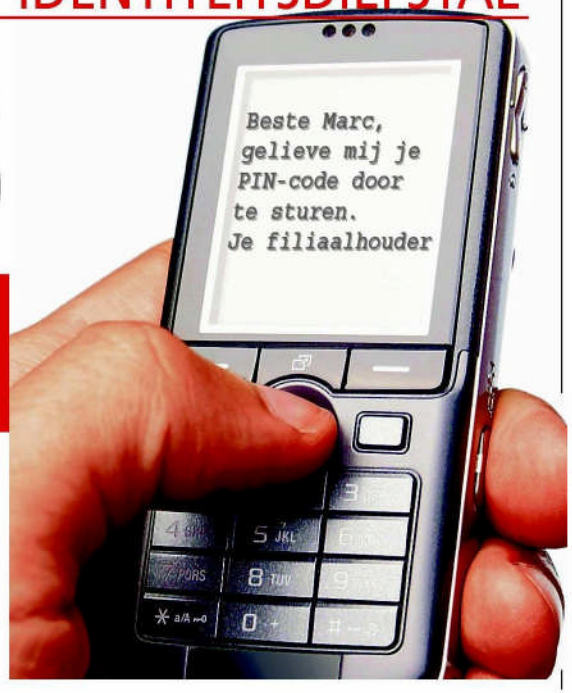
FOD ECONOMIE WAARSCHUWT VOOR NIEUWE 'IDENTITEITSDIEFSTAL'

VALSE SMS'JES

soms grap, soms fraude



De FOD Economie en beveiligingsexperts waarschuwen voor een nieuwe vorm van 'identiteitsdiefstal'. Op websites als 'smsbuzz' en 'anoniemsms' kan je onder een valse identiteit sms'jes versturen. Dat leidt niet alleen tot flauwe grappen – zo kan je bijvoorbeeld in de naam van je baas naar een collega sturen dat hij ontslagen is – maar ook tot diefstal en fraude.

JELLE RITS

Een nieuw fenomeen doet zich voor op het internet, waar websites als *Smsbuzz*, *Fakesms*, *Anoniempje*, *Smsanoniem* of *Anoniemsms* als paddenstoelen uit de grond schieten. Het principe is eenvoudig: je surft naar zo'n site en tikt een tekstbericht in. Vervolgens geef je het gsm-nummer in van een valse afzender (bijvoorbeeld Tim) en van de ontvanger (Jan). Je belt naar een 090X-nummer, drukt op verzenden en luttele seconden la-

ter krijgt Jan een sms van Tim.
De Federale Overheidsdienst Economie is «bezorgd» om deze «onschuldige vorm van grappenmakerij». «Dit is een vorm van identiteitsdiefstal, aangezien je je voordoet als iemand anders en er valse informatie wordt verspreid», zegt een woordvoerder.
Wij deden de test en inderdaad: zo'n valse sms ziet eruit als een gewone sms, verstuurd via gsm. Zo kan je je voordoen als de baas en naar een collega sturen dat hij op het matje moet komen. Of als vrouw van je beste vriend sms'en dat zij hem verlaat.
De websites maken ook openlijk reclame voor deze praktijk. Ze blijken zich bovendien bewust van de gevolgen: «Met deze dienst is het mogelijk om de verzender te wijzigen in een ander gsm-nummer. We vragen je wel om het hierbij zowel voor de verzender als de ontvanger leuk te houden. Het versturen van sms'jes voor pesten, bedreigen of intimideren kunnen we niet tegenhouden, maar dit wordt door ons wel afgekeurd.»

Goedgelovig

Volgens beveilingingsexpert Eddy Willems van *Kaspersky* is het gevaar van deze websites nog veel groter «omdat ze ook misbruikt kunnen worden door criminelen». «Een gekende praktijk is dat men zich voordoet als vertrouwenspersoon en verwijst naar 'een leuke website', waarna de nietsvermoedende ontvanger een virus op zijn computer binnenhaalt. Nog érger wordt het als 'de bankdirecteur' vraagt om de PIN-code van je bankkaart door te mailen. Veel mensen zijn goedgelovig en op het internet liggen zoveel gsm-nummers voor het grijpen.» De beveiligingsexpert wijst er in die zin ook op dat criminelen hun actieterrein steeds meer verleggen van het internet naar gsm's, «aangezien deze toestellen voor steeds meer kunnen gebruikt en dus ook misbruikt worden».
De gsm-operatoren staan bovendien machteloos, omdat de valse sms'en via buitenlandse platformen worden verstuurd. De FOD Economie raadt gedupeerden aan om klacht in te dienen bij de politie, al kunnen de sms-piraten volgens Willems vaak moeilijk opgespoord worden. «Toch kan je het soms ook merken als je een verdacht sms'je krijgt, bijvoorbeeld door het tijdstip dat niet klopt. Wees dus steeds op je hoede en ga hier zeker niet op in», besluit hij.

HET VERSTUREN VAN SMS'JES VOOR PESTEN, BEDREIGEN OF INTIMIDEREN KUNNEN WE NIET TEGENHOUDEN, MAAR WORDT DOOR ONS WEL AFGEKEURD
Uit reclame gespecialiseerde website