

Digitale criminaliteit

Wie betaalt de schade?

Nepagenten aan de deur, een gehackt alarmsysteem, autodiefstal zonder sleutel of een vals betaalverzoek van een oplichter. Criminaliteit verandert en krijgt steeds vaker een digitaal tintje. Bij welke verzekeraars kun je je hiervoor verzekeren?

● Criminaliteit verschuift steeds meer naar je digitale omgeving. Criminelen proberen dan niet je fysieke bezittingen, maar je geld of persoonsgegevens buit te maken. Volgens het Centraal Bureau voor de Statistiek (CBS) was in 2025 17% van de bevolking van 15 jaar en ouder slachtoffer van online criminaliteit. Dat zijn 2,5 miljoen mensen. Bij online criminaliteit gaat het bijvoorbeeld om misbruik van persoonsgegevens, een valse webshop, misleidende sms'jes, bankhelpdeskfraude, valse betaalverzoeken of phishingmails. Ook gestolen creditcard- of bankpasgegevens veroorzaken in veel gevallen financiële schade.

Bij sommige verzekeraars kun je terecht voor een cyberdekking. Van de 17 verzekeraars in ons onderzoek (zie het kader op de pagina hiernaast) bieden 7 inboedelverzekeraars een cyberverzekering aan. Bij ASR, AnsvarIdéa, Vereniging Eigen Huis, Nationale-Nederlanden en Univé is die standaard onderdeel van je inboedelverzekering. Bij AnsvarIdéa geldt standaard een basisdekking en krijg je tegen extra premie een uitgebreidere dekking. Bij verzekeraars ANWB en Unigarant is het mogelijk om te kiezen voor een aanvullende cyberdekking.

Aan deze zeven inboedelverzekeraars

legden we vier situaties van online criminaliteit voor: een valse betaallink, gestolen bankpasgegevens, identiteitsfraude en een nepwebsite. De cyberverzekering van ANWB en Unigarant geeft in geen van deze vier situaties dekking voor financiële schade. Wanneer je geld kwijtraakt aan cybercriminelen, kun je bij hen dus niet terecht. Wel vergoeden zij bepaalde kosten, zoals voor dataherstel. Of de kosten voor een

notaris, als je door online identiteitsdiefstal opnieuw moet bewijzen wie je bent. Bij de andere cyberverzekeringen hangt het van de situatie af of je verzekerd bent. Ook offline zijn er nieuwe vormen van criminaliteit bij gekomen. Denk aan nepagenten die je geld of sieraden proberen te stelen, een autodief die zonder sleutel je auto opent en start, of een inbreker die je slimme alarmsysteem hackt en uit-

Zo blijf je online scherp

- **Controleer het webadres van een betaalpagina.**
- **Stel voor elk account een uniek wachtwoord in en gebruik tweestapsverificatie.**
- **Zie je in een mail alleen een bedrijfsnaam staan? Check of het e-mailadres overeenkomt.**
- **Word je aangezet tot snel handelen? Wees in dat geval voorzichtig. Vaak wordt met 'blokkeren' of 'extra kosten' bedreigd.**
- **Geef nooit pincodes of wachtwoorden door.**
- **Bel bij twijfel je bank.**
- **In nepmails wordt vaak gevraagd gegevens te controleren.**
- **Staat er een link in de mail of sms? Controleer het webadres achter de link, door er bijvoorbeeld met je cursor op te gaan staan zonder erop te klikken.**
- **Open niet zomaar bijlagen.**

schakelt. Die laatste twee hebben ook een digitaal karakter. Een vierde vorm is skimming.

We legden ook deze 4 situaties voor aan de 17 inboedel- en reisverzekeraars in ons onderzoek. Daarnaast onderzochten we de voorwaarden van autoverzekeringen bij sleutelloze autodiefstal. Wanneer krijg je de schade vergoed?



Een valse betaallink

Je ontvangt een nepmail van een bank, webwinkel of overheidsinstantie. In de mail staat een link met een betaalverzoek. Waarschijnlijk let je inmiddels goed op waar je op klikt. Op de website van het Nationaal Cyber Security Centrum (ncsc.nl) staan veel tips om een nepmail te herkennen (zie het kader hiernaast). Maar ook als je goed oplet, kan het een keer misgaan. Heb je financiële schade door online criminaliteit, doe dan altijd aangifte en neem contact op met je bank. Ook als de schade onder je cyberverzekering valt, vergoeden verzekeraars pas als je bank dat niet doet. Maak je zelf geld over naar een valse rekening, dan gaat het om een zogeheten toegestane betaling. De bank hoeft die schade niet altijd niet te vergoeden. Als je na misleiding zelf geld overmaakt, krijg je je schade daarom meestal niet terug van de bank.

Stel: je klikt op een valse betaallink en maakt geld over. Bij welke cyberverzekeringen kun je in dat geval terecht voor een vergoeding? Ansvardéa, Vereniging Eigen Huis en Univé vergoeden deze schade. Bij ASR biedt de cyberverzekering geen dekking als je zelf geld overmaakt, maar je inboedelverzekering wel. Die vergoedt diefstal van geld tot €500. Ook als dat, zoals in ons voorbeeld, door oplichting wordt gestolen.



Gestolen bankgegevens

De afgelopen maanden kwamen meerdere grote en kleine hacks in het nieuws. Bij een hack van een bedrijf kunnen ook bank- of creditcardgegevens zijn gestolen. Hackers proberen vervolgens

met die gegevens geld van je rekening te halen of een betaling met je creditcard te doen. Dat gebeurt niet altijd direct. Soms merk je de fraude pas als je onverwachte afschrijvingen op je rekeningoverzicht ziet staan.

Maak je zelf geen geld over, maar gebruiken criminelen je bankpas- of creditcardgegevens? Dan gaat het om een 'niet-toegestane betaling'. De bank is wettelijk verplicht het afgeschreven bedrag terug te betalen. Alleen als de bank kan aantonen dat je grof nalatig bent geweest, mag zij een vergoeding weigeren.

Wat precies onder de norm 'grof nalatig' wordt verstaan, is niet zo lang geleden aangescherpt door het Klachteninstituut Financiële Dienstverlening (Kifid). Van grove nalatigheid is pas sprake als iemand weet dat hij mogelijk wordt opgelicht en toch zijn inloggegevens deelt. Daardoor moeten banken deze schade waarschijnlijk vaker vergoeden.

En hoe zit dat met de verzekeraars? Bij Nationale-Nederlanden, Vereniging Eigen Huis en Univé is schade door gestolen bankgegevens gedekt. Bij ASR valt dit onder de diefstaldekking van de inboedelverzekering. Let op: ook als je verzekeraar dekking geeft, geldt er vaak een maximumbedrag. Dat kan variëren van €500 tot €5000 per gebeurtenis. Bij sommige verzekeraars geldt een maximumbedrag per jaar.



Identiteitsfraude

Iemand steelt je persoonsgegevens en huurt op jouw naam een auto. Hij veroorzaakt daarna schade, waarvoor jij de rekening krijgt. Of de 'huurder' van de auto overtreedt de verkeersregels en er valt ineens een boete op je deurmat. Het gebruiken van de naam van iemand anders om aankopen te doen of iets te huren is een vorm van identiteitsfraude. Verzekeraars maken bij financiële schade onderscheid tussen directe en indirecte schade. In dit voorbeeld zijn de huurkosten de directe schade. De kosten van een aanrijding of boete zijn indirecte schade. De meeste cyberverzekeringen vergoeden

de kosten voor directe schade, de huurkosten dus in dit geval. Indirecte kosten komen vrijwel nooit voor vergoeding in aanmerking. Alleen Vereniging Eigen Huis vergoedt die. Bij Univé krijg je die kosten niet standaard terug, maar wel als de cybercrimineel je gegevens via online fraude te pakken heeft gekregen, zoals phishing, een hack of malware. Je krijgt dan alleen de kosten veroorzaakt door een eventuele aanrijding vergoed. Voor vergoeding van een boete kun je er niet terecht.

Is dit je overkomen en heb je juridische hulp nodig om je identiteit te herstellen? Dan kun je die via de cyberverzekering van Ansvardéa wel vergoed krijgen.



Nepwebsite

Je ziet online een aanbieding voor een leuke vakantie. De website ziet er betrouwbaar uit en de prijs is aantrekkelijk. Je boekt de reis en betaalt vooruit. Achteraf blijkt de website nep te zijn: de vakantie bestaat niet en je bent je geld kwijt. Dit heet ook wel online aankoopfraude. Wil je je geld terug, dan ►

Verzekeraars onder de loep

In het artikel noemen we bij elke situatie vooral de woon- en reisverzekeraars die in dat geval dekking bieden.

De volgende verzekeraars hebben we in ons onderzoek meegenomen: Allianz Direct, Ansvardéa, ANWB (inclusief Unigarant), ASN Bank, ASR, Centraal Beheer, De Goudse, FBTO, InShared, Interpolis, Klaverblad, Lemonade, Ohra, Nationale-Nederlanden (Bank), Univé, Vereniging Eigen Huis, Zevenwouden.



Zo houd je boeven buiten

- **Laat onbekenden nooit zomaar binnen.**
- **Vraag altijd om een legitimatiebewijs.**
- **Bel het bedrijf dat wordt genoemd om te controleren of er inderdaad een bezoek gepland staat.**
- **Bewaar sieraden en contant geld uit het zicht of op een afgesloten plek.**
- **Gebruik voor je slimme apparaten sterke wachtwoorden. En verander deze regelmatig.**
- **Installeer zo snel mogelijk de updates van je alarm-systemen en camera's.**
- **Heb je een auto met keyless entry? Bewaar de sleutel dan niet in de buurt van de voordeur of een raam.**

kun je alleen terecht bij Ansvardéa, Univé en Vereniging Eigen Huis. Al is de dekking bij alle drie niet onbeperkt. Bij de meeste verzekeraars draai je bij een nepwebsite zelf op voor de schade.



Aan de deur

De bel gaat. Er staan twee personen voor de deur die zeggen dat ze van de politie zijn, of van het energiebedrijf. Vaak geven ze aan dat ze iets in je huis moeten controleren. Terwijl de een je aan de praat houdt, loopt de ander ongemerkt verder. Na hun vertrek kom je erachter dat je sieraden en geld zijn verdwenen. Dit soort babbeltrucs hoor je steeds vaker. In 2025 nam het aantal meldingen met ruim 50% toe ten opzichte van het jaar ervoor. Neemt iemand ongemerkt spullen mee uit je huis, dan zien verzekeraars dat meestal als gewone diefstal. Braaksporen zijn vaak niet meer vereist bij diefstal uit je woning. Het wordt anders als je zelf spullen meegEEft. Bijvoorbeeld aan een nepagent die sieraden of een bankpas komt ophalen om ze 'veilig te stellen'. Geef je zelf spullen mee? Dan vergoeden verzekeraars de schade vrijwel nooit. Ze zien deze babbeltruc als oplichting of verduistering en die vallen niet onder je inboedelverzekering. Alleen De Goudse biedt hiervoor dekking via de allrisk-inboedelverzekering.



Open zonder sleutel

Ook autosleutels zijn slimmer geworden. Veel nieuwe auto's open je al door er alleen met de sleutel of pas in de buurt te zijn: keyless entry. Je haalt de sleutel niet meer uit je zak, vaak ook niet om de auto af te sluiten. Deze slimme autosleutel werkt met een draadloos signaal. Handig, maar ook kwetsbaar voor diefstal. Met speciale apparatuur kunnen auto-dieven dat signaal opvangen bij je voordeur of raam, als je je sleutel daar niet ver vandaan bewaart. Het signaal wordt vervolgens versterkt en doorgestuurd naar een tweede persoon die bij de auto staat. Door het sterke signaal 'denkt' de

auto dat de sleutel dichtbij is. Hij gaat open en de dief kan de auto starten. Het alarm gaat niet af. Vaak merk je de diefstal pas als de auto al lang weg is.

Werkt je autosleutel op deze manier en wil je een 'sleutellose' diefstal moeilijker maken? Bewaar de sleutel dan niet in de buurt van je voordeur of raam. Gebruik ook een RFID-blokker of Faraday-hoesje. Deze voorwerpen blokkeren het signaal, zodat dat niet met apparatuur kan worden opgepikt. Een andere optie is om de keyless entry uit te schakelen, als dat mogelijk is bij je auto. Tot slot: een stuurklem of extra beveiligingssysteem maken het onaantrekkelijk om je auto te stelen. Is het toch gebeurd? De meeste auto-verzekeraars vergoeden de schade als je een beperkt casco- of allriskverzekering hebt. Ben je verzekerd bij Bovag, Bovemij, Lancyr, Neerlandse, Univé, Vereniging Eigen Huis of Zero, dan valt sleutellose autodiefstal in de meeste gevallen niet onder de dekking.

Bij auto's met een hoog risico op diefstal stellen verzekeraars soms extra eisen aan de beveiliging. Dat geldt ook voor sommige auto's met keyless entry. Denk bijvoorbeeld aan een verplicht gecertificeerd beveiligingssysteem. Voldoe je niet aan de eisen, dan krijg je diefstalschade mogelijk niet vergoed.



Slim huis

Steeds meer huizen hebben een slim alarmsysteem met camera's of digitale sloten. Vaak bedien je die via een app. Maar wat als een inbreker het alarmsysteem hackt en daarna toeslaat? Lang niet alle woonverzekeringen stellen eisen aan de beveiliging van je huis. Het uitschakelen van het alarm door een inbreker heeft dan geen invloed op de vergoeding. De diefstal valt gewoon onder de dekking van de verzekering. Soms geldt er wel een beveiligingseis, bijvoorbeeld bij veel of kostbare inboedel. Zo'n eis komt voor bij Univé, Klaverblad, Vereniging Eigen Huis, Achmea-labels als Centraal Beheer, FBTO en Interpolis en oudere inboedelverzekeringen van

Nationale-Nederlanden. Bij de Achmea-labels geldt de beveiligingseis niet standaard, maar alleen als je diefstalgevoelige inboedel voor een hoger bedrag verzekert. Bij sommige verzekeraars, zoals Univé, moet je aantonen dat het alarm aanstond. Lukt dat niet, dan kan de verzekeraar je claim afwijzen.



Skimming

Het misbruiken van gegevens op je bankpas heet skimming. Criminelen lezen met behulp van een apparaatje je pasgegevens af bij een geld- of betaalautomaat. Vaak proberen ze ook je pincode te filmen met een verborgen camera. Daarna maken ze met die gegevens een fysieke kopie van je pas en gebruiken die om geld op te nemen. In Nederland komt deze vorm van criminaliteit vrijwel niet meer voor. In het buitenland gebeurt het nog wel.

Heb je schade door skimming? Vraag eerst na of je bank iets uitkeert. Doet die dat niet, dan kun je mogelijk bij je reisverzekeraar terecht als je tijdens je vakantie de dupe bent geworden. Dit geldt alleen voor de reisverzekeringen van Vereniging Eigen Huis en Klaverblad, en uitsluitend als je geld hebt meeverzekerd bij je bagagedekking. Dit is een aparte module. Kun je niet bij je bank of reisverzekering terecht? Een cyberdekking bij je inboedelverzekering biedt soms uitkomst. Met lang niet elke cyberdekking krijg je skimming vergoed, maar bij Nationale-Nederlanden en Vereniging Eigen Huis wel. Controleer ook in dit geval altijd eerst of je bank de schade vergoedt. ■

Je ervaring delen?

Stuur je reactie naar
lezerspost@consumentenbond.nl.
 We kunnen deze opnemen
 in de rubriek Reacties.



Mijn ervaring

'De impact is groter dan alleen het verlies van de sieraden'

Als er bij Ria Castelijin-Van der Veldt wordt aangebeld, meldt een man zich via de intercom. Hij zegt dat hij een pakketje voor haar burens heeft. Ze stelt voor om het pakketje in de lift te zetten, maar de man zegt dat hij het liever zelf naar boven brengt. Even later staan er twee mannen op haar etage. Als Castelijin naar het pakketje vraagt, zeggen ze dat de koerier het inmiddels aan iemand anders heeft gegeven. De mannen zeggen dat ze voor een loodgietersbedrijf werken. Een etage lager zou een lekkage zijn en het water kwam mogelijk uit haar appartement. 'Een lekkage wil je natuurlijk snel oplossen. Tegelijk was ik wel op mijn hoede.' Een van de mannen loopt direct naar de keuken en begint onder de gootsteen te rommelen. Na korte tijd zegt hij dat het probleem niet uit

haar appartement komt. Daarna vertrekken de twee weer. Later die dag ontdekt Castelijin dat er nergens in het appartementencomplex een lekkage is. Bovendien blijken er sieraden uit haar slaapkamer te zijn verdwenen. 'Ik dacht meteen aan die mannen. Een van hen moet kans hebben gezien om ongemerkt de slaapkamer binnen te gaan.' Ze doet aangifte bij de politie en neemt contact op met haar verzekeraar. Veel verwacht ze daar niet van. 'Ik dacht: ik heb ze zelf binnengelaten.' Maar de schade blijkt wél verzekerd. Castelijin krijgt een redelijke vergoeding, waardoor de financiële schade beperkt blijft. Maar de impact is groter dan alleen het verlies van de sieraden. 'Ik ben nog voorzichtiger geworden als er iemand bij me aanbelt.'