Laat je niet in de luren leggen!

Voor de meest recente preventietips surf naar
www.politiedeinzezultelievegem.be!

Politie

Deinze-Zulte-Lievegem

DE JUISTE KLIK!

Word niet te persoonlijk

- Wees zuinig met persoonlijke informatie: zet nooit je wachtwoord, telefoon-, rekening- en rijksregisternummer op het internet. Cybercriminelen kunnen hiermee een nepaccount aanmaken en doen alsof ze jou zijn.
- Beveilig je computer en mobiele toestellen en hou indringers buiten.
- Alles wat je online zet, blijft online. Zet je privacy settings aan en deel foto's en informatie alleen met vrienden en familie die je ook kent in de 'echte' wereld.
- Praat ook online niet met mensen die je niet kent. Soms doen mensen zich voor als iemand anders.
- Plaats geen vakantieplannen op sociale netwerksites. Potentiële inbrekers lezen misschien mee!
- Hoe langer en complexer 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!

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

1 Software up-to-date

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

2 Beveiligde wifi

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

3 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. Hierdoor verkleint het risico op informatielekken.

4 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.

PHISHING

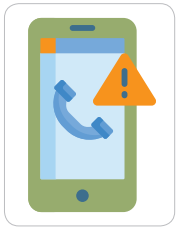
= Via een e-mailbericht word je naar **een valse website gelokt die sterk lijkt op de site van een bank of webshop.** Als je dan je gebruikersnaam en paswoord ingeeft, kan de fraudeur deze onderscheppen en gebruiken om transacties of aankopen uit te voeren.

SMISHING

= Een combinatie van de woorden sms en phishing is de poging van oplichters om **persoonlijke, financiële of veiligheidsinformatie via tekstbericht te verkrijgen.** Ze doen zich voor als betrouwbare bron, zoals een bank, kaartverstrekker, nutsbedrijf of dienstverlener.

VISHING

= een combinatie van de woorden 'voice' en 'phishing' is **een vorm van oplichting via de telefoon** waarbij de oplichters proberen om het slachtoffer te misleiden om persoonlijke, financiële of veiligheidsinformatie te geven of om geld aan hen over te maken (bijv. medewerkers Microsoft).



SPAM

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

VERDACHT BERICHT ONTVANGEN?

STUUR HET DOOR NAAR VERDACHT@SAFEONWEB.BE

Vóór de transactie:

- Controleer of het bedrijf achter de website duidelijk identificeerbaar is: een vast telefoonnummer, adres, BTW-nummer en de algemene voorwaarden.
- Ga na of het bedrijf geregistreerd is met een geldig ondernemingsnummer. Dit kan via de VIES-site van de Europese Commissie.
- Check of de website een kwaliteitslabel vermeldt en of de site ook daadwerkelijk aangesloten is bij dat betreffende label.
- Vermijd onbeveiligde of onbekende websites. 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 de goederen of diensten die hij aanbiedt, zeker als het gaat om een veilingsite.
- Achterhaal wat je werkelijk zal moeten betalen en of alle onkosten zijn inbegrepen. Wees ook 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 van de webshop. **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 bijvoorbeeld door een screenshot van de pagina te maken of deze 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 wanneer het product 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.

VEILIG WEBSHOPPEN? KIJK UIT JE DOPPEN!

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

Gestolen pc's, laptops, tablets en smartphones kunnen opgespoord worden, 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.

Smartphones & tablets

Diverse merken hebben een eigen app die je kan gebruiken om een gestolen of verloren toestel te lokaliseren.

Pc's & laptops

Online zijn er een aantal betalende en gratis versies van tracking software beschikbaar.

Wat te doen vooraf?

- Noteer vooraf 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.

Wat te doen bij diefstal?

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

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 aangifte doen op het commissariaat. **Enkel dan kan de politie iets ondernemen!** Dit kan door een afspraak te maken in één van onze commissariaten.

Wat kan je nog doen?

- Een klacht indienen bij het Europees Centrum van de Consument: www.eccbelgie.be.
- Een klacht indienen bij de FOD Economie: www.economie.fgov.be.
- Een klacht indienen op de consumentenlijn: 0800 120 33.
- Maak een melding op www.consumentenbedrog.be.
- Contacteer je bank en probeer een terugbetaling te bekomen.
- Bekijk de helpdesk van de website zelf.

eccbelgie.be
economie.fgov.be
consumentenbedrog.be
safeonweb.be

VERSTRIKT IN HETWWWEB?

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?

Kinderen & het internet

- 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?

Awel luistert naar kinderen en jongeren met een vraag, verhaal of probleem.
Bel **102** of surf naar **awel.be** !

Bij **Tele-Onthaal** kan je over alles praten waar je mee zit, wat je kwijt wil,...
Bel **106** of suf naar **tele-onthaal.be** !

Het **JAC** helpt jongeren tussen 12 en 25 aan een antwoord op vragen en problemen.
Surf naar **jac.be** !

Cyberpesten

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.

Op **childfocus.be** vinden kinderen en ouders informatie over verantwoord internetgebruik, cybercrime en seksualiteit op het internet.

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.

Stadionlaan 22/A, 9800 Deinze
09 244 24 00
PZ.DeinzeZulteLievegem@police.belgium.eu
www.politiedeinzezultelievegem.be
twitter.com/PolitiezoneDZL
facebook.com/PZDeinzeZulteLievegem

Politie
Deinze-Zulte-Lievegem