SETTORE D – CYBER RISK

COSA È ASSICURATO E CONTRO QUALI DANNI

ART. 71
OGGETTO DELL'ASSICURAZIONE

La Società si obbliga a risarcire/indennizzare all'Assicurato, nei limiti della somma assicurata indicata in Polizza (mod. 240469), quanto previsto dalle seguenti prestazioni:
- Home banking – Sottrazione illecita di fondi di cui all'art. 71.1;
- Acquisto on-line di cui all'art. 71.2;
- Cyber bullismo – Cyber stalking - Diffamazione di cui all'art. 71.3;
- Furto dell'identità digitale di cui all'art. 71.4;
- Responsabilità civile per violazioni della sicurezza della rete di cui all'art. 71.5;
- Supporto tecnico nel ripristino del sistema informatico 71.6;

ferma l'applicazione di franchigie, scoperti e/o limiti di risarcimento/indennizzo eventualmente previsti.

SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER – REGISTRAZIONE ALLA PIATTAFORMA

L'Assicurato, in aggiunta alle prestazioni assicurative, può usufruire di servizi aggiuntivi resi disponibili dal Service Provider tramite la sua piattaforma.
A tal fine, è necessario registrarsi al link **groupama-assicurazioni.cyberscp.it** inserendo, come da istruzioni a video, i seguenti dati:
- nome del Contraente;
- codice fiscale del Contraente;
- indirizzo e-mail del Contraente;
- numero di Polizza.

ART. 71.1 HOME BANKING - SOTTRAZIONE ILLECITA DI FONDI

La Società indennizza l'importo illegalmente sottratto dal Conto corrente on-line dell'Assicurato in caso di:
a) accesso non autorizzato tramite Malware che ha colpito il Sistema informatico;
b) divulgazione involontaria e/o colposa di Dati Personali a terzi a seguito di un'azione di Phishing, Smishing o Pharming.

La garanzia è prestata previa applicazione di una franchigia di euro 250,00 e con il limite massimo di euro 5.000,00 per sinistro e per anno assicurativo.
L'ASSICURATO dichiara, e tale dichiarazione si considera essenziale per l'efficacia della POLIZZA, di non essere a conoscenza di circostanze che possano determinare un SINISTRO.

HOME BANKING – SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.
Per rendere effettivo questo servizio, l'Assicurato deve dichiarare l'incidente al fornitore di servizi attraverso i canali previsti a tale scopo:
- chat all'interno della piattaforma del Service Provider
- telefono (al numero +39 08/09080284)
- o e-mail (all'indirizzo groupama-assicurazioni.cyberscp.it)

Il Service provider richiederà delle prove per dimostrare l'accaduto e successivamente verificherà che non vi siano malware installati sui dispositivi del Cliente ed esaminerà i siti Web in cui sono stati effettuati gli ultimi acquisti, per identificare possibili siti infetti o contraffatti.
Le e-mail ricevute verranno analizzate per identificare i casi di phishing.
Sarà inoltre emesso un rapporto forense a supporto delle attività legali e/o di recupero delle somme sottratte.
Le attività preventive sono sempre disponibili per l'Assicurato e permettono di monitorare e tenere sotto controllo la propria rete informatica.

ART. 71.2 ACQUISTO ON-LINE

La Società indennizza l'importo che l'Assicurato, indotto in maniera fraudolenta, ha pagato per il tramite di un pagamento elettronico per l'acquisto di un bene o servizio che:

- non viene consegnato o messo a loro disposizione entro 14 giorni dalla data concordata;
- presenta caratteristiche diverse rispetto a quelle oggetto della compravendita;
- non intendevano acquistare.

Il Pagamento elettronico deve essere avvenuto con:
- Carta di pagamento
- Portafoglio elettronico
- Bonifico bancario
- Download di un software utile ad effettuare il pagamento con una delle modalità indicate.

La garanzia è prestata previa applicazione di una franchigia di euro 75,00 e con il limite massimo di euro 3.000,00 per sinistro e per anno assicurativo.

ACQUISTO ONLINE - SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.
Il Service Provider richiederà di raccogliere le prove delle transazioni effettuate dall'Assicurato nel "processo di acquisto online" per analizzarle al fine di certificarne la veridicità.
Una relazione forense sarà messa a disposizione per supportare eventuali azioni legali nei confronti di eventuali siti internet "fraudolenti", eventuali "furti d'identità" occorsi.
La documentazione prodotta può essere fornita alle forze dell'ordine, al fine di supportare le opportune denunce.
Le attività preventive sono sempre disponibili per l'Assicurato e permettono di monitorare e tenere sotto controllo la propria rete informatica.

ART. 71.3 CYBER BULLISMO – CYBER STALKING – DIFFAMAZIONE

La Società mette a disposizione dell'Assicurato il Service provider per:
- eliminare da internet i contenuti utilizzati per portare a compimento il cyber bullismo;
- accedere al supporto di un esperto in materia di cyber bullismo;
- ottenere un rapporto di sorveglianza digitale dettagliato, in cui le informazioni del minorenne verranno tracciate su internet;
- ottenere raccomandazioni necessarie per correggere o cancellare qualsiasi aspetto indesiderato;
- usufruire di tecnici di informatica forense per determinare, attraverso l'analisi del dispositivo del minore, il tipo di molestia, la sua analisi e le prove certificate, se riscontrate.

La Società inoltre indennizza:
a) le spese legali sostenute dall'Assicurato per inoltrare istanza di oscuramento ai sensi di legge (legge 29 maggio 2017 n. 71 - disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo) al titolare del trattamento o al gestore del sito internet o del social media per terminare l'azione di diffamazione e/o cyber bullismo nei confronti dell'Assicurato;
b) le spese legali sostenute dall'Assicurato per rivolgersi al garante della privacy qualora il titolare del trattamento o il gestore del sito internet o del social media, di cui al punto a), non abbia ottemperato all'oscuramento entro 48 (quarantotto) ore;
c) le spese necessarie per le prime 10 (dieci) ore di supporto psicologico la cui necessità – certificata dal proprio medico curante – si potrebbe presentare in seguito alla diffamazione e/o al cyber bullismo subito dall'Assicurato.

La presente garanzia è prestata a condizione che:
1. l'Assicurato ha sofferto diffamazione e/o cyber bullismo;
2. la diffamazione e/o il cyber bullismo siano accaduti e scoperti dall'Assicurato durante il periodo di assicurazione;
3. la diffamazione e/o il cyber bullismo siano stati denunciati secondo quanto previsto dall'art. 74 Obblighi dell'Assicurato;
4. l'Assicurato deve denunciare l'accaduto alla società non appena possibile e comunque non oltre 30 giorni dalla scoperta dell'avvenuta diffamazione e/o cyber bullismo.

La garanzia è prestata con il limite massimo di euro 5.000,00 per sinistro e per anno assicurativo.

CYBER BULLISMO - SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.

- Tutte le prove digitali saranno raccolte per essere certificate, sia quelle nei dispositivi sia quelle presenti su Internet, sui sistemi di messaggistica dei social media o su sistemi come WhatsApp, Telegram o qualsiasi altro.
- Una volta raccolte le prove, saranno analizzate per identificare l'origine e/o eventuali responsabili.
- Il lavoro sarà coordinato con gli esperti, legali, psicologici o di polizia.
- Il rapporto forense, sarà messo a disposizione dei legali o direttamente a supporto di eventuali denunce alla polizia postale.
- Se necessario, verrà avviato il processo di rimozione delle menzioni su Internet.

Rimarrà attiva la sorveglianza digitale per consentire il monitoraggio delle menzioni "negative" e la successiva rimozione di quelle indesiderate.

Le applicazioni di sorveglianza digitale e di controllo parentale realizzano misure preventive raccogliendo informazioni ed elementi utili in caso di evento assicurato.

ART. 71.4 FURTO DELL'IDENTITÀ DIGITALE

La Società rimborserà:

- le **spese sostenute a seguito del Furto dell'Identità digitale** in conseguenza dell'utilizzo fraudolento di documenti d'identità falsificati e contenenti i Dati Personali degli assicurati per accedere illecitamente a linee di credito (compreso il costo per la richiesta di nuovi documenti). Dal rimborso resta escluso l'importo delle linee di credito;
- le **spese necessarie per le prime 10 ore di supporto psicologico** la cui necessità – certificata dal proprio medico curante – si potrebbe presentare in seguito al Furto dell'Identità digitale.

La garanzia è prestata con il limite massimo di euro 5.000 per sinistro e per anno assicurativo.

FURTO DELL'IDENTITÀ DIGITALE - SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.

In caso di evento che determini il furto della identità digitale:

- Vengono raccolti i dati dell'incidente, lo spoofing del profilo, le richieste di credito, lo spoofing dei dati bancari, le credenziali o i profili sostituiti.
- Vengono monitorate e raccolte, attraverso la piattaforma, tutte le menzioni esistenti sul web relative alle credenziali digitali sotto osservazione (Deep Infusion si occupa di monitorare continuamente i dati digitali del Cliente).

Il team forense verifica che non ci siano malware installati sul computer; i profili sui social network e gli account e-mail verranno esaminati per identificare eventuali accessi fraudolenti.
Nel caso fosse impossibile accedere ai profili digitali del cliente, verrà intrapreso il processo di ripristino / recupero / rigenerazione degli account e dei profili.
Nel caso in cui il furto di identità comporti una diffamazione o una perdita di reputazione, le menzioni online che hanno un impatto sull'immagine del cliente saranno monitorate da Deep Infusion e gestite per la rimozione, se necessario.
Verrà emesso un rapporto forense per accompagnare qualsiasi azione legale da intraprendere, e verranno anche emesse delle raccomandazioni per normalizzare la situazione da parte dell'Assicurato.

ART. 71.5 RESPONSABILITÀ CIVILE PER VIOLAZIONI DELLA SICUREZZA DELLA RETE

La Società si obbliga a tenere indenne l'Assicurato di quanto questi sia tenuto a pagare quale civilmente responsabile (capitale, interessi e spese) per danni provocati involontariamente a terzi a causa di un Attacco informatico al proprio Sistema informatico che abbia causato:

- l'indisponibilità del Sistema informatico del terzo danneggiato;
- l'alterazione, la cancellazione, il danneggiamento, un accesso non autorizzato o la divulgazione di Dati presenti nel Sistema informatico del terzo danneggiato.

La garanzia è prestata entro il massimale di euro 10.000,00.

RESPONSABILITÀ CIVILE DA VIOLAZIONI DELLA SICUREZZA DELLA RETE - SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.

L'analisi forense e la conseguente emissione del report permetterà di capire se la richiesta di risarcimento del terzo è giustificata o meno e si agirà in base ai risultati, in coordinamento con il team legale.
Tra i servizi preventivi, la suite di sicurezza è disponibile per identificare in anticipo se l'assicurato ha un malware infettivo che potrebbe diffondersi a terzi o contaminare siti o reti di terzi. In caso di incidente, verranno raccolte le informazioni identificate nella segnalazione di terzi per verificare l'esistenza dell'infezione, nonché la sua propagazione e i supporti coinvolti, browser, e-mail, accesso alla rete, etc.

ART. 71.6 SUPPORTO TECNICO NEL RIPRISTINO DEL SISTEMA INFORMATICO

La Società mette a disposizione dell'Assicurato un Service provider per:
- la **risoluzione di malfunzionamenti software del sistema informatico dell'Assicurato**, causati dall'introduzione di malware da parte di soggetti che abbiano operato abusivamente nelle suddette apparecchiature elettroniche;
- interrompere una **estorsione cyber** ripristinando il sistema informatico dell'Assicurato riportandolo alle condizioni di fabbrica, inclusa l'installazione del sistema operativo di cui l'Assicurato possiede licenza.

La Società, a nessuna condizione, pagherà e/o rimborserà l'ammontare richiesto durante l'estorsione cyber a titolo di riscatto.

Il Service provider, previo contatto telefonico da parte dell'Assicurato, finalizzato alla comprensione del problema informatico, prenderà in carico il bene Assicurato e procederà al ripristino dello stesso riportandolo alle condizioni di fabbrica inclusa l'installazione del sistema operativo di cui l'Assicurato possiede licenza.
In caso di estorsione cyber, l'Assicurato, pena la non validità della presente sezione, deve denunciare tempestivamente alla polizia postale (possibile anche via web attraverso sito della polizia di stato dedicato https://www.denunceviaweb.poliziadistato.it/polposta/) di essere vittima di estorsione cyber e non deve portare a conoscenza di alcuna persona – con l'eccezione delle persone che ne hanno diritto – l'esistenza della presente garanzia.

L'Assicurato deve comunque contattare il Service provider non appena possibile e non oltre 7 giorni dalla scoperta dell'avvenuto attacco informatico.

Ai fini dell'operatività della presente garanzia:
- è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider;
- si precisa che sono assicurabili, e quindi possono essere registrati nella piattaforma, fino a 5 dispositivi.

SUPPORTO TECNICO NEL RIPRISTINO DEL SISTEMA INFORMATICO - SERVIZI AGGIUNTIVI DEL SERVICE PROVIDER

Per poter usufruire di tali servizi, è necessario che l'assicurato proceda in maniera preventiva alla registrazione del dispositivo nella piattaforma del Service Provider.

I tecnici dell'helpdesk identificheranno la natura dell'evento. Se il recupero e/o la decontaminazione potrà essere effettuato da remoto, i dati dell'Assicurato saranno salvaguardati, l'apparecchiatura verrà decontaminata e i dati verranno successivamente archiviati nuovamente sul dispositivo.
Nel caso in cui la perdita di accesso ai dati contenuti nel dispositivo sia causata da un evento non gestibile da remoto, l'helpdesk sarà responsabile del ritiro del dispositivo per consegnarlo al laboratorio per il recupero dei dati.
Nei casi in cui l'attacco informatico sia avvenuto tramite ransomware, il team forense si impegnerà a raccogliere le prove, a verificare la veridicità della minaccia, e intraprendere le azioni necessarie per mitigarlo.
Anche in questo caso l'helpdesk sarà responsabile del ritiro del dispositivo per consegnarlo al laboratorio e procedere con il recupero / ripristino dei dati.

Le attività preventive si basano sull'utilizzo di un sistema protezione anti-malware tra i più avanzati e completi sul mercato (BitDefender Total security 2023) a disposizione degli assicurati.
Tali servizi di prevenzione dispongono di un sistema scansione automatica delle vulnerabilità che deve essere utilizzato periodicamente per mantenere il sistema dell'Assicurato nel miglior stato di sicurezza possibile.

ART. 72
ESCLUSIONI

L'Assicurazione non copre:
a) i sinistri accaduti prima della stipula del contratto;
b) le richieste di risarcimento conseguenti a fatti accaduti o noti all'assicurato prima della data di decorrenza del contratto;
c) danni dovuti a dolo o colpa grave degli assicurati;
d) i trasferimenti di denaro dovuti alla sottrazione fisica o allo smarrimento di Carte di pagamento;
e) le spese per revisioni, modifiche o miglioramenti, effettuate in occasione della rimessa in efficienza del Sistema informatico assicurato;
f) i danni derivanti da guasti o interruzioni o indisponibilità di sistemi di comunicazione, fornitura del servizio internet, fornitura di elettricità e di qualsiasi altra infrastruttura esterna che non sia sotto il controllo degli assicurati;
g) qualsiasi danno direttamente o indirettamente causato da, accaduto attraverso o in conseguenza di una guerra o di una guerra informatica;
h) i danni verificatasi direttamente o indirettamente in occasione di esplosioni o di emanazioni di calore o di radiazioni provenienti da trasmutazioni del nucleo dell'atomo, come pure in occasione di radiazioni provocate dalla accelerazione artificiale di particelle atomiche;
i) i danni in occasione di attacchi con armi chimiche, biologiche, biochimiche o arma elettromagnetica;
j) i danni dovuti a scarico, dispersione, infiltrazione, rilascio, fuga di sostanze pericolose o contaminanti o inquinanti;
k) i danni materiali e diretti al Sistema informatico, da qualunque causa determinato, che comportino l'impossibilità all'accensione dell'hardware;
l) i danni dovuti a confisca, requisizione, distruzione, danneggiamento del Sistema informatico, a seguito di ordini da parte di qualsiasi ente governativo, ente civile o militare;
m) i danni dovuti a utilizzo di software illegale o privo di licenza;
n) i danni dovuti a guasti, difetti, errori nella progettazione del Sistema informatico, che rendano lo stesso non adeguato allo scopo per cui è pensato il suo utilizzo;
o) i danni dovuti a un errore di codifica o sviluppo del Sistema informatico multe o sanzioni di qualsiasi natura a carico degli assicurati;
p) l'ammontare di eventuali riscatti pagati per far cessare un'Estorsione cyber e qualunque altro costo connesso all'Estorsione cyber;
q) i danni dovuti a perdite finanziarie conseguenti all'impossibilità di eseguire investimenti, cessioni, compravendite di titoli finanziari di qualunque tipo;
r) i danni conseguenti a violazione di leggi da parte degli assicurati;
s) i danni derivanti da Furto, violazione o divulgazione di brevetti o segreti industriali;
t) i danni derivanti da mancata rimozione, a seguito di denuncia o richiesta da parte di terzi, di contenuto, da siti o pagine web che siano sotto il diretto controllo degli assicurati;
u) i danni derivanti da mancata modifica, a seguito di avvertimento da parte dell'istituto di credito, delle credenziali di accesso al Conto corrente on-line;
v) i danni conseguenti ad una divulgazione illecita di Dati dal Sistema informatico dell'istituto di credito nel quale è aperto il Conto corrente on-line.

ART. 73
PERSONE NON CONSIDERATE TERZI

Non sono considerati terzi:
a) il coniuge, i genitori e i figli dell'assicurato, anche se non conviventi;
b) qualsiasi altra persona, parente o affine, che convive stabilmente con l'assicurato.

Se in caso di sinistro, il Sistema informatico degli assicurati è stato contaminato da un Malware, viene effettuato il ripristino del Sistema informatico danneggiato identificando la natura dell'evento.
Se il recupero e/o la decontaminazione può essere fatto da remoto, il dispositivo viene decontaminato,

i Dati vengono ripristinati e archiviati nuovamente sul dispositivo.
Nel caso in cui il ripristino dei Dati non è gestibile da remoto, il dispositivo viene inviato presso un laboratorio specializzato per procedere con il recupero dei Dati.

COSA FARE IN CASO DI SINISTRO

ART. 74
OBBLIGHI DELL'ASSICURATO

Entro 3 giorni lavorativi dalla data del sinistro o da quando se ne è avuta conoscenza o materialmente la possibilità, deve denunciare il sinistro alla Società o all'Agenzia alla quale è assegnata la polizza.
Nei casi di Home Banking – Sottrazione illecita di fondi, Acquisto on line, Cyber bullismo – Cyber stalking – Diffamazione, Furto dell'Identità digitale, l'Assicurato deve fare denuncia alle forze dell'ordine entro 72 ore da quando ne è venuto a conoscenza.
La Società può richiedere documentazione specifica su come è avvenuto e/o sulla relazione dell'assicurato riguardo alle persone e i beni coinvolti.
Non rispettare l'obbligo della denuncia del sinistro comporta la perdita del diritto all'indennizzo: totale in caso di dolo, parziale in caso di colpa grave (art. 1915 del Codice civile).
La Società non paga l'indennizzo se l'assicurato ha agito in accordo con i danneggiati o ne ha favorito le pretese.

ART. 75
GESTIONE DELLE CONTROVERSIE – SPESE LEGALI

Fin quando ne ha interesse, la Società può assumere la gestione della controversia a nome dell'assicurato indicando, se necessario, legali e tecnici e avvalendosi della collaborazione dell'assicurato e di tutti i diritti e azioni che gli spettano.
La Società paga le spese sostenute per resistere all'azione del danneggiato entro il limite di un quarto del Massimale stabilito in polizza per il Danno a cui si riferisce la richiesta. Se la somma dovuta al danneggiato supera il Massimale, le spese vengono ripartite fra la Società e l'assicurato.
La Società non paga le spese sostenute dall'assicurato per legali o tecnici che non sono stati nominati dalla Società, né multe, ammende o spese di giustizia penale.

LIMITI DI COPERTURA ESTENSIONE TERRITORIALE: SETTORE D – CYBER RISK

GARANZIA	DOVE
Cyber risk	Italia Stato della Città del Vaticano Repubblica di San Marino

TABELLA DI RIEPILOGO DI SCOPERTI, FRANCHIGIE E LIMITI DI INDENNIZZO: SETTORE D – CYBER RISK

GARANZIE	SCOPERTO PER SINISTRO	FRANCHIGIA PER SINISTRO	LIMITI DI INDENNIZZO
Home banking – Sottrazione illecita di fondi (art. 71.1)		euro 250,00	euro 5.000,00 per sinistro e per anno assicurativo
Acquisto on-line (art. 71.2)		euro 75,00	euro 3.000,00 per sinistro e per anno assicurativo
Cyber bullismo – Cyber stalking – Diffamazione (art. 71.3)			euro 5.000,00 per sinistro e per anno assicurativo
Furto dell'identità digitale (art. 71.4)			euro 5.000,00 per sinistro e per anno assicurativo
Responsabilità civile per violazione della sicurezza della rete (art. 71.5)			euro 10.000,00