ATT(H)ACK-ANTI-CYBER CRIME LAW IN SAUDI ARABIA

Topics

- Types of Cyber crimes
- Introducing Anti- Cyber Law

Downside of World Wide Web

With raise of the technology, evil minds keep themselves updated with indefinite and unethical routes through which they can trespass the scope of privacy of an individual or entity.

With this malignant issue fast rising, the legislature across the world have codified laws to tackle the menace of cyber-crimes.

What is a Cyber–Crime?

A crime that involves a computer and a network

Classification of Cybercrimes

Cybercrimes are broadly categorised into three categories namely

1. Cyber against **Individual**
2. Cyber against **Property**
3. Cyber against **Government**

Classification of Cybercrimes

1. **Cyber against Individual**
   - Email Spoofing
   - Spamming *(Spamming is the sending of an unsolicited email. What this means is that you send an email, generally an ad of some sort, to someone who has not requested to receive that information from you)*
   - Phishing *(**Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication)*
   - Cyber Stalking (*to harass or frighten someone, for example by sending threatening emails)*
   - Cyber Defamation *(**Cyber defamation** is not a specific criminal offense, but rather **defamation** or **slander** conducted via digital media, usually through the Internet)*
   - Cyber Pornography

Classification of Cybercrimes

2. **Cyber against Property**

- Credit Card Skimming
- Intellectual Property Crimes
- Software Piracy
- Identity Theft
- DDOS attack, hacking, virus transmission
- Cybersquatting, copyright infringement, IPR violations

Classification of Cybercrimes

3. Cyber against Government

- Denial of Service attack(Dos)
- E-mail Bombing
- Logic Bombing
- Data Diddling
- Sale of Illegal Articles (such as drugs, weapons, wildlife etc. is being facilitated by the Internet)
- Cyber Terrorism
- Pirated software
- Accessing confidential information

Data Diddling

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done.

Using this technique, the attacker may modify the expected output and is difficult to track.

This is one of the simplest methods of committing a computer-related crime

Data Diddling

Illustration 1
A keyboard operator processing orders at department store changed some delivery addresses and diverted several thousand dollars' worth of store goods into the hands of accomplices.

Illustration 2
A ticket clerk issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

Salami Attacks

These attacks are used for committing **financial crimes**. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say SAR 2 a month) from the account of every customer.

No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

The attack is called "**salami attack**" as it is analogous to slicing the data thinly, like a salami.

Trojans (Keyloggers)

Keyloggers are regularly used to log all the strokes a victim makes on the keyboard. This is quite threatening if a key logger is installed on a computer which is regularly used for online banking and other financial transactions.

Web Jacking

Just as **conventional hijacking** of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom.

The perpetrators have either a monetary or political purpose which they try to satisfy by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

Combating Cybercrime in KSA

The Anti-Cybercrime Act is the Kingdom's first set of laws designed to combat the growing threat of IT crimes.

Saudi Anti-Cybercrimes (the Law) was issued by Royal Decree Number M/17, dated 26th March 2007.

- This law consist of 16 provisions/articles, which set out the key definitions, scope and objective, sentences and fines.

Combating Cybercrime in KSA

1. Enhancement of information security.
2. Protection of rights pertaining to the legitimate use of computers and information networks.
3. Protection of public Interest, morals, and common values.
4. Protection of national economy.

Saudi Anti-Cyber Crime Law 2009 Article 3

CRIME
Spying on, interception or reception of data without legitimate authorization
Unlawful access to computers with the intention to threaten or blackmail any person
Unlawful access to a web site, or hacking a web site with the intention to change its design, destroy or modify it
Invasion of privacy through the misuse of camera-equipped mobile phones and the like.
Defamation and Infliction of damage upon others the use of various information technology tools and devices
Penalty: Prison Not exceeding 1 year and Fine up to 500,000 SAR

Saudi Anti-Cyber Crime Law **Article 4**

Acquisition of movable property or bonds through fraud or use of false name or identity

Illegally accessing bank or credit data with the intention of obtaining data information, the position of funds or types of services offered

Penalty: Imprisonment for a period not exceeding 3 years and a fine not exceeding 2 million riyals, or both

Saudi Anti-Cyber Crime Law **Article 5**

Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data
Causing the information network to halt or breakdown, removing , leaking or modifying or reconstructing existing or stored programs or data.
Obstruction of access to, distortion, and causing the breakdown of services by any means
Penalty: Imprisonment for a period not exceeding 4 years and a fine not exceeding three million riyals, or both

Saudi Anti-Cyber Crime Law Article 6

Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers
The preparation , publication and promotion of material for pornographic and gambling sites which violates public morals
The construction or publicizing of website on the information or data of any type, the IT system(s) or computer to promote or facilitate human trafficking
The construction or publicizing of a website on the information network(s) or computer linked data to act, deal or trade in narcotic and psychotropic drugs
Penalty : Imprisonment for a period not exceeding 5 years and a fine not exceeding three million riyals or both

Saudi Anti-Cyber Crime Law **Article 7**

The construction or publicizing of a website on the information network or on a computer for terrorist organizations to facilitate communication with leaders or members of such organizations, finance them, promote their ideologies, publicize methods of making incendiary devices or explosives or any other means used in terrorist activities

Unlawful access to a website or an information system directly or through the data network or any computer with the intention of obtaining data jeopardizing the internal or external security of the State or its national economy.

Penalty : Imprisonment for a period not exceeding 10 years and a fine not exceeding five(5) million riyals or both

Saudi Anti-Cyber Crime Law

Article 9:

Any person who incites, assists or collaborates with others to commit any of the crimes stipulated in this law shall be subject to a punishment not exceeding the maximum punishment designated for such crimes, if the crime is committed as a result of said incitement, assistance or collaboration, and he shall be subject to a punishment not exceeding half the maximum punishment designated, if the intended crime is not committed.

Saudi Anti-Cyber Crime Law

The Saudi Anti-Cyber Crime Law aims to secure the safe exchange of data, protect the rights of users of the computers and the internet and to protect the public interest and morals as well as people's privacy.

The Anti-Cybercrimes law has been amended to initiate **legal proceedings** against **social networking** sites such as Twitter for allowing accounts aiming at posting or in general dealing with adultery and the acts of homosexuality.

Recap of Cyber Crimes

Email Bombing

An **email bomb** is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Logic Bombing

A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Email Spoofing

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

Cyberstalking

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization for reasons of anger, revenge or control. It may include false accusations, defamation and slander.

Cyber-defamation

Cyber defamation is the publication or broadcast through any internet based media about slanderous statement about an individual or business that can be proven to be false and is published or spoken with the intention of harming that entity's reputation.

Credit Card skimming

Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction.

Salami Attack

Salami attacks are used for committing financial crimes in which the criminal make the alteration so insignificant that in a single case it would go completely unnoticed..

Software Piracy

Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold.

Identity Theft

Identity theft, also known as identity fraud, is a crime in which an imposter obtains key pieces of personally identifiable information, such as Social Security or driver's license numbers, in order to impersonate someone else.

Domain Name dispute

The **disputes** that arise over **domain names** involve "second level" domain names. Two identical second level domain names cannot coexist under the same top level domain. The second level name is the name directly to the left of the top-level domain name in an Internet address. For instance, in the address "www.microsoft.com", the second level domain name is Microsoft.

Data Diddling	**Data Diddling** is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done.
Sale of Illegal Articles	The **illegal items** are on display or **sale** online. Items ranging from drugs, narcotics, weapons, wildlife are easily available in the cyber world, be it bulletin boards, social networking sites or dedicated websites.
Denial of Services(DoS)	A **denial-of-service** attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources
Identity Theft	**Identity theft,** also known as identity fraud, is a crime in which an imposter obtains key pieces of personally identifiable information, such as Social Security or driver's license numbers, in order to impersonate someone else.
Financial Crime	**Financial Crime** involve money laundering where funds are laundered and moved around the globe using shell companies, intermediaries, fund managers, money transmitters etc. It also involves frauds ranging from cheque fraud, credit card fraud, medical fraud, bank fraud and scams and confidence tricks like the Nigerian fraud