

Achtergrond

De Surinaamsche Bank doet er alles aan om uw gegevens, transacties en online bankdiensten optimaal te beveiligen. Wij hechten grote waarde aan de bescherming van uw financiële informatie en passen passende technische en organisatorische beveiligingsmaatregelen toe om misbruik, fraude en ongeautoriseerde toegang te voorkomen.

Wij zijn ervan overtuigd dat duidelijke informatie bijdraagt aan een veilig gebruik van onze digitale diensten. Door u te informeren over onze beveiligingsmaatregelen en veilig online gedrag, helpen wij het risico op internetfraude te verkleinen en eventuele bezorgdheid weg te nemen.

Op deze pagina informeren wij u over:

- de beveiligingsmaatregelen die wij als bank hebben getroffen ter bescherming van uw gegevens en transacties; en
- de maatregelen die u zelf kunt nemen om veilig gebruik te maken van onze internetdiensten en fraude te voorkomen.

Samen zorgen wij voor een veilige digitale bankomgeving.

Actuele beveiligingszaken

Het is van groot belang dat u alert blijft op actuele beveiligingsrisico's en vormen van internetfraude. De Surinaamsche Bank draagt hier actief aan bij door u te informeren over veelvoorkomende fraudevormen en veilig gebruik van onze digitale diensten. Samen kunnen wij het risico op misbruik en fraude aanzienlijk beperken.

Phishing

Phishing is een vorm van internetfraude waarbij criminelen zich voordoen als een betrouwbare organisatie, zoals een bank, via e-mail, sms of andere digitale kanalen. Zij proberen u te misleiden om persoonlijke of financiële gegevens te verstrekken, zoals uw gebruikersnaam, wachtwoord, rekeningnummer, creditcardgegevens of andere vertrouwelijke informatie.

Vaak wordt u via een link doorgestuurd naar een valse website die sterk lijkt op de officiële website van de bank. Wanneer u daar uw gegevens invoert, komen deze in handen van fraudeurs, die vervolgens misbruik kunnen maken van uw rekening(en).



Twijfelt u aan de echtheid van een e-mail die zogenaamd van De Surinaamsche Bank afkomstig is?

- Klik niet op links (URL's) of bijlagen (attachments) in het bericht;
- Ga zelf rechtstreeks naar onze officiële Internet Banking pagina:
<https://my.dsb.sr/#/login>
- Neem bij twijfel contact met ons op via Bank Mail (in Internet Banking) of via ons Callcenter op telefoonnummer 471 100 (optie 8).

Advanced Fee Fraud (voorschotfraude)

Bij Advanced Fee Fraud worden via e-mail of chatberichten grote geldbedragen, prijzen of erfenissen aangeboden. U wordt vervolgens gevraagd een vergoeding te betalen voor bijvoorbeeld juridische kosten, douanerechten of het openen van een rekening.

In sommige gevallen wordt gesteld dat u een loterij heeft gewonnen waar u nooit aan hebt deelgenomen, of dat u een percentage ontvangt voor hulp bij het overmaken van geld van een buitenlandse rekening.

Ga nooit in op dergelijke berichten en betaal nooit vooraf kosten. Dit betreft fraude en u zult het beloofde bedrag niet ontvangen.

Standaard communicatie door De Surinaamsche Bank

De Surinaamsche Bank kan voor bepaalde diensten met u communiceren via e-mail of Whatsapp. Het is belangrijk dat u echte communicatie van frauduleuze berichten kunt onderscheiden.

De Surinaamsche Bank:

- zal u in e-mailberichten of Whatsapp persoonlijk benaderen waar mogelijk;
- zal geen e-mails of chatberichten sturen met verzoeken om uw wachtwoord, pincode, volledige creditcardgegevens of andere gevoelige informatie;
- zal u nooit vragen om vertrouwelijke gegevens via e-mail of telefoon te verstrekken;
- zal u niet via e-mail of chatberichten vragen om via een link in te loggen en uw beveiligingsgegevens in te voeren;



- maakt voor haar internetdiensten uitsluitend gebruik van beveiligde verbindingen.

Wanneer u twijfelt aan de echtheid van een bericht dat zogenaamd van De Surinaamsche Bank afkomstig is, meld dit via Bank Mail in Internet Banking of neem contact op met ons Callcenter.

Controleren van de echtheid van de DSB-website

De communicatie tussen uw apparaat en de Internet Banking website van De Surinaamsche Bank verloopt via een beveiligde verbinding.

Controleer altijd of:

- de website begint met **https://**;
- er een hangslot zichtbaar is in de adresbalk van uw browser;
- de URL correct gespeld is en verwijst naar de officiële DSB-website.

Klik op het hangslot in uw browser om het beveiligingscertificaat te bekijken en te controleren of dit aan De Surinaamsche Bank is uitgegeven. Let ook op de geldigheid van het certificaat en mogelijke spelfouten in de webadresbalk, aangezien frauduleuze websites vaak sterk lijken op de officiële website.

Twijfelt u over de echtheid van een website? Neem dan contact op met ons Callcenter via 471100 (optie 8) of meld dit via Bank Mail.

Te nemen beveiligingsmaatregelen

Bescherming van uw persoonlijke gegevens

- Houd uw wachtwoord, pincode en creditcardgegevens strikt geheim;
- Deel deze gegevens nooit met derden, ook niet via e-mail of telefoon;
- Gebruik sterke wachtwoorden met een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens;
- Wijzig uw wachtwoord en pincode regelmatig;
- Let erop dat niemand meekijkt wanneer u uw gegevens invoert (shoulder surfing);



- Sla uw wachtwoord niet op in browsers of op gedeelde apparaten;
- Vul uw Internet Banking gebruikersnaam en wachtwoord uitsluitend in op de officiële DSB Internet Banking website;
- Voer nooit uw pincode van uw pinpas of creditcard online in.

Bescherming van uw computer en apparaten

- Installeer regelmatig updates van uw besturingssysteem, apps en browsers;
- Gebruik actuele antivirus- en anti-malware software;
- Activeer een firewall op uw computer of apparaat;
- Gebruik geen illegale software of downloads van onbekende bronnen;
- Wees voorzichtig met het openen van e-mails en bijlagen van onbekende afzenders;
- Gebruik bij voorkeur een spamfilter om ongewenste e-mails te blokkeren;
- Beëindig altijd uw Internet Banking sessie nadat u klaar bent met bankieren.

Door uw software en apparaten up-to-date te houden, maakt u gebruik van de nieuwste beveiligingsprotocollen en verkleint u het risico op virussen, malware en ongeautoriseerde toegang.

Samen met onze beveiligingsmaatregelen draagt uw waakzaamheid bij aan een veilige en betrouwbare digitale bankomgeving.

