Security

Achtergrond

De Surinaamsche Bank stelt alles in het werk om uw gegevens en transacties zo goed mogelijk te beschermen. Wij zijn ervan overtuigd dat wij door het verstrekken van deze informatie, een bijdrage kunnen leveren aan een zo veilig mogelijk gebruik van de aangeboden internetdiensten, en hopen zodoende eventuele bezorgdheid bij u weg te kunnen nemen.

Op deze pagina geven wij aan welke beveiligingsmaatregelen wij als bank hebben genomen om internetfraude tegen te gaan, en welke aanvullende maatregelen u zelf kunt nemen.

Actuele beveiligingszaken

Het is erg belangrijk dat u in de strijd tegen computercriminaliteit op de hoogte blijft van actuele beveiligingszaken. De Surinaamsche Bank wil hier graag aan bijdragen door u deze informatie te verstrekken.

Phishing is een vorm van internetfraude, waarbij fraudeurs middels e-mailberichten de mensen (klanten) lokken naar een valse (bank) website, die een copy is van de echte website en ze daar niets vermoedend laten inloggen met hun inloggegevens (user-id en password), rekeningnummers, credit card nummers en/of andere persoonsgegevens. Dit onder het voorwendsel dat deze gegevens geactualiseerd moeten worden. Door de verrichte handeling krijgt de fraudeur de beschikking over de gegevens, die vervolgens gebruikt worden om bijvoorbeeld gelden van de rekening(en) af te schrijven. Als u twijfelt aan de echtheid van een e-mail welke u van de bank zou hebben ontvangen, klikt u dan niet op de attachment(s) of url(s) in het bericht. Maar bezoekt u zelf onze officiele internetbanking pagina via de URL: **https://my.dsb.sr/#/login**
Eventuele pogingen tot phishing of enige vermoeden daartoe, kunt u melden via Bank Mail, een optie in ons Internet Banking programma, maar u kunt ook bellen naar ons Callcenter op 471100 toestel 1279, 1307 en 1321.

Bij Advanced Fee Fraud worden er via e-mailberichten grote geldbedragen aangeboden, waarbij wordt gevraagd om een kleine vergoeding voor juridische kosten, het openen van een rekening of het betalen van douanerechten. Soms wordt gesteld dat het aangeboden geld afkomstig is van een loterij waar u nooit aan hebt meegedaan.

Soms wordt ook gezegd dat het geld op een overzeese rekening staat waar de rekeninghouder niet bij kan, en wordt u een percentage van het geld beloofd voor uw hulp. In alle gevallen wordt u verzocht een bepaalde vergoeding te betalen.
Ga nooit in op dergelijke e-mailberichten. Dit is ook een vorm van internetfraude, waarbij u nooit iets van het beloofde geld zal ontvangen.

Standaard wijze van communiceren door De Surinaamsche Bank

- De Surinaamsche Bank zal voor bepaalde diensten steeds vaker via e-mail met haar klanten communiceren. Hoe kunt u weten of deze mail berichten echt van ons afkomstig zijn, of dat het hier om fraude gaat?
- De Surinaamsche Bank zal u in een e-mail bericht altijd persoonlijk benaderen, en zal bijvoorbeeld geen aanhef zoals ‘Geachte klant’ gebruiken;
- De Surinaamsche Bank zal geen e-mail berichten met hyperlinks sturen, die u naar een website doorsturen waar u inloggegevens zoals wachtwoord of rekeningnummer moet invoeren;
- De Surinaamsche Bank zal u nooit vragen om persoonlijke- of gevoelige gegevens via e-mail of telefoon te verstrekken;
- Internet diensten die De Surinaamsche Bank beschikbaar stelt, maken gebruik van beveiligde internet verbindingen. Zie ‘Controleren echtheid van de De Surinaamsche Bank - website’ voor nadere informatie.
- Wanneer u als klant twijfelt aan de echtheid van een e-mail bericht, dat aangeeft afkomstig te zijn van De Surinaamsche Bank, dan kunt u dit melden via Bank Mail, een optie in ons Internet Banking programma.

Controleren echtheid van de DSB website

De communicatie tussen de DSB Internet Banking website en uw PC verloopt via een beveiligde verbinding, die tijdens het inloggen wordt opgezet. Overtuigt u zich daarom ervan dat de website die u bezoekt daadwerkelijk de DSB website is, en dat de verbinding met deze website beveiligd is.

De beveiligde verbinding, te herkennen aan een afbeelding van een gesloten hangslot en aangegeven met ‘HTTPS’, maakt gebruik van een beveiligingstechniek genaamd Secure Socket Layer (SSL). Wanneer u op het icoontje met het hangslot klikt dan verschijnt er een beveiligings-certificaat. Dit certificaat moet aangeven dat De Surinaamsche Bank de eigenaar van de website is.
Controleer of de gegevens en de rechtsgeldigheid kloppen, en dat het certificaat is uitgegeven door het internationale onafhankelijke certificeringinstituut Verisign Inc. Let

er ook op dat de aangegeven datum voor een valide certificaat niet is overschreden. Kijk ook goed naar de spelling van de opgezette verbinding. Vaak hebben imitatie websites een spelfout.

Attentie! DSB past voor de communicatie met de DSB website veilige protocollen toe, om maximale bescherming van uw gegevens en informatie te bewerkstelligen. Door regelmatig de laatste versies van programmatuur en updates te (laten) aanbrengen op de apparatuur welke u toepast om de website te bezoeken, denk hierbij aan een mobiele telefoon, een pc, een tablet enz., maakt ook u gebruik van veilige protocollen, waarmee een optimale bescherming van uitgewisseld verkeer wordt verkregen.

Twijfelt u over de echtheid van de website, neem dan contact op met ons Callcenter, telefoonnummer 471100 ext. 1279, 1302 of 1307. Buiten kantooruren kunt u dit melden via Bank Mail, een optie in ons Internet Banking programma.

Te nemen beveiligingsmaatregelen

Zorg ervoor dat uw persoonlijke gegevens zoals wachtwoord, pincode en creditkaartnummer niet in verkeerde handen vallen, waardoor derden zich ongewenst toegang tot uw rekening kunnen verschaffen. Tref daarom de volgende beveiligingsmaatregelen:

Bescherming van uw persoonlijke gegevens

- Schrijf deze gegevens niet op in notitieboekjes en dergelijke, geef ze niet aan anderen door en noem ze niet in een telefoongesprek of e-mail bericht;
- Kies geen voor de hand liggend wachtwoord zoals de naam van uw kind of huisdier, of het merk van uw auto. Maar maak beter een sterk wachtwoord, bestaande uit een combinatie van hoofd- en kleine letters, de cijfers 0 t/m 9 en speciale tekens. Het aantal karakters van het wachtwoord dient bij voorkeur groter dan 8 te zijnen wijzig uw wachtwoord regelmatig;
- Let op dat niemand meekijkt terwijl u uw wachtwoord intoetst (shoulder surfing);
- Beëindig de internet banking sessie zodra u klaar bent. Als u tussentijds even iets anders moet doen, schakel dan altijd uw schermbeveiliging in (screen saver);
- Sla uw wachtwoord niet op als dit wordt gevraagd, omdat onbevoegden dan eenvoudig opnieuw met uw userid kunnen inloggen; Ook kunnen Trojan-virussen het opgeslagen wachtwoord opsporen en versturen;

- Indien u uw wachtwoord eerder heeft opgeslagen, kunt u dit als volgt verwijderen: Ga naar Tools, en klik achtereenvolgens op Internet Options, tabblad Content, AutoComplete en Clear Passwords;
- Wees zeer voorzichtig met het invoeren van persoonlijke informatie op internet sites, en vergeet niet dat het beschermen van uw persoonsgegevens uw eigen verantwoordelijkheid is. Vul uw Internet Banking gebruikersnaam en wachtwoord alleen in op de Internet Banking website van de DSB tezamen met de I-Signer. Indien u nog geen I-Signer heeft, vraagt u het zo snel mogelijk aan.
- Vul nooit uw pincode van uw pinpas en/of creditcard online in.

Bescherming van uw computer

- Installeer steeds de laatst beschikbare versie van programmatuur en updates, en voorkom zo dat hackers of virussen misbruik kunnen maken van eventuele beveiligingsproblemen of -tekortkomingen in oudere versies;
- Wanneer u een Windows pc heeft, zorg er dan voor dat u niet langer gebruik maakt van Windows 7 maar in plaats daarvan van Windows 10;
- Installeer antivirus-software op uw computer en actualiseer deze regelmatig om uw computer te beschermen tegen virussen, en om te voorkomen dat hackers Trojan-virussen op uw computer installeren. Indien u als niet-commerciële gebruik(st)er niet over antivirus-software beschikt, is AVG Anti-Virus Free een prima alternatief. Dit programma mag u als niet-commerciële gebruik(st)er gratis downloaden van de website van de leverancier GRISOFT;
- Installeer en actualiseer anti-virus en anti-spyware software;
- Installeer en actualiseer een persoonlijke firewall (Windows beschikt standaard over een firewall);
- Gebruik geen illegale programma’s en computerspellen, omdat deze Trojan-virussen kunnen bevatten die bijvoorbeeld uw toetsaanslagen registreren (keyloggers), of uw persoonlijke informatie naar criminelen versturen;
- Gebruik een spam-filter om te voorkomen dat u voortdurend ongewenste e-mailberichten -zoals ongevraagde reclame- ontvangt;
- Beantwoord en open geen e-mailberichten waarvan de afkomst niet duidelijk is maar verwijder deze. Wees vooral voorzichtig met het openen van attachments (meegestuurde bestanden) omdat deze virussen kunnen bevatten en uw pc kunnen besmetten.