
Fraude via phishing (zoals het online ontfutselen van bankcodes) komt meer en meer voor. De fraudedossier zijn in 2018 verdrievoudigd in vergelijking met 2017.

Sociale media

De oplichters verzamelen bankcodes of andere persoonlijke gegevens door zich voor te doen als een bank, maar ook als de politie, een telecomoperator of een geïnteresseerde koper op een zoekertjessite. Ze doen dat door in een mail (of sms) of een berichtje op sociale media (als Whatsapp) een link te leggen naar een valse website, waar het slachtoffer dan nietsvermoedend de cijfercode van zijn bankkaart intikt, waarmee de fraudeurs dan de bankrekening plunderen.

De stijging van het aantal phishing-gevallen is vooral te wijten aan de manier waarop de criminelen te werk gaan. Ze stelen herhaaldelijk kleinere bedragen, maar aan het einde van de rit hebben ze veel buit gemaakt. In totaal gingen de fraudeurs vorig jaar aan de haal met meer dan 8 miljoen euro. In 2017 was dat maar 2,5 miljoen euro.



Geef fraudeurs geen kans

'Je moet goed opletten wil je niet het slachtoffer worden van phishing. Net zoals gauwdieven die hun kans schoon zien als je even afgeleid bent, rekenen phishingcriminelen erop dat je er je hoofd niet bijhebt.

De banken geven volgende tips mee: speel de fraudeurs niet in de kaart en doe je betalingen dan ook nooit impulsief; geef nooit je pincode of codes om te internetbankieren via e-mail, sociale media, sms of telefoon; typ altijd zélf het webadres van je bank in je browser of open zelf de app van je bank. Ga er niet naartoe via een onveilige link.

Als je toch bankgegevens hebt doorgegeven, moet je onmiddellijk Card Stop verwittigen (**www.cardstop.be of 070 344 344**) en jouw bankkaart laten blokkeren.

