euromex
rechtsbijstand | protection juridique

Safety World

Op virtuele koopjesjacht? Wees voorzichtig.

2 januari 2020

Van 3 tot 31 januari 2020 is het weer zover in België. De solden! Onze winkelstraten veranderen in koopjesparadijzen. Ook de online-winkels doen mee.
Heb je geen zin om je in de massa te begeven, en ga je op je PC op virtuele koopjesjacht? Wees alert! Je hebt dan misschien geen last van zakkenrollers, ook hier liggen er kapers op de kust. Ook voor fraudeurs is dit de ideale periode om een graantje mee te pikken.

Koop op veilige websites

Als het adres van de website begint met https (hypertext transfer protocol secure - met hangslotje) betekent dit dat het voor mensen met slechte bedoelingen vrijwel onmogelijk wordt om te weten welke gegevens verstuurd worden. Hiervoor heeft men een ssl- certificaat nodig per domeinnaam. Kijk ook naar de geldigheid van het certificaat. Klik hiervoor op het hangslotje en klik op “certificaten weergeven”. Hier kan je de geldigheid van het certificaat bekijken en vaststellen of het certificaat “in orde” is. Vertrouw enkel “groene” certificaten (die de EV- standaard (Extended Validation)) hebben doorlopen. Websites met een rood of geel gekleurd certificaat vermijd je best.

Bekijk ook de website in zijn geheel. Heeft de website een professionele uitstraling? Of staat het vol schrijffouten? Als de website amateuristisch is opgesteld, wees dan extra op je hoede.

Is de prijs te mooi om waar te zijn, dan ís het meestal ook te mooi om waar te zijn. Goederen die aan een abnormaal lage prijs worden aangeboden, zijn meestal niet ok. Hoed je ook voor namaak. Die designerhandtas aan een spotprijs is waarschijnlijk eerder nep dan echt. Dit soort producten wordt tegenwoordig ook meer en meer via sociale media aangeboden.

Dikwijls is het interessant om onlinediscussiefora en waarschuwingen van de consumentenbeschermingsautoriteiten te lezen. Ze kunnen gevonden worden door in de zoekmachines als trefwoorden de naam van de site + “bedrog”, “scam”, "fraude", "oplichting", … in te geven. Je zal snel te weten komen of de website via dewelke je iets wil kopen, wel te vertrouwen is.

Wees alert met e-mails. Oplichters misbruiken de naam van gekende websites. Bestudeer de mails zorgvuldig en kijk goed naar de tekens die na het apenstaartje (@) vermeld staan. Klik niet op links als je enigszins twijfelt.

Betaal veilig

Je online-aankopen koop je meestal met een debet- of kredietkaart. Dat is niet zonder risico's. Fraude met de bankkaart is een fenomeen dat steeds vaker voorkomt.

De algemene regel is dat betalen via de website veiliger is dan buiten de website.
Bij betalingen via vertrouwde websites ontvang je meestal een bevestiging via e-mail.
Als gevraagd wordt om via Western Union, MoneyGram, cheque, postwissel of Liberty Reserve te betalen, ga hier dan niet op in. Betaal best met een kredietkaart.

Wees alert voor phishing. Ontvang je een e-mail van je bank- of kredietkaartbedrijf? Dat is dan mogelijk een fraudeur die zich uitgeeft voor het bedrijf. Deze probeert dan om persoonlijke informatie te verkrijgen zoals je naam, je adres, je kaartnummer of je pincode. Deze fraudeurs worden steeds creatiever en de e-mails die je ontvangt ogen steeds realistischer.
Reageer nooit op twijfelachtige e-mails. **Weet dat geen enkele bank- of kredietkaartverstrekker via e-mail vertrouwelijke informatie of pincodes zal opvragen.**

Vertrouw je het niet? Werden je gegevens ontvreemd? Laat dan je kaart onmiddellijk blokkeren door Card Stop (070/344 344). Vanaf dat moment kunnen er in principe geen transacties meer worden uitgevoerd met de kaart. Gebeuren er toch nog transacties, dan zullen deze integraal vergoed worden door de bank of de kredietkaartinstelling. Je moet de uitgever van de kaart wel binnen dertien maanden na de betwiste transacties informeren over deze feiten.

En wat met de gelden die zijn verdwenen voordat de rekening geblokkeerd kon worden?
Als je nog altijd in het bezit bent van je kaart terwijl ze frauduleus werd gebruikt, worden alle verliezen die je op deze manier hebt geleden, terugbetaald. Als de bank of kredietinstelling kan bewijzen dat je zelf nalatig bent geweest of als er sprake is van bedrog of opzet dan zal je het verlies volledig zelf moeten dragen. De wet bevat geen definitie van het begrip 'grove nalatigheid', maar somt wel een aantal voorbeelden op. Bijvoorbeeld, je laat je kaart niet blokkeren.

Wat als je zelf een betaling hebt uitgevoerd die foutief blijkt te zijn?
Je schreef bijvoorbeeld een verkeerd bedrag over, of het rekeningnummer is foutief, of de begunstigde is verkeerd. In deze gevallen ben je zelf verantwoordelijk voor de informatie die je ingeeft bij de betaling. De bank of kredietkaartinstelling is niet altijd verplicht een controle uit

te voeren tussen de persoonlijke gegevens (naam, adres) van de begunstigde en het rekeningnummer. Contractueel kan bepaald zijn dat de bank enkel het rekeningnummer moet controleren. Het zal in deze situaties veel moeilijker zijn om een bank aansprakelijk te stellen voor de verkeerde betaling. Anderzijds is de bank wel verplicht om redelijke inspanningen te leveren om de onverschuldigde betaling terug te krijgen. De bank mag hier wel kosten voor in rekening brengen.

We adviseren om regelmatig je afrekeningen en uittreksels te controleren. Als je misbruik vaststelt, moet je onmiddellijk de kaart laten blokkeren en je bank of kredietinstelling contacteren om de verrichtingen te betwisten.

Veel succes in je jacht op koopjes! Maar blijf alert…

Met vriendelijke groeten

Christel Vandenbosch
communicatie
safetyworld@euromex.be

Generaal Lemanstraat 82-92 | B-2600 Berchem | T +32 3 451 44 00
Rue E. Francqui 1 | B-1435 Mont-Saint-Guibert | T +32 10 80 01 50

Follow us

Je Makelaar
Je beste
Verzekering