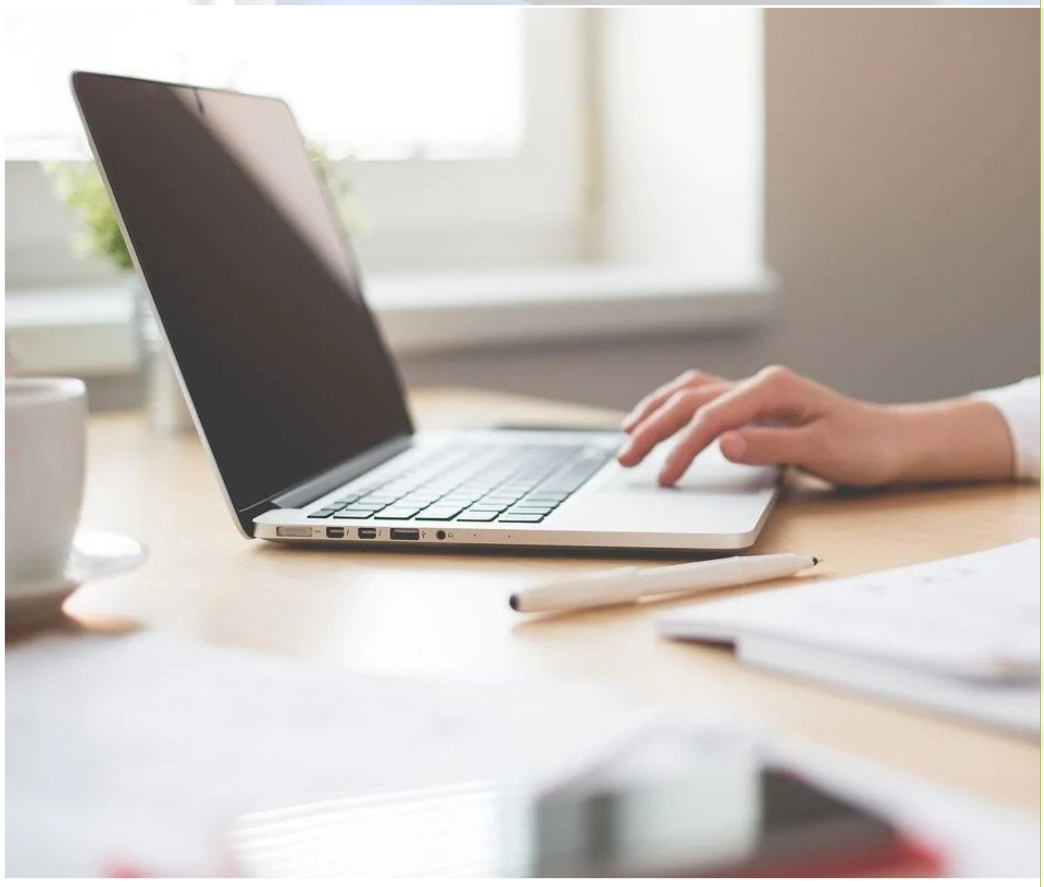
CRYPTUS CYBER
SECURITY PVT. LTD.

Module :- 1

Introduction to ethical hacking



What is Information Security

INFORMATION SECURITY
==========

DATA | INFORMATION

Data : Raw Facts
Information : Processed data or collection of data

Information Security : Covering up all the security aspects related to Information Technology.

ETHICAL HACKING / CYBER SECURITY
==========

Ethical - Means legal practices which should be performed.

Hacking - Hacking means accessing any data, information or any system with the permission of individual.

Hackers - Hackers are the most skilled and technical people who are profiecient in understanding the technical aspects.

TYPES OF HACKERS

1. BLACK HAT HACKERS - THese are the bad people whon access and gain resources of any individual for the sake of there own wealth. Parents wala person, usually comes in newspaper Eg. Shadow Brokers

2. WHITE HAT HACKERS - THese are those people who gains access and tamper the resource for the sake of the individual. EG. Rahul Tyagi, Abhijeet Singh, Sanjeev Multani ,Prabhankar Tripathi etc.

3. GREY HAT HACKERS - These are those hackers who hacks and gains resources for the sake of the society and culture.
Eg. Anonymous, Edward Snowden etc.

Other Categories

1. Script Kiddies - These are those people who steals the programs, ideas or any other method of hacking and perform hacks without any knoweledge.

2. Noobz - These are the new born technical babies who just arrived in the field of cyber security.

3. Crackers - These are those people who are good in cracking into a particular machine or a authentication check ,they crack into systems for a malicious purpose.

TYPES OF INFORMATION

1. Confidentials INformation - Aadhar Cards, Passwords, Birth Certificates, PAN Cards etc.
2. Financial Information - Financial Statements, Bank Details, Login Credentials for banking poractices etc.
3. Health Information - Policies, Diseases etc.
4. Personal Information - Address, Phone Numbers, DOBs etc.

Information Technology Act, 2000

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. It is based on the *United Nations Model Law on Electronic Commerce 1996* (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

Offences

List of offences and the corresponding penalties:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique	Imprisonment up to three years, or/and with fine up

		identification of another person.	to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.

67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures	Imprisonment up to ten years, or/and with fine.

		access or attempts to secure access to a protected system, then he is committing an offence.	
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000

International responses

G8

Group of Eight (G8) is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada.

In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

United Nations

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology.

ITU

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cyber security issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS).

In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime.

In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society.

Council of Europe

Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviours, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. [8] It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

European Union

The coat of arms of the European Cybercrime Centre

In 2001, the European Commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

In 2002, EU presented a proposal for a “Framework Decision on Attacks against Information Systems”. The Framework Decision takes note of Convention on Cybercrime, but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

Commonwealth

In 2002, the Commonwealth of Nations presented a model law on cybercrime that provides a legal framework to harmonise legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Convention on Cybercrime.

ECOWAS

The Economic Community of West African States (ECOWAS) is a regional group of west African Countries founded in 1975 it has fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cybercrime in ECOWAS that provides a legal framework for the member states, which includes substantive criminal law as well as procedural law.

GCC

In 2007, the Arab League and Gulf Cooperation Council (GCC) recommended at a conference seeking a joint approach that takes into consideration international standards.