The Economic Times
Don't get cheated

Date: 01/08/2016 | Edition: Bangalore | Page: 01 | Source: Riju Dave

Don't get Cheated

Fraudsters are finding innovative ways to cheat you via e-commerce and banking transactions as well as mobile calls and mail. Find out how to prevent these.

RIJU DAVE

If a stranger you met for the first time on a metro asked you to give him ₹10,000, would you do it? You don't have his contact details. You don't have his identity proof. And, no, you don't know if the money will be returned.

If you are shaking your head in disdain at the sheer naivety of the person who would give out his hard-earned money, take a look in the mirror. It could be you. Or, perhaps, it is you, if you were among the 36% of people who have been cheated in Internet scams, according to a survey by Telenor (*see 'Rising incidence...'*) early this year.

The easy access to victims is the reason they are readily stalked by fraudsters—whether you use a smartphone or a computer, are logged into social media or pay online bills, buy gadgets from an e-commerce website, or withdraw money from an ATM, you are a sitting duck. It helps if you have poor tech skills, trust freely and are lured by easy money.

As per the RBI data, 11,997 cases related to ATM, credit and debit cards as well as Net banking frauds were reported by banks in 2015-16. This, besides the 49,455 cyber security incidents, including phishing, scanning, malicious code, website intrusion, etc, (*see 'Scam terms'*) that were reported by the Indian Computer Emergency Response Team (CERT-In), in 2015. If, however, you take into account the unreported cases, these figures are a fraction of the frauds being unleashed in the country.

A new breed of scamsters is coming up with ingenious ways to circumvent security measures. "Earlier, an individual was hacking while sitting in a garage. Today, it is a more organised market, with syndicates all over the world using sophisticated ways to indulge in identity theft," says Mohan Jayaraman, Managing Director, Experian Credit Bureau (India), a global analytics firm that has just launched a tool to measure the probability of fraud in banking and insurance.

So rampant is fraud that RBI Deputy Governor S.S. Mundra has reiterated the need to provide relief to customers. "The RBI is examining whether to issue regulatory direction with regard to limiting the liability of customers on fraudulent transactions arising out of frauds and electronic banking transactions," he said at an event organised by the Banking Codes and Standards Board of India, in May this year.

But prevention being the better option, you need to protect yourself from the omnipresent scamsters. In the following pages, we shall tell you not only about the various modus operandi being used by scamsters but, more importantly, the ways in which to secure your finances and seek redressal if you are cheated.

ONLINE SHOPPING

Ensure that the website, seller and payment modes are secure before you binge on e-commerce sites.

There is no doubting the convenience of online shopping, be it for electronic gadgets or household appliances, clothes or furniture. Sadly, this has also led to new cheating techniques and sale/delivery loopholes.

Modus operandi

When you order online, it's possible that the product may not be delivered at all, or that you land a fake or damaged product. You may even get an empty package or, worse, one filled with stones. Ask Ghaziabad-based Santosh Kushwaha, 32, who ordered an iPhone6 worth ₹46,000 in 2015. "The packaging was flawless. It was laminated, the weight was right and it wasn't tampered with. But when I opened it, I found the box filled with stones," he says.

The problem can occur at any stage, for which you need to understand the sale and delivery process. There are sites that sell and deliver their own products like Fabindia. There are others that serve as a platform for various sellers. These are marketplaces, like Flipkart, Amazon or Snapdeal, which host products by different brands and sellers. These products may be delivered either by the site itself or the seller. In most cases, it's the seller who delivers. Some sites also provide special services, wherein product quality and delivery are guaranteed, for a premium. Here the site sources products from other sellers but conducts quality checks and delivers them itself. For instance, Flipkart is set to launch F-Assured, promising improved delivery service and stricter quality checks, while Amazon Prime is the paid service that offers similar advantages to its members. Here are the various points at which fraud can occur:

Fake website: Tech-savvy scamsters set up sites that look like genuine ones with similar logos and domain names. Some may create a dummy site with a product line-up that only exists online. The purpose is to extract money from vulnerable buyers and disappear.

Genuine site, fake seller: If you have not received a product, or it's damaged or fake, the scam could be by the seller or courier company, not the site itself. Though such sites scan the sellers hosted by them, weeding out frauds by checking themselves or going by buyers' ratings, it is not possible to identify all scamsters.

Courier company: Here, both the site and seller may not be to blame. If they fail to choose a reputed courier and go for cheaper fly-by-night operators, you could land a dummy package. A specific errant employee of the courier firm may also be responsible for the fake delivery.

Preventive steps

Check the site: If you want to try out new sites, make sure to check the domain name. Ensure the URL has 'https' (not just 'http') and a lock icon, and check the site's spelling. To find out who owns a particular domain name and if it's genuine, log in to *https://registry.in/WHOIS*, which is a searchable list of every domain currently registered in the world. If the site does not offer any contact details or has a vague exchange or return policy, abandon the site. You could also check the company's trust rating on *http://www.scamadviser.com* which will give you all the details about the firm and how safe it is to shop from the site. "Make sure the company has the right infrastructure, wherein you are able to track delivery and payment information," says Jayaraman of Experian.

Check seller's rating: If you have picked an established site, opt for product assurance services, if any. If you don't wish to pay extra, go through the buyer reviews and ratings for the seller to find out if he has a good reputation for delivery. "We take strict action against sellers who attract negative feedback about their service or are found to be engaged in selling products that are fake, in violation of copyright or any other applicable laws," says the Flipkart spokesperson.

Secure payment: As for payment, avoid direct payment to sellers. Opt for payment services like PaisaPay in eBay, which ensures that the seller is not paid by the site till the product is delivered, safeguarding your money. Also, do not pay via electronic bank transfers because it is difficult to retrieve the money once it has left the bank. Opt for payment via credit card that has a low credit limit and is used exclusively for online shopping, or for cash on delivery, to minimise risk. "An important safeguard is to make a video recording of the delivery, starting when the courier arrives till the package is opened, in a single loop without breaks," says Kushwaha. This is what served as proof and helped him get his money back, he says.

If you are cheated..

The first step is to get in touch with the website or the seller. If it's a fake site, it's impossible to seek redressal. Consider your money lost.

If you have opted for a safe site with a guaranteed exchange or money-back policy, you could write to the site, detailing the fraud, product details and mode of payment without giving sensitive information like your bank account number, etc. The site will conduct its verification within a specified time and revert. If the site doesn't respond, you could escalate it by registering a complaint with the district or state consumer redressal forum.

A good option is to put up the grievance on consumer complaint boards/sites. You could also upload your complaint or video on micro-blogging sites like Twitter with the company's handle. "The site was taking its time to resolve my issue, but when I posted my video on Twitter with its handle, the site responded immediately and my money was refunded in four days," says Kushwaha.

ASHWANI NAGPAL

VICTIM
SANTOSH KUSHWAHA
32 YEARS
GRAPHIC DESIGNER
GHAZIABAD

CRIME SCENE
E-COMMERCE SITE

YEAR
2015

AMOUNT INVOLVED
₹46,000

NATURE OF FRAUD
Bought a phone from an e-commerce site, but on opening the package, found stones instead of phone.

TIME TAKEN TO RESOLVE CASE
Got a refund within **four days** of posting a video on a micro-blogging site.

MY ADVICE

"Always make a video recording when you open a package for a product bought online."

DOs & DON'Ts

1. Shop through established e-retailers with transparent exchange and return policies.
2. Don't just consider low prices. Check the sellers' ratings and reviews by other buyers.
3. Do not pay via bank transfers. Use credit cards or opt for cash on delivery.
4. Avoid payments on mobile phones if you haven't installed firewalls or anti-virus software.
5. Make an uninterrupted video recording during delivery and opening of the package.

SOCIAL MEDIA

Be cautious while interacting on such sites and conduct background checks before giving away money for a good cause.

The popularity of social media like Facebook, micro-blogging sites like Twitter, dating sites, online consumer compaint forums, charity and crowdfunding sites have spawned a fresh set of scamsters that preys on the personal information posted unwittingly by members.

Modus operandi

There are various online shopping sites that require you to log in through Facebook or mail and this can be an easy entry point for fraudsters, who can misuse your bank details, phone numbers or mail login and password to clean out your account.

Social media: Beware also of friends' friends who ask you for money. They could have hacked your friend's account, created a duplicate one, sent requests to the friend's friends and asked for money. "One of my relatives, who is a scamster, asked several of my Facebook friends for money and two of them even ended up paying her," says Vidya Nagraj, a Chennai-based consultant.

Complaint forums: Be careful what information you volunteer on such sites. "I had put up my complaint regarding a wrong bank account number I had provided to an online shopping site for a refund," says Varun Kapila from Bengaluru. "I got a call from a person claiming to be from the site, who requested the correct account number. I didn't suspect anything and gave it to him. My account was soon wiped out, but thankfully it did not have too much money," he adds.

Crowdfunding and charities: Despite the noble sentiment involved, be wary about giving money without verifying the claims of the backers. On 26 February 2016, an Indian American, Manisha Nagrani, was arrested in the US for raising thousands of dollars via crowdfunding to help cover the cost of treating her blood cancer. She had been perfectly healthy all along.

Dating scams: Though this is more common abroad, it's not completely unknown in India. If you befriend someone on a dating site and the person starts demanding money for travelling to meet you or other emergencies, medical or otherwise, know it to be a fraud.

Preventive steps

You may not be able to seek redressal or have legal rights to claim the money lost because you either volunteered the money or information yourself. So the best you can do is avoid these. "Expose yourself only to the people you know on social media," says Jayaraman.

Don't give money without knowing how it is going to be used and make sure to use secure payment channels while giving money to charities or for crowdfunding.

DOs & DON'Ts

1. Do not befriend anyone you don't know on social media.
2. Do not reveal personal financial details on social media sites.
3. Do not pay money to an unknown friend's friend without checking with your friend.
4. Do not volunteer bank details or other critical information on complaint sites
5. Do not contribute to crowd funding without verifying and check if you know other backers.

BANK TRANSACTIONS

Banking fraud may be among the top online scams, but the RBI is in the process of reducing the liability of the customer.

According to the RBI, incidents of bank-related fraud, including cards, ATMs and Net banking, have risen from 8,765 in 2012-13 to 11,997 in 2015-16. "With the introduction of 'Chip and PIN' security feature, we have noticed a significant reduction in incidents of fraud in credit cards," says Vijay Jasuja, CEO, SBI Card. But the sheer volume of online and offline transactions makes it a fecund ground for fraud.

Modus operandi

Essentially, the only way to cheat when it comes to banking transactions is through identity theft, wherein your credit/debit card details or your bank account information is stolen. It is this theft that is carried out in a variety of ingenious ways by scamsters.

Online stealing: During e-shopping or bill payment, if you do not choose a safe site or payment channel, it is easy to steal your card information by intercepting the data. You can be routed to a fake site or the data can be copied through keystroke logging. Pharming ensures that the fraudster has your bank account or credit card number and CVV, which can be used for online transactions. Malware or virus can also be introduced in your computer which provides access to all the details stored in your e-mail. If you have saved your passwords and login details, these can be easily stolen. "Besides phishing and vishing, malware and breach incidents are the emerging threats when it comes to frauds," says Sanjay Silas, Head, Branch Banking, Axis Bank.

SIM swipe fraud: This is a relatively new technique, wherein the scamster contacts the mobile operator with fake identity proof and gets a duplicate SIM card. Your original SIM is deactivated by the operator. The fraudster generates one time password (OTP), which appears on his phone, and he carries out online transactions.

Fake calls and mails: "Vishing has become popular in the past few years and is done via a phone call. Customers, unknowingly, share their CVV number or OTP which is used for identity theft," says Jasuja. Hyderabad-based Bharat Naidu (*see picture*) knew better. "Last year, I got a call allegedly from Citibank, saying my points were about to expire and that they would transfer it to a new card, for which I would need to give the old card's CVV. I knew what was happening and gave them the wrong number," he says. Frustrated after a few attempts to get the details, the caller gave up. A month later he got a similar call. At that point he called up

DOs & DON'Ts

1. Do not give your phone number at public places or conduct transactions on public terminals.
2. If you change houses, inform the bank so that cards and statements are sent to the right address.
3. Check your bank and credit card statements. If you notice irregular charges, notify the bank.
4. Conduct ATM transactions preferably only at machines located inside bank branches.
5. Do not leave if ATM stalls. Report to security guard or bank official, or call up the bank.

Call your bank for card fraud..

HDFC Bank	**6160-6161 (for some cities)**
ICICI Bank	**1800 102 4242**
Kotak Mahindra	**1860 266 2666**
Axis Bank	**1800 209 5577**
IndusInd Bank	**1860 500 5004**
SBI	**1800 11 2211 (toll-free), or 080-26599990**
Bank of Baroda	**1800 102 4455**
PNB	**1800 180 2222**
Central Bank	**1800 200 1911**
IDBI Bank	**1800 200 1947**

MASTERCARD

In India, the toll-free number for assistance is **000-800-100-1087.**

Call from anywhere in the world to **1-636-722-7111.**

VISA CARD

In India, use Access Code **000 117,** then **800 765 96447111.**

Collect call from anywhere in the world to **+1 303 967 1090.**

BHARAT CHANDA

VICTIM
GIRISH NAIR
39 YEARS
ENTREPRENEUR
MUMBAI

CRIME SCENE
ATM

YEAR
2016

AMOUNT INVOLVED
₹20,000

NATURE OF FRAUD

Went to withdraw cash from an ATM. The three people there said it wasn't working. When he tried to withdraw, the machine stalled. He withdrew from another machine and left. The stalled money was withdrawn immediately, he later found.

TIME TAKEN TO RESOLVE CASE

Money credited back into the account after nearly **45 days.**

MY ADVICE

"Be careful at the bank ATMs that have no security guards or have people lurking inside."

the bank and asked them to replace the card. You should also be suspicious of any mails that ask you to give sensitive information.

Mobile phone apps: There are some apps that seek access to the data on your phone. Ensure that the app is safe because it is an easy way for fraudsters to seek critical information stored on your phone.

Public terminals or Wi-Fi: If you use laptops in public areas or conduct mobile transactions over public Wi-Fi, it can be intercepted and your card details stolen.

ATM withdrawals: This is another hot spot for fraudsters to gain access to your card data and PIN. Scamsters use hidden cameras and skimmers to gain information (*see Are you likely to be conned?*) from ATMs. Mumbai's Girish Nair (*see picture*) knows it well. "When I went to withdraw money from an ATM, the machine stalled. Later, I realised that the money had been withdrawn shortly after I had left," he says. He believes that the three men in the booth at the time had rigged the ATM and taken the cash.

Preventive steps

Be alert, install protective features on your phone and computer, and educate yourself. Here are some steps you can take to avoid fraud:

Register for SMS and e-mail alerts: This will help detect a transaction you haven't made. In such a case, call up the bank's customer care number (*see Call your bank...*). Also, if your mobile stops working for unusual reasons, check with your mobile operator.

Don't disclose details: "Never give Net banking password, ATM or phone PIN to anyone or respond to unknown mails or calls asking for account details," says Silas. Adds Jasuja: "No bank or credit card firm personnel is authorised to ask a cardholder for his card details."

Hide CVV, go virtual: "While entering the CVV on a site, ensure it is masked by asterisks and the number is not visible on screen. This is especially important when shopping on foreign websites where the CVV number is the only point of verification and approval," says Jasuja. Also, while transacting on websites, use a virtual keyboard to avoid keystroke logging and while using an ATM, cover the keypad with your hand.

Don't save details on sites: Many websites ask to save credit card details for future purchases. "But one should never ever save this information," says Naidu. Neither should you do it on any server, desktop, or mobile to avoid skimming and other frauds.

If you are cheated..

The moment you fear your credit card or bank account details have been compromised or a fraudulent transaction has taken place, call the bank and have the card blocked. Follow it up with a written complaint and declaration. The bank should respond in 30 days, and if it doesn't, lodge a complaint with the ombudsman (*https://www.rbi.org.in/commonman/English/Scripts/AgainstBankABO.aspx*).

If this doesn't help, complain to the district consumer redressal forum and then to the court of law.

Rising incidence of online scams

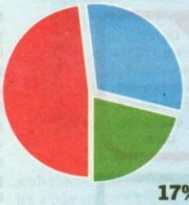
Indians are losing more money to Internet fraud than those in other Asian countries, reveals a Telenor survey.

36%
Indians cheated online.

₹8.19 LAKH
Average financial loss per person from Internet scams, compared with ₹6.81 lakh in Asia.

57%
Respondents know a friend or family member who has been a victim of online fraud.

MOST COMMON INTERNET SCAMS



25% Lottery scams

17% Fake bank e-mails

39% Work-from-home scams

14%
Respondents have been victims of identity theft.

7 in 10
Of the surveyed scam victims have lost money.

8 in 10
Respondents are confident they can protect themselves from online scams.

85%
Internet users are familiar with the term 'Internet scam' and feel open to online threats.

SOURCE: The survey was conducted by Telenor among 400 Internet users in the age group 18-65+years in India, Singapore, Thailand and Malaysia. This is India-specific data.

SCAM TERMS

Know what you are up against by going through the fraud jargon.

BOTNET

Also known as a zombie army, botnet is a network of computers that have been set up and infected with hidden software to send virus or spam to other computers on the Internet.

CLONING

The process involves using stolen credit card data to create a fake one. The data is often encoded on the magnetic strip of the card.

KEYSTROKE LOGGING

Here you unknowingly download a program that tracks every keystroke, allowing the fraudster to gain passwords and online banking and credit card information, and carry out identity theft.

MONEY MULES

Someone offers to send money into your account and asks you to transfer it to an overseas account. You get a commission, but you are laundering stolen money and can be prosecuted.

PHARMING

This involves guiding or routing you to a site that has been hijacked by scammers or to an identical destination for collecting critical information.

PHISHING

This is again a method of identity theft via e-mail. These spam mails act as if from a genuine agency or bank and trick you into parting with personal information like account details or passwords.

RANSOMWARE

This is a program that you unwittingly download which disrupts or disables your computer and then asks for a fee to fix the problem.

SCAREWARE

A malware, typically a pop-up, that appears on your screen and warns of virus on your computer. It then asks you to buy a software to rid your computer of the infection.

SHOULDER SURFING

If you are keying in your PIN at an ATM and someone looks over your shoulder.

SKIMMING

This process involves the use of portable devices, which skim the information from the magnetic strip on your ATM or credit card, and are installed on card-reading machines.

SMISHING

This is phishing on mobile phones and takes it name from SMS (short message service).

VISHING

This is short for 'voice phishing' and uses recorded messages in phones purported to be from a bank or other agencies to get you to part with account details or passwords.

VICTIM
BHARAT NAIDU
31 YEARS
ENTREPRENEUR
HYDERABAD

MY ADVICE

"Never save credit card details on e-commerce sites."

CRIME SCENE
MOBILE PHONE

YEAR
2015

AMOUNT INVOLVED
₹1.5 LAKH
CREDIT CARD LIMIT

NATURE OF FRAUD

Got two calls within a month, with the caller offering a new credit card and asking for details of the old credit card, including the CVV, to process the new one.

TIME TAKEN TO RESOLVE CASE

Shortly after the second phone call.

PHONE CALLS, E-MAILS

Phishing and vishing are among the most prevalent of frauds to have emerged in the past couple of years.

One would assume cheating someone over the phone or mail would be difficult, but it's probably one of the easiest ways. All it takes is confidence and smooth-talking on the part of the fraudster. Besides vishing and other attempts to snare credit card information over the phone, there are other ploys to not only draw out sensitive information, but also make you pay money. This happens not only via phone but also mails. The Nigerian advance fee and lottery scams have given way to new excuses to steal your money, almost all of them demanding some sort of payment for bigger rewards.

Modus operandi

Insurance plans: If you get a call or mail, saying some of your forgotten policies are due for maturity and that you need to pay some money to secure this amount, know it to be a fraud.

Work-from-home offers: According to the Telenor survey, this is the most common form of Internet scams accounting for 39% of frauds. This will typically entail an enticing job offer that requires you to first pay some fees and charges to be able to entitle you for the job. You are asked to deposit the money in a bank account and will never hear from the caller again.

Free gifts and loans: This scam involves

DOs & DON'Ts

1. Do not pay money for any scheme or product right after the first phone call.
2. Cross-question the caller who asks for crucial details.
3. If an offer on mail seems too good to be true, like a lottery or free gift, it is.
4. If a mail or call asks you to deposit fees or charges, it's probably a scam.
5. Ignore calls from unknown numbers and do not call back.

ARE YOU LIKELY TO BE CONNED?

Take this quiz and find out if you are a sitting duck when it comes online fraud.

Q1 ***Do you have the same passwords for all your accounts?***

YES NO

IF YES: It's impossible to remember the passwords for all online accounts, be it e-mails, banking or social media accounts. A single password for all accounts makes you susceptible to fraud. You are also unsafe if you have stored the passwords online, on mail or cloud. A good option is to have a **password manager** app, which digitally secures your passwords and can be accessed by one master password.

HOW TO SELECT A PASSWORD MANAGER

- **A** If the service provider stores your password vault on cloud, ensure it keeps only encrypted copy and can't access master password.
- **B** Pick a password manager app that offers two-step verification or authentication for extra layer of security.
- **C** Choose an app that automatically logs you off after some time of inactivity.
- **D** Use a complex master password, which has lower and upper case letters, characters and digits.

Q2 ***Do you open every mail with attachment from unknown senders?***

YES NO

IF YES: You have set yourself up for phishing and infecting your computer with virus. This is the easiest way to install malware in your comp. Do not open mails, especially attachments, if you can't identify the sender or the mail looks suspicious.

HOW TO IDENTIFY JUNK MAIL

- **A** Check the subject line. If it says 'urgent', 'you've won', 'verify', etc, delete it. These are ways to catch your attention.
- **B** Check sender name. If you don't know the person, but the subject line is personal or urgent, it's a hoax.
- **C** If the mail addresses you with generic terms like 'dear friend' or 'colleague', it could be fake.
- **D** If the mail specifically urges you to open the attachment, don't do it.

Q3 ***Do you have the provision to wipe your data via remote if it gets stolen?***

YES NO

IF NO: If your phone is stolen, all your information, including passwords and logins stored on mail or elsewhere, is open to use by fraudsters. Some phones have an in-built provision to remotely erase or lock the data on the phone. You can also install apps to do so.

Q4 ***Do you carry out transactions on your mobile phone over public Wi-Fi?***

YES NO

IF YES: If you have paid a bill or even checked your bank account on your smartphone, say, at an airport via Wi-Fi connection, you have invited scamsters to gain access to information by hacking your login and password and carrying out transactions from your account.

Q5 ***Do you cover the ATM keypad while keying in your PIN?***

YES NO

IF NO: Fraudsters can steal your PIN from an ATM by installing a secret camera or a fake keypad over the real one, and using skimmers in the slot that reads your card's magnetic strip. The skimmer copies card's information when you swipe it. This can be used to clean your account.

HOW TO DETECT AN ATM SKIMMER

- **A** Scan the machine. If the card reader is a different colour than the machine, or has a strange alignment, don't use it.
- **B** Compare all the ATMs in the booth. If one seems different in colour or alignment, avoid it.
- **C** Move the card reader slot. The machine is fixed firmly and no part should move or make a sound. If it does, it has been tampered with.
- **D** Check the keypad. If it's thicker, of a strange colour or askew, don't key in the PIN. A fake keypad is placed over the real one.
- **E** Look around for tiny cameras at the top of the machine or near the keypad.

Q6 ***Do you have anti-virus software on all devices including your smartphone?***

YES NO

IF NO: Most people have anti-virus software on PC or laptops, but none on smartphones, which they are increasingly using for all financial transactions. This makes it a sitting duck for phishing and hacking attempts, allowing access to critical financial information stored on your phone.

Q7 ***Do you routinely post personal data on social media like Facebook or put up all financial details on consumer complaint sites?***

YES NO

IF YES: Just because you are comfortable with your close set of friends and family over Facebook doesn't mean you can post all personal information. It's a surefire way for scamsters to misuse the information. Also be careful not to reveal too much on complaint sites.

Q8 ***If you get a call apparently from your banker or insurance company, do you volunteer information?***

YES NO

IF YES: Be very alert and suspicious of anyone who seeks personal financial information over the phone. No bank, insurance company or other financial firms will ask you for critical details over the phone. So either disconnect immediately or question the person in great detail to identify fraud.

securing basic information from any forms you have filled in any of the offline shops. You are then offered a free gift for being a valued customer, but of course, you have to pay a small charge. Similarly offers of interest-free loans that require paying a processing fee should be ignored.

Banking calls: If you get an urgent call saying your PIN is going to be deactivated, or account closed, and that you need to share your bank or card details to continue operating it, ignore it. Similarly offers for new credit cards or redemption of points that require divulging details should be avoided.

Preventive steps

"Avoid sharing personal details at public places like malls or shopping complexes on the pretext of holiday packages or gifts," says Silas. Do not reveal your financial or personal details on application forms, phone or mails.

Similarly, avoid responding to SMSes or mails received from unknown senders or ones that urge immediate action or attention (*see How to identify junk mail*). Remember that there is no legal recourse if you lose your money in this fashion. So stay alert and secure your hard-earned money.

Please send your feedback to *etwealth@timesgroup.com*