Cyber crime

Learning Outcomes

LO1	Fundamental understanding and Information on Cyber Crimes, Digital Forensics Objectives and Incident Detection and Response Reports.
LO2	Learn on how to prepare investigation on computer-related incidents or crimes and summarize.
LO3	Understand on digital forensics process, models and analysis by taking a systematic approach
LO4	Explore on evaluating needs, validating and testing digital forensics tools, Generating Incident Report Findings, and Emerging Cybercrime Trends and Issues

Course objectives

CO1	Enhancing awareness of recent Cyber Crime trends and learn Investigating Cyber Crimes
CO2	Introduce Cyberspace Infrastructure attacks and handling Organization Cybersecurity Issues
CO3	Understand Digital Forensics Process, Models, Analysis and Validation, Incident Detection and Response

Text Book(s)

T1	Computer Forensics and Cyber Crime - An Introduction 3rd Edition by Marjie T. Britz, Ph.D., Professor of Criminal Justice, Clemson University
T2	Bill Nelson, A. Philips, F. Enfinger, C. K. Steuart, Computer Forensics and Investigations, Course Technology (Cengage Learning), Indian edition, 2009
T3	Incident Response & Computer Forensics, 3rd Edition by Jason T. Luttgens and Matthew Pepe and Kevin Mandia
R1	Guide to Computer Forensics and Investigations: Processing Digital Evidence 5th Edition by Bill Nelson, Amelia Phillips and Christopher Steuart
R2	The Basics of Digital Forensics, by John Sammons
R3	Computer Network Security and Cyber Ethics 4th Edition, by Joseph Migga Kizza
R4	Computer Forensics_ Investigating Network Intrusions and Cyber Crime: EC-Council Press

Expectations from the course

- Understand Psychology
- Saving lives and finances
- Secondary income

FORM 5
THE PATENTS ACT, 1970
(39 of 1970)
and
THE PATENTS RULES, 2003
DECLARATION AS TO INVENTORSHIP
[(Section 10(6); Rule 13(6))]

1. Name of the Applicant(s):

We, BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE (BITS), PILANI, Pilani Campus, Vidya Vihar, Pilani, Jhunjunu District, Rajasthan – 333031, India, an Indian company

hereby declare that the true and first inventor(s) of the invention disclosed in the provisional specification filed in pursuance of my / our application numbered _____ dated 14 May 2021 are:

2. INVENTOR(S)

Name	Nationality	Address
Amit Dua	Indian	Birla Institute Of Technology & Science (BITS), Pilani Campus, Vidya Vihar, Pilani, Jhunjunu District, Rajasthan – 333031, India.
Shashank Gupta	Indian	Birla Institute Of Technology & Science (BITS), Pilani Campus, Vidya Vihar, Pilani, Jhunjunu District, Rajasthan – 333031, India.

Dated this 14 May 2021

CYBERCRIMES AND CYBER HYGIENE

AWARENESS FOR NETIZENS

AMIT DUA
AKASH JYOTI SAHOO
NISHEETH DIXIT

challenges that technologies face in cybersecurity

- Supply chain interconnection
- Hacking
- Phishing
- Lack of uniformity in devices used for internet access
- Lack of awareness

Case

- Rahul received a whatsapp forward with a link to a lucky draw game.
- What happened here?
- What could he have done here to prevent the crime?

- “Every case involving cybercrime that I’ve been involved in, I’ve never found a master criminal sitting somewhere in any country. It always ends up that somebody at the company did something they weren’t supposed to do. They read an email, went to a website they weren’t supposed to.“ - Frank Abagnale

Types of Cybercrime

- Phishing:
- Hacking:
- Smishing:
- Vishing:
- Identity theft:
- Cyber stalking:
- Ransomware attacks:
- Through malware:
- VOIP:

- Deepfake:
- Web Jacking:
- Data diddling:
- Denial of services (DoS):
- Drive by download attack
- Watering hole attack:
- Tailgating:
- Juice Jacking:
- Business Email Communication scams:
- Whaling attack:
- Using Digital voice assistants:

Different cyber crimes

- Debit card cloning

What we should do

Make sure you never give your ATM card and pin number to anyone, no matter how close they are

to you. Not even your closest relatives and family members.

Check for extra layering in the area where you insert your card for skimmers.

Also cover the keyboard while entering the pin because there may be suspicious cameras lying

around tracking the keys you enter.

Never share your card details, CVV number and OTP number with anyone over call or in person.

If you ever receive an OTP for any transaction which you did not initiate, then you should

immediately get your credit card and debit card blocked as it is possible that someone has made an attempt to steal your money.

RBI Guidelines

- If a third party was involved and took your money without your knowledge, then the bank is liable to pay you the exact amount that you have lost. If some sort of skimmer device was installed into the ATM because of which your card got cloned without your knowledge, then it is not your liability and the bank has to pay back your amount.

Cont.

- 2. If you lost your money due to some security flaw of the bank, or if your account got hacked, then the bank will have to pay the amount that you have lost.
- 3. Finally if the user has lost his money from his account because of a mistake on his part (shared his OTP orpasswords with another person) then the bank will not pay back the amount because it was entirely the person’s fault.

IT Act

- IT Act Section 66 for Computer Related offences,
- IT Act Section 66C for punishment for identity theft.
- IT Act Section 66D for punishment for cheating by personation using a computer resource.
- IPC Section 419 for punishment for cheating by personation.
- IPC Section 420 for cheating.
- IPC Section 468 for forgery.

No.	Title of the Module
M1	Introduction to Cyber Crime, Digital Forensics and Incident Handling
M2	Foundation for Forensics
M3	Computer Crime and Identity Theft/Fraud
M4	Digital Forensic Process, Analysis and Validation
M5	Disk Structures (File Systems) and Data-hiding techniques
M6	Network and Cloud Forensics; Mobile Device and Security
M7	Digital Forensic Tools and Labs
M8	Organizations and Cyber Crime, Criminology and Organized Crime
M9	Investigating Internet Crime and E-Mail Crime
M10	Cyberspace Infrastructure and Enterprise Security
M11	Incident Detection and Characterization
M12	Incident Response and software Tools
M13	Incident Report Writing
M14	Emerging Cybercrime Trends, Recommendations and Practical Issues
M15	Miscellaneous Topics

- What made me here?

- What is your commitment for this course

5 things to achieve

- Mental strength
- Physical strength
- Do one Challenge early
- Proximity is power
- Giving is actual living