking at their damages.
- Those who made the virus program especially to leak money are undoubtedly qualified robbers.

Cryptolocker: They send trickery e-mail. This letter may be in the form of a telephone bill. The invoice amount seems unusual. To see the detail of invoice, you are asked to press the button. When the button is pressed, a malicious program is installed on the person's computer. The installed program compresses all data and documents encrypted on the computer. Those who take this action later say in the e-mail that they send, we will send the password if you pay this much money.

Attacks on Computer Controlled Systems: Many systems are managed by computers today. For example oil pipelines, water, electricity and gas distribution systems of cities, traffic control system. Computer controlled systems have remote access. Therefore, they are open to all kinds of attacks.