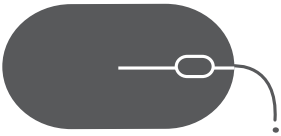
Politie
Schelde-Leie

tips & tricks tegen internetcriminaliteit

Laat je niet in de luren leggen

Uw veiligheid, daar gaan wij voor!

DE JUISTE KLIK



Het internet is meer dan een fantastische bron van informatie. We surfen om te communiceren, te spelen, muziek te beluisteren, te shoppen,... Maar - net als in 'het echte leven' - moet je oppassen met wie je omgaat en hoe je dat doet.

Word niet te persoonlijk

* Wees zuinig met persoonlijke informatie: zet nooit je wachtwoord, telefoon-, rekening- of rijksregisternummer op het internet. Cybercriminelen kunnen hiermee een nepaccount aanmaken.
* Alles wat je online zet, blijft online. Zet je privacysettings aan en deel foto's en informatie alleen met 'echte' vrienden en familie.
* Praat ook online niet met mensen die je niet kent. Soms doen mensen zich voor als iemand anders.
* Plaats geen vakantieplannen op sociale netwerksites. Inbrekers lezen misschien mee!.
* Hoe langer het wachtwoord, hoe veiliger. Gebruik een wachtzin: een lange zin is simpel te onthouden én veiliger. Je kan ook een beroep doen op programma's of 'wachtwoordkluizen' om het wachtwoord voor jou te maken én te onthouden. Deel je wachtwoord nooit met anderen.

Software up-to-date

* Houd je beveiligingssoftware up-to-date op al je apparaten.
* Update je internetbrowser en installeer goede antivirussoftware.
* **Beveilig ook je mobiele toestellen.** Ze bevatten veel persoonlijke gegevens, zoals e-mails, foto's, apps,... en zijn vaak gemakkelijk te kraken.

Beveiligde wifi

* Beveilig je wifi-netwerk thuis met een wachtwoord. Zo kan niemand gebruik maken van je draadloos internet.

Weg met wat je niet kent

* **Wees waakzaam voor links en bijlagen als je de afzender niet kent.** Ze kunnen schadelijke codes bevatten.
* Open nooit bijlagen met deze extensies: .pif, .com, .bat, .exe, .vbs, .lnk.
* Als je zelf bestanden als bijlage verstuurt, kies dan voor het meest 'inactieve' formaat, zoals een PDF.

Maak back-ups

* **Maak regelmatig een kopie van alle gegevens.** Met een back-up kan je immers verder werken en ben je geen unieke informatie kwijt.

HOAX

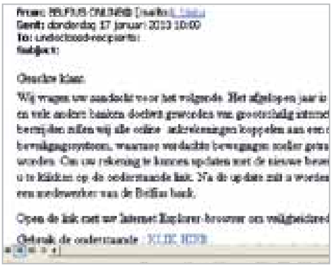
= een nepwaarschuwing. Je herkent deze aan de vraag om de e-mail naar al je contactpersonen door te sturen. Doe dit nooit! Het doel is om verwarring te stichten en mensen voor de gek te houden.

PHISHING

= via een e-mailbericht word je naar een valse website gelokt. Als je dan je gebruikersnaam en paswoord ingeeft, kan de fraudeur deze onderscheppen en gebruiken om transacties of aankopen uit te voeren.

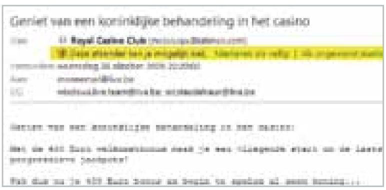
MALWARE

= schadelijke programma's zoals virussen, spyware en Trojaanse paarden. Deze leiden tot continue pop-ups, een virus op je harde schijf, mensen die aan je paswoorden kunnen en in het slechtste geval crasht je pc. Beveilig je computer en maak regelmatig een back-up.



SPAM

= ongewenste e-mails. Ze worden meestal door je e-mailfilter gevonden en in de map 'spam' geplaatst. Open deze mails niet en blokkeer ze met (veelal gratis) spamblockers.



Vóór de transactie:

* Controleer of het bedrijf achter de website duidelijk identificeerbaar is: een vast telefoonnummer, adres, BTW-nummer,...
* Ga na of het bedrijf geregistreerd is met een geldig ondernemingsnummer. Dit kan via de VIES-site van de Europese Commissie.
* Je kan de betrouwbaarheid van een website checken via Howard: the shoppingassistant.com. Hier kan je kan controleren waar en wanneer een website geregistreerd werd. Howard berekent ook een beoordelingsscore.
* Hou in het oog of alle transacties verlopen via beveiligde pagina's. **Veilige pagina's kun je herkennen aan het hangslotteken in de adresbalk van je browser en aan het webadres dat altijd begint met https.** De 's' staat voor secure.

Tijdens de transactie:

* Ga de serieuze bedoelingen van de verkoper na: stel vragen over hetgeen hij aanbiedt, zeker als het gaat om een veilingsite.
* Achterhaal wat je werkelijk betaalt en of alle onkosten zijn inbegrepen. Wees op je hoede als de prijs abnormaal laag is.
* Regel nooit je aankoop via een geldtransfersysteem zoals Western Union of Moneygram.
* Geef bij de aankoop enkel gegevens in die noodzakelijk zijn voor de bestelling. Geef nooit een rekeningnummer, wachtwoord of pincode door.
* Lees het verzend-, garantie- en retourbeleid. **Wist je dat je het recht hebt om binnen een periode van 7 werkdagen af te zien van de aankoop?**

Na de transactie:

* Bewaar alle gegevens over de aankoop, bv. door een screenshot af te drukken.
* Kijk achteraf de bankafschriften van je kredietkaart na.
* De verkoper is verantwoordelijk voor de verzending van je aankoop. Komt die niet aan, dan moet je in principe niet betalen. Ook als het beschadigd is, mag je het terugsturen en een nieuw exemplaar vragen.
* In geval van oplichting bij een aankoop die je hebt betaald met een kredietkaart, neem dan contact op met de uitgever van de betreffende kaart: meld het misbruik en vraag om de betaling ongedaan te maken.

WEBSHOPPEN? KIJK UIT JE DOPPEN!

Wist je dat een gestolen pc of smartphone kan opgespoord worden?

Dat kan als je tracking software of een app installeert. Van zodra het gestolen toestel weer op internet komt, stuurt het een signaal door naar een tracking station of e-mailadres. Hiermee kan de politie de standplaats van de pc of laptop achterhalen en de dader identificeren.

Wat te doen vooraf?

Noteer de gegevens van het toestel: serienummer, IMEI-nummer, merk, type en oproepnummer.

Installeer een app of tracking programma op het toestel. Afhankelijk van het toestel of merk zijn er verschillende mogelijkheden: ofwel hebben ze een eigen app, ofwel zijn er online betalende of gratis versies van tracking software beschikbaar.

Wat te doen bij diefstal?

Geef de gegevens van het toestel door aan de politiediensten. Laat weten dat er een app of tracking programma op geïnstalleerd is.

Slachtoffer van internetfraude?

Word je ondanks alle voorzorgen toch slachtoffer van internetcriminaliteit, dan kan je een aantal acties ondernemen. Eén en ander hangt af van de manier waarop en het nadeel dat je ondervond.

Doe aangifte bij de politie

Als slachtoffer kom je persoonlijk aangifte doen op het commissariaat. **Enkel dan kan de politie iets ondernemen.**

Wat kan je nog doen?

* Dien een klacht in bij het Europees Centrum van de Consument.
* Dien een klacht in bij de FOD Economie.
* Dien een klacht in op de consumentenlijn: 0800 120 33.
* Maak een melding op www.consumentenbedrog.be.
* Contacteer je bank of kredietkaartinstelling en probeer een terugbetaling te bekomen.

Waar naartoe?

eccbelgie.be

economie.fgov.be

consumentenbedrog.be

theshoppingassistant.com

VERSTRIKT IN HET WWWEB?

Hoe ga je als ouder met het internet binnen je gezin om? Hoe leer je je kinderen veilig internetten? Hoe breng je de risico's ter sprake?

Als ouder wil je je kinderen leren om zich tegen risico's op het web te wapenen. Begeleiden, praten, tonen,... net zoals je ze uitlegt hoe de straat veilig over te steken, kan je hen zo wegwijs maken op het web.

* Toon interesse: Wat doen ze op het internet? Wat denken ze over hun webervaringen? Bekijk eens samen hun profiel. Stimuleer hun kritische kijk.
* Maak afspraken en volg ze op: Hoeveel tijd aan de pc of tablet? Wanneer (bv. na huiswerk)? Waarvoor gebruik je de pc wel of niet? Welke info mag online en welke niet?
* **Maak bij discussies de link met het 'echte' leven.** Als je die vergelijking maakt, begrijpen kinderen vaak beter wat je bedoelt. Als je iets verbiedt, leg hen ook uit waarom.
* Vertel je kinderen dat eventuele controle of het gebruik van filters nodig is om hen te beschermen tegen ongepaste en ongewenste beelden of informatie. Bij jongeren ligt dit iets moeilijker en is communicatie en discussie belangrijk.
* Leer je kind om goede paswoorden aan te maken en deze regelmatig te wijzigen.
* **Leer hen basistechnieken aan om informatie te verzamelen over een persoon die hen lastigvalt:** hou conversaties bij, maak printscreens van foto's, bewaar mails of sms-berichten, meld het bij de sociale netwerksites (Report-button).
* Zet de pc op een zichtbare plaats.

Vragen? Tips & tricks? Een luisterend oor nodig?

click safe

www.clicksafe.be

Op deze site van ChildFocus vind je alle informatie over veilig en verantwoord internetten.

awel

bel 102 | awel.be

Awel luistert naar kinderen en jongeren met een vraag, verhaal of probleem.

Cyberpesten is het herhaald beledigen of vernederen via online media. Dit pesten kan verschillende vormen aannemen: een vals profiel, sturen van beledigende boodschappen of verspreiden van roddels.

Wat kan jij doen?

* Heb respect voor de ander in je taalgebruik en pest zelf ook niet.
* **Wat je in het echte leven niet doet, doe je ook niet op het net.**
* Informatie die je in het gewone leven voor jezelf houdt, geef je ook niet prijs op het web. Geef nooit paswoorden door, behalve aan je ouders.
* Wat je in het echte leven niet recht in iemands gezicht durft zeggen, tik je ook niet in.
* Zie je dat iemand gepest wordt op het internet, spreek erover met hem of haar en breng mensen in wie je vertrouwen hebt op de hoogte. Volg deze foto's, video's of beledigende boodschappen niet, ook al denk je 'Ach, het is maar om te lachen...'

Wat kan je doen als jij wordt gepest?

* Dan kan je er best met iemand over praten (vriend, ouder, leerkracht,...).
* Reageer niet op deze boodschappen. Neem geen wraak omwille van wat er over jou werd gezegd. Dit alles maakt de situatie vaak enkel erger. Negeren ontmoedigt pesters.
* **Ken en gebruik je rechten.** Zonder je toestemming afbeeldingen of videomateriaal van jou verspreiden is strafbaar in België. Aarzel niet om je rechten te laten gelden en stap samen met je ouders met bewijsmateriaal naar de politie.

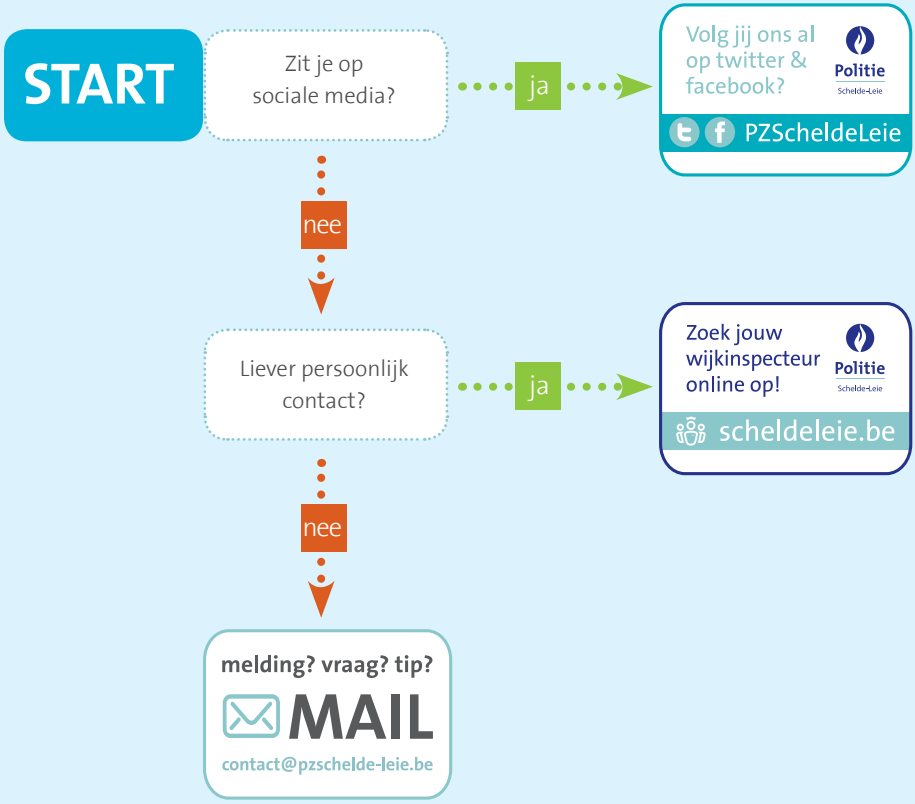
bel 106 | tele-onthaal.be

Bij Tele-Onthaal kan je over alles praten waar je mee zit, wat je kwijt wil,...

www.jac.be

Het JAC helpt jongeren tussen 12 en 25 aan een antwoord op vragen en problemen.

POLITIE SCHELDE-LEIE



POLITIEZONE SCHELDE-LEIE
De Pinte, Gavere, Nazareth, Sint-Martens-Latem

Florastraat 19, 9840 De Pinte
09 321 76 60
contact@pzschelde-leie.be
www.scheldeleie.be
www.twitter.com/PZScheldeLeie
www.facebook.com/PZScheldeLeie

Politie
Schelde-Leie