

## 13/04/2018 – ECOFIN – Internetoplichting blijft een probleem

Het internet biedt talloze opties op het vlak van kopen en verkopen (verkoopsites), het leggen van sociale contacten (emotiesites), het zich uitgeven voor betrouwbare derden (dienstverlenende - of ondersteunende sites),... Helaas zijn er ook veel risico's verbonden aan deze digitale vormen van communicatie. Met deze beknopte bijdrage wil het openbaar ministerie blijvend inzetten op informatieverstrekking en bewustmaking omtrent de gevaren van het internet, met specifieke focus op wat de burger zelf kan doen om zich te beschermen tegen deze welbepaalde vormen van oplichting. Voorkomen is immers altijd beter dan genezen.

Hieronder een aantal nuttige tips. Deze zullen u helpen om een eventuele financiële kater te vermijden.

### **Algemeen**

- Zorg dat uw computer, tablet en/of smartphone voldoende beveiligd en up-to-date is.
- Draag zorg voor uw (wifi-)paswoord en uw netwerk en verander regelmatig de paswoorden.
- Stuur nooit foto's door van uw identiteitskaart, rijbewijs, bankkaart of andere documenten of apps met persoonlijke gegevens. Wees alert voor identiteitsfraude door derden wanneer u deze foto's zelf als bewijs krijgt toegestuurd (verloren of gestolen documenten).
- Geef vertrouwelijke informatie nooit door via de telefoon, per SMS of via het internet. Voer geen verdere manipulaties uit via uw kaartlezer of gebruikelijke aanmeldingstool. Vermijd het consulteren van vertrouwelijke informatie via openbare (wifi-)netwerken.
- Scherm zoveel als mogelijk uw privéleven op sociale media en andere af. Controleer regelmatig uw privacy-instellingen (zeker bij gewijzigde algemene voorwaarden). Vermijd indien mogelijk ook kwetsbare informatie over uw beroepstoestand, gezinssituatie, burgerlijke stand, verblijfplaats,... Deze informatie geeft immers veel meer over u prijs dan u denkt.
- Staat er informatie van u ongewild of verkeerdelijk online? Contacteer de beheerder van de bewuste website voor de verwijdering of aanpassing ervan.
- Wees selectief bij het invullen van (online) petitie's, wedstrijdvragen, spelletjes, enquêtes, likeand-share,... Vaak vraagt men naar persoonlijke gegevens, uw GSM-nummer of uw emailadres. Tevens kent men uw interessevelden voor doelgerichte marketing.
- Lees ook effectief de algemene voorwaarden alvorens deze te aanvaarden. Zo voorkomt u stilzwijgende verlengingen van overeenkomsten, nuttelose abonnementen, automatische geldafhalingen, het doorgeven van uw informatie aan derden (al dan niet tegen betaling)...
- Denk bij (effectieve) oplichting niet alleen aan de politie. Informeer ook onmiddellijk de betrokken website, uw eigen bank, card-stop, uw telecomoperator, uw computerinstallateur, het meldpunt internetoplichting van de FOD Economie,...

### **Koop-verkoop**

- Check altijd de contactgegevens van de verkoper of de ondernemer via de openbare bronnen. Knipperlichten zijn o.a.: plotse wijzigingen (verblijfplaats, prijs,...), buitenlandse transacties, recent aangemaakte profielen, de (gebrekkige) taal van de communicatie (vertaalprogramma's), de prijs,...
- Zoek het ondernemingsnummer van de verkoper op via de Kruispuntbank der Ondernemingen (KBO) of de buitenlandse tegenhanger (bv. Kamer van Koophandel).
- Zoek op door wie, wanneer en waar de domeinnaam van de webshop werd geregistreerd (bv. via dns.be).
- Bewaar alle nuttige gegevens inzake de verlopen communicatie (liefst op de originele drager). Vraag desgevallend bijkomende inlichtingen aan de verkoper en stel gerichte inhoudelijke vragen.

- Woont de verkoper (relatief) dichtbij, ga dan zelf even langs om de goederen te bekijken en op te halen en betaal ter plaatse. Zo vermijdt u discussies of teleurstellingen, alsook het feit dat waardevolle pakketten (al dan niet bewust) verloren gaan of beschadigd raken.
- Bekijk op voorhand goed wat u werkelijk zult moeten betalen en of u bedenktijd heeft. Houd er ook rekening mee dat (luke)goederen een welbepaalde prijs hebben. Let aldus op met (nieuwe) goederen die goedkoop of onder tijdsdruk worden aangeboden (bv. leurdere). Koop geen goederen die u toch niet nodig heeft, zelfs al is de verkoper opdringerig of erg overtuigend. Vraag ook steeds een factuur of een bewijs van de aankoop (bv. een bij te leveren certificaat, garantieregeling,...).
- Let op bij de verhandeling van elektronische tickets (links), zeker voor grote evenementen, concerten en pretparken... of bij de verhandeling van waardebonnen met een unieke code. Het valt moeilijk te achterhalen of deze effectief (nog) geldig zijn. Vaak zijn deze ook op naam bij initiële aankoop of moeten deze voor een bepaalde datum extra gevalideerd worden.

## Betalingen

- Controleer of de betaling verloopt via een beveiligde site of een geëigende bankrekening. Let op met alternatieve betaalsystemen (anoniem) of betaalsystemen door middel van codetransfers (bv. Western Union, Moneygram, Ria, paysafecard, neosurf, Paypal,...). Betaal ook nooit meer dan de afgesproken prijs. Ook niet om gelden te deblokken, een account aan te maken of om zogenaamd onverwachte kosten te dekken.
- Een cheque ontvangen? Als je een cheque ontvangt van een koper, doe dan niets tot de bank heeft bevestigd dat het een echte (gedekte) cheque is. Dit neemt steeds enige tijd in beslag! Stort in afwachting zeker geen geld terug aan de koper. Ook niet wanneer schijnbaar een (veel) groter bedrag per cheque werd overgemaakt en de transactie wordt afgeblazen.
- Tel ook altijd de contante betaling na (wisseltruc).
- Let op met vertoonde betaalbewijzen op digitale dragers of print-screens. Controleer ook steeds de betaal - en/of valutadatum (niet in de toekomst) en of de overschrijving wel degelijk werd uitgevoerd (voldoende actief). Handel pas als het geld effectief op uw eigen rekening is toegekomen. Wees bijkomend alert tijdens de bankverlofdagen.
- Verifieer altijd de betaalgegevens, zeker bij grote en éénmalige betalingen. Vraag desgevallend om de factuur op verschillende manieren over te maken (controle). Kies bij terugkerende betalingen indien mogelijk voor een domiciliëring op uw rekening. Vul ook steeds alle gegevens (naam, adres, postcode, OGM,...) op het overschrijvingsformulier in. Dit maakt een bijkomende controle door uw bank mogelijk (overeenstemming).

## Verdachte berichten

- Krijgt u een e-mail dat u de loterij heeft gewonnen? U kunt niet winnen zonder deel te nemen...
- Krijgt u een e-mail van een kennis die uw hulp vraagt vanuit het buitenland? Contacteer die persoon telefonisch om te zien of hij/zij echt hulp nodig heeft en/of hij/zij zich wel daadwerkelijk in het buitenland bevindt en contacteer dan desgevallend eerst de diplomatieke kanalen. Schrijf niet zomaar geld over!
- Ontvangt u gratis waardebonnen? Check ook altijd even bij de winkelketen zelf.
- Let op met (buitenlandse) erfennissen, (buitenlandse) investeerders of grote staatsopdrachten (met ronkende titels), waarbij u eerst zelf geld dient over te maken. Een officiële regeling of mededeling zal nooit op die manier gebeuren.
- Let op voor illegale goksites.
- Stort bijdragen aan goede doelen die u kent. Vraag desgevallend een legitimatie (lidkaart).
- Hecht geen geloof aan buitensporige of snelle financiële rendementen (vaak op buitenlandse markten). Ook niet indien u de eerste keer wordt uitbetaald. Er zal immers steeds meer geld worden gevraagd of druk worden uitgeoefend, hoewel de investeringen totaal waardeloos zijn (zgn. boiler room fraude).

- Check ook altijd de URL en de extensie (adres), de spelwijze en de logo's. Vaak zal hieruit duidelijk worden dat de afzender vals is.

### **Emotioneel**

- Wees alert wanneer een kandidaat-partner om geld begint te vragen. Leent u geld of waardevolle goederen uit, zorg dan steeds voor een geschreven, gedateerde en door alle partijen ondertekende overeenkomst.
- Wees beducht wanneer u zich via de webcam of sociale media blootgeeft. Schakel de webcam ook steeds uit of plak deze af. Stuur u toch (naakt)foto's door voorzie deze dan van een watermerk of anonimiseer deze.
- Werk met een erkend relatiebureau of controleer de naam van de datingsite en de gegevens van uw kandidaat-partner op het internet.
- Wees beducht voor (buitenlandse) internetromances of valse profielen. Liefde maakt blind.
- Denk rationeel en toets even af bij vrienden/derden. Doe via het internet geen dingen die u in realiteit ook niet zou doen.

Meer tips vind je op [www.safeonweb.be](http://www.safeonweb.be)