"Bankwebsites en apps zijn absoluut veilig, maar gooi je codes niet te grabbel"

Phishers zijn extreem slim en sluw. Maar het grote aantal phishing-gevallen doet ook vragen rijzen bij de veiligheid van de websites voor online bankieren en de bankapps. Zijn die wel veilig? "Absoluut wel. Maar het is de manier van werken van die phishers die gewiekst en problematisch is", zo stelt ethisch hacker Stijn Jans bij de Inspecteur op Radio 2.

Stijn Jans is ethisch hacker en oprichter van Intigriti. Dat is een internationaal cyber security platform dat ethische hackers samenbrengt met bedrijven. De ethische hackers vallen de online systemen van bedrijven aan om op die manier bugs en tekortkomingen in het systeem bloot te leggen.

Jans is formeel: de websites en apps van banken zijn veilig. "Banken doen er alles aan om die systemen zo veilig mogelijk te maken Er worden enorm veel middelen, tijd en geld geïnvesteerd in veiligheidssystemen. Banken kunnen zich niet veroorloven dat er iets mis gaat. Dus die veiligheidstesten zijn voor banken heel belangrijk. Ze worden trouwens ook verplicht opgelegd door de overheid."

Phishers breken in omdat klanten codes delen

De systemen die banken bouwen om de websites en de app te beveiligen, voldoen aan alle veiligheidscriteria. Maar een systeem mag nog zo veilig zijn als maar kan, de zwakste schakel blijft de gebruiker. Als die 'slordig' is en in een moment van onoplettendheid codes doorgeeft, dan kan een crimineel inloggen op jouw account en op die manier geld stelen.

Sommige phishers kunnen zelfs inloggen op jouw bankaccount via de app die ze op hún smartphone installeren. Ze loggen dus in op jouw bankaccount vanop een ander toestel zonder dat jij dat in de gaten hebt. Jans legt uit hoe dat werkt:

Stap 1: De phisher maakt een valse website aan die als doel heeft slachtoffers aan te zetten tot een betaling.

Als slachtoffer kom je op de website terecht doordat je op een link klikt die je toegestuurd krijgt per mail, sms, WhatsApp of Messenger. Op zich maakt het niet uit op wat voor platform je terecht komt. Het kan een nagemaakte website van een bank zijn waarbij je een klein verrichting moet doen om een kaartlezer te bestellen. Evengoed leidt de link naar een valse betaalpagina van een koerier bedrijf zoals Bpost, DPD of DHL. De bedoeling is dat jij als klant gelooft dat je op dat platform een betaling moet doen.

Stap 2: De dader installeert de app van de bank van het slachtoffer op zijn telefoon.

Phishers weten veel over hun slachtoffer. De dader weet bij welke bank jij klant bent en installeert alvast de app op zijn smartphone. Om effectief te kunnen inloggen, heeft hij betaalcodes nodig.

Stap 3: Het slachtoffer denkt een betaling te doen maar genereert in werkelijkheid

codes waarmee de phisher kan inloggen.
Als ontwetend slachtoffer voer jij een betaling uit op een valse website. Je denkt een klein bedrag over te schrijven. Maar de phisher kijkt mee aan de andere kant. De codes die jij invoert om 'de betaling uit te voeren', zijn in werkelijkheid de codes die de phisher nodig heeft om in te loggen op de bankapp.

Stap 4: De phisher is ingelogd en kan nu in jouw naam bankverrichtingen uitvoeren en limieten aanpassen.

Maximumbedrag dient om je te beschermen
Bij veel banken staan er limieten op de som die je kunt overschrijven in de app. Volgens Jans is dat een goede maatregel. "Veel gebruikers ervaren het als een last dat je maar een beperkt bedrag kan overschrijven via de app. Weet dat het gebeurt voor je eigen veiligheid." Al waarschuwt Jans ook dat die bescherming niet waterdicht is. Phishers kunnen die omzeilen. "Ook in de app kun je limieten aanpassen. Om dat te doen, is er vaak een tweede stap nodig. Je moet dan iets bevestigen of een extra code intikken. Het kan best zijn dat de phisher je zover krijgt dat je ook die extra code doorgeeft."

Eén gouden raad: wees altijd voorzichtig. En neem ook deze 5 regels in acht:
- Controleer grondig de afzender van elke e-mail
- Klik nooit zomaar op een link in een e-mail
- Kijk goed op welke website je aan het surfen bent
- Geef nooit je betaalcodes door als daarnaar gevraagd wordt
- Bel onmiddellijk naar cardstop en de bank als je het slachtoffer bent van phishing. Doe ook een aangifte bij de politie

Bron: VRT Nieuws