EXPERIMENT NO.1

**Aim:** To study and document various real life attacks.

**Crime 1: UTI BANK HOOKED UP IN A PHISHING ATTACK**

**What happened**

A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported to be circulating amongst email users. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements. *"In case you have received any e-mail from an address appearing to be sent by UTIBANK, advising you of any changes made in your personal information, account details or information on your user id and password of your net banking facility, please do not respond. It is UTI Bank's policy not to seek or send such information through email. If you have already disclosed your password please change it immediately",* the warning says.

If any unsuspecting account holder enters his login id, password, transaction id and password in order to change his details as 'advised' by the bank, the same info is sent vide mailform.cz (the phisher's database).

**How it happened**

After investigation, it was found that Mailform is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny. As per the findings of UTI Bank's security department, the phishers have sent more that 1,00,000 emails to account holders of UTI Bank as well as other banks. Though the company has kicked off damage control initiatives, none of the initiatives are cent percent foolproof.

**Conclusion**

The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system. However, reliable sources within the bank and security agencies confirmed that the losses due to this particular attack were zilch.

**Crime 2: OFFICIAL WEBSITE OF MAHARASHTRA GOVERNMENT HACKED**IT experts were trying to restore the official website of the government of Maharashtra, which

**What happened**

was hacked in the early hours of Tuesday, 20 September 2007.

**How it happened**

According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia. According to a senior official from the state government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

**Conclusion**

The state government website contains detailed information about government departments, circulars, reports, and several other topics, but damage was nil.

**Crime 3: Hackers steal £650 million from global banks, 2015**

**What happened**

For a period of two years, ending in early 2015, a group of Russian-based hackers managed to gain access to secure information from more than 100 institutions around the world. They were then able to impersonate online bank staff to authorise fraudulent transfers, and even order ATM machines to dispense cash without a bank card.

**How it happened**

The cyber criminals used malware to infiltrate banks' computer systems and gather data,

**Conclusion**

It was estimated that around £650 million was stolen from the financial institutions in total.

**Crime 4: JP and Morgan Chase & Co target of giant hacking conglomerate, 2015**

**What happened**

Late in 2015, three men were charged with stealing data from millions of people around the world, as part of a hacking conglomerate that spanned the best part of a decade. The trio themselves allegedly described the incident as “one of the largest thefts of financial-related data in history”. Thought to have been operating out of Israel, the trio targeted major corporations, including major US bank JP Morgan Chase & Co, stealing personal data and then selling it on to a large network of accomplices. Along with personal data, the hacking group also stole information related to company performance and news, which allowed them to manipulate stock prices and make enormous financial gain.

**How it happened**

Using more than 200 fake identity documents, they were able to facilitate large scale payment processing for criminals, and illegal bitcoin exchange, and the laundering of money through approximately 75 shell companies and accounts globally.

**Conclusion**

The group stole information from more than 83 million customers from JP Morgan alone, and are thought to have made hundred of millions of dollars in illegal profits.

**Crime 5: 16 years old Infiltrating NASA**

**What happened**

It was in 1999 that a young hacker with the nickname of comrade, better known as Jonathan James, accomplished this exploit at the age of 16.

On June 29 and 30, 1999, this young hacker made a mess of NASA using a simple Pentium computer. He gained access by breaking the password of a server belonging to the government agency located in Alabama. He was able to freely roam the network, and stole several files, including the source code of the International Space Station.

**Conclusion**

According to NASA, the value of the documents stolen by James was estimated at around $1.7 million. To stop the attack, NASA was forced to turn off its systems and reboot them, incurring a loss of $41,000. The capture of the young hacker was fast, with NASA doing everything it could to find him.