



# CYBER CRIME

## UICSA(RDVV)

- MCA-CYBER LAWS AND INFORMATION SECURITY
- BCA-CYBER SECURITY

DISHA TIWARI

# WHAT IS DIGITAL FORENSICS?

- ❑ Extracting evidence from computers or other digital devices .Usually involves extracting the contents of files and interpreting their meaning.

- ❑ **Cyber Crimes:**

**Cyber crimes** are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.



# CYBER CRIMES

- ❑ *Hacking*
- ❑ *Child Pornography*
- ❑ *Cyber Stalking*
- ❑ *Denial of service Attack*
- ❑ *Virus Dissemination*
- ❑ *Software Piracy*
- ❑ *IRC Crime*
- ❑ *Credit Card Fraud*
- *Net Extortion*
- ❑ *Phishing*
- ❑ *Internet Fraud*



## ❑ Financial Fraud/Online Banking Frauds:

This pertains to anything that  
Uses fraudulent solicitation to  
Prospective victims to conduct  
Fraudulent transactions.

## ❑ Credit Card Frauds And Identity

**Theft:** The unauthorized and illegal use of a  
credit card to purchase property.



# IMPACTS OF DEMONETIZATION IN INDIA:

- ❑ Demonetization Seems To Have Caused A Dip In Online Fraud Cases As Not A Single Complaint Has Been Registered Since The Last 50 Days, Said Officers From The Thane Cyber Cell.
- ❑ **On 8 November 2016, The Government Of India Announced The Demonetisation Of All ₹ 500(US\$7.40) And ₹ 1,000(US\$15) Banknotes Of The Mahatma Gandhi Series.**

❑

"After The Government Ban On Rs 500 And Rs 1,000 Notes, Many Citizens Have Started Using Plastic Money. They Have Also Started Visiting Their Banks On A Regular Basis And Keeping A Check On Their Account Books To Exchange Or Deposit Money. Also, They Have Been In Constant Touch With The Banks. People Have Been Victims Of Cyber Hackers And Card Cloning Experts With An Average Of Seven Complaints Registered Every Day With The Cyber Cell.

Experts Said That The Most Common Way Of Extorting Money From People Is By Calling Them While Posing As A Bank Representative And Telling Them To Renew Their Card In Case Of An Expiry.



## EXAMPLE OF CREDIT CARD FRAUDS:

- ❑ Amit Tiwari had many names, bank accounts and clients. None of them were for real. With a plan that was both ingenious and naïve, the 21-year-old engineering student from Pune tried to defraud a Mumbai-based credit card processing company, CC Avenue, of nearly Rs 900,000. He was arrested by the Mumbai Police on August 21, 2003 after nearly an year of hide and seek with CC Avenue. Amit will remain in custody till Friday, August 29.



# HERE'S HOW IT HAPPENED...



- ❑ CC Avenue verifies and validates credit cards of buyers for over a thousand e-commerce Web sites. It conducts checks like IP mapping, zip code mapping and reverse lookup of telephone numbers. Amit Tiwari found a way to bypass them. In May 2002, Vikram Tiwari signed up for CC Avenue's services. In November, he requested the company to deal with his son, Amit, who offered Web designing services on [www.mafiaz.com](http://www.mafiaz.com). CC Avenue's security team confirmed his credentials through bank signature verification, driving license and his HDFC Bank debit card. Everything was genuine.



- ❑ Amit processed several transactions, worth Rs 311,508, via CC Avenue from November 2002 to February 2003. Then the transactions stopped. In April 2003, CC Avenue began receiving charge-backs from the credit card holders, who denied using mafiaz.com's Web designing service. Amit had assumed the identities of these 'customers', and purchased mafiaz.com's services with credit card details that he found on the Net. He was both the buyer and the seller. Calls to Amit's house in Lucknow went unanswered. Legal notices came back unclaimed. Amit had disappeared without a trace.



# THREE-IN-ONE FRAUDSTER:



- ❑ In June 2003, Sachin Deshpande and Jeevan Palani signed separate agreements with CC Avenue to provide Web designing services through their sites [www.infocreek.org](http://www.infocreek.org) and [www.ewebstestarter.com](http://www.ewebstestarter.com).
- ❑ The company's risk-management team found that both these sites had ripped off content and even the client list from foreign sites with similar names. It was similar to Amit's.
- ❑ Vishwas Patel, the CEO of CC Avenue, spoke to Sachin over the phone and found that he sounded just like Amit - "young and immature". They decided to hold back payment.
- ❑ Then, a person called Shoab Sharif sought the services of CC Avenue. Vishwas and his team again spotted a similar pattern. They held back payment on various pretexts. "He sounded desperate," says Vishwas. So they decided to trap him.



# TRAPPED:

- ❑ CC Avenue's accounts manager asked Shoaib to come to Mumbai to collect a cheque of Rs 40,000.
- ❑ On August 21, a young man walked into Vishwas's office. He introduced himself as Shoaib Sharif. Vishwas immediately recognized him as Amit. (He had seen Amit's photograph from his driver's license).
- ❑ Vishwas then called the Mumbai Police, who rushed to his office and picked up the lad. At the Santa Cruz police station, the boy confessed right



# FLAW IN LAW :

- ❑ Senior Inspector Kishore Patil said they would treat it as a case of fraud and Section 65 (tampering with computer source documents) of the Information Technology Act 2000 on Sunday.



# WAYS AND MEANS :



- ❑ Clad in t-shirt and jeans, Amit looks like any other collegian. But when this 21-year-old speaks of his exploits, he assumes the air of an expert.
- ❑ He got some credit-card details through a popular hacker chat room. But he created the rest. He explains, "Each credit card has a country code number, a bank code number and then some other digits. If you find out these first two sets of numbers, it is very easy to create a credit card number. That's what I did."
- ❑ Amit then used proxy servers to camouflage his real location and pass CC Avenue's IP checks.



# TALENT MISUSED :



- ❑ Amit says he used the money to pay capitation fees at the engineering college where he studies. But he continued to defraud CC Avenue because "it was easy".
- ❑ Listening to him, Vishwas is amazed at the boy's knowledge of the system.
- ❑ Vishwas says, "He has tremendous talent. I don't want to ruin his career. That's why I hope he will use his intelligence to plug security holes rather than exploit them."



# CHANDIGARH: RETIRED GOVT EMPLOYEE SHARES ATM PIN WITH CALLER, LOSES MORE THAN Rs 93,000.

- ❑ IN ANOTHER case of cyber crime, a retired government official fell prey to a conman posing as a bank official who duped him of more than Rs 93,000. The Kharar police has registered a case in this connection.
- ❑ The Investigation Officer (IO), Assistant Sub-Inspector (ASI) Bhupinder Singh, told Chandigarh Newslines that the complaint was lodged by Kharar resident B B Mittal at the state cyber cell in Phase 4 on October 5 last year.
- ❑ In his complaint, Mittal said that a man, who introduced himself as Rahul and a technical support official of a private bank, started calling his wife on her mobile number in September last year and got his mobile number from her. The accused called him and told him that his debit card had been blocked and he needed the first four digits of his debit card number.



- According to the IO, after taking the first four digits of the debit card, the accused then asked for the PIN number of the debit card from Mittal and then withdrew money from his account through 18 transactions between September and October.
- “After providing the PIN number, Mittal received a message from the bank that Rs 93,800 was withdrawn from his account. He spoke to his son and went to the bank to inquire about the withdrawal,” added the IO.



- ❑ After reaching the bank, the officials told Mittal and his son that they did not make any call to them. Sensing the fraud, Mittal first went to the Chandigarh State Cyber Cell in Sector 17 and then Punjab State Cyber Cell in Phase 4. He lodged a complaint with the cyber cell authorities who, after conducting the inquiry, directed the local police to register a case.
- ❑ Acting on the complaint, a case was registered at Kharar (city) police station under Section 420 (cheating) of the Indian Penal Code (IPC) and Section 65 (tampering with computer source documents) of the Information Technology Act 2000.



THANK YOU

