Section 66C: Punishment for identity theft.

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

This is a very important provision provided by Information Technology Act. Hitherto, what we have seen is theft of movable property. Now this section provides punishment for stealing identities. Then, what are identities; one's user names, passwords, card pin numbers etc are identities. If someone fraudulently or dishonestly make use of some such identities then it is an offence.

Under this provision cases related to phishing, tele-phishing (vishing), misuse of bank accounts online, Debit, Credit Card misuse etc.

Phishing is to acquire critical information such as usernames, passwords, and credit card details often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. A typical narration of complaint will be that the victim is having a bank account, he is getting an un-solicited e-mail with a similar web page of the bank where the victim has bank account, and in the e-mail it is mentioned "Dear valued customer on our routine check up we found something wrong with your account and you are requested to revalidate the account", underneath a hyperlink is given. If gullible victim believe it and click on the link which will open in a new page the victim is made to enter critical information of his online bank account like user names, passwords etc. The gullible victim think that the given information will go to the bank but in fact it will land in the hands of online fraudster. Once the fraudster knows the Internet banking user name and password with in no time he will transfer amounts that are left the victim bank account.

Another variant of phishing is the victims get e-mail pretending from Income Tax Dept with a e-mail content " Dear Values tax payer, there is tax refund for you and you are requested to furnish your bank details to credit you tax refund to your account". The fake e-mail will have national emblem on it. If Gullible people fall prey to such e-mail and click on the link it will seek critical information of his bank account then people will be defrauded.

The registration of case can be under 66 – C IT Act and relevant other provisions of IPC. In these cases there is deception, wrongful loss to the victim and wrongful gain to fraudster; hence section 420 IPC can be invoked. Further an e-mail, which is an electronic record, pretending Income Tax Dept is sent that means a fake electronic record (document) is produced as if genuine to deceive the victim and hence section 471 IPC can also be invoked. Thus the registration of the case can be under section 66-D IT Act, 420 and 471 IPC. However once an IT Act provision is invoked in the FIR then as per the legal stipulation the investigation of such an offence shall be of and above the rank of Inspector of Police.

For instance a phishing case committed pretending Income Tax Dept can be discussed in detail, focussing the line of investigation, evidence shall be gathered from FIR to charge sheet. A typical complaint will be as mentioned below. The section law applicable are 66-C IT Act, 420 & 471 IPC.

"To
The SHO,
……Police Station.
TS State.

Sir,

I submit that I have ICICI Bank account bearing number A/c 123456789 and I have Internet Banking Facility and Debit card on my account. I do all my transactions from my house where I have internet connection. I have my e-mail ID abc@xyz.com and mobile number 9848012345 that are associated with my bank accout.

While this is so on 01-01-2015 I received an e-mail to my e-mail ID from an e-mail ID as if from Income Tax Department mentioning that that I have tax refund to claim and a link is given below. Believing it to the true I clicked on the link given there and it lead me to a new webpage where I was made to enter my bank account number, Internet user name and password, my mobile number that is associated with my bank account etc. After I entered all those details when I checked the page went blank.

But to my surprise an amount Rs 90,000/- was deducted from my bank account such mobile alerts came on to my phone. Immediately I realised that these transactions are being done without my knowledge and contacted the bank authorities who informed that three laptops were purchased online through e-Bay a online shopping website.

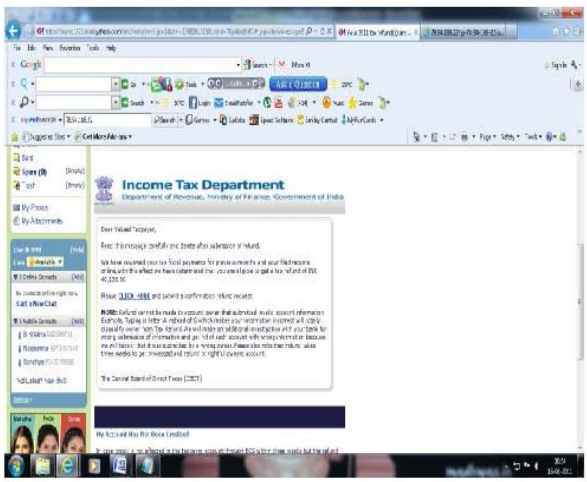
Thus I suspect that some culprit in the name of Income Tax Dept sent false e-mail and deceiving me collected by bank account critical information and misused my bank account details and caused my wrongful loss of Rs 90,000/- .

Therefore I request that necessary action may be taken in this regard

Sincerely

Xxxxxxx

"



Phishing - standard operating procedure (SOP)

In the line of investigation the following standard operating procedure (SOP) may be followed:-

- The Investigating Officer shall react fast. He shall collect the print of the e-mail that the victim has received before independent mediators or under the cover of a certificate issued under section 65 – B Indian Evidence Act by the victim towards documentary proof that such deceptive e-mail was in fact received by the victim.

- Then the I.O shall contact the concerned bank to know the route of the amounts and to that effect shall collect the transaction statement of the bank account for which the misused debit card was used.

- The IO shall also collect information about the goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) purchased and the amounts were used. If the amounts were used to buy goods online, then it shall be known as to what was the merchant website? And what was shipping address to which the delivery of goods was made? Further it shall also be known which the courier service was? And what are the IP Addresses that are associated with the fraudulent transactions.

- Physical verification of the addresses that were collected for the IP Address end user, shipping address of the goods shall be made.

  By working out these leads the case can be detected or can be taken to a logical conclusion.

- Once the fraudster is identified, under his confession the tool of offence which may a desk computer / laptop shall be recovered and it shall also be forwarded to the FSL for the purpose of analysis and

to know whether the deceptive e-mail that was sent to the victim is available in such materiel object or not.

This is the basic investigation that can be conducted in a case of phishing, however depending on the case the line of investigation and the leads to be worked out may differ

Cases of Debit & Credit Cards misuse:-

Further under this provision cases of Debit & Credit Cards frauds can also be investigated. Debit /Credit card is a plastic card issued by banks. These are accepted as legal tender at ATM centres and shops & establishments. Debit & Credit Cards misuse cases include skimming and cloning, shoulder surfing, swapping of cards at ATM centres etc.

Skimming and cloning is that the card's critical information is collected by a small gadget namely a 'skimmer' that may be installed at the ATM machine's slot and pinhole camera is fitted above in the ATM centre. These will be deceptively placed to collect the card critical information from the magnetic strip of the card and the PIN numbers while they are pinned by the user. By using such fraudulently gained information new card which is called 'a clone' will be created and such counterfeit cards are misused. In these cases the Card will be with the victim but amounts are drawn from a different place.

Skimmers vary in size and they will be in the size; they will be in the size of a cigarette box but modern skimmers are so small in size they can be fitted into the slot of an ATM where usually the cards are inserted while drawing amounts. Skimming may also occur at retail outlets – bars & restaurants, petrol filling stations etc.

Skimming and cloning – The line of investigation:-

- The line of investigation in these cases shall be finding out the place of compromise of the card. That means knowing from the victim, before the fraud has happened, what was his genuine transaction? Place of compromise is where the critical data of the card was stolen by the fraudster, before it was misused.

- Once this is known an effort can be made to work out leads at the place of compromise. The place of compromise can be an ATM centre or a place where the victim made a purchase of goods at any shop. If such place is identified then it can be visited and an effort may be made to collect CC camera footage, verification can be made for the presence of any skimming gadget etc.

- The transaction statement of the bank account of the victim can be collected and the ATM centres from which cash withdrawals are made can identified basing the ATM centre ID and from such an ID further the physical location of the ATM centre can be identified and

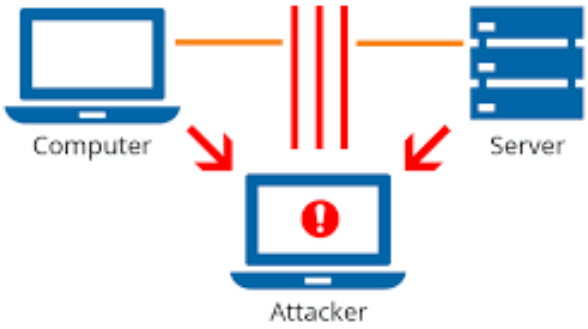
further by contacting the concerned bank nodal team CC camera footages of the culprits can be identified, and thus efforts can be made to identify the culprits.

Sometimes the cloned cards are used for purchasing goods at shops and establishments, and hence such shops and establishments shall be identified. Those shall be visited and the sales people who allowed the un-authorised transactions may be examined for working out leads / clues to identify the culprits.

- Thus in these cases the identification of the place of compromise and place of withdrawals of the amounts or places (shops) where the card is being swiped is very essential to work out clues and leads towards detection of the case.

Man in the middle attack:-

The card critical data can also be compromised by '**man in the middle attack'** which means that the victim may be making purchases of goods or services online on an unprotected website then the critical data that will be transferred online in an unencrypted way which may be tapped by any hacker who reads the data in the mid way. This is further elaborated that, while online financial transactions are made the card numbers, bank account numbers, passwords, pin numbers, CVV numbers etc will traverse from the victim's computer to the bank server and also to the merchant's server. During such transmission critical data may be captured and by using so collected information a new card (a clone) may be created and misused.



Shoulder surfing is also committed at ATM centre. When the victim visits and while doing his genuine transaction the fraudster looks at the victim's card and notes down the card number and PIN number etc and by using such fraudulently gained information online purchases can be made.

Shoulder surfing – line of investigation:-

In these cases also the place of compromise may be identified, at such place the CC camera footages may be collected. In these cases usually goods or services will be purchased online. Thus, the details of such purchases including the shipping addresses can be secured and efforts can be worked out to trace the culprit.

Further in all the case wherein the goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) were purchased online, the IP Addresses along with date and time can be collected from the bank and also from the merchant website and efforts can be made to the trace

the culprit by finding out the user details of the IP Addresses from the concerned Internet service provider (ISP)

Tele phishing or vishing is a fraudulent technique where in the victim receive a phone call from a stranger who pretends to be bank employee and further deceptively states that the account of the victim is being linked to ADHAAR, and for doing so collects details of card including CVV number from the gullible victim. The culprits further deceives the victim saying that while his account is connected to ADHAAR a code is generated and the same reflected on to the mobile number of the victim and subsequently calls the victim secure the one time password (OTP) from the victims. The victim will realise the fraud only when he receives mobile alerts for the amounts deducted from his bank account. By the time the illegal transaction are completed.

Thus vishing is a kind of social engineering technique of convincing people to reveals confidential information of the debits cards and by using same fraudulent transactions are made.

In these cases the section of law that is attracted for issuing FIR is 66-C IT Act and 420 IPC.

Tele phishing or vishing – The line of investigation:-

- In these cases an important lead is mobile number from which the victim was called when he was deceived. For such mobile number call data records (CDRs) can be secured, and further customer application form (CAF) along with the address and ID proof that were furnished at the time of getting SIM can be obtained and efforts can be made to work out clues and leads to trace the culprit.
- In addition to this, what were the service or goods that were purchased and from which website (merchant website) such purchases were made can also be identified from the transaction statement of the bank account of the victim, and by contacting the merchant website the shipping address i.e., delivery address of the goods can be known and thus efforts can be made to trace the fraudster.
- Usually the misuses of debit card in these cases will done by purchasing goods (laptops, mobile phones etc), or services (mobile recharge, booking tickets etc) online. Therefore, if the IOs can act fast and alert any of the organisations i.e., bank, merchant website, payment gateway, acquirer bank etc the illegal transaction can be aborted and charge back (restoration of the amounts) can be secured to the victim.
- Further the IP Address corresponding to the online transactions can be collected from the bank or merchant website (web stores). The user details for such IPs can be collected from the ISP and basing on the same the address of the fraudster can be secured.
- Physical verification of the addresses that were secured for the subscriber address of SIM, shipping address and IP end user shall be made.
- If mobile recharges are made the details of the numbers foe which recharges were made can be ascertained and their subscriber details be known from the mobile service provider (MSP and such

addresses shall be verified for knowing where they made the recharge etc details.

- Verification with courier service boy who delivered goods at the shipping address will also be a good lead to detect the case.
- IO shall not forget to examine who ever may be the circumstantial witness i.e., the representative of bank, merchant website, courier service so that the case can be established with proper orall and circumstantial evidences.

Further other types of card frauds may be lost and stolen card frauds: These types of frauds happen when the card is lost and lands up in the hands of another person who can misuse it or the card is stolen by a fraudster and subsequently misused. Cards are also stolen at ATM centres. The fraudster in the pretext of helping the victim while he draws the amount may take away the card of the victim and hands over a duplicate card to the victim.

***