Checklist Veilig Internetbankieren

Samen houden we bankieren veilig

Betaalvereniging Nederland

VEILIG BANKIEREN

Veilig internetbankieren: iedereen werkt hieraan mee

Nederlandse banken hechten veel waarde aan de beveiliging van het internetbankieren. Daar besteden banken dan ook veel aandacht aan: internetbankieren is bij ons goed beveiligd.

Beveiliging is echter een gezamenlijke verantwoordelijkheid van de bank en haar klanten. Gebruikers van online bankdiensten dienen zelf ook op een aantal maatregelen te nemen en niet in te gaan op vreemde of verdachte verzoeken.

Wij geven u graag een aantal tips die elke internetbankierder in acht moet nemen. Hieronder vindt u een uitleg wat u vooraf, tijdens en bij het afsluiten van internetbankieren kunt doen om online bankieren veilig te houden.

WAT U VOORAF KUNT DOEN

Anti-virus programma	Gebruik een anti-virus programma en zorg dat dat steeds up-to-date blijft.
Firewall	Installeer een firewall.
Anti-spyware programma	Gebruik een anti-spyware programma en zorg dat deze steeds up-to-date blijft.
Spamfilter	Gebruik een spamfilter en verwijder meteen e-mails waarover u twijfelt.
Recente updates besturingssysteem	Gebruik de meest recente updates van het besturingssysteem (Windows, Mac OS, etc.) en zet de automatische update-functie van deze systemen aan.
Recente versies software	Gebruik de meest recente versies van alle software die u gebruikt (Microsoft Office, Adobe (PDF), Firefox, etc.). Gebruik ook van deze programma's de automatische update functie.
Wachtwoord op draadloos netwerk	Als u een draadloos netwerk (Wifi) gebruikt, zorg dat deze ten minste is beschermd met een wachtwoord. Check verder of uw netwerkprovider en/of de leverancier van uw draadloze netwerk nog meer adviezen geeft over beveiliging.
Meerdere gebruikersaccounts	Maak ten minste twee gebruikersaccounts aan op uw computer; één om software op uw computer te installeren, de andere - met minimale privileges - voor dagelijks gebruik.
Voorkom besmetting door websites	Voorkom besmetting van uw computer: bezoek bijvoorbeeld geen duistere websites.
Voorkom besmetting USB-stick	Gebruik uw USB-stick niet zomaar op elke computer.

Checklist Veilig Internetbankieren

Samen houden we bankieren veilig

Geïnfecteerde apparaten	Is uw computer toch geïnfecteerd met malware of vermoedt u dit? Gebruik deze computer dan niet meer voor internetbankieren. Controleer vanaf een andere computer de transacties op uw rekeningen. Gebruik een virusscanner om de malware op te sporen en te verwijderen.
Inlogcodes	Geef nooit op een onbekende website persoonlijke (bank)gegevens af. Op onbekende websites moet u beslist geen inlogcodes afgeven. Inlogcodes voert u alleen in op de speciale en beveiligde internetbankieren-pagina's van uw bank.
Negeer e-mail berichten	Negeer e-mail berichten die zogenaamd van uw bank afkomstig zijn en waarin u wordt gevraagd inlichtingen te verstrekken over uw rekening(en) of waarin u om inlogcodes wordt gevraagd. De bank zal dit verzoek nooit ongevraagd via mail doen. Ook zal een bank u nooit ongevraagd een mail sturen met het verzoek een 'security update' te installeren. Ga dan ook nooit in op dergelijke verzoeken.
Voorkom misbruik bankrekening	Laat uw bankrekening niet misbruiken voor criminele doeleinden. Meer informatie hierover vindt u op http://www.veiligbankieren.nl/geldezels. Let op: een geldezel is strafbaar!
Melden afgegeven gegevens	Heeft u onverhoopt toch persoonlijke gegevens gegeven aan een verdachte partij? Meld dit dan direct bij uw bank.
Melden verlies of diefstal	Meld verlies of diefstal van authenticatiemiddelen (bijvoorbeeld uw bankpas) direct bij uw bank.
Alarmeer uw bank	Sla alarm als u een nieuw beveiligingsmiddel en/of nieuwe beveiligingscode van uw bank verwacht en deze niet aankomt.

Checklist Veilig Internetbankieren

Samen houden we bankieren veilig

Betaalvereniging Nederland

VEILIG BANKIEREN

WAT U TIJDENS HET INTERNETBANKIEREN KUNT DOEN

https://	Check het internetadres van uw bank. Is dit correct gespeld en begint de webpage naam met https://. De ‘s’ staat voor ‘secured’ (=beveiligd).
Veiligheidsslotje	Check of u het veiligheidsslotje op het scherm ziet staan. Een beveiligde pagina is te herkennen aan de aanwezigheid hiervan. Vanaf het scherm waarop u inlogt totdat u uitlogt werkt u op de beveiligde webpagina’s van uw bank waarop dit slotje te zien is: 
Type zelf in	Type bij voorkeur zelf de naam van uw bank zelf in op de web browser.
Afwijkende wijze aanloggen	De bank gebruikt altijd dezelfde werkwijze voor het aanloggen, het goedkeuren van betalingen, etc. Wijkt deze werkwijze een keer af: stop dan met het doen van uw bankzaken. Probeer het op een andere computer opnieuw of probeer het later nog een keer. Als u dan weer een afwijkende werkwijze ziet, neem dan contact op met uw bank.
Check de betaling	Check altijd de betaling voordat u de transactie autoriseert: Klopt het door u ingevulde rekeningnummer van de begunstigde? Klopt het overgeboekte bedrag? Klopt de datum waarop u de transactie wilt uitvoeren?
Check de autorisatie	Een aantal banken geeft bij autorisatie van de transacties aan hoeveel transacties u doet en de hoogte van het bedrag. Check deze informatie altijd!

WAT U BIJ HET AFSLUITEN VAN INTERNETBANKIEREN KUNT DOEN

Check rekeningoverzicht	Voordat u uitlogt, check altijd uw rekeningoverzicht en mogelijk ook de toekomstige opdrachten. Check dat hier alleen opdrachten staan die u heeft opgegeven.
Log uit	Zorg ervoor dat u altijd uitlogt van het internetbankieren voordat u wegloopt bij uw computer.