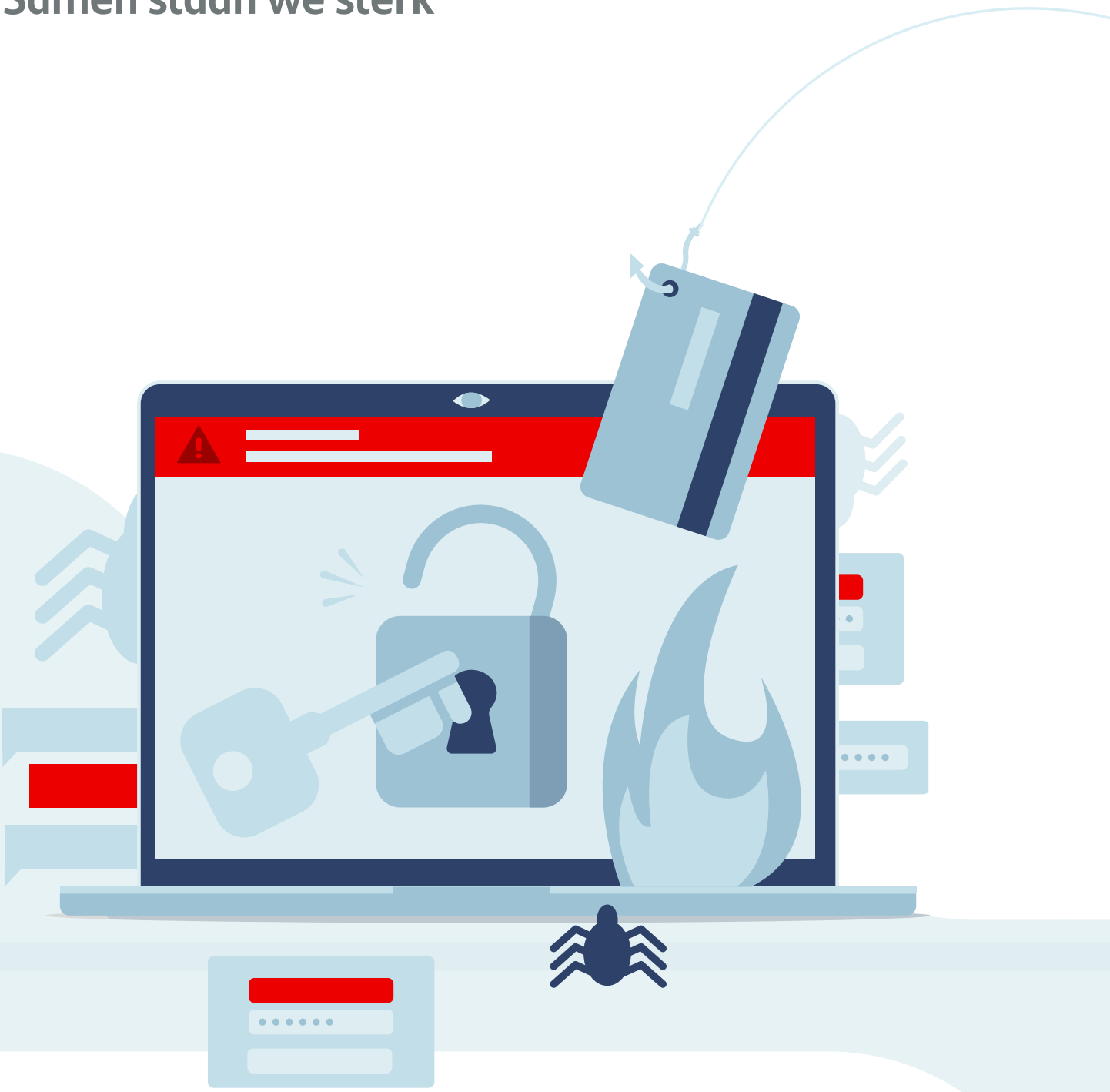
Santander Consumer Bank

Veilig online bankieren

Samen staan we sterk



Inhoudstafel

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: uw bank biedt een beveiligde omgeving aan, terwijl u als klant ook heel wat zaken zelf kan doen om uw online veiligheid te verbeteren. In dit e-book vertellen we u 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 u 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.

Hebt u zelf vragen over online bankieren? Of twijfelt u 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 uw 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 toepassing itsme®, de elektronische identiteitskaart of een kopie van uw identiteitskaart. Ook voor het wijzigen van gegevens worden deze veiligheidsprocedures gebruikt.

Persoonlijke toegangscode spaarrekening

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

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

De code die u per mail ontvangt, moet aangepast worden op het moment dat u zich de eerste keer aanmeldt op ons online platform. Dit kan enkel met een wachtwoordsleutel die we versturen naar het telefoonnummer dat u hebt opgegeven bij het openen van de rekening. Aangezien dit telefoonnummer enkel kan gewijzigd worden mits inachtname 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 u om een referterekening op te geven. Dat is een zichtrekening op uw naam bij een andere Belgische bank. Als u geld wil opnemen van uw 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 doet u makkelijk met uw gebruikersnaam en persoonlijke code. Wil u echter geld overschrijven naar uw referterekening of uw persoonlijke gegevens wijzigen, dan hebt u ook een unieke sms-code nodig. Die code wordt verstuurd naar het mobiele nummer dat u hebt opgegeven bij het openen van de rekening.

Hoe houdt u 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 u het risico beperken. We vatten enkele belangrijke tips voor u samen!

Kies uw wachtwoorden wijs

Dat uw wachtwoord beter niet bestaat uit uw familienaam en uw geboortedatum en dat u beter niet overal hetzelfde wachtwoord gebruikt, dat hoeven we u wellicht niet meer uit te leggen.

Maar wist u 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.

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

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 u 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.

Enkele tips

- Phishingmails stellen u vaak voor een **ultimatum** of een soort **bedreiging**. Als u niet betaalt, wordt uw account zogezegd afgesloten, of zal u een boete krijgen.
- Betrouwbare organisaties zullen nooit **vertrouwelijke informatie** opvragen via e-mail. Als u dus een onverwachte e-mail ontvangt die bankgegevens, wachtwoorden, adressen, rijksregisternummers … opvraagt, kan u maar beter op uw 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.

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

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

Enkele tips

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

Hoe bezorgd u 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.

... 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.

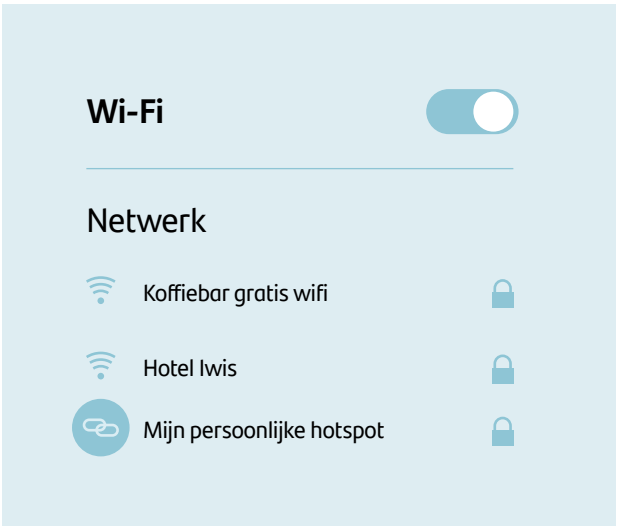
Een andere optie is dat ze zich voordoen als familie. Geef dus ook nooit vertrouwelijke informatie door via berichten en wees op uw hoede als een familielid u contacteert met een nieuw nummer en meteen vraagt om het oude nummer te verwijderen of om geld te storten.

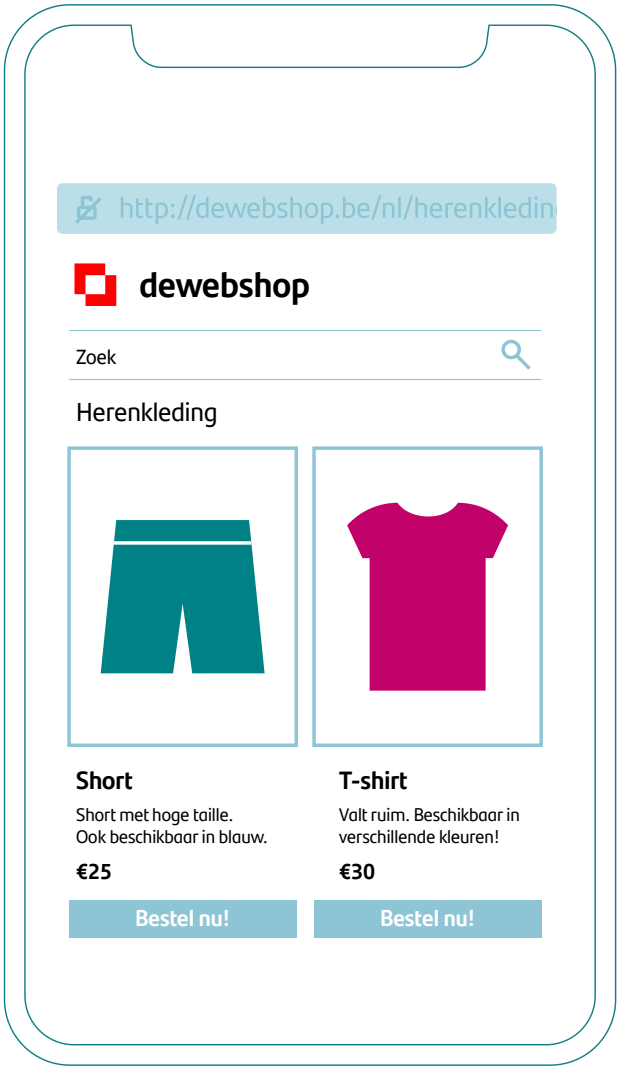
Extra tip: Cybercriminelen gebruiken nooit de voornaam van de persoon van wie ze zich voordoen. Blijf alert als u een dergelijke bericht ontvangt.

Bezint voor u verbindt

Onveilige internetverbindingen zijn de speeltuin van cybercriminelen. Via een onbeveiligd netwerk kunnen ze immers makkelijker inbreken in uw computer, tablet of smartphone. In heel wat horecazaken kan u 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 uw mobiele data-abonnement om te surfen.

Bekijk ook altijd goed de URL als u naar een website surft of als u online aankopen doet. Beveiligde pagina's herkent u 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.





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

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 uw mobiele data om te surfen.

Kijk uit wat u deelt

Sociale media-kanalen zoals Facebook, Instagram en TikTok zorgen dat u leuke momenten kan delen met familie, vrienden en kennissen. Maar wees aandachtig als u foto's of video's online zet. Wat voor u een detail is, kan voor iemand met slechte bedoelingen interessante informatie zijn. Trots uw nieuwe huis tonen aan uw volgers? Leuk, maar zorg dat de straatnaam en het huisnummer niet in beeld zijn, en verwijder de locatie-gegevens bij de foto. Deelt u een foto van uw werkplek? Check dan vooraf of er geen gevoelige informatie op uw scherm staat.

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

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

Roep de hulp in van technologie

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

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

Iets verdachts gezien? Meld het!

Een vreemde mail, verdacht telefoontje of een raar bericht ontvangen? Of bent u jammer genoeg het slachtoffer geworden van cyber-criminelen? Dan doet u 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 u terecht?

Phishing of smishing melden

Vermoedt u dat u een frauduleuze mail of vals bericht ontvangen hebt? Dan kan u dit doorsturen naar verdacht@safeonweb.be. Daarna verwijdert u de mail of het bericht best.

Dit mailadres wordt beheerd door het Centrum voor Cybersecurity België (CCB). Verdachte berichten, links of bijlages worden gecontroleerd en eventueel geblokkeerd, zodat ze geen verdere slachtoffers kunnen maken.

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 u elk geval van fraude of misleiding doorgeven: https://meldpunt.belgie.be/meldpunt/nl/welkom. Na het invullen van een vragenlijst krijgt u advies over welke stappen u best neemt.
- U kan ook rechtstreeks contact opnemen met de politie. De website Safe on Web vertelt u hoe u dit best aanpakt.
- Bent u het slachtoffer geworden van financiële fraude, gelinkt aan uw bankzaken of beleggingen? Dan kan u ook meteen de FSMA, de Autoriteit voor Financiële Diensten en Markten, contacteren.

Onze medewerkers staan elke werkdag van 8.30u tot 18u telefonisch of via mail voor u klaar | 02/588 96 26 | www.santanderconsumerbank.be