Veilig internetbankieren

Malware en dan met name de digitale bankrovers die bekend staan onder de naam "**bankingtrojanen**" worden natuurlijk steeds geavanceerder, vandaar dat er ook steeds meer maatregelen worden genomen door onder andere de banken om uw daar tegen te beschermen.

Ook de fabrikanten van beveiligingssoftware zitten op dit gebied niet stil en ontwikkelen met enige regelmaat nieuwe technologieën en beveiligingsproducten waarmee u uw online veiligheid met betrekking tot het "**internetbankieren**" kunt optimaliseren.

In deze handleiding gaan we dieper in op het "**internetbankieren**" en de daarbij behorende veiligheid en zullen we tevens adviezen geven hoe u zelf uw beveiliging kunt optimaliseren.

Inhoud

Heeft u vragen over deze uitgave of over bepaalde artikelen dan verwijzen wij u graag naar het forum, waar u met uw vragen terecht kunt bij "Forum feedback & mededelingen" onder de categorie PC Web Plus actueel.

Registreren op het forum

Registratie op het forum van PC Web Plus is geheel gratis en u heeft alleen een e-mail adres nodig voor het activeren van uw account.
Na registratie krijgt u volledige toegang tot alle sub-forums en kunt u uw vragen stellen en of vragen beantwoorden in de diverse secties.
Hieronder een overzicht van de verschillende sub-forums die beschikbaar zijn.

- www.pcwebplus.nl/phpbb

Twee Factor Authenticatie

Iedere Nederlandse bank maakt gebruik van een zogenaamde '**Twee Factor Authenticatie**" bij de ING bank gaat dit middels een zogenaamde **TAN** en **PAC code** en bij de Rabobank, ABN Amro en Forits via een "Random Reader", "E-Reader", "Accesskey" of vergelijkbaar apparaatje die middels de bijbehorende pas van de betreffende rekening éénmalige inloggegevens kan genereren.

Deze inloggegevens worden real-time gegeneerd en in vergelijking met de **TAN** en **PAC code** van de ING die via een zogenaamde papieren lijst en of SMS beschikbaar zijn lijkt dit systeem op het eerste oog natuurlijk veel veiliger maar is dat werkelijk ook wel het geval?

In de eerste plaats verschillen hierover de meningen, maar in principe hangt de veiligheid af van het feit hoe kwaadwillende toegang tot de betreffende gegevens kunnen krijgen. Om de gegevens van een papieren lijst fysiek in handen te kunnen krijgen zal er bijvoorbeeld simpel gezien een inbraak benodigd zijn, of deze lijst moet op een verkeerd adres bezorgd zijn.

Bij de **TAN** en **PAC codes** die via SMS worden verzonden is het natuurlijk een heel ander verhaal, een simpel stukje malware op uw telefoon kan eenvoudig alle gegevens onderscheppen en doorsturen.

Phishing & Malware

In de basis zijn "**Phishing**" en "**Malware**" als het gaat om de digitale bankrovers die bekend staan onder de naam "**bankingtrojanen**" onlosmakelijk met elkaar verbonden, de "**Phishing**" is bedoeld om de gebruiker middels "**Social Engineerings-technieken**" te misleiden en op deze manier vertrouwelijke gegevens te kunnen buitmaken.

Deze "**Phishing**" bericht zijn natuurlijk alom bekend waarin uw wordt gevraagd om uw gegevens te verifiëren, U in dient te loggen om de nieuwe aangescherpte beveiliging van de betreffende bank te activeren en noem maar op.

Ondanks dat er op deze manier nog steeds veel slachtoffers worden gemaakt die de dupe worden van online oplichting betreffende het "**internetbankieren**" gebruiken de "cybercriminelen" steeds geraffineerdere manieren om uw persoonlijke gegevens te ontfutselen, dit gebeurd dus niet alleen meer via de zogenaamde “phishing” berichten maar simpelweg met geavanceerde malware.

Eveneens een goed voorbeeld is de zogenaamde **Gataka Trojan** die een extra scherm toont wanneer u bijvoorbeeld de legitieme website van de ING bezoekt met de vraag om een extra TAN-code.
Dit soort "**bankingtrojanen**" kunnen vervolgens man-in-the browser aanvallen uitvoeren, waarbij de cybercriminelen op de achtergrond transacties voorbereiden en manipuleren. Meldingen waarbij een extra autorisatie stap is vereist, of uw TAN-code geverifieerd dient te worden moeten alle alarmbellen al doen gaan rinkelen natuurlijk.

Fraude - Identiteit

Heel veel mensen denken nog steeds dat "cybercriminelen" aan alleen een gebruikersnaam en wachtwoord van bijvoorbeeld de ING bank niets hebben, er kunnen namelijk geen transacties worden uitgevoerd zonder gebruik te maken van **TAN** en **PAC codes**, deze gedachte is dan ook vaak te omvatten in de bekende uitspraak "Wie niets te verbergen heeft hoeft zicht geen zorgen te maken".

Heel kort omschreven gaat deze spreekwoordelijke vlieger natuurlijk niet op, want zodra een cybercrimineel alleen maar toegang heeft en zo uw bank en rekeninggegevens, betalingsoverzichten en tenaamstellingen kan bekijken kan dit alleen al erg interessante en bruikbare informatie zijn voor het plegen van fraude en welke vorm van misbruik dan ook.

Middels deze verkregen gegevens zou het al mogelijk zijn om een "**automatisch incasso**" uit te voeren, zodat er geld van uw rekening wordt geschreven en het erop lijkt dat u hier zelf toestemming voor heeft gegeven. Wanneer er van deze situatie sprake zou zijn kan het nog wel eens lastig worden om aan te tonen dat de "**automatisch incasso**" op onrechtmatige manier is uitgevoerd. Banken gaan er namelijk (bijna) altijd vanuit dat de betreffende bedrijven toestemming hebben.

Naast deze fraude en of beter gezegd criminaliteit met betrekking tot het "**internetbankieren**" wordt ook via de zogenaamde "scam-telefoontjes" geprobeerd u geld afhandig te maken. Ook deze manier van oplichting is gebaseerd op "**Social Engineerings-technieken**" waarbij de cybercrimineel u doet geloven dat er problemen met uw computer zijn, zoals onder andere de aanwezigheid van malware.

Maak gebruik van HTTPS Everywhere.

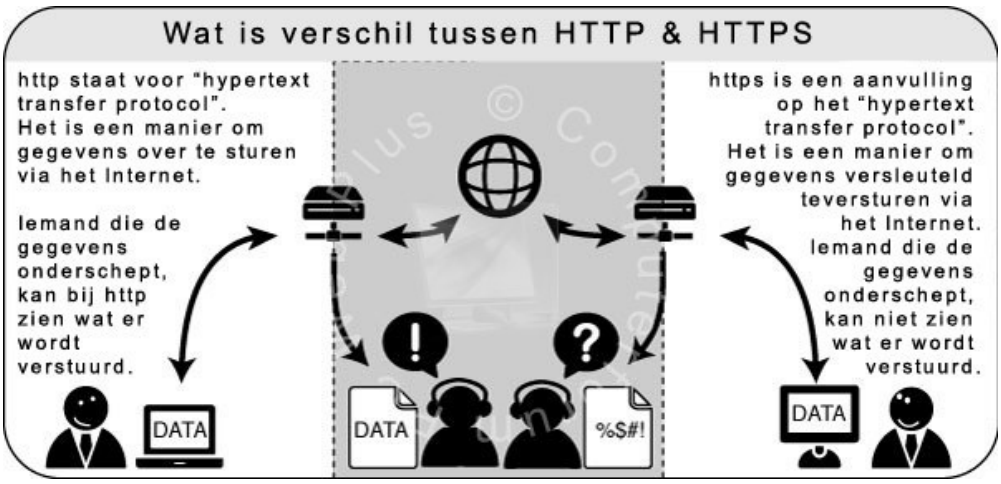
HTTPS Everywhere is een browserplug-in, extensie of beter gezegd een aanvulling voor Internet Explorer, Mozilla Firefox en Google Chrome die er voor zorgt dat bezoekers van een website direct via een versleutelde verbinding (HTTPS) contact maken met de betreffende website. Wanneer **HTTPS Everywhere** in de gebruikte browser is geinstalleerd zal deze bij het bezoeken van een website controleren of er een **HTTPS-verbinding** is.

Indien deze beschikbaar is zal er automatisch een versleutelde c.q. beveiligde verbinding met de betreffende website worden opgezet Wanneer er geen **HTTPS-verbinding** beschikbaar is zal er gewoon via HTTP een verbinding worden opgezet.

Aangezien we over het internet steeds meer en meer gevoelige informatie versturen, zoals adresgegevens, bankgegevens, financiële transacties, maar ook persoonlijke al dan niet vertrouwelijke gegevens via e-mail en chatberichten.

Het is dus van essentieel belang om ervoor te zorgen dat die gegevens niet door kwaadwillenden kan worden onderschept. U kunt dit eenvoudig beschermen door gebruik te maken van een beveiligde verbinding, die de betreffende gegevens versleutelt waardoor ze onleesbaar worden voor derden.

Onderstaand ziet u schematisch het verschil tussen HTTP en HTTPS weergeven.



Hoe u HTTPS Everywhere kunt installeren en gebruiken leest u op het forum.

Versleutel uw DNS verkeer.

Middels het programma **DNSCrypt** is het mogelijk om het verkeer via het Domain Name System (DNS) te versleutelen waarbij het programma actief is tussen de DNS-server en de gebruiker. "Dat betekent dat je meer privacy en veiligheid hebt en dat niemand kan zien wat je online doet". DNSCrypt beschermt echter niet de verbinding die je browser daarna opzet met de betreffende website, daarvoor is namelijk HTTPS bedoeld.

Doordat de communicatie tussen computers en de OpenDNS-servers wordt versleuteld kan onder meer worden voorkomen dat bij een surfsessie derden meekijken en MITB/ MITM (Man In The Browser & Man In The Middle) aanvallen uitgevoerd kunnen worden door middel van kapen van de DNS-server.

Hoe u DNS-Crypt kunt installeren en gebruiken leest u op het forum.

Wat is DNS?
DNS (Domain Name System) is een client-server-systeem, waarbij de gebruiker door middel van het DNS-protocol een aanvraag doet bij de DNS-server en de DNS-server hier weer op antwoord dit word ook wel 'lookup' / 'reverse-lookup' genoemd, de gevraagde domeinnamen worden namelijk omgezet in IP-adressen.
Meer informatie over het versleutelen van uw DNS-verkeer en aanverwante artikelen kunt u nalezen op de onderstaande links.

- Alternatieve DNS servers
- DNS Changer-malware
- DNSSEC (Domain Name System Security Extensions) Validator

Extra bescherming voor uw browser.

HitmanPro.Alert is een extra beveiligingslaag die u kunt gebruiken om uw online veiligheid te optimaliseren, dit is een gratis tool die als Windows service actief is en **real-time bescherming** biedt tijdens uw browsersessies.

Zodra uw computer geïnfecteerd is zal HitmanPro.Alert dit detecteren en een waarschuwing tonen, deze extra beveiligingslaag is dus uitermate geschikt om uw online veiligheid bij het online bankieren, bestellen bij webshops en dergelijke te waarborgen.

HitmanPro.Alert biedt dus extra bescherming tegen de zogenaamde "**Banking-Trojanen**" die momenteel erg populair zijn bij de cybercriminelen, door deze extra beveiliging wordt het voor "Banking-Trojanen" onmogelijk gemaakt om transactiegegevens te wijzigen voor-dat het wordt gecodeerd en verstuurd naar de bank.

HitmanPro.Alert beschermd u dus tegen de zogenaamde Man-in-the-Browser aanvallen, waarbij de cybercriminelen op de achtergrond gebruik maken van jouw eigen sessie met de bank en de gegevens zonder dat u het merkt manipuleren om bijvoorbeeld de trans-acties te wijzigen.

Meer informatie over het gebruik van HitmanPro.Alert kunt u nalezen op de onderstaande links.

HitmanPro.Alert nstalleren en gebruiken.

HitmanPro.Alert - review

Extra bescherming voor uw browser.

Prevx SafeOnline is een beveiligingsprogramma die bescherming biedt tegen internetfraude, steeds meer en meer versturen we over het internet gevoelige informatie zoals persoonlijke gegevens, bankgegevens, financiële transacties maar ook privé gevoelige informatie via e-mail en chatberichten. Het is dus van essentieel belang om ervoor te zorgen dat die gegevens niet door kwaadwillenden onderschept kunnen worden.

Met behulp van **Prevx SafeOnline** kunt u zich hier tegen wapenen om uw privacy gevoelige gegevens en uw online identiteit te waarborgen.

Dit programma maakt gebruik van een zogenaamde kernelniveau vergrendeling van het gebruikte besturingssysteem en de browsers om alle gebruikersinformatie en bijbehorende referenties te beschermen.

Meer informatie over het gebruik van Prevx SafeOnline kunt u nalezen op de onderstaande link.

Prevx SafeOnline installeren en gebruiken.

Handige links

⇒ Overizicht gratis virusscanners

⇒ Overzicht fratis malwarescanners

⇒ Overzicht gratis firewalls

⇒ Wat is de beste virusscanner anno 2013

⇒ Pas op voor phishing berichten

⇒ Hoe malware een system infecteert en kan binnendringen

⇒ Wie creëren er malware? waarom en wat zijn de gevolgen.

⇒ Gevolgen van het gebruik van illegale software, cracks & keygens.

Beveiligingsupdates voor Windows bieden bescherming bieden tegen nieuwe en doorlopende bedreigingen van uw privacy en uw computer. De beste manier om beveiligingsupdates te krijgen is het inschakelen van automatische updates van Windows en op de hoogte te blijven van actuele zaken op het gebied van beveiliging. Op de onderstaande link leest u hoe u de automatisch updates kunt instellen en hoe u kunt controleren of er updates voor Windows beschikbaar zijn.
Installeren van essentiële updates voor Windows.

Naast het installeren van de beschikbare updates voor Windows is het ook heel belangrijk om uw overige software up-to-date te houden, verouderde software kunnen namelijk kwetsbaarheden bevatten die misbruikt kunnen worden door kwaadaardige programma's zoals virussen en malware. Op de onderstaande links kunt u nalezen hoe u uw software up-to-date kunt houden.

Adobe Flash Player updaten
Java Updates installeren
Qualys BrowserCheck
Secunia PSI