



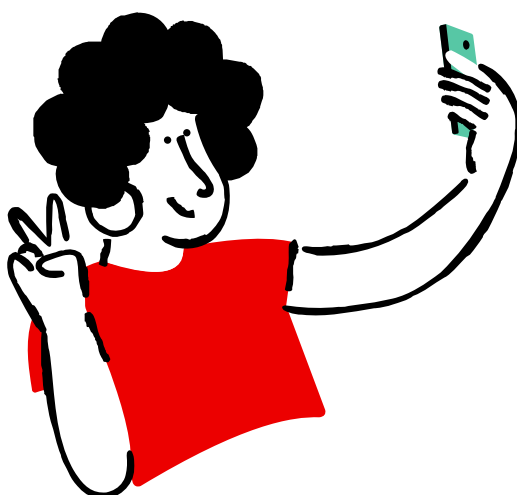
Veilig online bankieren



Samen staan we sterk

Inhoudstafel

Online veiligheid, een gedeelde verantwoordelijkheid.....	03
Santander Consumer Bank: een veilige online omgeving.....	04
Online veiligheid zit in het DNA van onze groep.....	04
Onze online veiligheidsprocedures.....	05
Hoe hou je het zelf veilig online?	07
Kies je wachtwoorden wijs.....	07
Let op voor phishing.....	07
En voor smishing.....	09
Bezint voor je verbindt.....	10
Kijk uit wat je deelt.....	11
Roep de hulp in van technologie.....	12
Iets verdachts gezien? Meld het!	13



Online veiligheid, een gedeelde verantwoordelijkheid



De voorbije jaren zijn bedrijven, organisaties en overheidsdiensten massaal overgestapt op digitale toepassingen. Ook in de bankwereld is de digitale evolutie duidelijk merkbaar. Niet alleen online banken, maar ook traditionele banken maken steeds meer gebruik van sterk beveiligde apps en online toepassingen. De constante focus op en de verdere ontwikkeling van IT-beveiliging zorgt ervoor dat online bankieren in alle veiligheid kan verlopen.

Maar online veiligheid is een gedeelde verantwoordelijkheid: je bank biedt een beveiligde omgeving aan, terwijl je als klant ook heel wat zaken zelf kan doen om je online veiligheid te verbeteren. In dit e-book vertellen we je graag hoe we online bankieren samen veilig houden. We tonen welke maatregelen we bij Santander Consumer Bank nemen en leggen uit voor welke risico's je zelf waakzaam moet blijven.

Santander Consumer Bank: een veilige online omgeving

Het wereldwijde web biedt oneindig veel mogelijkheden en kansen, en daar maken wij als online bank dankbaar gebruik van. Maar die mogelijkheden brengen een maatschappelijke verantwoordelijkheid met zich mee. Bij Santander Consumer Bank werken we dan ook onophoudelijk aan een veilige online bankomgeving voor mensen en bedrijven.

Online veiligheid zit in het DNA van onze groep

Samen staan we sterk tegen cybercriminelen. Dat geldt niet alleen voor onze klanten, maar ook voor onze interne werking. Online fraude stopt niet bij de landsgrenzen en daarom werken we als één internationale groep aan een optimale cyberveiligheid.

Bij Santander Consumer Bank willen we meer bewustzijn creëren rond online veiligheid. Zo wordt het internet een plaats waar iedereen op een veilige manier kan bankieren. Die bewustwording begint bij onze eigen medewerkers. Als groep investeren we voortdurend in nieuwe opleidingen (workshops, phishing-testen, live hackings ...) voor ons personeel zodat ze snel cyberdreigingen kunnen herkennen en rapporteren aan de juiste instanties.

Heb je zelf vragen over online bankieren? Of twijfel je aan de betrouwbaarheid van een bericht uit onze naam? De medewerkers van onze klantendienst staan elke werkdag van 9.00 tot 18.00 uur klaar om al je vragen te beantwoorden, via telefoon, via mail of via chat.



Onze online veiligheidsprocedures

Ook op het vlak van IT-veiligheid nemen we bij Santander Consumer Bank geen enkel risico. Om cybercriminelen geen kans te geven, werkten we een aantal specifieke veiligheidsprocedures uit.

Beveiligde controle van identiteit en contactgegevens

Bij het openen van een online spaarrekening maken we een link tussen de identiteit van de klant en zijn contactgegevens. We gebruiken hiervoor de beveiligde eID of een kopie van je identiteitskaart. Ook voor het wijzigen van gegevens worden deze veiligheidsprocedures gebruikt.

“
Ook op het vlak van
IT-veiligheid nemen we bij
Santander Consumer Bank
geen enkel risico.
”



Persoonlijke toegangscode spaarrekening

Na het openen van een spaarrekening ontvang je van ons een e-mail met daarin je rekeningnummer, gebruikersnaam en toegangscode. Om te vermijden dat deze toegangscode in verkeerde handen zou vallen (bijvoorbeeld doordat je e-mailadres gehackt wordt), werken we met tijdelijke codes.

De code die je per mail ontvangt, moet aangepast worden op het moment dat je de eerste keer aanmeldt op ons online platform. Dit kan enkel met een wachtwoordsleutel die we versturen naar het telefoonnummer dat je hebt opgegeven bij het openen van de rekening. Aangezien dit telefoonnummer enkel kan gewijzigd worden mits inachtnaam van een strikt beveiligde procedure, verloopt dit in alle veiligheid.

Enkel overschrijven naar eigen rekening

Bij het openen van een nieuwe online spaarrekening vragen we je om een referterekening op te geven. Dat is een zichtrekening op jouw naam bij een andere Belgische bank. Als je geld wil opnemen van je spaarrekening bij Santander Consumer Bank, dan kan dit alleen maar door een overschrijving naar deze referterekening.

Als de referterekening online gewijzigd wordt, dan vragen we om eerst een bedrag vanaf die rekening naar de online spaarrekening bij onze bank over te schrijven. Op die manier kunnen we de identiteit opnieuw controleren.

Unieke sms-code voor elke transactie

Inloggen op ons online platform doe je makkelijk met je gebruikersnaam en persoonlijke code. Wil je geld overschrijven naar je referterekening of je persoonlijke gegevens wijzigen, dan heb je ook een unieke sms-code nodig. Die code wordt verstuurd naar het mobiele nummer dat je hebt opgegeven bij het openen van de rekening.



“Om cybercriminelen geen kans te geven, werkten we een aantal specifieke veiligheidsprocedures uit.”

Hoe hou je het zelf veilig online?

De veiligheid van online bankieren wordt bepaald door de security-oplossingen van de banken, maar zeker ook door het gedrag van de gebruikers. Cybercriminelen gaan steeds sluwer te werk, maar door alert te blijven, kan je het risico beperken. We vatten enkele belangrijke tips voor je samen!

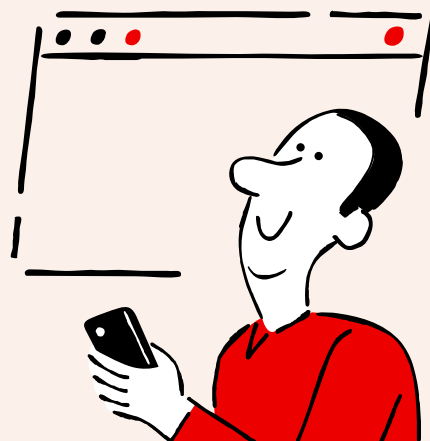
Kies je wachtwoorden wijs

Dat je wachtwoord beter niet bestaat uit je familienaam en je geboortedatum en dat je beter niet overal hetzelfde wachtwoord gebruikt, dat hoeven we je wellicht niet meer uit te leggen. Maar wist je ook dat het veiliger is om lange wachtwoorden te kiezen, in plaats van een complexe combinatie van letters, cijfers en symbolen? Zo duurt het eeuwen om het wachtwoord 'kiphondkatkonijnvogel' te kraken, terwijl 'Ng3h7!a/' al na 3 dagen ontcijferd kan worden.

Let op voor phishing ...

Met valse e-mails proberen cybercriminelen mensen te misleiden om informatie of geld te ontfutselen. Ze doen zich vaak voor als betrouwbare organisaties zoals banken, overheidsinstanties of internetproviders. Maar hoe kan je deze valse e-mails van de echte onderscheiden?

- Bekijk het e-mailadres van de afzender grondig. E-mailadressen zijn moeilijk na te maken, dus vaak worden er algemene adressen zoals @gmail.com of @mail.com gebruikt. Soms staan er ook spelfouten in de adressen, bijvoorbeeld satnander in plaats van Santander.



Maak een nieuw wachtwoord

ErIsGeenVuiltjeAanDeLucht



Maak een nieuw wachtwoord

53j7!H



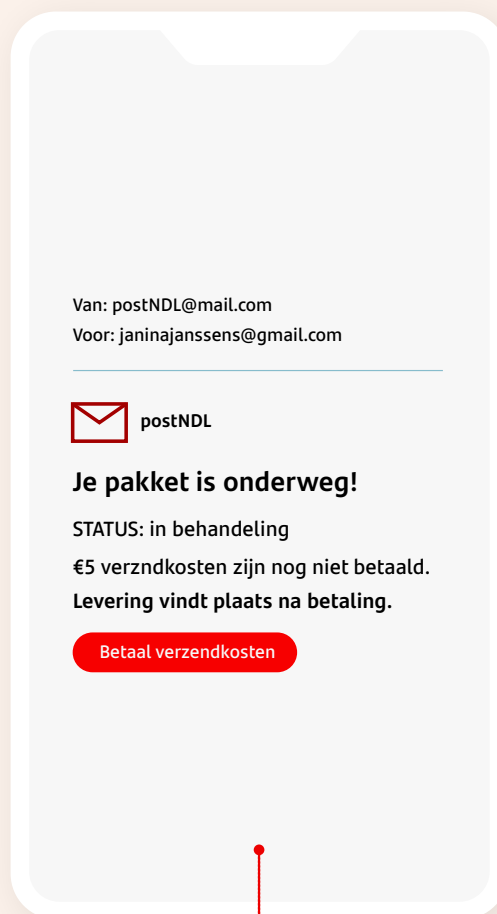
*Tijd voor een nieuw wachtwoord?
Dan is het bovenste voorstel de veiligere optie.*

ENKELE TIPS

- Phishingmails stellen je vaak voor een ultimatum of een soort bedreiging. Als je niet betaalt, wordt je account zeggend afgesloten, of zal je een boete krijgen.
- Betrouwbare organisaties zullen nooit vertrouwelijke informatie opvragen via e-mail. Als je dus een onverwachte e-mail ontvangt die bankgegevens, wachtwoorden, adressen, rijksregisternummers ... opvraagt, kan je maar beter op je hoede zijn.
- Let niet alleen in het e-mailadres, maar ook in de rest van de tekst op spel- en grammaticafouten. Cybercriminelen sturen wereldwijd valse e-mails rond, zonder de taal van het land te spreken.
- Phishingmails bevatten soms ook een bijlage. Hoogstwaarschijnlijk is dit software die criminelen gebruiken om gegevens of zelfs geld vanop de computers of mobiele toestellen van hun slachtoffers te stelen. Niet openen en onmiddellijk verwijderen is de boodschap.



In deze mail wordt verwezen naar een onbetaalde factuur, zonder meer info te geven. Ook word je voor een ultimatum gesteld: betaal nu of je account wordt afgesloten. Laat je hier niet door opjagen en blijf alert.



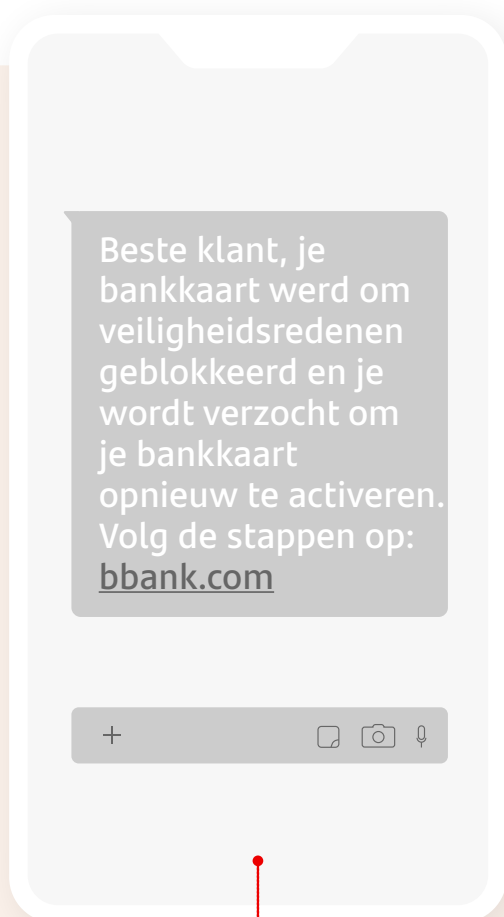
Deze mail lijkt afkomstig van de pakjesdienst postNDL, maar heeft een mailadres dat eindigt op @mail.com. Ook de spelfouten kunnen hier een belletje doen rinkelen.

... en voor smishing

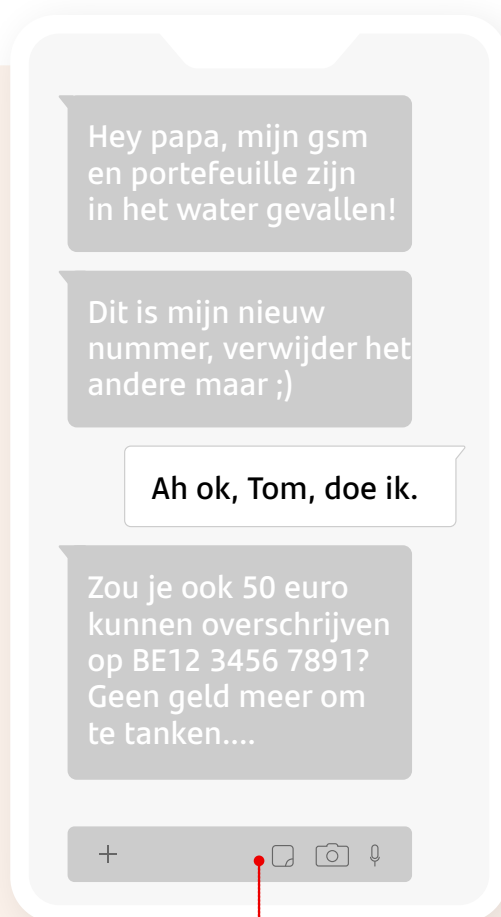
Phishing beperkt zich echter niet tot e-mails. Sms-berichten en instant messages, zoals Whatsapp, worden eveneens gebruikt om informatie of geld te stelen. Ook hier doen cybercriminelen zich voor als banken, bedrijven of overheden.

Een andere optie is dat ze zich voordoen als familie. Geef dus ook nooit vertrouwelijke informatie door via berichten en wees op je hoede als een familielid je contacteert met een nieuw nummer en meteen vraagt om het oude nummer te verwijderen of om geld te storten.

Extra tip: Cybercriminelen gebruiken nooit de voornaam van de persoon van wie ze zich voordoen. Blijf alert als je een dergelijke bericht ontvangt.



Banken zullen je nooit via sms vragen om online vertrouwelijke informatie door te geven. Heb je toch zo'n bericht ontvangen? Neem dan eerst contact op met je bank voor je op de link klikt.



Hoe bezorgd je als ouder ook bent, bij dit bericht zouden de alarmbellen moeten afgaan. De zoon gebruikt nergens zijn naam, vraagt om zijn oude nummer te verwijderen en verzoekt meteen om geld te storten op een nieuw rekeningnummer.

Bezint voor je verbindt

Onveilige internetverbindingen zijn de speeltuin van cybercriminelen. Via een onbeveiligd netwerk kunnen ze immers makkelijker inbreken in je computer, tablet of smartphone. In heel wat horecazaken kan je tegenwoordig gratis surfen op de guest WiFi. Handig, maar vaak gaat het om netwerken die niet beveiligd zijn. Maak hier dus liever geen gebruik van en gebruik je mobiele data-abonnement om te surfen.

Wi-Fi



Netwerk



Koffiebar gratis wifi



Hotel Iwis



Mijn persoonlijke hotspots



In een koffiebar werken kan een leuke afwisseling zijn, maar besef dat het gratis netwerk niet beveiligd is. Maak een persoonlijke hotspot met uw smartphone en gebruik je mobiele data om te surfen.

Wi-Fi



Netwerk



Koffiebar gratis wifi



Hotel Iwis



Mijn persoonlijke hotspots



<http://dewebshop.nl/herenkleding>



dewebshop

Zoek



Herenkleding



Short

Short met hoge taille. Ook beschikbaar in blauw.

€25

Bestel nu!

T-shirt

Valt ruim. Beschikbaar in verschillende kleuren!

€30

Bestel nu!

Op het eerste zicht lijkt er niets opmerkelijks aan deze webshop. Check zeker de URL voor je hier je gegevens invult. Deze verklaart namelijk dat het om een onveilige verbinding gaat.

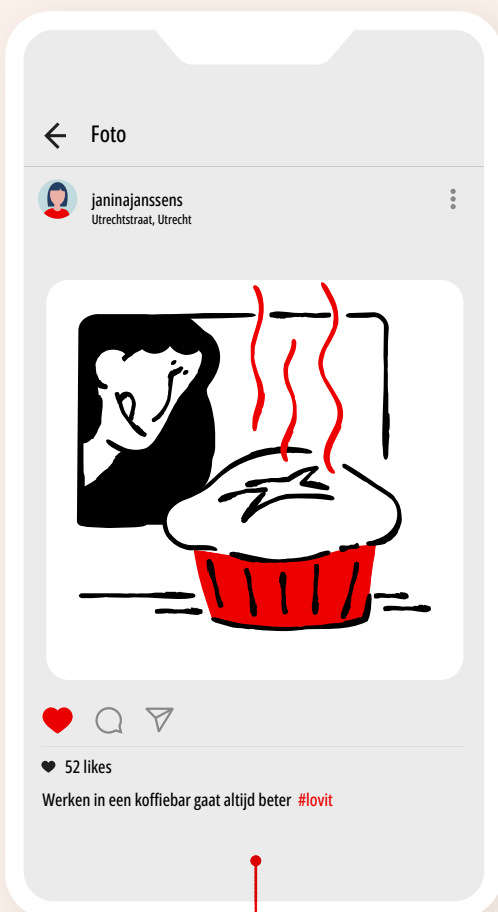
Bekijk ook altijd goed de URL als je naar een website surft of als je online aankopen doet. Beveiligde pagina's herken je aan het slotje voor het adres.

Ook het eerste deel van de URL is belangrijk: adressen die starten met 'https://' zijn beveiligd, adressen met 'http://' zijn dat niet.

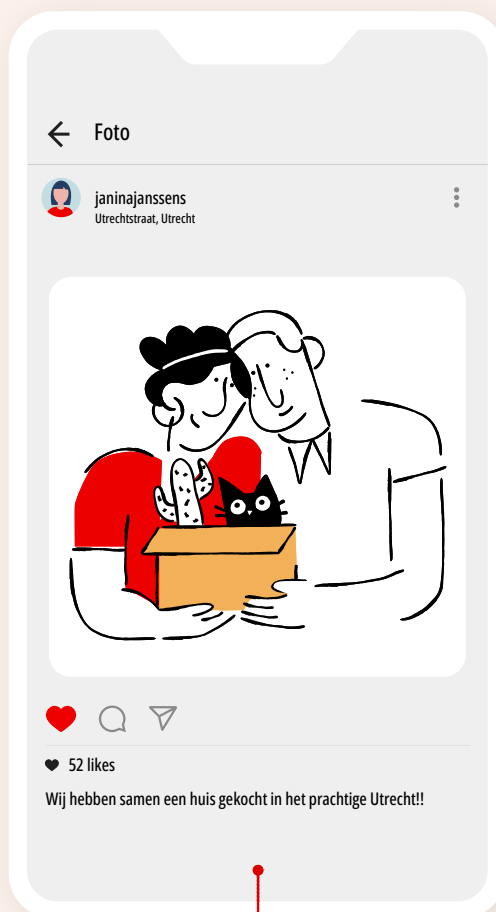
Kijk uit wat je deelt

Sociale media-kanalen zoals Facebook, Instagram en TikTok zorgen dat je leuke momenten kan delen met familie, vrienden en kennissen. Maar wees aandachtig als je foto's of video's online zet. Wat voor jou een detail is, kan voor iemand met slechte bedoelingen interessante informatie zijn.

Trots je nieuwe huis tonen aan je volgers? Leuk, maar zorg dat de straatnaam en het huisnummer niet in beeld zijn, en verwijder de locatiegegevens bij de foto. Deel je een foto van je werkplek? Check dan vooraf of er geen gevoelige informatie op je scherm staat.



Gezellig aan het werk in een hippe koffiebar? Leuk beeld, maar je zorgt beter dat je bankkaart niet zichtbaar is. Let er ook op dat de info op je scherm niet leesbaar is.



Hoe blij je ook bent met je nieuwe stulpje, als je deze foto deelt, kent iedereen je exacte adres – ook mensen met minder goede bedoelingen.

Roep de hulp in van technologie

Er bestaan heel wat apps en toepassingen waarmee je je laptop, tablet of smartphone kan beschermen tegen aanvallen van buitenaf. Spyware, malware of onveilige links worden op die manier geblokkeerd nog voor je ze opent of aanklikt. Handig, alleen is het belangrijk om deze software en het besturingssysteem van je toestel up-to-date te houden. Zo geniet je steeds van de meest recente beveiligingsoplossing.



“

Het is belangrijk
om de software en het
besturingssysteem van je
toestel up-to-date te houden.

”



De melding dat je smartphone moet geüpdatet worden, leg je best niet naast je neer. Updates zorgen voor meer veiligheid en beschermen jou en je toestel beter tegen cyberaanvallen.

Iets verdachts gezien? Meld het!

Een vreemde mail, verdacht telefoontje of een raar bericht ontvangen? Of ben je jammer genoeg het slachtoffer geworden van cyber-criminelen? Dan doe je er goed aan om het voorval te melden bij de juiste instanties. Het lijkt soms een druppel op een hete plaat, maar ook hier geldt de uitspraak “samen sterk”.

Waar kan je terecht?

Phishing of smishing melden

Vermoed je dat je een frauduleuze mail of vals bericht ontvangen hebt? Dan kan je dit melden via het meldformulier op <https://www.fraudehelpdesk.nl/fraudhelpdesk-the-dutch-national-anti-fraud-hotline/>

Nadat je het bericht hebt gemeld, kan je het best verwijderen.

Slachtoffer van cybercriminaliteit?

Wie het slachtoffer werd van een cyberaanval, doet er zeker goed aan om dat te melden. Wees zeker niet beschaamd om aangifte te doen, iedereen kan in de val van oplichters trappen.

- Bij het centrale meldpunt kan je elk geval van fraude of misleiding doorgeven: <https://business.gov.nl/running-your-business/security-and-fraud/reporting-fraud-and-deception/>
- Je kan ook rechtstreeks contact opnemen met de politie: <https://www.politie.nl/onderwerpen>



**Onze medewerkers staan elke werkdag
van 9.00u tot 18.00u telefonisch of via mail voor je klaar.**



02/588 96 26



www.santanderconsumerbank.nl



Mail



Santander
Consumer Bank