

CYBER SECURE

PROSPECTUS

Introduction:

With an increase in internet penetration and higher use of digital platforms, cyber fraud is growing at an increasing rate. An individual may unknowingly fall prey to various incidents like unauthorised online transactions, phishing, email spoofing, etc. which can result in financial losses. Apart from this individuals are also at the risk of reputation loss due to cyber bullying, defamation etc due to exposure to social media.

Cyber Secure policy ensures that you get optimum protection against potential cyber threats and risks.

Cyber Secure provides protection to an individual and his family against losses arising due to cyber risks and frauds like unauthorised online transactions, phishing, email spoofing, cyber bullying and defamation, data recovery due to cyber-attack, media liability and identity theft cover. It also takes care of consultant fees, legal fees, etc. concerning the cyber-attack.

Scope of the Policy:

The Policy broadly offers following covers.

- **Digital Theft of Funds** – this will cover financial losses arising due to theft of funds from the bank account, mobile wallets, debit/ credit cards due to unauthorised access, hacking, phishing, introduction of malware, etc.
- **E-Reputation Loss and E-Extortion Threat** – the policy will reimburse the cost of IT specialist, counselling costs, legal costs, lost wages due to incidents of cyber bullying or defamation. The policy will also cover legal costs, cost of IT specialist or money paid to end an Extortion threat
- **Data Recovery** – the policy covers cost of IT specialist to restore data lost, altered, corrupted or destroyed due to malware, virus, cryptoware, etc.
- **Media Liability** – this will cover amount legally liable towards a third party for defamation, breach of privacy, etc. resulting from the insured's online media activities

Additional Cover:

The following Additional cover is also available on payment of additional premium:

- **Identity Theft Cover** - the policy will reimburse the costs (fees/ expenses) incurred due to identity theft, counselling costs, lost wages, etc.
- **Value Added Services**
 - **Identity Monitoring** - We will provide 24/7 dark web monitoring services which helps stop a data breach from becoming identity theft
 - **Cyber education** - We will provide a service which is an effective approach to enhance cyber security awareness
 - **Cyber training** - We will help You to reduce the likelihood of a cyber attack through training programs.

- **Incident Response – Helpline** - From investigation to dealing with a cyber emergency, Our Incident Response team helps resolve all aspects of a digital scam or cyber attack with industry-leading expertise
- **Incident Response – Online Guided Version** - We will provide an automated support portal to assist You in triaging and responding to cyber incidents
- **Digital Health Check** - We provide service for a customizable risk assessment questionnaire as a robust method for tailored evaluations and provides a comprehensive risk score
- **Attack surface Management (ASM)** - It's a platform service, where all internet connected business assets: domains, subdomains, IPs, ports, and services can be monitored continuously for cyber security vulnerabilities and potential attack vectors and other related services
- **Wi-fi Scan** - This service provides Insured to explore security vulnerabilities and potential threats within their WIFI network, utilizing advanced scanning techniques to identify and address concerns proactively
- **Safe Browsing** - This service helps to safeguard online experience, by shielding the Insured from websites that could compromise their privacy
- **Endpoint Protection (iOS & Android)** - Insured mobile device is fortified with cutting-edge security standards and features, ensuring it remains free from potentially unwanted programs
- **Service Provider education and awareness content** - We have designed an education and awareness program which will help the Service Providers to reduce the likelihood of a cyber attack
- **QR Code Scanner** - QR Code Scanner allows to scan and access encrypted information in QR codes and barcodes safely by checking any links they may contain.

Value Added Services UIN: IRDAN152RP0001V03202021/A0125V01202425

Limit of Liability

Our liability to pay or indemnify under this contract for each and every Loss and for all Loss in the aggregate shall not exceed the Limit of Liability during the Policy period.

Each sublimit of liability specified in the Schedule is part of the Limit of Liability and is the maximum We shall pay for the Insuring clause during the Policy period.

In the event of the sub limit in respect of an Insuring clause being completely exhausted on payment of a Claim, No further liability shall attach to Us in respect of the Insuring clause to which the sub limit applies

Exclusions:

1. Dishonest or Improper Conduct
2. Bodily Injury
3. Property Damage
4. Any activities carried out for business or professional purposes
5. Intellectual Property and Trade Secrets
6. Prior Acts
7. Any loss or damage caused by the order of any government authority.
8. War
9. Terrorism including cyber terrorism.
10. Government Authority
11. Non-Fiat Currency

12. Outage/ Disturbance Loss
 13. Illegal Use of Data
 14. Unauthorized Collection of Data
 15. Prior Notification
 16. Insolvency
 17. Immoral/Obscene Services
- [Kindly refer Policy wordings for detailed list of exclusions]*

Cancellation/Termination/Refund

The insured can cancel the policy at any time during the term, without assigning any reason, by giving notice in writing to the Company

The Company shall-

- Refund proportion premium for unexpired policy period, if the term of the policy is upto one year and there is no claim(s) made during the policy period.
- Refund premium for the unexpired policy period, in respect of policy with the term more than one year and the risk coverage for such policy years has not commenced.

The Company can cancel the policy only on the grounds of established fraud, by giving minimum notice of 7 days to the insured.

Reporting a Claim:

Claim should be reported as soon as reasonably practicable during the Policy Period or the Discovery Period (if applicable) for any actual Theft of funds, E-reputation loss, Extortion Loss, Data Extortion Threat, Extortion Threat, loss, alteration, corruption or destruction of Data, which may give rise to payment under this Policy.

List of Documents (non-exhaustive) to be submitted in the event of loss:

1. Submission of fully completed and signed claim form,
2. Copy of FIR lodged with police authorities / cyber cell and/or duly acknowledged copy of a Police Complaint,
3. Copies of legal notice received from any affected person/entity,
4. Copies of summons received from any court in respect of a suit filed by an affected party/entity,
5. Copies of correspondence with Bank and/or Mobile Wallet with regard to Theft of funds;
6. Legal notice served on any Bank and/or Mobile Wallet company for Theft of funds,
7. Original and/ or attested invoices for expenses incurred on all costs being claimed under this policy
8. Any other document as required to investigate the Claim or Company's obligation to make payment for it.

Reimbursement will only be in INR.

Obligations of the Policyholder:

- Insured should disclose all material information correctly at time of filling the proposal form
- In case of any change / modification / addition to the already declared information, Insured should immediately bring it to Company's notice

- Disclosure of other material information during the policy period.
- Non-disclosure of material information may affect the claim settlement.

The Policy schedule and policy wording is provided on the basis of the duly filled signed, dated and stamped proposal form provided by the Insured. Any deviation may affect the claim settlement.

NOTE:

For detailed Terms and Conditions, Coverages, Exclusions etc., please go through the copy of the Policy Wording which can be collected from any of our branches or downloaded from company web site www.zurichkotak.com.

**STATUTORY WARNING - PROHIBITION OF REBATES
(Under Section 41 of Insurance Act 1938)**

- 1) No person shall allow or offer to allow, either directly or indirectly as an inducement to any person to take out or renew or continue an insurance in respect of any kind of risk relating to lives or property, in India, any rebate of the whole or part of the commission payable or any rebate of the premium shown on the Policy, nor shall any person taking out or renewing or continuing a Policy accept any rebate, except such rebate as may be allowed in accordance with the published prospectuses or tables of the Insurer.
- 2) Any person making default in complying with the provisions of this section shall be liable for a penalty which may extend to ten lakh rupees.