HOW TO PREVENT IDENTITY THEFT?

IFE Academy
Education Simplified

INVESTORS FINANCIAL EDUCATION ACADEMY

Phone : 044 - 2814 3044 email : bulletin@ifea.in www.ifea.in

Protect Your Kid

Identity Fraud

Sharing is Caring...?

01

Be careful not to tell anyone any private information, including bank information. Make any ATM transactions yourself.

OMG, Selfie Time!

02

Social media can backfire, especially if you take sensitive photos or share any information. Double-check your posts!

More Mail?!

03

When credit card offers and other documents come into the mailbox, don't leave them lying around! Shred all mail before trashing them.

Who You Gonna Call?

04

If you do find evidence of identity fraud, call your police and the bank. Always file a report if you see accounts you didn't open.

Kotak eterm | kotak life

Securing your family costs even less than your daily Petrol cost

Why wait?
#LaterMaybeLate

ACT NOW

Key Benefits

- Three Plan Options
- Additional Protection with Riders
- Tax Benefits*
- Step-Up# option to increase your cover
- 3 Payout Options

Koi hai... hamesha

BEWARE OF SPURIOUS PHONE CALLS AND FICTITIOUS/ FRAUDULENT OFFERS
IRDAI is not involved in activities like selling insurance policies, announcing bonus or investment of premiums. Public receiving such phone calls are requested to lodge a police complaint.

Kotak e-Term Plan: UIN:107N104V01, Form No: N104, Kotak Permanent Disability Benefit Rider: UIN: 107B002V03, Form No: B002, Kotak Critical Illness Plus Benefit Rider: UIN: 107B020V01, Form No: B020, Ref No: KLI/18-19/E-EM/236.
This is a non-participating pure protection plan. For more details on risk factors, terms and conditions please read sales brochure carefully before concluding a sale. For more details on riders please read the Rider Brochure. #Step-Up option can be availed only at time of inception / purchase of the policy. *Tax benefits are subject to conditions specified under section 10(10D) and section 80C of the Income Tax Act, 1961. Tax laws are subject to amendments from time to time. Customer is advised to take an independent view from tax consultant. ^The above illustration is for a 30 year old healthy male, non-smoker who has chosen the Life Option with Level Recurring Payout Option and a sum assured of ₹1 Cr. and PT/PPT of 45 years with annual premium of ₹7,200. The Above premium figures are exclusive of Goods and Services Tax and Cess. Goods and Services Tax and Cess thereon, shall be charged as per the prevalent tax laws over and above the said premiums. The per day premium shown above has been calculated as (Annual Premium / 365, i.e. 7,200 / 365 = 19.73)

Kotak Mahindra Life Insurance Company Ltd. Regn. No.: 107, CIN: U66030MH2000PLC128503, Regd. Office: 2nd Floor, Plot # C - 12, G- Block, BKC, Bandra (E), Mumbai - 400 051. Website: www.insurance.kotak.com | Email: clientservicedesk@kotak.com | Toll Free No.: 1800 209 8800.
Trade Logo displayed above belongs to Kotak Mahindra Bank Limited and is used by Kotak Mahindra Life Insurance Company Ltd. under license.

Kotak eterm | kotak life

Securing your family costs even less than your daily packet of bread

₹1 CR. LIFE COVER
For less than ₹20 PER DAY*
₹1 CR. LIFE COVER

Why wait?
#LaterMaybeLate

ACT NOW

Key Benefits

- 3 Three Plan Options
- Additional Protection with Riders
- Tax Benefits*
- Step-Up® option to increase your cover
- 3 Payout Options

Koi hai... hamesha

BEWARE OF SPURIOUS PHONE CALLS AND FICTITIOUS/ FRAUDULENT OFFERS
IRDAI is not involved in activities like selling insurance policies, announcing bonus or investment of premiums. Public receiving such phone calls are requested to lodge a police complaint.

Kotak e-Term Plan: UIN:107N104V01, Form No: N104, Kotak Permanent Disability Benefit Rider: UIN: 107B002V03, Form No: B002, Kotak Critical Illness Plus Benefit Rider: UIN: 107B020V01, Form No: B020, Ref No: KLI/18-19/E-EM/237.
This is a non-participating pure protection plan. For more details on risk factors, terms and conditions please read sales brochure carefully before concluding a sale. For more details on riders please read the Rider Brochure. ®Step-Up option can be availed only at time of inception / purchase of the policy. *Tax benefits are subject to conditions specified under section 10(10D) and section 80C of the Income Tax Act, 1961. Tax laws are subject to amendments from time to time. Customer is advised to take an independent view from tax consultant. #The above illustration is for a 30 year old healthy male, non-smoker who has chosen the Life Option with Level Recurring Payout Option and a sum assured of ₹1 Cr. and PT/PPT of 45 years with annual premium of ₹7,200. The Above premium figures are exclusive of Goods and Services Tax and Cess. Goods and Services Tax and Cess thereon, shall be charged as per the prevalent tax laws over and above the said premiums. The per day premium shown above has been calculated as (Annual Premium / 365, i.e. 7,200 / 365 = 19.73)

Kotak Mahindra Life Insurance Company Ltd. Regn. No.: 107, CIN: U66030MH2000PLC128503, Regd. Office: 2nd Floor, Plot # C- 12, G- Block, BKC, Bandra (E), Mumbai - 400 051. Website: www.insurance.kotak.com | Email:clientservicedesk@kotak.com | Toll Free No.: 1800 209 8800.

HOW TO PREVENT IDENTITY THEFT?

IFE Academy

Education Simplified

Regd. office : Park View, Basement, 85/17, G.N.Chetty Road, T.Nagar, Chennai - 600 017.
email : bulletin@ifea.in www.ifea.in

First Edition: 2020

About this book

With the digital transformation around, transacting with Money has become so simple. But we need to be very careful on protecting our money in this digital world. We need to understand the ways in which we might be attacked digitally and how cautious we need to be to prevent this.

We have collated the information of how cyber attacks happen these days. We hope you would find this information useful.

Happy reading!

Rs.40/-

Published by
Investors Financial Education Academy
Park View, Basement, 85/17, G.N.Chetty Road,
T.Nagar, Chennai - 600 017.

Cybercrime

People are likely to spend a good deal of time thinking about investment risk. However they need to think about more personal security issues, such as the safety of their online financial transactions and information stored on their personal electronic devices. While most people recognize that online fraud or cybercrime is a potential threat, few know how or why they may be at risk.

Cybercrime is a dangerous crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Cybercrime basically defined as any criminal activity that occurs over the Internet. There are many examples such as fraud, malware such as viruses, identity theft and cyber stalking. In present environment, since most information processing depends on the use of information technology, the control, prevention and investigation of cyber activities is vital

to the success of the Organizations, Government's agencies and individuals. Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there is highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes. Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits promptly. They are using their capability to snip, deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today.

Categories of Cybercrime

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category.

- **Property:** This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use malicious software to gain access to a web page with confidential information.

- **Individual:** This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyber stalking, distributing pornography and trafficking.
- **Government:** This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

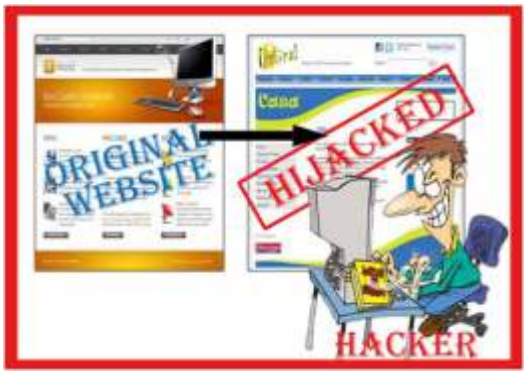
Types of Cyber crime

- **Unauthorized Access and Hacking:**

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. The persons involved in these kinds of activities are called as "hackers". Hackers try to gain access to resources through the use of password cracking software. Hackers also monitor what users do on their computer and also import files on their computer. A hacker could install several programs on to their system without their knowledge. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

- **Web Hijacking:**

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.



- **Cyber Stalking:**

This is a type of online harassment wherein the victim is endangered to a barrage of online messages and emails. Normally, these stalkers know their victims and they use the Internet to stalk. Stalking may be followed by serious violent acts such as physical harm to the victim. It means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

- **Virus Attack or Malicious Software:**

This software, also called computer virus is Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to gather sensitive information or data or causing damage to software present in the system.

- **Online Gambling:**

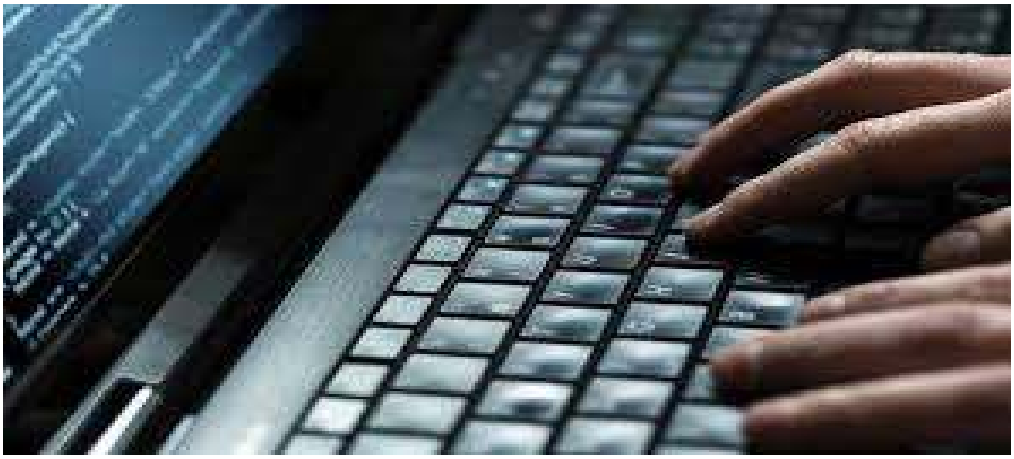
There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of Hawala transactions and money laundering over the Internet have been reported.

- **Email spoofing :**

Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

- **Child soliciting and Abuse:**

This is also a type of cybercrime in which criminals solicit minors via chat rooms for the purpose of child pornography. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the



internet. In recent times, Government has been spending a lot of time monitoring chat rooms visited by children in order to reduce and prevent child abuse and soliciting.

- **Phishing:**

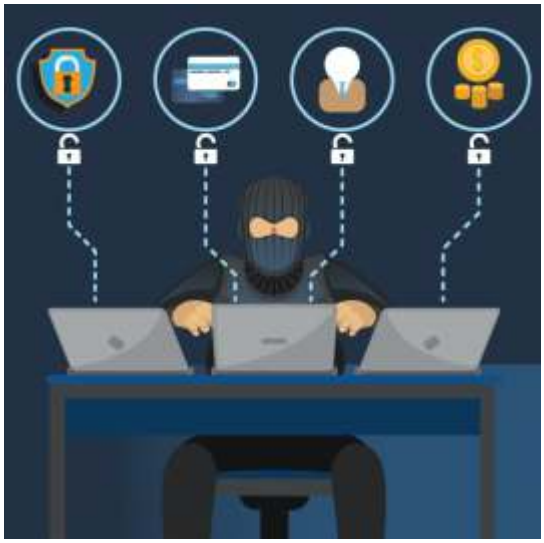
Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

Apart from the above Types of Cyber crime, the most important type is "Identity Theft".

- **Identity Theft:**

Identity theft also known as identity fraud is a crime in which the accused obtains the key pieces of personally identifiable information. Identity theft refers to the fraudulent use of someone's name and personal information in order to obtain credit, loans, etc. Identity theft is using someone else's identity intentionally to gain a financial advantage or any other benefit in the person's name. It is when thieves steal the individual's personal information to gain access to their bank account or use the information for committing fraud or a crime.

Types of Identity Theft



Criminal Identity theft: Criminal Identity theft occurs when someone who has been arrested for committing a crime presents himself as another person, by using that person's details and information. This results in the filing of criminal

record against the victim who may have no idea about the crime committed or may not learn about the crime until it's too late or when the court summons.

Financial Identity theft: Financial Identity theft refers to the taking over of the victim's account by the criminal by stealing his personal information. Thus, financial identity theft is the outcome of Identity theft. The ultimate goal of the criminals is to obtain the credit card in the name of the victim or to

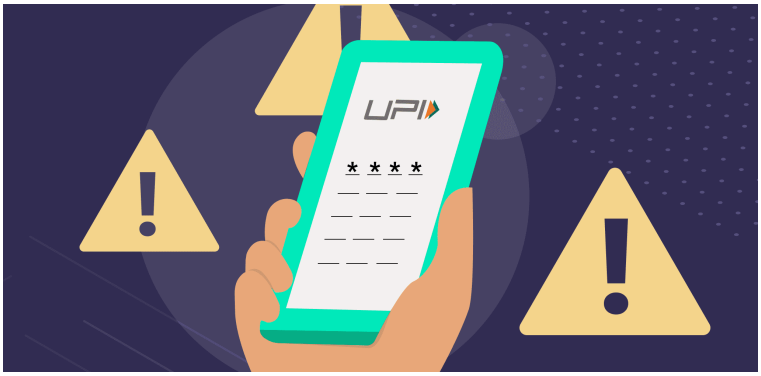
withdraw the amount from the victim's account. This includes taking a loan on the victim's name, writing the cheques on the victim's name or transferring money from the victim's account. Also, using goods and services by claiming to be someone else come into financial identity theft.

Synthetic Identity Theft: Synthetic Identity theft is the most common identity theft in which original identities are completely or partly forged. It is committed by the criminals by combining the fake credentials and the legitimate personal information of the victim in order to create a fake document. This false document can be used by the criminal to apply for a loan, obtain a duplicate license, apply for credit, etc.

Cybercrime in Digitalization world: In the recent times with the development of technologies, many new modes of fraudulent activities are also being evolved. Sometimes this technological development doesn't act as a boon with the evolvement of new kinds of Cyber crime activities. With the evolvement of digitalization around the world many kinds of criminal activities are being done. Here are some points that are to be kept in mind while paying digital payments in order to escape from the digitalization frauds.

- The explosion of smart phones with internet and multiple modes of payment methods have evolved the environment in fraudulent activities. Eg: Payment requests made on the Unified Payments Interface (UPI) by sharing of QR codes on WhatsApp.

- While making payments on UPI, the hackers would misuse the request feature on UPI by sending fake payment requests with the message stating "Enter your UPI PIN". However, it is to be noted that one need to enter PIN only while sending money. Do not pay or enter UPI PIN for receiving money.
- Hackers share a QR code over Whatsapp asking for the code to be scanned to receive money in their account. This QR code, a feature in some UPI apps, is in fact a collect request and scanning and entering the PIN is acceding to their request. Again one needs to scan QR only to make payments. Do not Share card number, expiry date, PIN, OTP etc. with anyone.
- Hackers ask users to install screen-sharing apps such as Screen share, any desk, and Team viewer and use them to get access to bank credentials. These apps are not malware, but they do grant access of the mobile data to the third party. Do not: Download third-party apps such as Screen share, any desk, and Team viewer to enable/receive payments.



- Hackers manage to get a duplicate SIM which provides them access to one-time passwords. They do this by pretending to be from a mobile company and asking the individual to forward an SMS containing the SIM card number to activate the duplicate SIM. Do not: Respond to texts, emails from unknown addresses to click on links.

Preventive measures to be taken to escape from Cybercrime:

- Computer users must use a firewall to protect their computer from hackers. Most security software comes with a firewall. Turn on the firewall that comes with their router as well.
- Computer users are recommended to purchase and install anti-virus software such as McAfee or Norton Anti-Virus. AVG offers free anti-virus protection.
- It is advised by cyber experts that users must shop only at secure websites. They should never give their credit card information to a website that looks suspicious or to strangers.

- Users must develop strong passwords on their accounts that are difficult to guess. Include both letters and numerals in their passwords. They must continuously update passwords and login details. By changing login details, at least once or twice a month, there are less chances of being a target of cybercrime.
- It is suggested to monitor children and how they use the Internet. Install parental control software to limit where they can surf.
- Make sure that social networking profiles such as Facebook, Twitter, YouTube, MSN are set to private. Check their security settings and be careful what information users post online. Once it is on the Internet, it is extremely difficult to remove.
- Secure mobile devices. More often than not, people leave their mobile devices unattended. By activating the built-in security features, they can avoid any access to personal details. Never store passwords, pin numbers and even own address on any mobile device.

- Protect Data to avoid criminals to hack. Use encryption for most sensitive files such as tax returns or financial records, make regular back-ups of all important data, and store it in a different location.
- Users must be alert while using public Wi-Fi Hotspots. While these access points are convenient, they are far from secure. Avoid conducting financial or corporate transactions on these networks.
- Users must be alert while charging in the public. These hackers also start hacking the electronic devices when they are being plugged for charges in public places. This is called Juice jacking.
- Protect e-identity. Users must be careful when giving out personal information such as name, address, phone number or financial information on the Internet. Make sure that websites are secure.

- Avoid being scammed: It is suggested that users must assess and think before they click on a link or file of unknown origin. Do not open any emails in inbox. Check the source of the message. If there is a doubt, verify the source. Never reply to emails that ask them to verify information or confirm their user ID or password.

CYBER LAWS

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1. Cyber crimes under the IT Act:

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- Un-authorised access to protected system Sec.70
- Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

2. Cyber Crimes under IPC and Special Laws:

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

3. Cyber Crimes under the Special Acts:

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Act

FAQ's:

1. What is data leakage? How will you detect and prevent it?

Data leak is nothing but data knowledge getting out of the organization in an unauthorized manner. Data will get leaked through numerous ways in which – emails, prints, laptops obtaining lost, unauthorized transfer of data to public portals, removable drives, pictures etc. There are varied controls which may be placed to make sure that the info doesn't get leaked, many controls will be limiting upload on web websites, following an internal encryption answer, limiting the emails to the interior network, restriction on printing confidential data etc.

2. What are the various categories of Cybercrimes?

Cybercrimes can be basically divided into three major categories –

- Cybercrimes against persons,
- Cybercrimes against property, and
- Cybercrimes against Government.

3. Is Cyber harassment also a Cybercrime?

Cyber harassment is a distinct cybercrime. Various kinds of harassment do occur in cyberspace. Harassment can be sexual, racial, religious, or other. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cybercrime of a grave nature.

4. Is there any comprehensive law on Cybercrime today?

As of now, we don't have any comprehensive laws on cybercrime anywhere in the world. This is the reason that the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain. Cybercrimes fall into that grey area of Internet law which is neither fully nor partially covered by the existing laws. However, countries are taking crucial measures to establish stringent laws on cybercrime.

5. What are Phishing and Pharming?

Phishing and Pharming are the most common ways to perform identity theft which is a form of cyber-crime in which criminals use the internet to steal personal information from others.

6. What is the punishment for Cybercrime in India?

Computer hacking: The individual who hacks the computer or computer devices will get an imprisonment up to 3 years or a fine. Government protected system: An act of trying to gain access to a system which is a protected system by the government, will result in imprisonment for 10 years and a heavy fine.

Notes

Notes

Notes

Notes

Kotak Premier Endowment Plan
Individual Non Linked Participating Savings Life Insurance Plan

kotak life

Guarantee@ a great start to fulfill your dreams

Key Features

- **5%** Guaranteed# Additions of 5% p.a. of the Basic Sum Assured for the First 5 Policy years
- Accrual of Reversionary bonus* from 6th policy year onwards
- Structured Payout for 5/10 years as per your choice
- Comprehensive Death benefit

Timeline of your Benefits

Premium: ₹35,000^ p.a. for 15 years

Maturity Benefit at 20th year @8%# ₹10,74,667 @4%# ₹6,94,416

5th year | 10th year | 15th year | 20th year

Guaranteed# Additions of ₹23,560 p.a. in the first 5 years

You Pay ₹35,000 p.a. for 15 years i.e. ₹5,25,000

You May Get (at 20th year) @8%# ₹10,74,667 @4%# ₹6,94,416

BEWARE OF SPURIOUS PHONE CALLS AND FICTITIOUS/ FRAUDULENT OFFERS
IRDAI is not involved in activities like selling insurance policies, announcing bonus or investment of premiums. Public receiving such phone calls are requested to lodge a police complaint.

Kotak Premier Endowment Plan UIN: 107N079V02, Form No: N079, Ref. No.: KLI/19-20/E-EM/559.
This is a Savings-cum-protection oriented Participating Endowment Plan. Above example is for a 35 year old healthy male for PT/PPT of 20/15. For above illustration Sum Assured chosen is ₹4,71,190. ^The above premium figures are exclusive of Goods and Services Tax and Cess. Goods and Services Tax and Cess thereon, shall be charged as per the prevalent tax laws over and above the said premiums.
#The guaranteed and non-guaranteed benefits are applicable only if all due premiums are paid and policy is in-force. *Please note that Bonuses are NOT guaranteed and may be as declared by the Company from time to time. These bonuses will be accrued from the 6th policy year onwards till the end of the policy term and will be payable either on maturity or death. For more details on risk factors, terms and conditions please read sales brochure carefully before concluding a sale. *The assumed non-guaranteed rates of return chosen in the illustration are 4% p.a. and 8% p.a. These assumed rates of return are not guaranteed and they are not the upper or lower limits of what you might get back as the value of your policy is dependent on a number of factors including future investment performance. The actual experience may be different from the illustrated. Tax laws are subject to amendments from time to time. Customer is advised to take an independent view from tax consultant.
Kotak Mahindra Life Insurance Company Ltd. Regn. No.: 107, CIN: U66030MH2000PLC128503, Regd. Office: 2nd Floor, Plot # C- 12, G- Block, BKC, Bandra (E), Mumbai – 400 051. Website: https://insurance.kotak.com | Email: clientservicedesk@kotak.com | Toll Free No. – 1800 209 8800.
Trade Logo displayed above belongs to Kotak Mahindra Bank Limited and is used by Kotak Mahindra Life Insurance Company Ltd. under license.

Kotak Premier Moneyback Plan
Participating Anticipated Endowment Plan

kotak life

Many Dreams, One Premier Solution

Key Features

Premier Payment Benefit - Pay for only Half the Term[A]

Premier Protection Benefit - Additional benefit of Basic Sum Assured on Accidental Death

Premier Payout Benefit - Guaranteed[@] payout will range from 110% to 130% of Sum Assured

Timeline of your Benefits

Premium: ₹40,000[1] p.a. for 10 years

	5th year	10th year	15th year	20th year
Payouts →	₹66,362	₹66,362	₹66,362	@4%[#] p.a. ₹2,81,044 @8%[#] p.a. ₹5,38,862

Balance Sum Assured + Maturity Addition + Accrued Reversionary Bonus[^] (if any) + Terminal Bonus[^] (if any)

You Pay ₹40,000[5] p.a. for 10 years i.e. ₹4,00,000

You May Get Guaranteed[@] Payout at 5th, 10th & 15th year ₹66,362 + **Total Maturity Payout on 20th year** @4%[#] p.a. ₹2,81,044 @8%[#] p.a. ₹5,38,862 = **Total Payout*** @4%[#] p.a. ₹4,80,130 @8%[#] p.a. ₹7,37,948

BEWARE OF SPURIOUS PHONE CALLS AND FICTITIOUS/ FRAUDULENT OFFERS
IRDAI is not involved in activities like selling insurance policies, announcing bonus or investment of premiums. Public receiving such phone calls are requested to lodge a police complaint.

Kotak Premier Moneyback Plan UIN: 107N083V02, Form No: N083, Ref. No.: KLI/19-20/E-EM/555.
This is a participating anticipated endowment plan. For more details on risk factors, terms and conditions please read the sales brochure carefully before concluding a sale. The above illustration is for a 35 year old healthy male. Policy Term 20 years & Premium Payment Term of 10 years and Sum Assured chosen is ₹3,31,812.
[1]The Above premium figures are exclusive of Goods and Services Tax and cess. Goods and Services Tax and Cess thereon, shall be charged as per the prevalent tax laws over and above the said premiums. For substandard lives, extra premium may be charged based on Kotak Life Insurance underwriting policy. [5]Premium Paying Term & Plan Term Options: 8 years for 16 year term, 10 years for 20 year term and12 years for 24 year term. *Total Guaranteed Payouts (for inforce policies) over the term of the policy will be 110% of Sum Assured, 120% of & Sum Assured & 130% of Sum Assured for policy terms of 16yrs, 20yrs & 24yrs respectively. [#]The assumed non-guaranteed rates of return chosen in the illustration are 4% p.a. and 8% p.a. These assumed rates of return are not guaranteed and they are not the upper or lower limits of what you might get back as the value of your policy is dependent on a number of factors including future investment performance. The actual experience may be different from the illustrated. ^Please note that Bonuses are NOT guaranteed and may be as declared by the Company from time to time. Benefits under this plan are dependent upon the performance of participating funds. Tax laws are subject to amendments from time to time. Customer is advised to take an independent view from tax consultant.
[@]The benefits are Guaranteed only if policy is in force and all the premiums are paid.
Kotak Mahindra Life Insurance Company Ltd. Regn. No.: 107, CIN: U66030MH2000PLC128503, Regd. Office: 2nd Floor, Plot # C- 12, G- Block, BKC, Bandra (E), Mumbai - 400 051. Website: https://insurance.kotak.com | Email:clientservicedesk@kotak.com | Toll Free No. – 1800 209 8800.

About IFE Academy

IFE Academy was established in 2011 as a Not-for-Profit entity to promote Financial Education. IFE Academy conducts Investor Awareness Programs across the country with the support of other market participants. www.ifea.in is a comprehensive website on Financial Education. It has various sections such as Videos, Puzzles & Games, Financial Calculators and Library. It gives a holistic view on financial education combining various aspects such as Savings, Investments, Credit, Insurance and Pension at a single place. IFE Academy periodically publishes Investor Educational materials and distributes it to general public.

IFE Academy
Education Simplified

Investors Financial Education Academy

Regd. office : Park View, Basement, 85/17, G.N.Chetty Road, T.Nagar, Chennai - 600 017.
email : bulletin@ifea.in www.ifea.in