



BE SAFE ! – BETAALKAARTFRAUDE VOORKOMEN

<p>WAT IS BETAALKAARTFRAUDE ?</p>	<p>Het gebruik van betaalkaarten biedt tal van troeven. Vanuit veiligheidsoogpunt is de reductie van cash geld een belangrijk instrument om het diefstalrisico tegen te gaan zowel bij de klant als de handelaar. Hoewel deze betaalkaarten over het algemeen goed beveiligd zijn, komt fraude voor in het dagelijkse gebruik of bij online aankopen op het internet.</p> <p>Betaalkaartfraude is de verzamelterm voor het misbruik van de betaalkaartgegevens van iemand anders om aankopen te kunnen doen, geld af te halen, enz..</p> <p>Vanuit deze optiek is het wenselijk bijkomende tips aan te reiken over het veilig gebruik, teneinde het risicobewustzijn voor dit fenomeen te bevorderen.</p>
<p>WELKE ZIJN DE GEBRUIKTE METHODES ?</p>	<p>Tegenwoordig zijn de voornaamste gebruikte methodes om de financiële identiteit van een persoon onrechtmatig te weten te komen « skimming », « phishing » en « shouldersurfing ».</p> <p>« Skimming » is een techniek waarbij de gegevens op de magneetstrook van een betaalkaart gekopieerd worden met behulp van een klein technisch toestelletje (skimmer) dat vooraf op de geldautomaat wordt geïnstalleerd. De pincode wordt meestal gefilmd met een mini-camera, eveneens geïnstalleerd op de geldautomaat. De gekopieerde gegevens worden overgezet op blanco kaarten. Op die manier kan de dader dan het geld, dat op de rekening van het slachtoffer staat, gebruiken. Dit soort van fraude komt vooral voor aan betaalautomaten of betaalterminals (bvb. benzinstation), enz.</p> <p>De « phishing » methode wordt op internet gebruikt. Het slachtoffer wordt (via een mail waarin bijvoorbeeld wordt gevraagd op een link te klikken), naar een valse site gestuurd die sterk lijkt op de site van een bank of een commerciële site. Wanneer het slachtoffer zijn gebruikersnaam en paswoord ingeeft, worden deze rechtstreeks gerecupereerd door de « phisher » die deze dan zal gebruiken om transacties of aankopen uit te voeren.</p> <p>« Shouldersurfing » is een techniek waarbij de fraudeur over de schouder van het slachtoffer meekijkt terwijl deze zijn of haar pincode ingeeft. Het slachtoffer wordt dan afgeleid door de fraudeur doordat deze bvb. uitleg vraagt over de geldautomaat, de weg vraagt,... Tijdens deze afleiding steelt de fraudeur de betaalkaart, waarna hij zo snel mogelijk geld gaat afhalen met de gestolen kaart en pincode.</p>

**HOE ZICH TE
BESCHERMEN ?**

Om u te beschermen tegen de onrechtmatige toe-eigening van de bankidentiteit (met name « skimming » en « phishing »), vindt u hieronder enkele elementaire preventietips.

Algemeen.

Wees altijd **waakzaam** en gebruik geen betaalkaart als u iets verdachts ziet op de geldautomaat of in de omgeving ervan.

- ⇒ Controleer regelmatig uw **rekeninguittreksels** en meld onmiddellijk eventuele frauduleuze transacties aan uw bank;
- ⇒ **verscheur** alle documenten waarop gevoelige informatie geschreven staat en gebruik bij voorkeur een versnipperaar;
- ⇒ voer je pincode altijd **buiten het zicht van anderen** in (door bijvoorbeeld je vrije hand te gebruiken om het toetsenbord af te schermen) ;
- ⇒ pas op voor personen die u informatie vragen op straat of per telefoon (interviewers, tevredenheidsenquête, enz.) en geef hen **geen enkele gevoelige informatie**.

Op internet :

- ⇒ beantwoord nooit **e-mails** die u vragen om **gevoelige informatie** mee te delen (adres, kaartnummer, code, enz.), om uw rekening te controleren. Weet dat uw bank u nooit dergelijke informatie zal vragen want zij heeft die al ter beschikking;
- ⇒ geef **geen gevoelige informatie door via internet** (aan vrienden, via sociale netwerken, enz.) want die kan zonder dat u het weet worden onderschept;
- ⇒ **download geen bestanden** die u ontvangen heeft van personen die u niet kent;
- ⇒ controleer altijd **de URL** van de site waarop u uw gebruikersnaam en uw paswoord gaat invoeren. Een beveiligde site begint met « https » en een klein gesloten geel hangslotje onderaan rechts op uw scherm;
- ⇒ doe regelmatig updates van uw **antivirusprogramma en besturingssysteem**.

**SLACHTOFFER VAN
FRAUDE MET EEN
BETAALKAART ?**

Als u het slachtoffer bent van een fraude met een betaalkaart, reageer dan zo vlug mogelijk.

- ⇒ Bel **naar Card Stop** om uw kaart te blokkeren (070/344.344);
- ⇒ **neem contact op met uw bank**;
- ⇒ ga een **klacht indienen** op het politiecommissariaat van uw zone.

Als u een inbreuk op internet heeft vastgesteld en u bent zelf geen slachtoffer, meld deze dan op www.ecops.be.

**BIJKOMENDE
INFORMATIE ?**

Indien u meer informatie wenst over bankkaartfraude, kunt u de volgende internetsites raadplegen :

- ⇒ <http://www.polfed-fedpol.be/>
- ⇒ <https://besafe.ibz.be>
- ⇒ http://economie.fgov.be/nl/binaries/consumers_internetguide_nl_tcm325-36236.pdf
- ⇒ www.web4me.be
- ⇒ www.saferInternet.be