Bal Bharati
PUBLIC SCHOOL
Sector – 21, Noida
Phone : 0120-2534064, 2538533 / E-mail : bbpsnd@yahoo.co.in
Website : http://bbpsnoida.balbharati.org

CYBER SAFETY AWARENESS HANDOUTS

CLASS IX – XII

(TERM II)

Pause | Think | Connect

Stay Safe Online

CYBER CRIMES

- **FAKE CALLS FRAUDS**

  What we are discussing here is related to vishing, also known as voice phishing. Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank representative or someone from the bank's technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. After giving a false sense of security, the caller then tricks the victim into giving away their personal and confidential data such as:

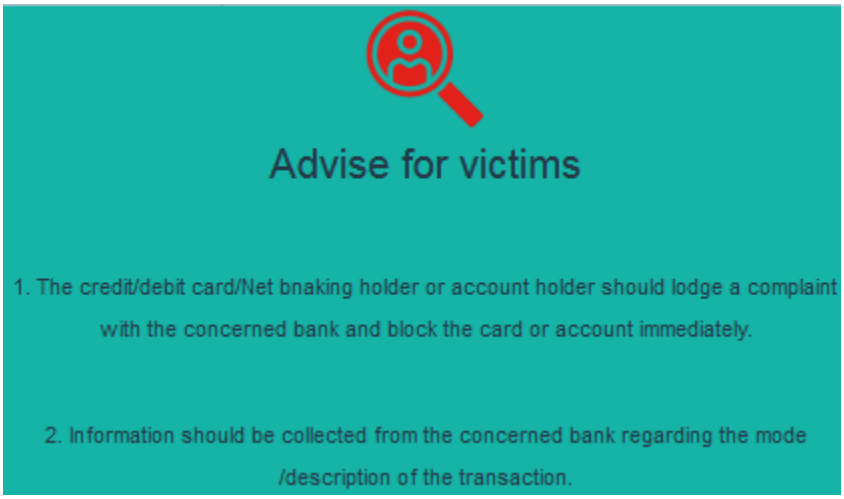
  • One-Time-Password (OTP)
  • Credit/debit card number
  • The card's CVV number [Card Verification Value – 3 to 4 digit number printed on the flip side of the card]
  • Expiry date
  • Secure password
  • ATM pin
  • Internet Banking login ID and password and other personal information

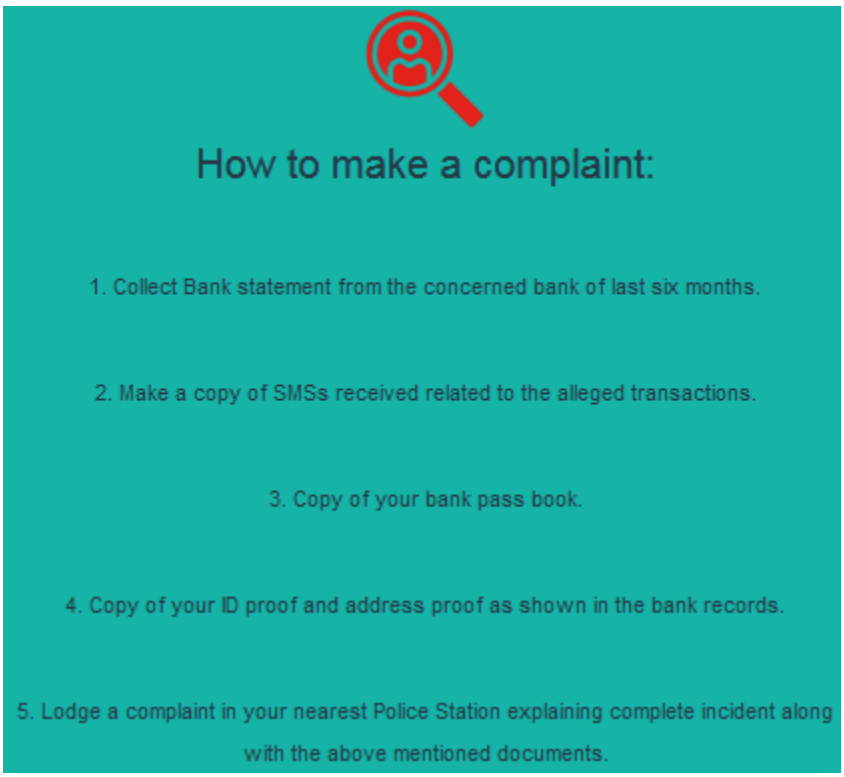
  With all such crucial information at hand, the fraudster can easily carry out illegal financial transactions using the victim's name.

PREVENTIVE MEASURES/PRECAUTIONS

1. Banks or any of their representatives never send their customers email/SMS or call them over phone to ask for personal information, password or one time SMS (high security) password. Any such e-mail/SMS or phone call is an attempt to fraudulently withdraw money from the customer's account through Internet Banking. Never respond to such email/SMS or phone call.
2. Never respond to emails/embedded links/calls asking you to update or verify User ID/Password/Debit Card Number/PIN/CVV, etc. Inform your bank about such email/SMS or phone call. Immediately change your passwords if you have accidentally revealed your credentials.
3. Do not provide any personal or confidential information on a page which might have come up as a pop-up window.

4. Always remember that information like password, PIN, TIN, etc., are strictly confidential and are not known even to employees/service personnel of the bank. You should therefore, never divulge such information even if asked for.
5. Never provide your identity proof to anyone without any genuine reason.
6. Never click on any links in any e-mail to access the bank's site.
7. Access your bank website only by typing the URL in address bar of browser.
8. Do not provide your bank account details to emails offering a job or claiming that you have won a lottery. Avoid opening attachment of emails from unknown senders.
9. Avoid accessing Internet banking accounts from cyber cafes or shared PCs.
10. When on your bank website, look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.
11. Keep your system up to date





- **INSURANCE FRAUDS**

In this type of fraud hundreds of people fall in the trap of fake insurance calls. The fraudulent callers are increasingly ingenuous and appeal to our sense of fear and greed to part with personal details and money. We have compiled here the different kinds of calls they make. If you come across any of these, just disconnect the call.

Fake Call 1: This is a call from an LIC service branch; you can transfer the existing policies to new policies for better returns.

Fake Call 2: There is an annual equity bonus lying unclaimed in your Account, which will be transferred to your Insurance Agent/govt. Please deposit money in a certain bank account to avoid this transfer.

Fake Call 3: Your insurance agent purchased insurance policy of Xyz Company at the time of purchasing your LIC policy. Dividends from policy of Xyz Company will be transferred to your agent and xyz insurance company. Please deposit money to transfer this money to your account.

Fake Call 4: You are entitled to loyalty bonus for being a valued customer. This bonus is transferred to agent code instead of your code. Give policy details so that the bonus is properly transferred to you.

Fake Call 5: We are calling from Insurance Verification Department. Give your PAN Card number, Bank Details and Aadhaar number to complete the verification process.

Fake Call 6: Your insurance policy is up for cancellation and your money will be transferred to your agent and LIC. Give personal details, policy details, bank account details and secure code behind card to complete electronic transfer of money.

Fake Call 7: We are calling to check if you would like to raise an objection for Bonus cancellation on your policies. If you do not raise any objection, then LIC agent gets 40% and local branch gets 60%. Send Rs30,000 along with PAN Card and Aadhaar Number to raise any objection.

Fake Call 8: Give your insurance policy and other details for verification. If you do not give these details, your payments and pension will be blocked.

Fake Call 9: Stop paying premiums towards your existing policy since it has lapsed due to some reason. Surrender it and buy a new one.

Fake Call 10: Your insurance policies are running in loss. I will get a new policy which will recover all the money and make a profit for you.

Fake Call 11: Surrender your existing policy because a new policy is being offered with better terms, and you no longer need to continue with the existing policy.

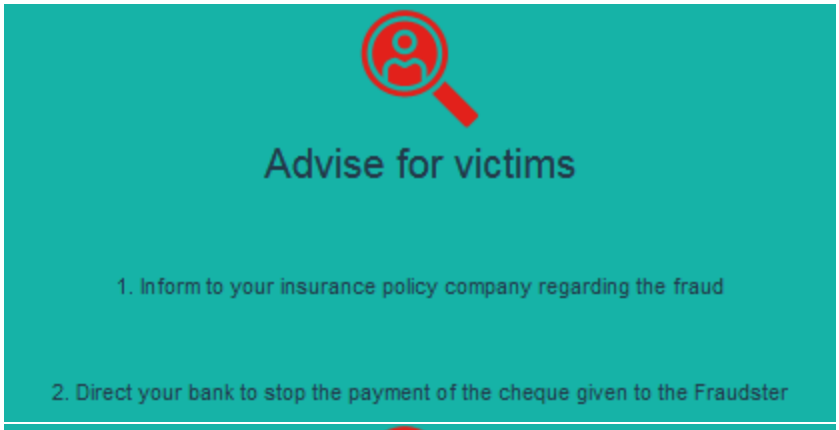
Fake Call 12: I am an LIC employee and I can offer a special bonus and larger returns when you buy a policy from me.

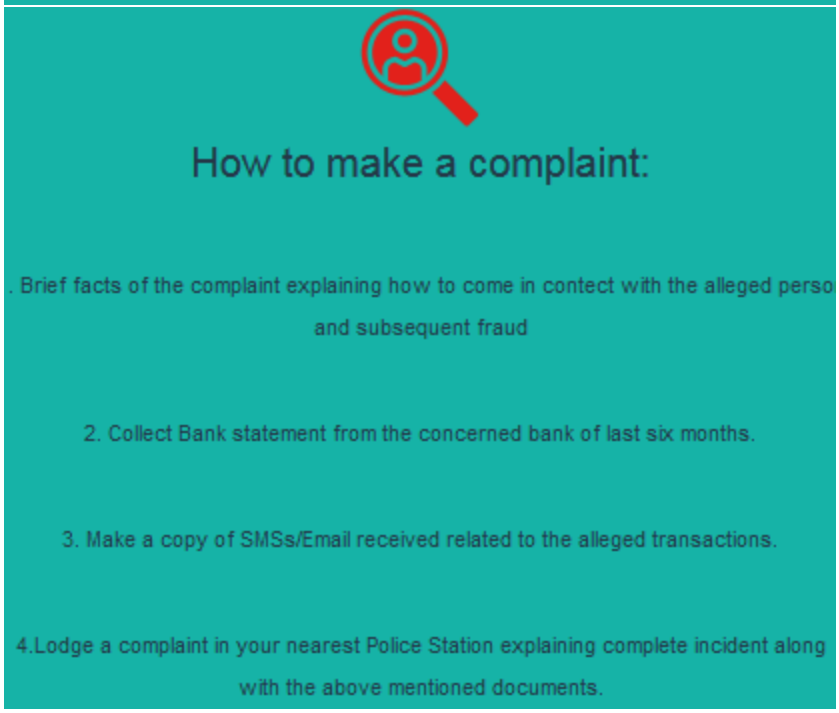
Fake Call 13: You were cheated by the company and I thought it was our moral duty to inform you. If you buy a new policy I can cancel the previous one and get all your money back.

Fake Call 14: I am calling from IRDAI. You are entitled to the bonus on your life insurance policy. But to realise the cheque, you have to make an investment first. And today is the last day

Fake Call 15: There was a mistake in your policy and it is useless. You need to correct it for which you have to pay Rs20,000.

Fake Call 16: Agents make a lot of money in bonus and commissions when they sell a policy to you. I can get it reversed but you need to buy a policy first.





- **LOTTERY SCAM**

  In this type of scam where the sender requests to help in facilitating the transfer of a substantial sum of money, generally in the form of an email. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. If money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer.

  In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

  - Either they have won a lottery worth millions of dollars; or
  - Their help is required for transferring of illegal money from some foreign Country; or
  - Goods are offered at throwaway prices; or
  - In some cases, the victim's address book in her emailing list is compromised and emails sent to all contacts from ID asking for money to bail her out from a perilous situation;

  The victims are trapped in a phased manner and are generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost.

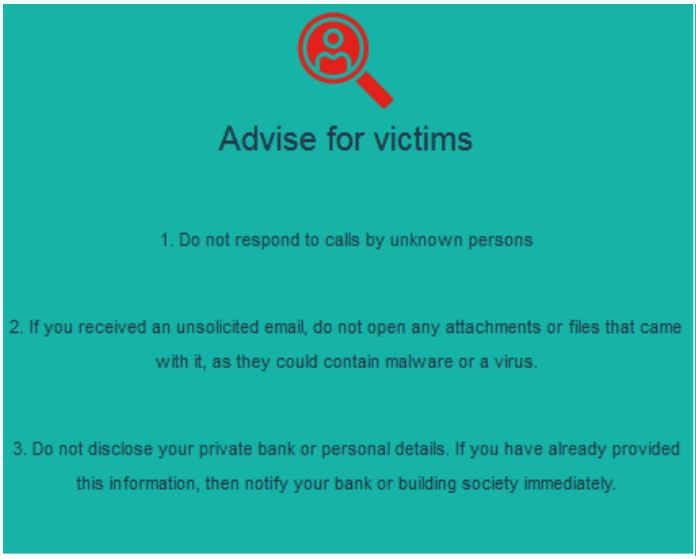
  The victims apparently receives a spam email and respond to the same and end up paying money to some unknown persons for a nonexistent purpose.

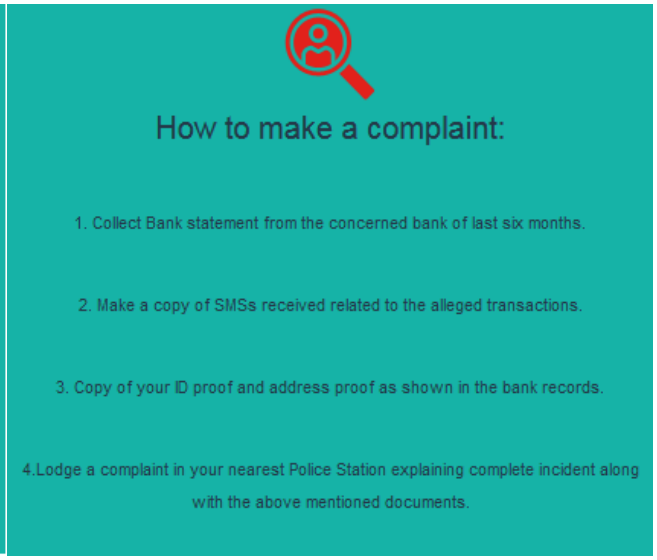
  Such crimes are generally carried out from foreign locations. Money is either deposited in offshore accounts or in some carrier account in India.

PREVENTIVE MEASURES/PRECAUTIONS

- Have you received an SMS or email saying that you have won a prize in a lottery? It's a scam. Do not respond
- Never respond to fake lottery winning related calls/SMS/Emails
- Have you received an SMS or email about transferring of money into your account? It's a scam. Do not respond
- Have proper spam filters in your email account

Follow the thumb rule : Never transfer funds to unknown persons or entities in anticipation of high returns. This is never going to happen



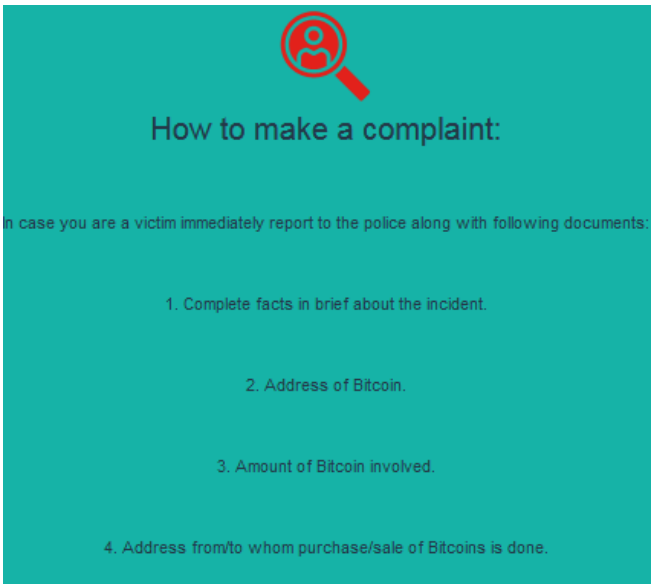


- **BITCOIN**

The legal framework regarding crypto-currencies is yet to be laid down. RBI has not given any licence/authorization to any entity/company to deal with any virtual currency.

In the absence of a legal framework, it is not advisable for citizens to deal with virtual currencies such as Bitcoins

These currencies are normally used by criminals operating on the dark web or the hidden web. Legal, bonafide businesses do not normally use Bitcoins. Therefore any request for business transaction in Bitcoins should raise suspicious and should be avoided



- **CHEATING SCAMS**

In this type of scam, the sender, generally through an email, requests help in facilitating the transfer of a substantial sum of money. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. Once money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer.

In such matters the victims normally allege that they have received emails from unknown sources wherein they have been informed that:

• Either they have won a lottery worth millions of dollars; or
• Their help is required for transferring of illegal money from some African Country; or
• They have been selected for an overseas job, generally a hotel job in some European/American country; or
• Goods are offered at throwaway prices; or
• In some cases, the victim's address book in her emailing list is compromised and emails sent to all her contacts from her ID asking for money to bail out from a perilous situation;

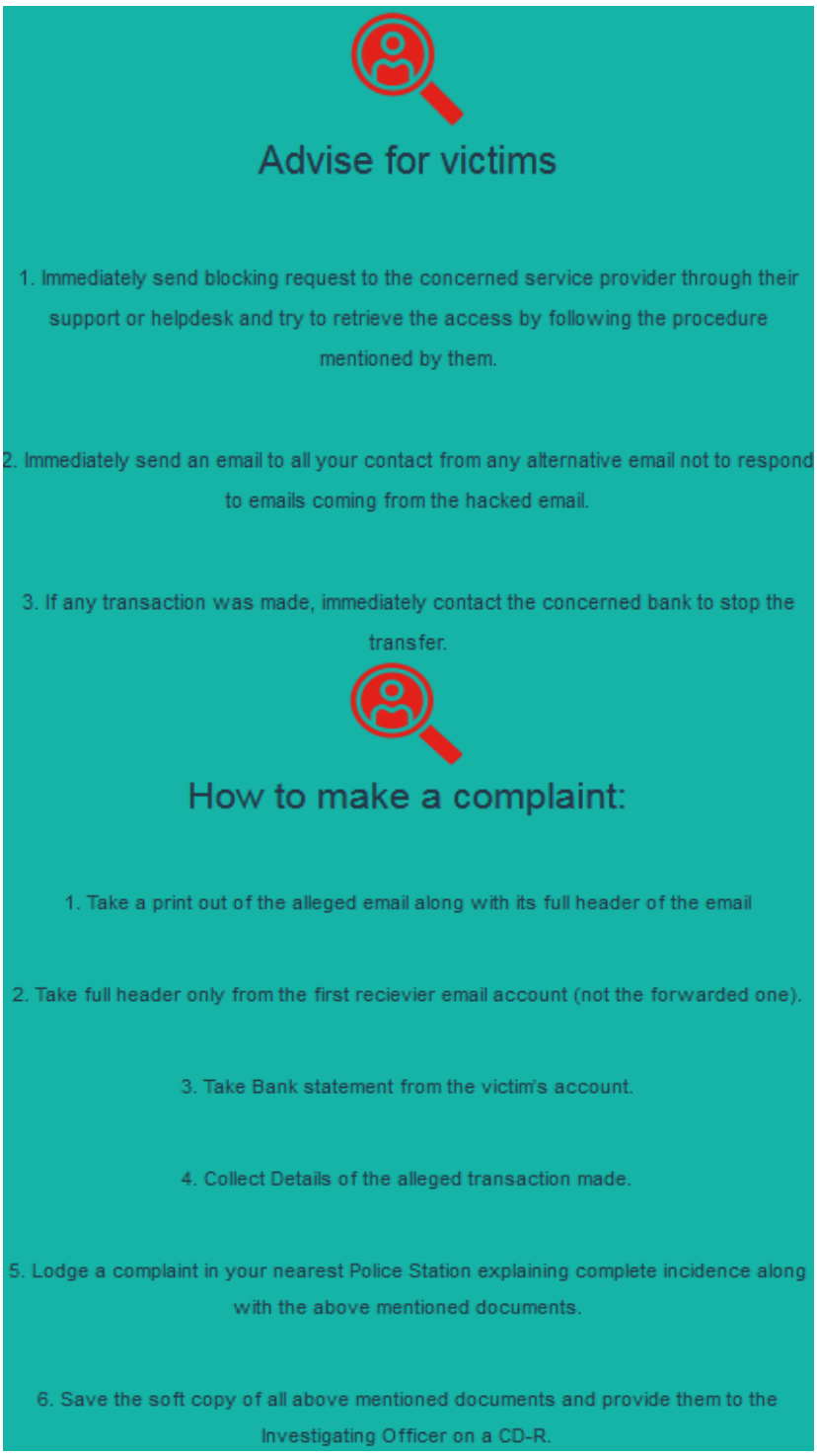
The victims are trapped in a phased manner and are generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost.

The victims apparently receive a spam email and respond to the same and ends up paying money to some unknown persons for a nonexistent purpose.

Such crimes are generally carried out from foreign locations. Money is either deposited in offshore accounts or in some courier account in India.

PREVENTIVE MEASURES/PRECAUTIONS

1. Do not chat with strangers over net. Fraudsters and scammers prowl on the internet looking for victims.
2. Never send money or give credit card details, online account details or copies of personal documents to anyone you don’t know or trust and never by email.
3. Avoid any arrangement with a stranger who asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
4. Do not agree to transfer money for any unknown person. Money laundering is a criminal offence.
5. Verify the identity of the contact by calling the relevant organization directly – find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.
6. Check credentials of foreign enteties through the concerned Embassies and High Commissions, Counselates etc.
7. Do an internet search using the names or exact wording of the letter/email to check for any references to a scam – many scams can be identified this way.
8. If you think it’s a scam, don't respond — scammers will use a personal touch to play on your emotions to get what they want.
9. Remember there are no get-rich-quick schemes: if it sounds too good to be true it probably is a trap.



- **ONLINE TRANSACTIONS FRAUDS**

  In such matters, the complainant alleges that some unknown person had withdrawn money/ made transactions through his/her credit/debit cards through online purchasing. In most of these cases purchasing is done by using following crucial information of the credit/debit card :

  1. The 16 Digit Credit/Debit Card Number

  2. The validity of the Credit/Debit card

  3. The 3 digit confidential Card Verification Value (CW) or the One-Time-Password (OTP) sent on the registered mobile number of the Debit Card holder.

While it may be that the Card Number and the validity of the card is made available to the fraudsters through insider in the bank, the OTP is procured by them by deceiving the account holder to share the OTP on the pretext that it is required for account verification, etc.

PREVENTIVE MEASURES/PRECAUTIONS

1. Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.

2. During a transaction, keep your eye on your card. Make sure you get it back before you walk away.

3. Monitor your bank and credit card statements.

4. Monitor your credit report.

5. Never store Credit Card information online.

6. Never make use of Credit Card on Public Computer.