Uitspraak Geschillencommissie Kifid nr. 2023-0531

(mr. dr. S.O.H. Bakkerus, voorzitter, prof. mr. M.L. Hendrikse, mr. M.E.J. Bracco Gartner, leden en mr. R.E. van Lambalgen, secretaris)

Datum uitspraak	14 juli 2023
Klacht van	De consument
Tegen	bunq B.V., gevestigd te Amsterdam, verder te noemen de bank
Aard uitspraak	Bindend advies
Uitkomst	Vordering toegewezen
Bijlage	Relevante bepalingen uit de algemene voorwaarden

Samenvatting

Niet-toegestane betalingstransacties. Op 20 juli 2022 kon de consument niet inloggen op de bunq-app op zijn telefoon. Hij heeft de app daarom opnieuw geïnstalleerd op zijn telefoon. Twee dagen later, op 22 juli 2022, kreeg de consument een (frauduleus) sms-bericht waarop hij heeft gereageerd en vervolgens heeft hij onbewust de fraudeur toegang gegeven tot zijn betaalrekening. De commissie komt tot de slotsom dat de consument wel nalatig is geweest, maar niet grof nalatig. Dat de consument op de link in het frauduleuze sms-bericht geklikt heeft, is op zich grof nalatig. In dit geval zijn het sms-bericht van de fraudeur en de sms-berichten van de bank door elkaar gaan lopen. Het beroep van de bank op artikel 7:529 lid 1 BW slaagt daarom niet. Dit betekent dat de bank het bedrag van de niet-toegestane betalingstransacties (€ 14.500,-) aan de consument dient te betalen.

1. Procedure

1.1 De behandelend commissie, verder te noemen de commissie, beslist op basis van het reglement en op basis van de door partijen aan Kifid ingestuurde documenten inclusief bijlagen. Het gaat om: 1) het klachtformulier van de consument; 2) het verweerschrift van de bank; 3) de repliek van de consument; 4) de dupliek van de bank: 5) de aanvullende informatie van de consument; 6) de aanvullende informatie van de bank; 7) de reactie van de consument op het schikkingsvoorstel van de bank; en 8) de pleitnota van de advocaat van de bank.

1.2 Partijen zijn opgeroepen voor een hoorzitting op donderdag 25 mei 2023. De consument nam deel aan de hoorzitting. Namens de bank namen deel mevrouw mr. [naam 1], (advocaat), mevrouw [naam 2], (juridisch medewerker) en de heer mr. [naam 3], (head of legal bunq).

1.3 Na de hoorzitting is de enkelvoudige commissie uitgebreid met de leden prof. mr. M.L. Hendrikse en mr. M.E.J. Bracco Gartner, naar een meervoudige commissie. Partijen zijn hierover geïnformeerd.

1.4 De consument en de bank hebben gekozen voor een bindend advies. Dit betekent dat partijen elkaar aan de uitspraak kunnen houden.

2. Het geschil

Wat is er gebeurd?

2.1 De consument heeft een betaalrekening bij de bank. Hierop zijn de Algemene voorwaarden bunq van toepassing. De relevante bepalingen hiervan zijn opgenomen in de bijlage bij deze uitspraak.

2.2 Op 20 juli 2022 had de consument problemen met de bunq-app op zijn telefoon. Hij heeft de app daarom verwijderd van zijn telefoon en daarna opnieuw geïnstalleerd. Bij het installeren van de app op zijn telefoon, kreeg hij een sms-bericht van de bank met daarin een 'magic link'. De consument heeft op de 'magic link' geklikt en daarmee zijn mobiele telefoon met de naam "iPhone (5)" toegang gegeven tot zijn betaalrekening.

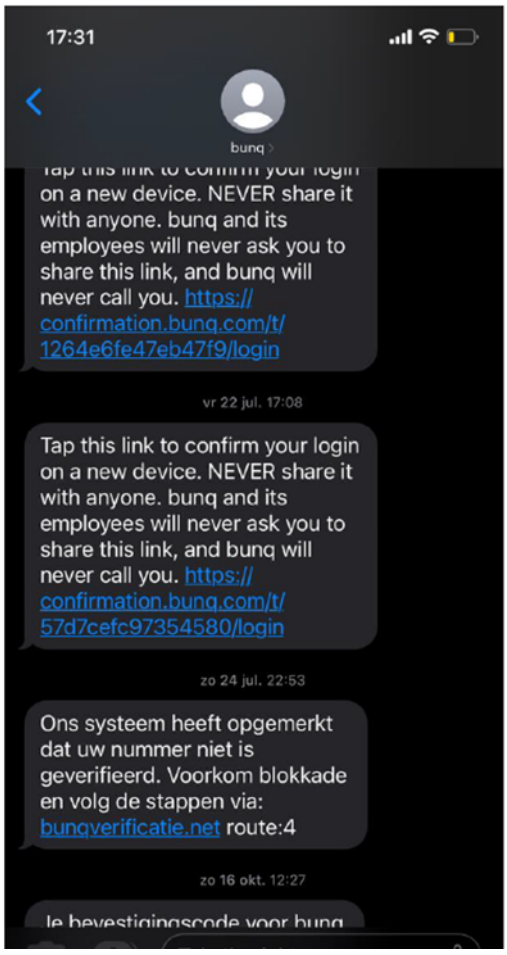
2.3 Vervolgens kreeg hij een bevestiging per e-mail:

> *"Hey [voornaam consument],*
>
> *We zien dat je net bent ingelegd op **iOS: iPhone (5)** en willen even checken of jij het echt bent.*
>
> *Als je niet onlangs op een nieuw toestel bent ingelogd en denkt dat dit iemand anders is geweest, verander dan zo snel mogelijk je inloggegevens in de app onder Beveiliging & Instellingen. Als je geen toegang meer tot je bunq account hebt, neem dan contact op met ons support team op support@bunq.com."*

2.4 Op 22 juli 2022 om 17:06 uur heeft de consument een sms-bericht ontvangen. De consument heeft de volgende screenshot overgelegd van dit sms-bericht:

2.5 De consument heeft op deze link geklikt. Vervolgens kwam hij in een ogenschijnlijke bunq-omgeving terecht waar hij zijn inloggegevens heeft ingevuld.

2.6 Op 22 juli 2022 om 17:08 uur heeft de consument een sms-bericht ontvangen van de bank met daarin een 'magic link'. De consument heeft de volgende screenshot overgelegd van dit sms-bericht:



2.7 De consument heeft op de 'magic link' geklikt en daarmee een mobiele telefoon met de naam "iPhone" toegang gegeven tot zijn betaalrekening.

2.8 Vervolgens kreeg hij een bevestiging per e-mail:

> *"Hey [voornaam consument],*
>
> *We zien dat je net bent ingelegd op **iOS: iPhone** en willen even checken of jij het echt bent.*
>
> *Als je niet onlangs op een nieuw toestel bent ingelogd en denkt dat dit iemand anders is geweest, verander dan zo snel mogelijk je inloggegevens in de app onder Beveiliging & Instellingen. Als je geen toegang meer tot je bunq account hebt, neem dan contact op met ons support team op support@bunq.com."*

2.9 Op 23 juli 2022 zijn er verschillende betalingen gedaan vanaf de betaalrekening van de consument (met een totaalbedrag van € 14.549,33). Deze betalingen zijn gedaan met een iPhone.

2.10 Op 23 juli 2022 in de avond heeft de consument contact opgenomen met de bank.

De klacht en vordering

2.11 De consument vindt dat de bank de bedragen die van zijn rekening zijn afgeschreven moet vergoeden. Hij vordert een vergoeding van de bank van € 14.500,- te vermeerderen met wettelijke rente over dit bedrag vanaf 23 juli 2022.

2.12 De consument geeft aan dat hij niet heeft ingestemd met de betalingstransacties van 23 juli 2022. Verder betwist hij dat hij grof nalatig is geweest. Hij dacht dat het sms-bericht van 22 juli 2022 nog bij het verificatieproces van 20 juli 2022 hoorde. Nadat hij op de link in het (frauduleuze) sms-bericht van 17:06 uur had geklikt, kwam hij in een omgeving terecht die er exact hetzelfde uitzag als de bunq-omgeving waar hij zich op 20 juli 2022 in bevond. Hier heeft hij zijn code ingevoerd. Vervolgens kreeg hij om 17:08 uur wederom een sms-bericht van de bank. Toen hij op de link in dat sms-bericht klikte, kwam hij in de bunq-omgeving terecht en werd hem gevraagd om te verifiëren dat hij een telefoon met de naam "iPhone" aan het registreren was. De consument heeft een iPhone, vandaar dat het verschil tussen "iPhone (5)" (de naam van zijn eigen telefoon) en "iPhone" hem niet direct was opgevallen. Na deze tweetraps-verificatie waande hij zichzelf compleet geverifieerd en veilig. Achteraf beseft hij dat dat het moment was waarop hij een vreemd apparaat (met de naam "iPhone") toegang heeft gegeven tot zijn bunq-account.

Het verweer

2.13 De bank heeft verweer gevoerd tegen de stellingen van de consument. Primair stelt de bank dat de consument niet heeft voldaan aan zijn verzwaarde motiveringsplicht. Subsidiair stelt de bank dat de consument grof nalatig heeft gehandeld in de zin van artikel 7:529 lid 1 Burgerlijk Wetboek (BW).

3. De beoordeling

3.1 Dit geschil draait om de vraag of de bank de bedragen die van de rekening van de consument zijn afgeschreven moet vergoeden.

Juridisch kader

3.2 Een transactie waarmee de consument niet heeft ingestemd, wordt volgens artikel 7:522 lid 2 BW als niet-toegestaan aangemerkt. In deze zaak staat niet ter discussie dat de transacties van 23 juli 2022 dergelijke niet-toegestane betalingstransacties zijn.

Op grond van artikel 7:528 lid 1 BW moet de bank in geval van een niet-toegestane betalingstransactie de consument onmiddellijk het bedrag van de niet-toegestane betalingstransactie terugbetalen. Op die regel bestaat een uitzondering: volgens artikel 7:529 lid 1 BW draagt de consument alle verliezen die uit niet-toegestane betalings-transacties voortvloeien, indien deze zich hebben voorgedaan doordat hij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen. Artikel 7:524 BW bepaalt onder meer dat consumenten zich moeten houden aan de veiligheidsregels van de bank. Deze veiligheidsregels zijn opgenomen in artikel 40 van de algemene voorwaarden bunq (zie bijlage).

Voldaan aan verzwaarde motiveringsplicht?

3.3 Alhoewel het aan de bank is om te stellen en – bij gemotiveerde betwisting – te bewijzen dat sprake is van grove nalatigheid door de consument, rust op de consument een 'verzwaarde motiveringsplicht'. Dat betekent dat de consument tenminste enig inzicht dient te geven in de wijze waarop een derde toegang heeft kunnen krijgen tot zijn bunq-account, zodat de bank zich daarover een beeld kan vormen. Een andere regel zou de bank voor onaanvaardbare risico's van misbruik plaatsen.[1]

3.4 De bank stelt zich op het standpunt dat de consument niet aan zijn verzwaarde motiveringsplicht heeft voldaan. De commissie volgt de bank niet in dit standpunt. De consument heeft namelijk duidelijk aangegeven dat hij op 22 juli 2022 een (achteraf bezien) frauduleus sms-bericht ontving, dat hij op die link geklikt heeft en dat hij vervolgens kort daarna een 'magic link' van de bank ontving waarmee hij een apparaat met de naam "iPhone" toegang heeft gegeven tot zijn bunq-account. De consument heeft dit verder onderbouwd door middel van de screenshots die hij heeft ingebracht. Naar het oordeel van de commissie heeft de consument hiermee voldoende inzicht gegeven en daarmee aan zijn verzwaarde motiveringsplicht voldaan.

Grof nalatig?

3.5 Vervolgens is de vraag aan de orde of de consument grof nalatig is geweest. Er zijn drie punten waarop de consument mogelijk grof nalatig heeft gehandeld:

[1] Zie GC Kifid nrs. 2014-144, 2019-733 en 2021-0141.

1) het klikken op de link in het frauduleuze sms-bericht van 17:06 uur;
2) het klikken op de 'magic link' van 17:08 uur en het accorderen van een apparaat met de naam "iPhone";
3) het negeren van de e-mail waarin aangegeven wordt dat er is ingelogd op iOS:iPhone.

3.6 De commissie zal deze drie punten achtereenvolgens bespreken.

Het frauduleuze sms-bericht van 17:06 uur

3.7 De bank stelt dat de consument om 17:06 uur grof nalatig heeft gehandeld door op de link in het frauduleuze sms-bericht te klikken. Volgens de bank had de consument kunnen en moeten begrijpen dat het sms-bericht van 17:06 uur niet door de bank was gestuurd. De bank wijst erop dat berichten van dezelfde afzender in één sms-keten worden getoond. Het frauduleuze sms-bericht staat echter niet in de sms-keten van de bank, terwijl de andere sms-berichten van de bank wel allemaal in dezelfde keten staan. Dit is zichtbaar in de screenshot die de consument heeft overgelegd (zie 2.6 hiervoor). Verder staat in de sms-keten van de bank bovenaan de naam "bunq" vermeld. Boven het frauduleuze sms-bericht staat echter geen "bunq" maar "SMS". Verder stelt de bank dat de link in het frauduleuze sms-bericht duidelijk afwijkt van links die de bank in eerdere sms-berichten heeft verstuurd. De consument brengt hiertegen in dat de bank meerdere links hanteert (waaronder together.bunq.com, nl.bunq.com, www.bunq.com en https://bunq.me).

3.8 De commissie overweegt dat als iemand zonder duidelijke aanleiding een sms-bericht ontvangt met het verzoek om op een link te klikken, dat argwaan zal (moeten) oproepen. Dat geldt zeker in de huidige tijd waarin phishing een veel voorkomende vorm van fraude is en waar de bank ook (terecht) haar klanten voor waarschuwt. De consument had kunnen zien dat het sms-bericht niet afkomstig was van de bank, omdat het bericht niet in de sms-keten van de bank stond. Dat de consument op de link in het sms-bericht van 17:06 uur geklikt heeft, is op zich grof nalatig. Echter in dit geval zijn het sms-bericht van de fraudeur en de sms-berichten van de bank door elkaar gaan lopen. Het proces waardoor de fraudeur toegang heeft gekregen tot het account op 22 juli 2022 kan namelijk niet los worden gezien van de gebeurtenissen van 20 juli 2022. Op die dag kon de consument niet inloggen op zijn bunq-app. De consument had daarom de app opnieuw geïnstalleerd op zijn telefoon en vervolgens via de 'magic link' zijn telefoon toegang gegeven tot zijn bunq-account. Het is goed voorstelbaar dat het sms-bericht van 22 juli 2022 om 17:06 uur voor het gevoel van de consument logischerwijs volgde op de eerdere problemen met de bunq-app en de verificatie-procedure die hij op 20 juli 2022 moest doorlopen.

3.9 Daar komt bij dat de consument om 17:08 uur, dus vrijwel meteen nadat hij zijn inloggegevens in de (achteraf bezien frauduleuze) omgeving had ingevuld, een bevestigings-sms kreeg van de bank met daarin een 'magic link'. Dit sms-bericht stond in de sms-keten van de bank en kwam de consument bovendien bekend voor (aangezien de bank hem op 20 juli 2022 ook al een 'magic link' had gestuurd). De omstandigheid dat de consument het (legitieme) sms-bericht van 17:08 uur binnen twee minuten na het (frauduleuze) sms-bericht van 17:06 uur ontving, kan de consument het gevoel hebben gegeven dat dat hij bij de tweede stap van de verificatieprocedure was aanbeland en dat het eerste sms-bericht (van 17:06 uur) daarmee ook legitiem was. Kortom: hoewel de consument om 17:06 uur twijfels had moeten hebben omtrent de betrouwbaarheid van het (frauduleuze) sms-bericht van 17:06 uur, is hij door het sms-bericht van de bank om 17:08 uur op het verkeerde been gezet. Onder die omstandigheden is de commissie van oordeel dat geen sprake is van grove nalatigheid bij de consument.

<u>De 'magic link' van 17:08 uur</u>

3.10 De bank stelt dat de consument om 17:08 uur grof nalatig heeft gehandeld door via de 'magic link' een apparaat met de naam "iPhone" – en dus niet "iPhone (5)" – toegang te geven tot zijn bunq-account. In de schriftelijke stukken heeft de bank aangegeven dat de 'magic link' geopend dient te worden vanaf het apparaat dat de gebruiker toe wil voegen. Indien de bevestigings-sms dus naar het oude, bij de bank bekende apparaat is gestuurd, betekent dit dat de link van de bevestigings-sms doorgestuurd moet worden naar en ingevoerd moet worden op het nieuwe apparaat – aldus de bank in haar schriftelijke stukken. De consument heeft aangegeven dat hij op de 'magic link' geklikt heeft, vervolgens in de bunq-omgeving terecht kwam en daar de vraag kreeg of hij "iPhone" wilde verifiëren (wat hij vervolgens gedaan heeft door zijn pincode in te voeren). Naar het oordeel van de commissie strookt deze beschrijving met de tekst van het sms-bericht van 17:08 uur ("*tap this link to confirm you login on a new device*"). De commissie gaat er daarom vanuit dat het "doorsturen van de magic link naar de iPhone" (zoals de bank het noemt) betekent dat de consument op zijn eigen telefoon de inlog op een apparaat met de naam "iPhone" heeft geaccordeerd.

3.11 Ook hier zijn de gebeurtenissen van 20 juli 2022 van belang. Op 20 juli 2022 had de consument namelijk ook al een 'magic link' ontvangen, toen hij de app opnieuw op zijn eigen telefoon wilde installeren. Ter zitting heeft de bank bevestigd dat de 'magic link' ook nodig is wanneer de app opnieuw op hetzelfde apparaat geïnstalleerd wordt. Het klikken op de 'magic link' en het accorderen van de 'login on a new device' zijn dus niet alleen stappen die doorlopen moeten worden om de app op een *nieuw* apparaat te installeren, maar ook stappen die doorlopen moeten worden om de app opnieuw op *hetzelfde* apparaat te installeren. Om die reden had de 'magic link' van 22 juli 2022 met het verzoek om de 'login on a new device' te accorderen, de consument niet vreemd hoeven voorkomen.

3.12 Wel is het de vraag of het verschil tussen "iPhone (5)" en "iPhone" de consument had moeten opvallen. De consument heeft aangegeven dat hij zijn telefoon niet bewust de naam "iPhone (5)" heeft gegeven en dat Apple die 5 er waarschijnlijk heeft bijgeplakt vanwege het aantal IOS-installaties dat hij heeft gehad. De commissie vindt dit een aannemelijke verklaring. Verder is het verschil tussen "iPhone (5)" en "iPhone" niet heel opvallend. Dat het de consument niet is opgevallen, kan daarom niet als grof nalatig aangemerkt worden.

<u>De e-mail van de bank</u>

3.13 Tot slot stelt de bank dat de consument grof nalatig heeft gehandeld door de in 2.8 genoemde e-mail te negeren. De commissie gaat hier niet in mee. In de e-mail wordt weliswaar gesproken van een "nieuw toestel", maar aangezien de consument op 20 juli 2022 een soortgelijke e-mail had gekregen toen hij de app opnieuw *op zijn eigen telefoon* installeerde, hadden de woorden "nieuw toestel" geen alarmbellen hoeven doen afgaan bij de consument. Wat hem wel had kunnen opvallen, is dat de e-mail van 22 juli 2022 het over "iPhone" heeft en niet over "iPhone (5)". Zoals hiervoor al overwogen, is het verschil tussen "iPhone (5)" en "iPhone" echter niet zodanig in het oog springend dat het de consument had moeten opvallen. De commissie vindt het daarom niet grof nalatig dat de consument geen actie heeft ondernomen na de e-mail van 22 juli 2022.

Slotsom

3.14 De consument heeft wel nalatig gehandeld, maar niet grof nalatig. Het beroep van de bank op artikel 7:529 lid 1 BW slaagt daarom niet. Dit betekent dat de hoofdregel van artikel 7:528 BW van toepassing is. Met andere woorden: de bank dient het bedrag van de niet-toegestane betalingstransacties (€ 14.500,-) aan de consument te betalen.

3.15 Verder heeft de consument wettelijke rente gevorderd (over het bedrag van € 14.500,-) vanaf 23 juli 2022. De commissie overweegt dat artikel 7:528 BW bepaalt dat de bank, in geval van een niet-toegestane betalingstransactie, de betaler *onmiddellijk* het bedrag van de niet-toegestane betalingstransactie terugbetaalt en *in elk geval uiterlijk aan het einde van de eerstvolgende werkdag*, nadat hij bekend is geworden met de transactie of daarvan in kennis is gesteld. In deze zaak komt 'de eerstvolgende werkdag' neer op (maandag) 25 juli 2022. Dus vanaf die datum is wettelijke rente verschuldigd.

4. De beslissing

De commissie beslist dat de bank binnen vier weken na de dag waarop deze beslissing aan partijen is verstuurd, een bedrag van € 14.500,- aan de consument betaalt, te vermeerderen met wettelijke rente over dit bedrag vanaf 25 juli 2022 tot aan de dag van algehele betaling.

Deze uitspraak is bindend. Of u tegen deze uitspraak beroep kunt instellen, kunt u nalezen in regel 7 van het Reglement Commissie van Beroep Kifid – vanaf 1 april 2022, te vinden op de website www.kifid.nl/reglementen-en-statuten. In regel 18.1 van dat reglement is bepaald dat beroep kan worden ingesteld tot 6 weken na de dag van deze uitspraak. Meer informatie over het instellen van beroep kunt u vinden op de website www.kifid.nl/in-beroep-gaan-bij-kifid.

Binnen 2 weken na verzending van de uitspraak kunt u schriftelijk verzoeken een overduidelijke vergissing in de uitspraak zoals een schrijffout, een verkeerde naam/datum of een rekenfout te herstellen. De beslissing in de uitspraak kan hiermee niet ter discussie worden gesteld. Ook kunt u binnen 2 weken na verzending van de uitspraak schriftelijk verzoeken de uitspraak aan te vullen als u vindt dat niet op alle onderdelen van uw vordering is beslist. Dit ziet niet op de situatie waarin u meent dat de Geschillencommissie Kifid niet op al uw argumenten is ingegaan. Meer informatie hierover staat onder vraag 58 en 59 van het Reglement Geschillencommissie Kifid – vanaf 1 april 2022, te vinden op de website www.kifid.nl/reglementen-en-statuten.

Contactgegevens Klachteninstituut Financiële Dienstverlening

Telefoonnummer: 070 - 333 8 999
Website: www.kifid.nl

Bijlage - Relevante bepalingen uit de Algemene voorwaarden bunq

40. Algemene beveiliging van je account

Om je geld en je account veilig te houden, zullen we moeten samenwerken. Hieronder vind je hoe.

Neem alsjeblieft adequate maatregelen en span je naar beste kunnen in om ongewenste toegang tot en gebruik van je account te voorkomen. Doe alsjeblieft hetzelfde voor de informatie die je via onze diensten verzamelt.

Om je op weg te helpen hebben wij veiligheidsvoorschriften opgesteld. Onderstaand de belangrijkste voorschriften:
- houd je inlogcodes en andere beveiligingsfeatures strikt geheim, deel ze niet met anderen en gebruik ze nooit ergens anders dan in de officiële bunq apps of in onze officiële web interface;
- zorg ervoor dat niemand anders dan jij je passen gebruikt;
- zorg ervoor dat je telefoon en je andere apparaten beveiligd zijn (stel in ieder geval een vorm van toegangsbeveiliging in, bijvoorbeeld een inlogcode);
- gebruik altijd de laatste versie van onze apps en zorg dat het besturingssysteem van al je apparaten up-to-date en in orde is (geen illegale software);
- wanneer je de bunq app of web interface in het openbaar gebruikt, kijk dan over je schouders om zeker te zijn dat er geen ongeautoriseerde mensen meekijken;
- controleer je account in ieder geval eens per twee weken;
- breng jezelf op de hoogte van veelvoorkomende (online) oplichtingspraktijken, zoals phishing;
- meld onregelmatigheden altijd direct en volg onze instructies.

Wij zullen nooit om jouw inlogcodes of andere zaken gerelateerd aan de beveiliging van je account vragen via de telefoon, email of WhatsApp. Mocht je berichten van ons ontvangen die je niet (helemaal) vertrouwt, neem dan alsjeblieft onmiddellijk contact met ons op via de support chat. Mocht je ooit berichten ontvangen van een verdacht telefoonnummer of e-mailadres die claimen van bunq te zijn, klik dan alsjeblieft niet op een link, verstrek geen persoonlijke informatie en deel geen inloggegevens via zo'n link en meld het onmiddellijk aan ons.

Wees je alsjeblieft bewust van phishing. Phishing betreft andere mensen die proberen om jouw inlogcodes of andere vertrouwelijke informatie te verkrijgen. Veelvoorkomende phishing manieren vinden plaats via online websites zoals Marktplaats, betreft personen die zich voordoen als medewerker van bunq of van een overheidsinstantie (zoals de Belastingdienst). Klik nooit op links die je niet herkent en vul nooit gegevens in op websites die je niet bekend voorkomen.

Als je niet zeker weet of iemand je probeert te phishen, neem dan zo snel mogelijk contact met ons op zodat we je kunnen helpen.

Volg deze veiligheidsvoorschriften alsjeblieft te allen tijde. Kijk voor een volledig overzicht van onze voorschriften op Together.