Veilig bankieren

Het internet opent een venster op de wereld maar het stelt uw computer ook open voor een wereld waarin niet alle mensen goede bedoelingen hebben. Veiligheid is voor bpost bank van het allergrootste belang. Wij treffen alle nodige maatregelen om een maximale veiligheid te garanderen voor onze website en uw bankverrichtingen.

Die maximale veiligheid wordt verzekerd door een ketting waarin uw computer één schakel is. Als gebruiker dient u er echter ook zelf voor te zorgen dat deze veiligheidsketting zo stevig mogelijk is.

Daarom is het belangrijk dat u de drie gouden regels volgt. Zo helpt u mee de veiligheid op alle niveaus te handhaven en vermijdt u de risico's en gevaren die ons op het internet bedreigen.

De maatregelen van bpost bank ter beveiliging van haar website

Voor bpost bank is de veiligheid van de bankverrichtingen van het grootste belang. Daarom heeft bpost bank veiligheidsmaatregelen getroffen, onder andere:

- De veilige verbinding (vandaar "https:" in het adres) die de in- en uitgaande informatiestromen codeert. Zo wordt de uitwisseling van gegevens beveiligd.
- De elektronische handtekening: de koppeling van een kaartlezer van bpost bank aan uw pincode. Daardoor ontstaat een elektronische handtekening die slechts één keer geldig is. Na drie pogingen wordt uw bankkaart geblokkeerd.
- Met PCbanking staan uw gegevens en uw verrichtingen niet op uw computer maar op de maximaal beveiligde en door firewalls beschermde servers van de bank. Er worden voortdurend controles uitgevoerd om de bescherming en veiligheid soepel en snel aan te passen als reactie op nieuwe bedreigingen.

  PCbanking gebruikt 2 types van handtekeningen:

  - Handtekening M1 (kaartlezer): met deze handtekening kunt u zich enkel identificeren wanneer u zicht aanmeldt in PCbanking.
  - Handtekening M2 (kaartlezer): met deze handtekening ondertekent u uw verrichtingen.

  Opgelet

  bpost bank vraagt u nooit om u aan te melden met een "M2" handtekening of om een verrichting te ondertekenen met een "M1" handtekening. Wanneer men u een dergelijke vraag stelt, teken dan niets en neem onmiddellijk contact op met ons.

  Wanneer moet u ondertekenen?

  Telkens u ons een opdracht geeft moet u ondertekenen, net zoals u een papieren document zou moeten ondertekenen.

  Om het gebruik van PCbanking te vergemakkelijken, hebben we voor de overschrijvingen enkele uitzonderingen op deze regel voorzien.

  Wanneer moet u een overschrijving ondertekenen?

  Normaal dient u elke Belgische, Europese en internationale overschrijving te ondertekenen. Om uw betalingen in PCbanking te vergemakkelijken en te versnellen, hebben we enkele vrijstellingen voorzien. U moet de overschrijving

niet ondertekenen als de rekening van de begunstigde een Belgische rekening is die:

- reeds gekend is in uw lijst van bewaarde begunstigden

  of

- deel uitmaakt van de meest gebruikte rekeningen in België (bijvoorbeeld rekeningen van de overheid, telecommunicatiebedrijven, energieleveranciers, verzekeringsmaatschappijen, ...)

- **en**

- U de limiet van 2.500 EUR per dag of 5.000 EUR per week niet overschrijdt. Deze limiet houdt rekening met verrichtingen uitgevoerd via PCbanking.

Drie gouden regels voor veilig internetbankieren

Een veilig internet, dat belangt iedereen aan. Vandaar dat bpost bank de Drie Gulden Regels voor Veilig Internet lanceert. Zo houden we het internet en internetbankieren veilig én leuk.

1. **Ga NOOIT in op een mail die zogezegd van bpost bank komt en waarin u gevraagd wordt om**, bijvoorbeeld:
   - uw kredietkaartnummers op te geven;
   - uw persoonlijke code te bevestigen;
   - een programma te installeren om extra mogelijkheden aan PCbanking te verbinden enz.

   Hoe goed zo een mail er ook uitziet en hoe betrouwbaar "bpost bank " hij lijkt, u gaat er nooit op in. Vaak schermt zo een mail met veiligheid: "we doen dit met het oog op uw veiligheid enz." Gewoon niet op ingaan: bpost bank zal u nooit om vertrouwelijke informatie vragen via een onbeschermd kanaal. Wij zullen u enkel vertrouwelijke informatie vragen in een vertrouwelijke omgeving: in het kantoor of na een deugdelijke toegangscontrole aangemeld onder PCbanking.

2. **Kijk ALTIJD even na of u wel degelijk op een échte bpost bank-website zit.**
   U kunt de echtheid van de bpost bank-sites controleren aan de hand van het hangslotje onderaan rechts in uw browser (bv. Internet Explorer 6, Internet Explorer 7, Firefox). Klik op het hangslot en let erop dat het adres altijd eindigt op .be als u vanuit een e-mail naar één van onze sites surft .

3. **Installeer een antivirussoftware en voer regelmatig een update uit**.
   Internet opent een venster op de wereld maar het opent ook uw computer voor de wereld en daar lopen heus niet alleen eerlijke mensen rond. Daarom grendelt u met goede antivirussoftware de toegang tot uw computer af. Geregeld updaten is de boodschap. De beveiligingssoftware is in een voortdurende strijd gewikkeld met mensen met minder eerlijke bedoelingen. Vandaar de geregelde bijwerkingen die u best zo snel mogelijk installeert.
   Een verdacht mailtje gekregen? Met bijvoorbeeld de vraag bpost bank-kredietkaartnummers of codes mee te delen of te bevestigen? Stuur het meteen door naar security.alert@bpostbank.be. Onze veiligheidsverantwoordelijken gaan er onmiddellijk achteraan. Want internet moet veilig én leuk blijven. U kunt ook de informatie raadplegen die van u een waakzame internetgebruiker maakt en goede gewoonten aannemen om veilige financiële verrichtingen uit te voeren!

Hoe word ik een waakzame internetgebruiker?

Om veilig op het internet te surfen, houdt u zich het best aan de drie gouden regels maar volgt u ook volgende aandachtspunten op.

- Hou hackers tegen met behulp van een firewall die de in- en uitgaande informatiestroom controleert.
- Bescherm u niet alleen tegen virussen, maar ook tegen spyware met een betrouwbaar antispywareprogramma dat u regelmatig bijwerkt. Sommige antivirusprogramma's beschermen uw computer ook tegen spyware. U kunt een niet-exhaustieve lijst raadplegen van de programma's die gratis of tegen betaling verkrijgbaar zijn in de computerwinkel of op het internet.
- Voer regelmatig een volledige scan van uw computer uit met behulp van uw antivirusprogramma.
- Beveilig uw draadloze internetverbinding om te voorkomen dat de buren of mensen die zich in uw buurt bevinden uw snelle internetverbinding gebruiken zonder dat u dat weet. Verander de wachtwoorden die met uw apparatuur worden meegeleverd, en verander ook de naam van uw netwerk (SSID). Gebruik een versleutelingssysteem zoals WPA2 of minstens WEP. Roep eventueel de hulp in van een specialist voordat u deze wijzigingen doorvoert.
- Installeer altijd de recentste versie van een browser. Die bevat doorgaans de laatste technische veiligheidssnufjes.
- Installeer de veiligheidsupdates van uw besturingssysteem.
- Raadpleeg het lexicon voor meer informatie over de technische termen.

Goede gewoonten

- Vertel niemand de geheime code van uw veiligheidsmodule (de pincode van uw betaalkaart).
- Schrijf uw pincode nergens op.
- PCbanking en uw bankkaart zijn persoonlijk en mogen niet door verschillende mensen worden gebruikt.
- Sluit uw PCbanking-programma na gebruik correct af door te klikken op de knop "Afmelden" links op het scherm.

Algemeen:

- bpost bank zal u nooit vertrouwelijke informatie vragen via e-mail. Als iemand probeert om persoonlijke gegevens van u te krijgen via e-mail of een pop-upvenster (phishing), antwoord daar dan niet op maar verwittig security.alert@bpostbank.be.
- Pas op als iemand u opbelt in verband met eventuele fraude met uw kredietkaart of uw rekening. Er doet namelijk een nieuwe vorm van bedrog de ronde, zogenaamde vhishing (voice-phishing). Die bestaat erin dat de klanten van een bank worden opgebeld om hen zogezegd in te lichten over fraude. De beller vraagt dan of zij willen terugbellen naar een bepaald nummer en zich daar willen identificeren met vertrouwelijke gegevens (nummer, codes, ...). Laat u niet bang maken en ga vooral niet in op dit deze soort verzoeken. Neem contact op met uw kantoor, phonebanking of security.alert@bpostbank.be, via de nummers die u kent en nooit via nummers die u in zulke boodschappen ontvangt. Buiten de werkuren, en als u absoluut zeker wilt zijn, kunt u uw kaart laten blokkeren via Card Stop (0,30 euro/min)
- Als u ontdekt dat uw PCbanking frauduleus wordt gebruikt (verrichtingen, onjuiste bedragen enz.) neem dan contact op met bpost bank Wij nemen dan de nodige maatregelen.
- Let op voor e-mails die u winst beloven, waarin u verneemt dat u geld op uw rekening gaat krijgen of dat u geld moet bewaren voor onbekenden. Het gaat

altijd om bedrog en de verzender is er alleen maar op uit om uw rekening leeg te halen. Meer info op http://www.spamsquad.be/nl/home.html.
- Vermijd valse websites. Klik nooit op een link die u via een e-mail ontving om toegang te krijgen tot een beveiligde site. Deze links leiden u niet altijd naar de site die u denkt. Om u naar een vertrouwde site te begeven, maakt u bij voorkeur gebruik van de links in uw favorieten. Let bijzonder goed op als u uw computer deelt met uw kinderen.
- Wees altijd voorzichtig als u een nieuw programma installeert. U moet altijd goed weten wat u precies installeert en waar het programma vandaan komt.
- Gebruik nooit publieke computers (cybercafé) om uw bankverrichtingen uit te voeren. U weet niet of die computers zijn besmet met virussen of andere programma's die de veiligheid van uw transacties in gevaar kunnen brengen.
- Wantrouw bijlagen bij uw e-mails. Als u niet zeker bent waar ze vandaan komen, maakt u ze best niet open.
- Antwoord nooit op spammail en klik niet op de links in het bericht aangezien u op die manier het bestaan van uw mailbox bevestigt en nadien nog veel meer ongewenste berichten zult ontvangen. Wis deze berichten of gebruik een antispamfilter. Let goed op als u via internet aankopen doet.
- Deel uw kredietkaartnummer niet mee als u niet van plan bent iets te kopen. Sommige sites vragen een kredietkaartnummer om zogezegd te controleren of u meerderjarig bent maar gebruiken daarna uw kaart om zonder uw medeweten aankopen te doen.

Bij illegaal gebruik van uw gegevens

- U hebt een verdachte e-mail gekregen? Iemand vraagt u om de nummers van uw kredietkaarten van bpost bank of uw pincodes mee te delen of te bevestigen? Stuur die e-mail meteen door naar security.alert@bpostbank.be.

- Bij verlies of diefstal van uw bankkaart, of bij mogelijk misbruik, neemt u onmiddellijk contact op met: de Helpdesk van PCbanking op 022 / 012345 van maandag tot vrijdag van 8 tot 20 uur en zaterdag van 9 tot 19 uur of zodra de Helpdesk toegankelijk is als u de feiten hebt vastgesteld buiten de vermelde werkuren.

- Als u een kaartlezer en een bpost bank-bankkaart gebruikt, moet u contact opnemen met: CardStop (7 dagen per week, 24 uur per dag) op het nummer 070 344 344 en de Helpdesk van PCbanking op 022/012345 van maandag tot vrijdag van 9 tot 17 uur en zaterdag van 8u30 tot 12 uur of zodra de Helpdesk toegankelijk is als u de feiten hebt vastgesteld buiten de vermelde werkuren.

- Geef verlies of diefstal van uw kaart binnen 24 uur aan bij de politie van de plaats waar het verlies of de diefstal is gebeurd.

Lexicon

- **Adware**: software die reclame bevat. "Ad" betekent "advertentie, reclame" in het Engels. Adware is gratis software waarin reclame wordt gemaakt.
  Adware is meestal geen spyware (= software die uw computer bespioneert) omdat de gebruiker vooraf op de hoogte wordt gebracht dat de software reclame zal bevatten.

- **Antivirus**: software (zie lijst) waarmee u computervirussen kunt opsporen en verwijderen van eender welke drager (vaste schijf, diskette, cd-rom enz.). Een antivirusprogramma is alleen maar doeltreffend als u regelmatig de nodige

updates installeert. Er komen immers altijd nieuwe virussen bij en het programma speelt daar zo snel mogelijk op in. Aan u om deze bijwerkingen te installeren.

- **Browser**: programma waarmee u op het internet kunt surfen. De twee meest gebruikte browsers op de markt zijn Internet Explorer (van Microsoft) en Netscape Navigator (van Netscape).

- **Firewall**:een systeem (software of apparatuur) dat ongeoorloofd verkeer verbiedt van en naar uw computer of uw netwerk. Alle berichten van en naar het internet verlopen via de firewall die alle informatie scant. Als de firewall gegevens vindt die niet beantwoorden aan de veiligheidscriteria, laat hij die gegevens niet door.

- **Kaartlezer**: een veiligheidsmodule waarmee u uw bankverrichtingen kunt uitvoeren bij bpost bank. U kunt die lezer alleen gebruiken op voorwaarde dat u een gebruikersnummer hebt, een bankkaart van bpost bank en de geheime pincode van die kaart.

- **Phishing**: phishing is een samentrekking van fishing (vissen) en phreaking (computerfraude). Het gaat hier om mensen die hengelen naar vertrouwelijke gegevens (zoals wachtwoorden of andere persoonlijke gegevens) door zich bij de slachtoffers voor te doen als iemand die zij vertrouwen en die de gevraagde informatie nodig heeft. Het is in feite een supergevaarlijke vorm van spam. De berichten vertellen de geadresseerden vaak dat er een probleem is met hun rekening en vragen dan om op een website inlichtingen te geven over die rekening en over zichzelf.

- **Spam**: ongewenste e-mail. Deze berichten worden massaal verstuurd en bevatten doorgaans commerciële boodschappen (verkoop van geneesmiddelen, gokwedstrijden, deelname aan loterijen). De inhoud van spam is vaak illegaal, bedrieglijk en/of schadelijk. De verzender maakt zich meestal niet bekend.

- **Spyware**: dit is software die zich in uw computer nestelt, u bespioneert terwijl u op het internet surft en uw gebruikersgegevens steelt.
  Spyware verstopt zich vaak in freeware of shareware die u kunt downloaden van het internet. Spyware kan de bestanden op uw vaste schijf scannen, andere spyware installeren, cookies lezen, uw internetstartpagina wijzigen enz. Spyware kan ook uw vertrouwelijke gegevens lezen en ze doorsturen naar oplichters op het internet. Die gebruiken uw gegevens dan om u ongevraagde reclame (spam) toe te sturen of verkopen ze door aan anderen.

- **SSID**: staat voor Service Set Identifier. Het is de naam van uw Wifi-netwerk die verspreid wordt en die uw toegangspunt tot alle draadloze computers identificeert.

- **Virus**: een computervirus is een programma dat zich op uw computer installeert zonder dat u dat wilt of zelfs maar weet. Het kan zich verbergen in eender welk bestand (attachment) dat u van het internet bent gaan halen. Een computervirus zet zich vast op een ander programma, vernielt het of vervangt het door een ander programma. Het kan uw apparatuur beschadigen, programma's verwijderen, de snelheid van uw computer vertragen enz.

- **Vishing**: samentrekking van Voice (stem/spraak) en Phishing (zie verder). Een telefonische oproep, meestal vooraf opgenomen, informeert u zogezegd over ongewone activiteiten op uw kaart of uw rekening die waarschijnlijk verband houden met een poging tot fraude en vraagt u om terug te bellen naar een telefoonnummer waar u zich moet identificeren aan de hand van vertrouwelijke gegevens.

- **Wifi**: Wireless Network = draadloos netwerk..

Interessante links

Meer info over ongewenste e-mail (spam): http://www.spamsquad.be/nl/home.html

Meer info over ongewenste programma's en advies om ze te vermijden: http://www.ibpt.be

- **Anti-virus**:
  Gratis: Avast, Antivir, ...
  Tegen betaling: BitDefender, Kaspersky, McAfee, Norton Symantec, Panda, ...

- **Firewalls**:
  Gratis: Zone alarm, ...
  Tegen betaling: Norton, ...

- **Antispywareprogramma's**:
  Gratis: Adaware, Spybot, ...
  Tegen betaling: Kaspersky, ...

- Er bestaan ook **complete pakketten** met antivirus- en antispywareprogramma's en firewalls: BitDefender, McAfee, Norton Symantec...