दि न्यू इन्डिया एश्योरन्स कंपनी लिमिटेड
The New India Assurance Company Limited
(भारत सरकार का उपक्रम / Government of India Undertaking)

पंजीकृत एवं प्रधान कार्यालय : न्यू इन्डिया एश्योरन्स बिल्डिंग, 87, महात्मा गांधी मार्ग, फोर्ट, मुंबई - 400 001.
Regd. & Head Office : New India Assurance Building, 87, M. G. Road, Fort, Mumbai - 400 001.
(GSTIN No. : 27AAACN4165C3ZP / IRDA Registration No. : 190 / CIN No. : L66000MH1919GOI000526)

जारीकर्ता कार्यालय / Issuing Office :

PROSPECTUS FOR MY CYBER INSURANCE POLICY

(UIN No. IRDAN190RP0111V01202223)

Who are covered ?

Individuals who use internet. This Policy provides protection to Insured against loss or damage which arises directly from personal use of computer system and internet and results in the occurrence of the specified events defined in the policy, viz. Unauthorised transactions and/or online purchase transactions during the Policy Period.

What are the coverages ?

Section I : Unauthorized Transaction

Insurer shall pay Insured, up to the limit mentioned in the Policy Schedule, for Insured's direct financial loss arising out of

a) theft of funds due to an Unauthorized Transaction, and first occurring during the Policy Period and reported to Bank / debit or credit card issuer/mobile or digital wallet, as the case may be, and Insurer, within 48hours upon discovery (and in any case during the Policy Period) of such transaction. And;

b) as a consequence of Insured being a victim of a Cyber Incident or Hacking, provided that the Insured report to the issuing bank or the Mobile Wallet company within 48 hours after discovery of the Theft of Funds.

c) Theft of funds arising due to unauthorized access, malicious act or malware phishing, spoofing stand covered.

Section II : Online purchase transactions

Insurer will reimburse Insured for his/her Direct and Pure Financial Loss due to transactions on the internet via payment card or Mobile Wallet that he/she has been dishonestly induced to enter by a Third Party by electronic means to make a purchase of goods or services which are not delivered or rendered; provided that :

Insured can show that he/she has made reasonable attempts to seek a recovery or refund from the Third Party and/or seller of the goods and services to indemnify him/her for his/her financial loss; and

The fraud event is reported by insured to his/her card issuer or bank or other relevant entity within 48 hours of discovery by him/her; and

Insured card issuer or bank or other relevant entity refuses in writing to reimburse his/her for transactions made by him/her as a result of the fraud.

What shall be the sum insured ?

Option I	-	SI Rs. 15,000
Option II	-	SI Rs. 25,000
Option III	-	SI Rs. 50,000
Option IV	-	SI Rs. 1,00,000

Policy Period - Annual

Premium :

For option I	-	₹ 375 + GST
For option II	-	₹ 500 + GST
For option III	-	₹ 750 + GST
For option IV	-	₹ 1000 + GST

Deductible :

For option I & II	-	5% of claim amount subject to minimum of Rs. 500
For option III & IV	-	5% of claim amount subject to minimum of Rs. 1000

Documents required :

I . For policy issuance :

Completely filled and signed proposal form

KYC documents

(In case of any non-disclosure or mis-representation, the policy shall stand void ab initio, i.e. no liability shall attach to the insurers)

II . For Claims : Documents to the submitted at the time of a claim

a. Duly completed and signed claim form

b. Copy of complaint filed with the Police / Cyber Cell

c. Letter from the bank/ financial institution stating reason for non-admission of liability

Claim Procedure :

1. The policy holder has to report any incident which may lead to claim immediately to the insurer and latest within 48 hours of occurrence of loss
2. For claim intimation, the Policy holder may contact us at 1800 209 1415 or write to us at customercare.ho@newinia.co.in or contact nearest New India Assurance office
3. Policy holder has to file an E compliant at National Cyber Crime Reporting Portal
4. The payment of claims is dependent on Insured's providing all necessary information. Upon learning of any circumstances likely to give rise to a claim, Insured must provide all relevant documents including receipts, bills, if any, and other records in support of Insured's claim.
5. All claims are paid in INR. If Insured suffer a loss which is in a foreign currency, the amount will be converted into INR at the exchange rate on the date of the loss.

(Claims would deemed to have been suffered by the insured only if he/she has himself/herself initiated the transaction triggering the loss and which is admissible in accordance with the policy terms and conditions)

1) Grievance Redressal as stated in the policy clause and as updated from time to time www.newindia.co.in

2) Insurance Ombudsman details as stated in the policy clause and as and when amended as available in the website https://ecoi.co.in/ombudsman.html.

DO's And DONT's : Please FOLLOW the DO's and DONT's attached with this Prospectus.

STAY AWARE. STAY SAFE

For detailed terms and conditions, please get in touch with nearest New India office.

My Cyber Insurance

DO's AND DON'Ts

General :

DO's :

- Be cautious of suspicious looking pop ups that appear during your browsing sessions on internet.
- Always check for a secure payment gateway (https:// - URL with a padlock symbol) before making online payments / transactions.
- Keep the PIN (Personal IdentificationNumber), password, and credit or debit cardnumber, CVV, etc., private and do not sharethe confidential financial information withbanks/ financial institutions, friends or even family members.
- Keep hard-to-Guess Passwords or Passphrases. Password should have a Minimum of 8-10 Characters using uppercase letters, lowercase letters, numbers and Special Characters. Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Always scan unknown Universal Serial Bus (USB)drives / devices before usage.
- Turn on two-factor/multi-factor authentication where such facility is available.

DONT'S

- Avoid saving card details on websites /devices / public laptop / desktops.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links. Always delete mail/ SMS from unknown sources.
- Do not share copies of chequebook, KYC documents with strangers for device / computer security
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices. And do not Respond to fake phone calls or emails requesting for confidential data.

For safe internet browsing

- Avoid visiting unsecured / unsafe / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices.
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad locksymbol), more so when an email or SMS link is redirected to suchpages.

For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also becaptured through compromiseddevices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodically.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz.cyber cafe, etc.) for financial transactions.

Please FOLLOW the DO's and DONT's

STAY AWARE. STAY SAFE

Pls Note : This list is illustrative in nature and not exhaustive.