Cyberdekking

Bijzondere voorwaarden

Model 01.25

TURIEN&CO ASSURADEUREN

Inhoudsopgave

Bijzondere voorwaarden Cyberdekking
model 01.25

1. BELANGRIJKE INFORMATIE OVER DEZE DEKKING

De cyberdekking is onderdeel van uw inboedelverzekering. Als uw inboedelverzekering wordt beëindigd, eindigt automatisch en gelijktijdig ook deze cyberdekking.

Deze bijzondere voorwaarden vormen samen met de algemene voorwaarden en uw polis de volledige voorwaarden van uw cyberdekking bij ons. Neem de tijd om deze documenten zorgvuldig te lezen, zodat u de dekking begrijpt. Controleer ook of uw gegevens op uw polis correct zijn. Is iets niet correct? Dan moet u dat onmiddellijk aan ons laten weten. Dit kan namelijk gevolgen hebben voor de dekking als u een schade meldt. De dekking is het risico dat u hebt verzekerd. Bewaar de documenten op een veilige plaats, zodat ze beschikbaar zijn als u een schade wilt melden. Wij raden u aan om regelmatig te controleren of uw dekking nog steeds aan uw behoeften en wensen voldoet. Veranderen uw gegevens, bijvoorbeeld uw naam, adres of uw gezinssamenstelling? Geef dat dan direct aan ons door. Dit kan namelijk invloed hebben op de premie van uw cyberdekking of de behandeling van uw schademeldingen.

In deze bijzondere voorwaarden leest u wanneer de cyberdekking geldt, welke risico's u ermee verzekert, welke schade wij vergoeden en wat uw rechten en plichten zijn. Aan het eind vindt u een omschrijving van de begrippen die we hebben gebruikt in deze voorwaarden.

Contact

Hebt u algemene vragen? Neem dan contact op met uw assurantieadviseur of kijk op www.turien.nl.

Wilt u een schade melden? Neem dan contact op met Sedgwick. Sedgwick is een specialist op het gebied van schadeafhandeling en aangesteld om uw schade snel en vakkundig af te handelen. U kunt Sedgwick op de volgende manieren bereiken:

- per post: Westerstraat 21, 3016 DG Rotterdam; of
- telefonisch: 010-3009024 (op werkdagen van 09:00 uur tot 16:00 uur); of
- per e-mail: cyberverzekering@nl.sedgwick.com.

2. WANNEER GELDT DEZE CYBERDEKKING?

Belangrijk: deze cyberdekking geldt alleen als u 18 jaar of ouder bent en zolang u in Nederland woont.

- **Cyber Compact:** uw gezinsleden zijn standaard meeverzekerd. Uw gezinsleden hebben alleen recht op dekking zolang ze bij u wonen op het bij ons bekende adres in Nederland.
- **Cyber Compleet**: u kunt uw gezinsleden meeverzekeren. Dat staat dan op uw polis. Maar uw gezinsleden hebben alleen recht op dekking zolang ze bij u wonen op het bij ons bekende adres in Nederland.

De cyberdekking geldt 24 uur per dag wereldwijd.

Op uw polis staat welke dekking (Cyber Compact en/of Cyber Compleet) u hebt en welke vergoedingen daarbij horen. In artikel 3 van deze bijzondere voorwaarden vindt u een samenvatting van deze dekkingen en vergoedingen. In artikel 4 van deze bijzondere voorwaarden beschrijven we de dekking, de uitsluitingen en eigen risico's.

3. SAMENVATTING VAN DE DEKKING

In de volgende tabellen leest u in het kort wat elke rubriek van deze dekking inhoudt. Op uw polis ziet u welke eigen risico's en verzekerde bedragen bij de verzekerde rubrieken horen. De artikelnummers in de tabel verwijzen naar hoofdstuk 4 van deze bijzondere voorwaarden. Daar leest u meer over de dekking, de uitsluitingen en de eigen risico's van de rubrieken.

3.1. Cyber Compact

Voor de rubrieken die deel uitmaken van Cyber Compact geldt dat u hiervoor alleen bent verzekerd als:

- op uw polis staat dat u Cyber Compact hebt verzekerd; en
- u de premie voor deze dekking hebt betaald.

Rubriek	Dekking	Omschrijving	Artikel
A	**Cyberhulplijn**	U krijgt toegang tot de Cyberhulplijn. Die helpt u om mogelijke cyberaanvallen en risico's voor uw elektronische apparatuur te herkennen. U krijgt technisch advies om cyberaanvallen te voorkomen en om veilig online te blijven. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.	4.1
B	**Cyberrisico Online Tool**	U krijgt toegang tot de Cyberrisico Online Tool: een hulpmiddel waarmee u een zelfscan kunt uitvoeren. Deze tool geeft u vervolgens een persoonlijke cyberveiligheidsscore. Bovendien krijgt u tips om u te helpen veilig online te blijven.	4.2
C	**Schade door hacking**	Hacking betekent dat iemand, zich doelbewust en met kwade bedoelingen op u richt en onbevoegd toegang krijgt tot uw elektronische apparaat. Is uw elektronische apparatuur tijdens een cyberaanval gehackt? Dan vergoeden wij de kosten om deze te repareren, herstellen of vervangen. Dat doen we tot maximaal het bedrag dat op de polis staat.	4.3

3.2. Cyber Compleet

Voor de rubrieken die deel uitmaken van Cyber Compleet geldt dat u hiervoor alleen bent verzekerd als:

- op uw polis staat dat u Cyber Compleet hebt verzekerd; en
- u de premie voor deze dekking hebt betaald.

Rubriek	Dekking	Omschrijving	Artikel
A	**Cyberhulplijn**	U krijgt toegang tot de Cyberhulplijn. Die helpt u om mogelijke cyberaanvallen en risico's voor uw elektronische apparatuur te herkennen. U krijgt technisch advies om cyberaanvallen te voorkomen en om veilig online te blijven. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.	4.1
B	**Cyberrisico Online Tool**	U krijgt toegang tot de Cyberrisico Online Tool: een hulpmiddel waarmee u een zelfscan kunt uitvoeren. Deze tool geeft u vervolgens een persoonlijke cyberveiligheidsscore. Bovendien krijgt u tips om u te helpen veilig online te blijven.	4.2
C	**Schade door hacking**	Hacking betekent dat iemand, zich doelbewust en met kwade bedoelingen op u richt en onbevoegd toegang krijgt tot uw elektronische apparaat. Is uw elektronische apparatuur tijdens een cyberaanval gehackt? Dan vergoeden wij de kosten om deze te repareren, herstellen of vervangen. Dat doen we tot maximaal het bedrag dat op de polis staat.	4.3
D	**Cyberafpersing**	Hebben criminelen uw elektronische apparatuur tijdens een cyberaanval vergrendeld en vragen zij geld om deze te ontgrendelen? Dan bieden wij u technische ondersteuning om te bepalen om wat voor soort aanval het gaat. Lukt het om de aanval te stoppen zonder losgeld te betalen? Dan vergoeden wij de kosten om uw elektronische apparatuur te herstellen. Dat doen we tot maximaal het bedrag dat op uw polis staat. Is losgeld betalen de enige mogelijkheid om uw elektronische apparatuur te ontgrendelen? Dan vergoeden wij het bedrag dat u betaalt tot maximaal het bedrag dat op uw polis staat. Hiervoor is vooraf onze uitdrukkelijke goedkeuring nodig.	4.4
E	**Online aankoopfraude**	Hebt u online een (digitaal) product gekocht of hebt u online betaald voor een (digitale) dienst, maar ontdekt u dat de website of verkoper frauduleus is? Dan vergoeden wij uw schade. Op uw polis staat welk bedrag wij maximaal vergoeden.	4.5
F	**Social engineering**	Social engineering betekent dat cybercriminelen u verleiden om geld naar hen over te maken. Bent u hiervan slachtoffer? Dan vergoeden wij de schade die u daadwerkelijk hebt geleden tot maximaal het bedrag dat op uw polis staat.	4.6
G	**Cyberpesten**	Bent u slachtoffer van cyberpesten of van een ernstige en kwaadwillende inbreuk op uw privacy? Dan vergoeden wij professioneel advies en bijstand van een erkende dienstverlener om u te helpen om verder cyberpesten of inbreuk op uw privacy te voorkomen. U mag deze dienstverlener zelf kiezen. Wij vergoeden de kosten tot maximaal het bedrag dat op uw polis staat. Als onderdeel van deze rubriek vergoeden wij ook de kosten voor psychologische hulp.	4.7
H	**Identiteitsdiefstal**	Heeft iemand uw identiteitsgegevens gestolen? Dan kunt u een juridisch adviseur inschakelen om te helpen om uw identiteit te herstellen. De kosten hiervoor vergoeden wij. Loopt u door identiteitsdiefstal kosten uit loondienst mis? Dan krijgt u daarvoor ook een vergoeding. Wij vergoeden de kosten tot maximaal het bedrag dat op uw polis staat.	4.8

4. DEKKING: TEGEN WELKE RISICO'S BENT U VERZEKERD?

4.1. Rubriek A: Cyberhulplijn

4.1.1. Dekking

U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) contact opnemen met de Cyberhulplijn op telefoonnummer 0800-0232357. De deskundige medewerkers kunnen u helpen om de beveiliging van uw elektronische apparatuur te verbeteren. Zij helpen te voorkomen dat virussen uw elektronische apparatuur infecteren. Ook kunnen ze beoordelen of uw persoonsgegevens zijn gestolen. Dan kunt u passende maatregelen nemen tegen nadelige gevolgen.

4.2. Rubriek B: Cyberrisico Online Tool

4.2.1. Dekking

U krijgt toegang tot cyberbeveiligingssoftware die u helpt online veilig te blijven. De software beoordeelt meer dan zeventig risicofactoren om uw cyberveiligheidsscore te bepalen. U ontvangt een persoonlijke cyberveiligheidsscore en rapporten. Hierdoor krijgt u inzicht in uw digitale voetafdruk: de sporen die u op internet achterlaat. Ook ontdekt u op welke manieren uw informatie, geld of privacy in gevaar kan komen. De dekking bestaat uit:

a. monitoring van maximaal 10 persoonlijke e-mailadressen per gezin;
b. beveiliging tegen kwetsbaarheid voor 10 elektronische apparaten per gezin;
c. bescherming tegen kwetsbaarheden van routers; en
d. training en waarschuwingen voor online oplichting.

Let op: voor het gebruik van de Cyberrisico Online Tool moet u zich registreren op: https://www.turien.nl/mijncyberveiligheid. De Cyberrisico Online Tool wordt uitgevoerd door Dynarisk.

4.3. Rubriek C: Schade door hacking

4.3.1. Dekking

Zijn een of meer van uw elektronische apparaten tijdens een cyberaanval gehackt? Dan bent u daarvoor verzekerd. Wat gebeurt er als uw apparatuur gehackt is?

1. U moet zo snel mogelijk contact opnemen met de Cyberhulplijn. Doe dat ook als u een cyberaanval vermoedt. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.
2. De deskundige medewerkers van de Cyberhulplijn helpen u om uw elektronische apparatuur zo goed mogelijk te herstellen. Dat doen zij telefonisch of via het online platform.
3. Heeft hun hulp geen succes? Dan vergoeden wij de kosten om uw elektronische apparatuur te repareren of te vervangen. Dit doen we tot maximaal het bedrag vermeld in uw polis, verminderd met de herstelkosten die mogelijk al gemaakt zijn.

4.3.2. Verlies van gegevens

Bij verlies van gegevens tijdens de cyberaanval proberen we de gegevens te herstellen. Maar als dat niet lukt, vergoeden we niet de schade door het verlies van de gegevens.

4.3.3. Storing aan apparatuur

Is er een storing aan uw elektronische apparatuur of werkt de apparatuur niet? En komt dat niet door een cyberaanval? Dan vergoeden wij de schade niet. De Cyberhulplijn bepaalt of er sprake is van een cyberaanval.

4.3.4. Uitsluitingen bij schade door hacking

Wij betalen geen vergoeding voor:

a. financiële schade die ontstaat doordat u de elektronische apparatuur niet kunt gebruiken door de cyberaanval of terwijl de apparatuur wordt gerepareerd;
b. elektronische apparatuur die op naam staat van, en eigendom is van uw bedrijf;
c. fysieke beschadiging, verlies of diefstal van de hardware of software;
d. kwaadwillige schade aan de hardware of software die niet rechtstreeks door de cyberaanval is veroorzaakt;
e. slijtage of geleidelijke achteruitgang van de prestaties van uw elektronische apparatuur;
f. schade aan uw elektronische apparatuur door mechanische defecten;
g. elektronische apparatuur met een jailbreak;
h. data die van een extern opslagmedium of uit de cloud of vergelijkbare online opslag- of back-upfaciliteit worden gehackt, waardoor uw identiteit wordt gestolen of wordt gebruikt voor het plegen van frauduleuze handelingen;
i. verlies van data waarvoor geen back-up is gemaakt:
   - op een extern opslagmedium dat niet verbonden is met het apparaat dat is getroffen;
   - in de cloud of op een vergelijkbare online opslag- of back-upfaciliteit.
j. digitale informatie die niet kan worden hersteld.

4.3.5. Eigen risico bij hacking

Moet de elektronische apparatuur worden gerepareerd of vervangen zoals staat in 4.3.1 bij punt 3? Dan betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

4.4. Rubriek D: Cyberafpersing

4.4.1. Dekking

We bieden technische ondersteuning en technische beveiligingsmaatregelen als uw elektronische apparatuur doelwit is van cyberafpersing.

Wat gebeurt er als u slachtoffer bent van ransomware?

1. U moet zo snel mogelijk contact opnemen met de Cyberhulplijn. Doe dit zodra u de cyberafpersing op uw elektronische apparatuur opmerkt. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.
2. De deskundige medewerkers van de Cyberhulplijn helpen u om te bepalen om wat voor soort aanval het gaat. Zij bepalen of uw elektronische apparatuur volledig of gedeeltelijk moet worden geblokkeerd.
3. Afhankelijk van de analyse van de aanval bepalen de medewerkers van de Cyberhulplijn wat de beste aanpak is. De Cyberhulplijn adviseert u niet over de vraag of u het gevraagde losgeld moet betalen.
4. Vindt u dat het betalen van losgeld de enige optie is? Dan vraagt u een autorisatiecode of bevestiging aan onze Cyberhulplijn. Zodra de Cyberhulplijn de betaling heeft goedgekeurd, kunt u het losgeld betalen en vergoeden wij het bedrag tot maximaal het bedrag vermeld in uw polis.

Let op! Hebt u het losgeld betaald, maar deblokkeert de aanvaller uw elektronische apparatuur niet, of eist de aanvaller meer losgeld? Dan moet u verder advies inwinnen bij onze Cyberhulplijn. U moet dan niet meer losgeld betalen.

Kiest u ervoor om het losgeld niet te betalen? Dan helpt de Cyberhulplijn u om uw elektronische apparatuur te herstellen, inclusief de data waarvan een back-up is gemaakt in de cloud of op een extern opslagmedium.

4.4.2. Uitsluitingen bij cyberafpersing:
Wij betalen geen vergoeding voor:
a. losgeld waarbij u niet vooraf een autorisatiecode of bevestiging van de Cyberhulplijn hebt gekregen;
b. financiële schade die ontstaat doordat u de elektronische apparatuur niet kunt gebruiken door de cyberafpersing;
c. elektronische apparatuur die op naam staat van, en eigendom is van uw bedrijf;
d. persoonlijke gegevens en bestanden die door de cyberafpersing zijn beschadigd of niet kunnen worden hersteld.

4.4.3. Eigen risico bij cyberafpersing
Voor elke schade die wij vergoeden, betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

4.5. Rubriek E: Online aankoopfraude

4.5.1. Dekking
Hebt u online een voorwerp of dienst gekocht voor persoonlijk gebruik en ontdekt u daarna dat de website/het handelsplatformverkoper frauduleus is? Dan bent u slachtoffer van online aankoopfraude. Hiervoor ontvangt u een schadevergoeding. Maar alleen als u dit voorwerp of deze dienst hebt gekocht via een digitale transactie of een bankoverschrijving.

Als u slachtoffer bent van online aankoopfraude?
1. U moet zo snel mogelijk contact opnemen met de Cyberhulplijn. Doe dit zodra u erachter komt dat u slachtoffer bent van deze fraude. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.
2. U moet aantonen dat u pogingen hebt gedaan om contact op te nemen met de verkoper om uw online aankoop alsnog (zonder fysieke beschadiging of gebreken) geleverd te krijgen of om uw geld terug te krijgen.
3. U moet binnen 24 uur nadat u de fraude hebt ontdekt contact opnemen met de uitgever van uw betaalkaart of uw bank om verdere verliezen door deze fraude te voorkomen.

Let op! In sommige gevallen vergoedt de uitgever van uw betaalkaart of uw bank deze transacties. Alleen als die dat niet doet, vergoeden wij deze transacties aan u. We hebben daarom een schriftelijk bewijs nodig dat de uitgever van uw betaalkaart of uw bank deze transacties niet vergoedt. Bovendien moet u hebben voldaan aan alle voorwaarden van de uitgever van uw betaalkaart of uw bank.

Let op! Deze dekking is niet bedoeld om u schadeloos te stellen voor aankopen op een betrouwbare website, waarbij de verkoper:
- failliet gaat;
- de verzekerde voorwerpen of diensten niet levert;
- de verzekerde voorwerpen of diensten beschadigd of gebrekkig levert.

Als het om een of meer van deze situaties gaat, moet u contact opnemen met de verkoper of de Nederlandse consumentenwetgeving raadplegen.

4.5.2. Uitsluitingen bij online aankoopfraude:
Wij betalen geen vergoeding voor:
a. online aankopen waarbij u hebt betaald met contant geld, cryptogeld zoals bitcoins, vouchers of spaarpunten;
b. ongeoorloofde transacties op uw bankrekening doordat de online aankoopfraude heeft geleid tot het klonen (kopiëren) van uw betaalkaarten of tot identiteitsdiefstal;
c. transacties die door de uitgever van uw betaalkaart of uw bank worden vergoed.

4.5.3. Eigen risico bij online aankoopfraude:
Voor elke schade die wij vergoeden betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

4.6. Rubriek F: Social engineering

4.6.1. Dekking
Hebt u een frauduleus e-mailtje of tekstbericht ontvangen met het verzoek om geld over te maken van uw persoonlijke bankrekening naar een bankrekening van iemand anders? En hebt u dat gedaan? Dan vergoeden wij het bedrag dat u hebt overgemaakt tot maximaal het bedrag dat op uw polis staat.

Wat gebeurt er als u slachtoffer bent van social engineering?
1. U moet zo snel mogelijk contact opnemen met de Cyberhulplijn. Doe dat zodra u erachter komt dat u slachtoffer bent van social engineering. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357.
2. U moet binnen 24 uur nadat u de fraude hebt ontdekt contact opnemen met uw bank, zodat die kan proberen de transactie tegen te houden of kan traceren waar het geld is gebleven.
3. U moet aantonen dat u redelijke maatregelen hebt genomen om:
   a. de identiteit van de persoon die heeft geprobeerd geld van u te krijgen vast te stellen en controleren;
   b. vast te stellen dat de persoon het recht had om de betaling te ontvangen.

Let op! In sommige gevallen vergoedt uw bank deze transacties. Alleen als die dat niet doet, vergoeden wij deze transacties aan u. We hebben daarom een schriftelijk bewijs nodig dat uw bank deze transacties niet vergoedt. Bovendien moet u hebben voldaan aan alle voorwaarden van uw bank.

4.6.2. Uitsluitingen bij social engineering
Wij betalen geen vergoeding voor:
a. een overschrijving vanaf een zakelijke rekening;
b. fraude met voorschotten, waarbij u een aanzienlijk geldbedrag wordt beloofd in ruil voor een vooruitbetaling, waaronder ook betalingen via een digitale transactie. Voorbeelden hiervan kunt u vinden op: https://www.politie.nl/onderwerpen/internetoplichting.html;
c. transacties die door uw bank worden vergoed;
d. als u geen redelijke maatregelen heeft genomen om:
   - de identiteit van de persoon die heeft geprobeerd geld van u te krijgen vast te stellen en controleren;
   - vast te stellen dat de persoon het recht had om de betaling te ontvangen.

4.6.3. Eigen risico bij social engineering
Voor elke schade die wij vergoeden betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

4.7. Rubriek G: Cyberpesten

4.7.1. Dekking

Bent u slachtoffer van cyberpesten of een inbreuk op uw privacy? Dan kunt u professioneel advies inwinnen bij een (juridisch) adviseur. Die kan u helpen de online inhoud waaruit het cyberpesten bestaat, te onderdrukken. Dat wil zeggen het onvindbaar maken van deze informatie op internet. Wij vergoeden daarvoor maximaal het bedrag dat op uw polis staat.

Daarvoor gelden deze voorwaarden:

- Cyberpesten: het cyberpesten moet van zeer beledigende aard zijn en meer dan vijf keer zijn voorgekomen.
- Inbreuk op uw privacy: het online delen van bijzonder gevoelige informatie moet kwaadwillend zijn en moet gebeurd zijn via een elektronisch apparaat.

Let op! Voldoet uw situatie niet aan de voorwaarden? Dan betekent dit niet noodzakelijk dat u geen geldige rechtszaak hebt. U kunt dan onafhankelijk juridisch advies inwinnen. Maar deze cyberdekking vergoedt de kosten hiervan niet.

Cyberhulplijn

Bent u ervan overtuigd dat u het slachtoffer bent van cyberpesten of een inbreuk op uw privacy? Neem dan contact op met de Cyberhulplijn. U kunt van maandag tot en met vrijdag (van 08:30 uur tot 21:00 uur) bellen naar de Cyberhulplijn op telefoonnummer 0800-0232357. De deskundige medewerkers beoordelen of u aan de voorwaarden voldoet om uw schade te melden. Als zij uw melding en uw bewijs accepteren, dan vergoeden wij juridisch advies en juridische bijstand tot maximaal het bedrag dat op uw polis staat.

Psychologische hulp

Bent u het slachtoffer van cyberpesten of een inbreuk op uw privacy? En heeft uw huisarts of een gekwalificeerde psycholoog vastgesteld dat u hierdoor geestelijk letsel hebt geleden? Dan vergoeden wij als onderdeel van het verzekerd bedrag voor deze rubriek de begeleiding door een erkende deskundige psycholoog die is geregistreerd bij de Nederlandse Instituut van Psychologen (NIP).

4.7.2. Uitsluitingen bij cyberpesten

Wij betalen geen vergoeding:

a. als de persoon die u pest een gezinslid is of als er gezinsleden behoren tot de personen die u pesten;
b. voor rechtsbijstand om schadevergoeding van de dader te eisen. Die rechtsbijstand vergoeden we alleen als de vordering tot schadevergoeding een bijzaak is in de juridische procedure die wordt ingesteld om verwijdering van de informatie of het stoppen van de aanhoudende pesterijen te eisen. Maar alleen als die vordering tot schadevergoeding de kans niet vermindert dat de rechter die eisen toewijst;
c. voor financiële schade doordat u uw dagelijkse taken niet kunt uitvoeren, zoals werken of persoonlijke bezigheden;
d. als u de informatie die u wilt laten verwijderen zelf al in het publieke domein hebt geplaatst, of als die informatie algemeen bekend is.

4.7.3. Eigen risico bij cyberpesten

Voor elke schade die wij vergoeden betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

4.8. Rubriek H: Identiteitsdiefstal

4.8.1. Dekking

Bent u het slachtoffer van identiteitsdiefstal? Dan krijgt u een vergoeding voor juridische kosten en gederfde inkomsten uit loondienst.

Wat gebeurt er als uw identiteit gestolen is?

1. U moet hiervan zo snel mogelijk (online) aangifte doen bij de politie. Een kopie van de aangifte moet u naar ons sturen.
2. Wij vergoeden de juridische kosten tot maximaal het bedrag dat op uw polis staat om u te helpen:
   a. het gebruik van uw identiteit te stoppen;
   b. uw kredietwaardigheid te herstellen;
   c. uw elektronische geld, bankrekening, hypotheek of lening te herstellen;
   d. de gegevens met betrekking tot uw echte naam of identiteit te wijzigen of corrigeren;
   e. u te verdedigen bij een rechtszaak die tegen u is aangespannen door een schuldeiser, incassobureau of een andere entiteit die optreedt namens een schuldeiser wegens het niet betaling van goederen of diensten of wanbetaling van een lening;
   f. een civiel vonnis ongedaan te maken dat ten onrechte tegen u is uitgesproken.
3. Wij vergoeden gederfde inkomsten uit loondienst tot maximaal het bedrag dat op uw polis staat. Hiermee bedoelen wij de tijd die u niet op uw werk hebt kunnen doorbrengen. Dit gaat om verlof dat u hebt opgenomen (exclusief ziektedagen) om uw identiteit te corrigeren na de diefstal van uw identiteit.

4.8.2. Uitsluitingen bij identiteitsdiefstal

Wij betalen geen schadevergoeding voor:

a. het afwikkelen van frauduleuze financiële transacties na diefstal van uw identiteit, zoals het terugbetalen van schulden en andere betalingsverplichtingen of van het op uw naam verkregen krediet;
b. het verlies van inkomsten uit onderneming of zakelijke activiteiten als zelfstandige, of gederfde inkomsten door de diefstal van een commerciële identiteit;
c. het verlies of de aansprakelijkheid door het gebruik van een motorvoertuig dat is gekocht, geleased of gehuurd door frauduleus gebruik van uw identiteit, waarbij civiele of strafrechtelijke maatregelen tegen u zijn genomen op basis van misbruik van uw identiteit door iemand anders;
d. het verlies of de aansprakelijkheid door het kopen of huren van onroerend goed waarbij uw identiteit is gebruikt, waarbij civiele of strafrechtelijke maatregelen tegen u zijn of zijn genomen op basis van misbruik van uw identiteit door iemand anders;
e. betalingen die u betwist op basis van de kwaliteit van goederen of diensten;
f. gederfde inkomsten, kosten of uitgaven vanwege een schade die wij niet vooraf hebben beoordeeld;
g. rekeningtransacties of transacties die u betwist op basis van de uitvoering (of niet-uitvoering) van elektronische overschrijvingen of andere mondelinge of schriftelijke instructies of aanwijzingen;
h. een incident van identiteitsdiefstal waarvoor u geen aangifte bij de politie hebt gedaan.

4.8.3. Eigen risico bij identiteitsdiefstal

Voor elke schade die wij vergoeden betaalt u een eigen risico. Hoe hoog dat eigen risico is, staat op uw polis.

5. ALGEMENE BEPALINGEN VOOR ALLE RUBRIEKEN

5.1. Algemene uitsluitingen

Niet alles is verzekerd. In de algemene voorwaarden en in deze bijzondere voorwaarden staan uitsluitingen, dat zijn gebeurtenissen waarbij de schade niet vezekerd is. In de algemene voorwaarden staan onder andere de volgende uitsluitingen genoemd:

- schade door ernstige conflicten (molest);
- schade door opzet, grove schuld of roekeloosheid;
- schade door natuurrampen;
- schade door atoomkernreacties;
- schade door fraude;
- schade door het niet nakomen van verplichtingen.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is. Raadpleeg deze voorwaarden voor de exacte omschrijving.

Welke schade is nog meer niet verzekerd?

Onderstaande uitsluitingen gelden voor deze cyberdekking:

1. Wij vergoeden geen schade onder rubrieken van deze voorwaarden die u op andere partijen kunt verhalen, zoals uw bank, de uitgever van uw betaalkaart, of een betalingsplatform.
2. Wij vergoeden geen schade die voortkomt uit een gebeurtenis vóór de ingangsdatum of na beëindiging van uw cyberdekking.
3. Wij vergoeden geen schade door een grootschalige cyberaanval of een potentiële grootschalige cyberaanval.
4. Wij vergoeden bovendien niet:
   - het verlies van cryptomunten en andere virtuele valuta, zoals bitcoins, of enige andere schade die verband houdt met cryptomunten;
   - schade die verband houdt met non-fungible tokens (NFT's);
   - schade die verband houdt met gokken.

5.2. Algemene voorwaarden

Deze voorwaarden gelden voor alle vergoedingen volgens deze cyberdekking:

- Wij zijn niet verplicht om vergoeding te betalen als u een of meer verplichtingen die in de voorwaarden of op uw polis staan niet bent nagekomen.
- Wij betalen nooit meer dan de maximumbedragen per rubriek zoals op uw polis staat.
- U mag niet uitsluiten dat u schade, verlies of aansprakelijkheid kunt verhalen op een ander. U mag dat ook niet beperken.
- Kunt u schade, verlies of aansprakelijkheid verhalen op een ander? Dan gaat u ermee akkoord dat wij dat doen, zover dat wettelijk is toegestaan. U moet er alles aan doen om ons hierbij te helpen.
- U moet op het moment dat u deze dekking aanvraagt inwoner zijn van Nederland en dat tijdens de looptijd van deze dekking blijven. Bent u van plan om naar een ander land te verhuizen? Dan moet u zo snel mogelijk contact met uw assurantieadviseur of met ons opnemen. Uw cyberdekking eindigt op het moment dat u buiten Nederland gaat wonen.

5.3. Verplichtingen bij schade

Naast de verplichtingen die in de Algemene voorwaarden en in de verschillende rubrieken van deze bijzondere voorwaarden staan, geldt het volgende:

Bij een gebeurtenis die kan leiden tot een vergoeding van de schade, bent u ten eerste verplicht dat zo spoedig mogelijk te melden. U moet dat doen door contact met Sedgwick op te nemen. U kunt Sedgwick op de volgende manieren bereiken:

- per post: Westerstraat 21, 3016 DG Rotterdam; of
- telefonisch: 010-3009024 (op werkdagen van 09:00 uur tot 16:00 uur); of
- per e-mail: cyberverzekering@nl.sedgwick.com.

Ten tweede bent u verplicht om de schade zo veel mogelijk te voorkomen en beperken. Van de noodzakelijke kosten die u hierbij maakt, vergoeden wij maximaal eenmaal het betreffende bedrag per gebeurtenis, zoals op uw polis staat. Deze vergoeding geldt boven het verzekerde bedrag voor de betreffende rubriek.

Ten derde moet u binnen een redelijke termijn alle informatie aan ons geven die nodig is om de schade te beoordelen. Dat betreft in ieder geval:

- uw polisnummer (dat staat op uw polis);
- alle originele facturen, ontvangstbewijzen en (zo nodig) de politieaangifte;
- de aankoopbewijzen van voorwerpen of diensten waarvoor u een schadevergoeding vraagt. Als u die niet kunt overleggen, beslissen wij of wij de schade wel of niet vergoeden.

Komt u één of meer van deze verplichtingen niet na en zijn onze belangen hierdoor geschaad? Dan verliest u uw recht op een uitkering.

5.4. Wijziging van de cyberdekking

Veranderingen in uw situatie kunnen ervoor zorgen dat de gegevens op uw polis niet meer kloppen. Wijzigingen moet u schriftelijk aan uw assurantieadviseur of Turien & Co. doorgeven. Wij beoordelen het wijzigingsverzoek en bevestigen schriftelijk of we de cyberdekking voortzetten en onder welke voorwaarden.

6. OMSCHRIJVING VAN BEGRIPPEN

In deze bijzondere voorwaarden gebruiken we bepaalde begrippen. In dit onderdeel lichten we toe wat we daaronder verstaan.

Aankoopbewijs
Onder *aankoopbewijs* verstaan we het originele bewijs dat u iets hebt gekocht, met de details van de artikelen die u hebt gekocht. Het aankoopbewijs moet op uw naam staan. Hebt u geen aankoopbewijs? Dan moet u een ander bewijs geven waaruit duidelijk blijkt dat u de artikelen zelf hebt gekocht.

Back-up
Een *back-up* is een kopie van de bestanden die op een computer, tablet of smartphone staan, zoals foto's, video's, muzieknummers, tekstbestanden en belastingaangiften. De back-up staat in de cloud of op een extern opslagmedium.

Bederfelijke goederen
Bederfelijke goederen zijn producten die na verloop van tijd door hun omgeving bederven. Denk hierbij bijvoorbeeld aan voedsel, parfum, medicijnen, cosmetica en chemicaliën.

Beschadiging
Een *beschadiging* is alle plotselinge en onvoorziene fysieke schade die ontstaat door een oorzaak buiten uzelf om, waardoor uw elektronische apparatuur niet meer of niet goed meer werkt. Denk aan schade ontstaan door brand of water.

Betaalkaarten
Met *betaalkaarten* bedoelen we creditcards, bankpassen, chip- en pinkaarten, oplaadkaarten, cadeaubonnen en prepaidkaarten die door creditcardbedrijven, banken of winkels zijn uitgegeven.

Bijzonder gevoelige informatie
Bijzonder gevoelige informatie is informatie in woord of beeld over uw privéleven, gezondheid, afkomst, politieke opvattingen, religieuze overtuigingen of financiële zaken:

- die wij als persoonlijk en vertrouwelijk beschouwen; en
- waarvoor u redelijke maatregelen hebt genomen om ze vertrouwelijk te houden.

Cyberaanval
Bij een *cyberaanval* gaat het om de volgende kwaadwillende of frauduleuze handelingen die op afstand via elektronische apparatuur worden uitgevoerd:

- onbevoegde toegang tot, of onbevoegd gebruik van uw elektronische apparatuur;
- wijzigingen die zijn aangebracht, corruptie die is veroorzaakt, beschadiging, manipulatie, verduistering, verwijdering van hardware, software en databestanden op uw elektronische apparatuur;
- het overbrengen, aanbrengen of invoeren van een computervirus of andere schadelijke software, waaronder ransomware op uw elektronische apparatuur;
- beperking of belemmering van de toegang tot uw elektronische apparatuur; en
- overname van een account, waarbij de fraudeur de controle over uw elektronische accounts overneemt en de toegang tot deze diensten en platformen voor u blokkeert. Denk aan accounts van bankrekeningen, creditcards, e-mail en sociale media.

Cyberafpersing
Er is sprake van *cyberafpersing* als kwaadwilligen met software de toegang tot uw elektronische apparatuur blokkeren of versleutelen, of dreigen dat te doen als u geen losgeld betaalt. En ook als zij dreigen persoonlijke gegevens en bestanden te verwijderen of openbaar te maken als u geen losgeld betaalt.

Cyberpesten
Er is sprake van *cyberpesten* als iemand u online lastigvalt of pest via e-mail, chatberichten of in de sociale media, maar alleen als dat kwetsend is en leed, angst of een vorm van geweld veroorzaakt.

Digitale informatie
Gegevens die in een digitale vorm zijn gemaakt en vastgelegd, noemen we *digitale informatie*. Voorbeelden hiervan zijn: software, games, apps, ringtones, e-books, online bladen en digitale media zoals muziek, film en televisie. Digitale informatie kan aan u worden geleverd in een tastbare vorm, bijvoorbeeld op cd, dvd of usb-stick, of in niet-tastbare vorm, zoals een download of stream.

Digitale transactie
Een *digitale transactie* is een betaling (transactie) via een online bankrekening.

Eigen risico
Het *eigen risico* is het bedrag dat u zelf moet betalen voor elke schade die wij vergoeden.

Elektronische apparatuur/apparaten
Onder *elektronische apparatuur* verstaan wij alle persoonlijke apparaten die met een netwerk zijn verbonden, bijvoorbeeld een desktop, laptop of netbook, smartphone, tablet, wearable device, slim huishoudelijk apparaat en router. U gebruikt deze apparaten niet voor uw bedrijf en ze staan ook niet in verbinding met uw bedrijf.

Financiële schade
Financiële schade is een persoonlijk verlies dat in geld is uit te drukken.

Fraude
Fraude is een vorm van opzettelijk bedrog. Zaken worden bewust anders voorgesteld dan ze zijn om een voordeel te behalen ten koste van anderen.

Geestelijk letsel
Een acute stressstoornis, zwaar geestelijk leed of psychisch letsel waaraan u lijdt door cyberpesten noemen we *geestelijk letsel*. Een gekwalificeerde huisarts of psycholoog moet dit geestelijk letsel hebben vastgesteld.

Gezinslid
Een *gezinslid* is een partner, ouder, (stief-, pleeg- of adoptie)kind, broer of zus die bij u inwoont op het adres in Nederland dat bij ons bekend is.

Grootschalige cyberaanval
Een *grootschalige cyberaanval* is een cyberaanval die is bedoeld om een groot aantal software- en hardware gebruikers te treffen.

Hacker
Een *hacker* is iemand die zich doelbewust en met kwade bedoelingen op u richt en onbevoegd toegang krijgt tot uw elektronische apparaat.

Herstellen
Met *herstellen* bedoelen we:

- het terugbrengen naar hoe het elektronische apparaat werkte voordat de cyberaanval plaatsvond, inclusief het terugplaatsen van een back-up als die er is; of
- het terugbrengen naar hoe het elektronische apparaat was toen u het kocht. Dat houdt in dat we het besturingssysteem opnieuw installeren en dat we de applicaties die de winkelier of fabrikant toen had geïnstalleerd opnieuw downloaden.

Identiteitsdiefstal
Identiteitsdiefstal is diefstal van uw persoonlijke gegevens of van documenten over uw identiteit. Door de identiteitsdiefstal:

- haalt iemand frauduleus geld van uw (online) bankrekening; of
- wordt u aansprakelijk gesteld om voorwerpen of diensten te betalen die frauduleus door iemand met uw identiteit zijn gekocht.

Inbreuk op uw privacy
Er is sprake van *inbreuk op uw privacy* als iemand anders dan uzelf kwaadwillig online bijzonder gevoelige persoonlijke informatie deelt via elektronische apparatuur.

Jailbreak
Het omzeilen van beveiligingssystemen die door fabrikanten op elektronische apparatuur zijn aangebracht noemen we *jailbreak*.

Kwaadwillige schade
Kwaadwillige schade is schade die opzettelijk of doelbewust door iemand anders dan uzelf is veroorzaakt.

Kwaadwillige software
Kwaadwillige software is software die de bedoeling heeft om kwaadwillige schade te veroorzaken.

Onbevoegd
Onbevoegd betekent zonder de benodigde toestemming of autorisatie.

Online bankrekening
Een *online bankrekening* is een rekening die u via elektronische apparatuur kunt gebruiken, zoals uw bankrekening, creditcardrekening of PayPal-rekening.

Ransomware
Ransomware is software om uw elektronische apparatuur te vergrendelen totdat u losgeld betaalt.

Redelijke maatregelen
Onder *redelijke maatregelen* verstaan wij dat u gecontroleerd hebt met wie u contact hebt. Dat doet u onder meer door de officiële website van het bedrijf te googelen en het rekeningnummer dat op de factuur staat te controleren, en bijvoorbeeld door na te gaan of u of een gezinslid een factuur verwacht.

Schademelding
U doet een *schademelding* als u om een vergoeding vraagt voor schade waarvoor u bent verzekerd in de rubrieken A tot en met H van deze cyberdekking.

Social engineering
Bij *social engineering* proberen cybercriminelen u te verleiden geld aan hen te betalen. Dat doen zij door u over te halen om een e-mail, chatbericht, sms-bericht of website te openen van bedrijven of personen die u kent of vertrouwt, maar die in werkelijkheid niet echt (fake, nep) zijn. Het doel is om:

- uw persoonsgegevens of inloggegevens in handen te krijgen om daarmee fraude te plegen; of
- u over te halen om een nepfactuur te betalen.

Van social engineering is in ieder geval sprake als één of meer van de volgende technieken zijn gebruikt:

- **Phishing** = hierbij "vissen" criminelen per e-mail naar wachtwoorden, betaalgegevens of pincodes.
- **Spear phishing** = hierbij doen criminelen zich voor als iemand die u kent en vragen om hen geld te lenen.
- **Smishing** = hierbij "vissen" criminelen per sms naar wachtwoorden, betaalgegevens of pincodes.
- **Vishing** = hierbij "vissen" criminelen telefonisch naar wachtwoorden, betaalgegevens of pincodes.
- **Pharming** = hierbij "vissen" criminelen via een gemanipuleerde website naar wachtwoorden, betaalgegevens of pincodes.
- **Phishing malware** = hierbij is uw apparaat geïnfecteerd met schadelijke software bedoeld om persoonlijke (bank)gegevens te verkrijgen. Voorbeelden van schadelijke software zijn een virus, worm of een trojan.
- **Spoofing** = hierbij ontvangt u een frauduleus telefoontje van iemand die zich voordoet als een medewerker van uw bank, een helpdesk of een overheidsinstantie, met de bedoeling om u geld over te laten maken naar een bankrekening van iemand anders.

Verkoper
Een bedrijf dat bij de Kamer van Koophandel is geregistreerd en dat in winkels of op internet rechtstreeks goederen en diensten aan consumenten verkoopt.

Verzekeringnemer
Onder *verzekeringnemer* verstaan we de natuurlijke persoon (mens) die deze cyberdekking afgesloten heeft en die op uw polis staat.

Voorwerp en dienst
Met *voorwerp en dienst* bedoelen we alle producten, werkzaamheden en digitale informatie, behalve:

1. namaak- of nepgoederen;
2. bederfelijke goederen;
3. aandelen, obligaties, valuta en digitale activa;
4. goederen die u op afbetaling hebt gekocht of waarbij sprake is van een financierings- of leaseconstructie, of goederen die u niet volledig hebt betaald;
5. goederen die in beslag zijn genomen of illegaal zijn verklaard door een regering, douane of overheidsorgaan;
6. dieren, vee en levende planten;
7. juwelen, horloges, vuurwapens, edele metalen, edelstenen, kunst, antiquiteiten en verzamelobjecten;
8. contant geld of equivalenten daarvan, reischeques of tickets;
9. onroerend goed;
10. (onderdelen van) motorvoertuigen, motorfietsen, scooters, vaartuigen en vliegtuigen;
11. abonnementen.

U, uw, uzelf
Met *u, uw en uzelf* verwijzen we naar u als verzekeringnemer en uw gezinsleden als u voor gezinsdekking hebt gekozen; dat staat op uw polis.

Wearable device
Een *wearable device* is draagbare technologie, zoals een smartwatch en smartglasses.

Wij, ons, onze, Turien & Co.
Met *wij, ons, onze en Turien & Co.* verwijzen we naar Turien & Co. Assuradeuren in Alkmaar.

Zeer beledigend
Iets is *zeer beledigend* als het in digitale communicatie of digitale informatie (in woord of in beeld) als zeer kwetsend, schokkend of immoreel wordt beoordeeld door de medewerkers van de Cyberhulplijn. Dat gaat dus verder dan alleen controversieel, beledigend of getuigend van slechte smaak.