Almelo, 10 november 2019

Bankpas en pincode ontvreemd: hoe veilig is elektronisch bankieren?

Digipassen bieden betere veiligheid dan generieke cardreaders.

De aanleiding voor mijn onderzoekje naar elektronisch bankieren bij Nederlandse banken is dat mijn vader van inmiddels bijna 85 jaar deze zomer begon met elektronisch bankieren. Van het één kwam het ander en voor ik het wist, was ik de veiligheidsaspecten van elektronisch bankieren met elkaar aan het vergelijken. Art Huiskes, onderzoeksjournalist

---

Stelt u zich de volgende situatie eens voor. Er meldt zich iemand aan de deur die een pakketje voor u heeft. Om dat pakketje in ontvangst te nemen, vertelt de bezorger u dat u eerst 1 euro moet pinnen. U laat zich uiteindelijk door de vlotte babbel(truc) van de bezorger overtuigen, pint 1 euro en neemt het pakketje in ontvangst. Enkele uren later komt u tot uw grote schrik tot de ontdekking dat uw bank- en spaarrekening volledig zijn leeg getrokken. Of een ander scenario: u pint in een drukke en overvolle winkel aan de kassa en later op de markt wordt u bijna omver gelopen door een ruziënd stel. Een paar uur later komt u er vervolgens achter dat uw bank- en spaarrekening volledig zijn leeggehaald. Misschien fictieve scenario's voor u, maar allerminst onwerkelijk, omdat het mensen zoals u en ik wel degelijk is overkomen.

Voor alle duidelijkheid, wat is er in bovenstaande gevallen precies gebeurd? U bent in eerste instantie waarschijnlijk ten prooi gevallen aan het opslaan of afkijken van uw pincode. Daarna bent u het slachtoffer geworden van de omwisseling of diefstal van uw bankpas. In het eerste geval heeft u waarschijnlijk gepind op een nep-pinapparaat. Dit neppe pinapparaat heeft echter geen betaling uitgevoerd, maar alleen uw ingetoetste pincode nauwkeurig opgeslagen. De bezorger heeft bij het verwijderen van uw bankpas uit dit apparaat heel slinks en ongemerkt uw pas verwisseld voor een eender exemplaar van diezelfde bank. In het tweede geval heeft iemand van eerder genoemd ruziënd stel al in de winkel tijdens het pinnen over uw schouder heen uw pincode afgekeken. Later, op de markt tijdens de bewust door hen gecreëerde verwarring, heeft iemand van datzelfde criminele stel vervolgens uw bankpas ontvreemd.

Keuzevrijheid in bank, geen keuzevrijheid in veiligheid systeem

Natuurlijk, u belt meteen uw bank zodra u zich bewust bent van de omwisseling of diefstal van uw bankpas. Maar dit soort internetcriminelen zijn razendsnel en vaak is het leed al geschied voordat u zich bij uw bank kan melden. Kan een dergelijk scenario zich bij alle banken voordoen, vraagt u zich nu misschien af? Het onthutsende antwoord daarop is NEE, want sommige banken zijn vanwege de inrichting van hun elektronisch bankieren hiervoor duidelijk gevoeliger dan andere. U moet weten dat banken in hun afwegingen kosten en gebruikersgemak soms voor laten gaan op absolute veiligheid. Het bestaande systeem is met extra gebruikershandelingen of met aanvullende procedures zeker nog een stuk veiliger te maken. Maar kosten en gebruikersgemak spelen een grote rol in de keuzes voor de inrichting van het elektronisch bankieren. Deze realiteit betekent dat je als klant daarin maar weinig keuzevrijheden hebt. Behalve de keuze voor jouw bank kun je bijvoorbeeld niet kiezen voor een grotere veiligheid van het elektronisch bankieren. Tenminste niet zonder veel moeite en met het nodige verstand van zaken. (daarover verstrek ik in de laatste alinea nog enkele tips) Het gevolg hiervan is dat bij bepaalde banken bepaalde vormen van misbruik meer voor de hand lijken te liggen dan bij andere banken.

ABN-Amro en Rabobank onveiliger vanwege gebruik generieke cardreaders
Voor alle duidelijkheid, inloggen bij de bank via een webbrowser - meestal op PC of laptop - wordt internetbankieren genoemd. Inloggen via de mobiele bankapp op smartphone of tablet wordt mobiel bankieren genoemd. Om in te loggen op internetbankieren kun je bij ABN-Amro, Knab en Rabobank gebruik maken van jouw bankpas+pincode en een apparaatje genaamd e.dentifier (abn-amro), cardreader (knab) of raboscanner. Dergelijke apparaatjes worden ook wel cardreaders genoemd. Wanneer je jouw bankpas in zo'n cardreader steekt en vervolgens jouw pincode intoetst, genereert deze de noodzakelijke inlog- en betaalcodes voor internetbankieren. Dit geldt eveneens voor bijzondere betalingen binnen mobiel bankieren. Om daadwerkelijk te kunnen betalen of over te schrijven moet je bij ABN-Amro en Knab vervolgens nog een code van het beeldscherm overtoetsen op de cardreader of bij de Rabobank een afbeelding van het beeldscherm scannen. Op deze manier identificeer je jezelf als rekeninghouder doormiddel van bankpas+pincode+cardreader. Het feit wil echter dat cardreaders per definitie niet persoonsgebonden, maar generiek van aard zijn. Dat wil zeggen dat elke cardreader van de desbetreffende bank te gebruiken is met elke bankpas+pincode van klanten van diezelfde bank. In eerder genoemde scenario's, waarin internetcriminelen net jouw pincode en bankpas hebben bemachtigd, is het gebruik van de juiste generieke cardreader voldoende om de volledige toegang tot jouw bank- en spaar-rekening te krijgen. In no-time zullen ze alle bedragen overgeheveld hebben naar een criminele (tussen)rekening. Tenminste, zolang jouw gestolen bankpas nog niet door de bank is geblokkeerd.

Om in te loggen via jouw webbrowser (internetbankieren) heb je bij Knab ook nog een gebruikersnaam en een wachtwoord nodig. Een dergelijke voorzorgsmaatregel maakt pasmisbruik, ondanks het gebruik van een generieke cardreader, al een stuk minder aannemelijk.

Hoewel banken zeggen dat ze dergelijke uitzonderlijke transacties in veel gevallen tijdig zullen blokkeren, bestaat hierover in de praktijk maar weinig zekerheid. Bovendien, zou u willen afwachten of uw bank wel of niet tijdig ingrijpt? U moet dan maar afwachten of u ooit nog iets van uw gestolen geld terugziet! Bankgaranties zijn tegenwoordig lang niet meer zo stellig als in de begintijd van het elektronisch bankieren. Banken wijzen tegenwoordig al snel met de beschuldigende vinger naar de in hun overtuiging onzorgvuldige klant. De mantra's waarvan zij zich dan gemakshalve bedienen, bestaan vooral uit verwijten van grove onzorgvuldigheid. Tegenwoordig is financieel misbruik immers bijna altijd het gevolg van ingenieuze babbeltrucs of geavanceerde (digitale) misleiding. Banken hanteren opportuun dat dit de eigen verantwoordelijkheid van hun klanten betreft. Van oudsher stellen banken zich eigenlijk alleen garant voor de gevolgen van misbruik als direkt gevolg van gecompromitteerde banksoftware.

Zelfs als jij alle betalingshandelingen al jaren standaard met jouw mobiele bankapp en/of mobiel bevestigen uitvoert (mobiel bevestigen is de variant waarbij je bankiert via de webbrowser maar toestemming geeft via de mobiele bankapp) blijft de mogelijkheid van misbruik met jouw bankpas+pincode+generieke cardreader wagenwijd openstaan. Hoewel je cardreaders op het eerste gezicht dus lijkt te kunnen vermijden, blijven deze cardreaders+bankpas+pincode beschikbaar als standaard inlog- en betaalmethode. Zowel ABN-Amro als Rabobank bevestigen dat het niet mogelijk is om op speciaal verzoek de e.dentifier of raboscanner definitief als inlogmogelijkheid te verwijderen uit elektronisch bankieren. Jammer, want dit zou jouw betalingsomgeving een stuk veiliger maken met alleen nog de strikt gepersonaliseerde inlogmogelijkheid van jouw mobiele bankapp.

Complimenten aan ING, SNS, ASN en Regiobank voor gebruik digipassen
Er bestaan echter al heel lang inherent veiligere methoden, die een forse extra hindernis opwerpen voor internetcriminelen. Het betreft hier het gebruik van zgn. digipassen voor internetbankieren en voor bijzondere transacties binnen mobiel bankieren. Digipassen zijn gepersonaliseerde digitale apparaatjes die na het ingeven van een 5-cijferige code bepaalde inlog- en betaalcodes genereren. In aanleg vergelijkbaar met cardreaders, maar digipassen+5-cijferige code maken echter géén gebruik van jouw bankpas+pincode. Het betreft namelijk een volstrekt onafhankelijke manier van inloggen. Daardoor zul je jouw digipas+5-cijferige code als vanzelf ook vaker gescheiden van jouw bankpas (lees: thuis) bewaren. Wat je niet regelmatig gebruikt in de publieke ruimte kan overeenkomstig ook minder snel worden gecompromitteerd. Qua gebruik is het vergelijkbaar met jouw mobiele bankapp+5-cijferige code. Jouw smartphone fungeert in dat geval als digipas.

Ter vervanging van de verouderde TAN-codes die de bank voorheen naar jouw mobiel sms'te, biedt de ING nu of mobiel bevestigen via jouw smartphone of een zgn. ing-scanner (digipas met kleurencode-scanfunctie) voor mensen zonder smartphone. SNS, ASN en Regiobank bieden al langer zgn. digipassen. Daarnaast bieden alle banken mobiel bevestigen aan via jouw smartphone. Het grote voordeel van deze beide systemen is dat zowel jouw smartphone als deze digipassen volstrekt individueel zijn. Dit betekent dat om in te loggen op jouw rekening je of een 5-cijferige code moet invoeren in jouw mobiele bankapp of een 5-cijferige code op jouw digipas. Omdat de digipassen geen gebruik maken van jouw bankpas+pincode is toegang tot jouw rekening vanwege eerder geschetst misbruik op deze manier onmogelijk. Tel daarbij op dat om in te loggen via jouw webbrowser (internetbankieren) je bij ING een gebruikersnaam en een wachtwoord nodig hebt en het lijkt erop dat ING de beveiliging van jouw rekening prima voor elkaar heeft.

Helaas biedt de ING-app dan wel weer als enige de mogelijkheid om via de simpele autorisatie van een QR-code jouw ING-app op een tweede digitaal apparaat naar keuze te installeren. In aanleg handig voor eigen gebruik, maar funest als een internetcrimineel jou een dergelijke QR-code toestuurt. Ondanks duidelijke waarschuwingen hiervoor in de app zijn hier de afgelopen tijd toch aardig wat mensen ingetuind. Qua veiligheid is het natuurlijk de kat op het spek binden om een gepersonaliseerde hoogst beveiligde bankapp doormiddel van een op een betalingscode lijkende QR-code op meerdere apparaten te kunnen installeren. Je vraagt je meteen af wie zoiets heeft bedacht? Mijns inziens een majeure (en vooralsnog voortdurende) misser van de ING. Maar zoals eerder al gezegd, gebruikersgemak gaat wel vaker voor op gebruikersveiligheid.

Uiteraard kan jouw gestolen bankpas - dit geldt natuurlijk voor iedere bank - nog altijd worden misbruikt om geld of artikelen mee te pinnen, maar hiertegen kun je tenminste een degelijke dagelijkse limiet instellen, die de schade behoorlijk kan beperken. Een dergelijke voorzorgsmogelijkheid is standaard beschikbaar bij alle banken.

Per saldo zijn individuele digipassen een stuk veiliger dan generieke cardreaders
Hoewel internetbankieren, mobiel bankieren en mobiel bevestigen op zichzelf erg veilig zijn, kan de mogelijkheid van het toestaan van standaard toegang via bankpas+pincode+ generieke cardreader deze veiligheid alsnog ernstig compromitteren. ABN-Amro en Rabobank bieden vooralsnog zo'n standaard zwakkere toegang, zonder extra voorzorgsmaatregelen zoals Knab wel biedt. Een ketting is helaas maar zo sterk als zijn zwakste schakel. Generieke cardreaders zijn tegenwoordig daarom de spreekwoordelijke zwakste schakel van het elektronisch bankieren. Natuurlijk zijn ABN-Amro en Rabobank hiervan op de hoogte. Maar gebruikersgemak en invoeringskosten wegen vooralsnog blijkbaar zwaarder dan uw gebruikersveiligheid. Deze banken spreken al jaren hun voornemen uit om hun cardreader op termijn uit te faseren. In het licht van bovenstaande mag je je echter afvragen waarom hiermee niet meer haast wordt gemaakt?

Opgemerkt moet worden dat het niet de cardreaders zelf zijn die onveilig zijn. Op zichzelf zijn de cardreaders namelijk erg veilig. Het is vooral de combinatie van bankpas+pincode+ generieke cardreader en het regelmatige pas- en pincode-gebruik in de publieke ruimte die het geheel kwetsbaar maakt. Helemaal als er geen gebruikersnaam en wachtwoord zijn vereist om in te loggen op internetbankieren. Dit omdat het het aannemelijk maakt dat het een vaardige crimineel lukt om al deze drie zaken bijeen te sprokkelen. Digipassen werken daarentegen volstrekt onafhankelijk van bankpas+pincode en worden als gevolg daarvan meestal gescheiden (lees: thuis) bewaard. Dit maakt het voor een crimineel op zijn minst noodzakelijk om bij jou in te breken om jouw digipas te bemachtigen, zonder enige garantie dat hij daarmee ook jouw 5-cijferige code verkrijgt. Individuele digipassen werpen daarmee automatisch een effectievere drempel op tegen misbruik van elektronisch bankieren dan generieke cardreaders doen.

Belangrijkste aanbevelingen tegen pasmisbruik en app-misbruik

Pasmisbruik overkomt je, omdat het systeem voor elektronisch bankieren niet waterdicht is!

De kortste klap voor gecompromitteerde banken **(ABN-Amro, Rabobank)** om hun beveiliging van internetbankieren op korte termijn te verbeteren, is het invoeren van de verplichting om in te loggen middels een unieke gebruikersnaam en een wachtwoord. Een heel stuk degelijker is natuurlijk de uitrol van digipassen in plaats van de huidige generatie kwetsbare generieke cardreaders.

Het middels een QR-code autoriseren van de bankapp op een tweede apparaat naar keuze **(ING)** kan een stuk veiliger, indien het wordt gecombineerd met het gebruik van de al bestaande digipas. Op deze manier is het niet langer aannemelijk dat mensen nog met een snelle babbeltruc worden verleid.

In hun reaktie op pré-publicatie van dit artikel erkennen deze banken in principe het gevaar van misbruik door de combinatie van bankpas+pincode+generieke cardreader. Ze bagatelliseren het tegelijkertijd ook door te stellen dat er door de toename van contactloos betalen tegenwoordig minder gelegenheid bestaat om de pincode af te kijken. Toch moeten pashouders nog regelmatig hun pincode invoeren, als ze hun maximale limiet voor contactloos betalen van € 50 hebben bereikt.

Tenslotte stellen de banken dat phishing (internetbankieren via een frauduleuze link en website) een veel groter probleem vormt dan pasmisbruik. Dit mag misschien zo wezen, maar tegen phishing kun je jezelf met het nodige gezonde verstand prima beschermen. Pasmisbruik overkomt je, omdat het systeem voor elektronisch bankieren zelf niet waterdicht is!

Wat kun je doen om jezelf beter te beschermen?

Er van uitgaande dat je klant bent bij ABN-Amro of Rabobank en dat je geen zin hebt om van bank te wisselen. Wat kun je in dat geval doen om jezelf beter te beschermen? Een bankwissel lijkt mij namelijk een dagtaak, vanwege het op de hoogte brengen van al mijn betalingscontacten van mijn gewijzigde bankrekening. Ik gaf al aan dat je als klant van één van deze banken niet zonder meer kunt kiezen voor een inherent grotere veiligheid van het elektronisch bankieren. Tenminste niet zonder veel moeite en met het nodige verstand van zaken. Toch is er één ding dat je wel kunt doen. Je kunt jouw bankkantoor namelijk expliciet verzoeken om een extra bankpas zónder standaard toegang tot elektronisch bankieren. Op deze manier zorg je ervoor dat je uiteindelijk over twee bankpassen beschikt - liefst natuurlijk ook met twee verschillende pincodes - waarvan slechts één bankpas nog toegang geeft tot

elektronisch bankieren. In dat geval kun je de door jouw bank gecompromitteerde veiligheid als gevolg van hun generieke cardreader effectief omzeilen. Immers, als je vervolgens slechts nog dié bankpas - dié expliciet géén toegang meer geeft tot internetbankieren - gebruikt om te pinnen op pinapparaten of betaalautomaten, dan leidt misbruik van deze bankpas+pincode+generieke cardreader niet langer automatisch tot toegang tot jouw elektronisch bankieren. Overigens kun je dergelijke specifieke voorkeuren of instellingen hoogstwaarschijnlijk niet standaard online regelen en vergt dit wel een persoonlijk bezoekje en nadere uitleg aan jouw bankkantoor.

Art Huiskes
Onderzoeksjournalist

E. art.huiskes@gmail.com