Laat je niet in de luren leggen!

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

Politie

Deinze-Zulte-Lievegem

DE JUISTE KLIK!

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.

Word niet te persoonlijk

- Zet nooit je wachtwoord, telefoon-, rekening- en rijksregisternummer op het internet. Cybercriminelen kunnen hiermee een nepaccount aanmaken en doen alsof ze jou zijn.
- 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 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. Cijfers, hoofdletters en symbolen maken je wachtwoord moeilijker te kraken. Het belangrijkste is echter **tweestapsverificatie** (2FA) in te schakelen voor een extra bescherming. Je kan ook een beroep doen op programma's of 'wachtwoordkluizen' om het wacht-woord voor jou te maken én te onthouden. Deel je wachtwoord nooit!

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.

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.

5 Let op voor SPAM

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.

PHISHING

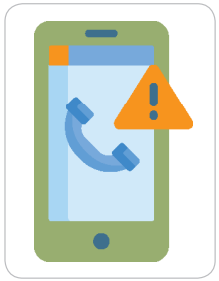
= Via een e-mailbericht word je naar **een valse website gelokt die sterk lijkt op de site van een bank of webshop.** Als je dan je gebruikersnaam en paswoord ingeeft, kan de fraudeur deze onderscheppen en gebruiken om transacties of aankopen uit te voeren.

BELEGGINGSFRAUDE

= Beleggingsfraude of 'Boiler room' fraude is een vorm van oplichting waarbij fraudeurs je **fictieve of waardeloze aandelen of financiële producten** aanbieden.

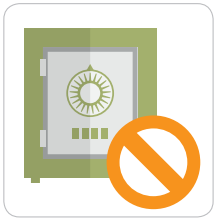
HULPVRAAGFRAUDE

= Fraudeurs **doen zich** via e-mail, sms of appberichten **voor** als **één van jouw dierbaren.** Of omgekeerd: ze schrijven je dierbaren aan in jouw naam. Ze vragen om dringende **financiële hulp.** De berichten komen zeer geloofwaardig en echt over. Als slachtoffer wil je natuurlijk je familielid of vriend 'helpen' en heb je de neiging om het geld onmiddellijk te storten.



KLUISREKENINGFRAUDE

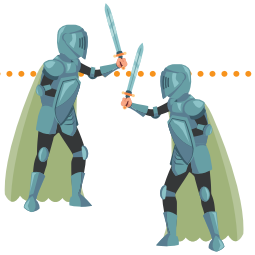
= Oplichters benaderen je meestal in twee stappen: ze sturen je eerst een phishingbericht om je **persoonlijke bankcodes** te ontfutselen. Zo proberen ze toegang te krijgen tot je rekening. Daarna bellen ze je op. Ze **doen zich dan voor als een medewerker van je bank** en vragen je om geld over te schrijven naar een zogezegd nieuwe, veilige rekening.



VERDACHT BERICHT ONTVANGEN?

STUUR HET DOOR NAAR VERDACHT@SAFEONWEB.BE

JEZELF WAPENEN TEGEN FRAUDE!



Fraudeurs maken gebruik van verschillende technieken om je in de val te doen lopen. Als je de signalen kan herkennen ben je al een hele stap verder. Met onderstaande **5 T's** voorkom je al heel wat onheil. Maak je je zorgen over de toenemende dreiging van cybercriminaliteit en phishing? Blijf dan op de hoogte via de gratis **Safeonweb app**.

TE MOOI

- De charmes van knappe mannen en vrouwen, de buitenkans van je leven, een uitzonderlijk lage prijs,...
- Onrealistische voorstellen zoals een spaarrekening met 8% opbrengst.
- Als het te mooi is om waar te zijn, dan is het dat ook.

TWIJFEL

- Niemand is vrij van online fraude. Maar je kan wel de alarmsignalen herkennen.
- Begin te twijfelen als de werkwijze vreemt aanvoelt bijv. buiten de website om.
- Taalfouten, een vreemd mailadres, ...
- Doe de phishing- en/of de beveiligingstest op safeonweb.be

TIJDSDRUK

- Er wordt een acute situatie gesimuleerd bijv. je kaart wordt NU geblokkeerd, ik heb dringend geld nodig,...
- Fraudeurs spelen in op angst om onmiddellijk te handelen bijv. dit aanbod is slechts tijdelijk geldig!

TRAINING

- Leer jezelf goede gewoontes aan.
- Wees zuinig met je mailadres.
- Volg geen link maar tik zelf de website in van de bank of instelling.
- Check bij de instantie of het bericht klopt.
- Informeer je, neem je tijd en zorg voor de juiste beveiliging.

TIPS

- Geef nooit je codes om te internetbankieren via e-mail, sociale media, sms of telefoon.
- Ga nooit via een link naar een betaalsite of mobiele app van je bank.
- Typ altijd zelf het adres van de betrokken website in je browser of open de mobiele app.

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.

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.

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 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.

TO DO: DE 6DE T! 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.

Bel onmiddellijk CARD STOP

Heb je een financieel nadeel geleden? Bel dan onmiddellijk CARD STOP op het nummer **078 170 170**! Dit kan **24u/24**. Verwittig ook je bank en vraag je kaartnummers op.

Fraudecel van je bank inlichten

Vermoeden van fraude of misbruik van je bankapplicatie? Raadpleeg onmiddellijk de **website van je bank**.

Ook in geval van **verlies of diefstal van je mobiel toestel** (smartphone, tablet, smart watch, andere wearables) is het aangeraden om je betaalapplicaties **preventief** te laten **blokkeren**.

Volg zorgvuldig de stappen die je bank aangeeft en dien een klacht in bij de politie als je bank je hierom vraagt.

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.

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, veiligonline.be** en **pegi.info** 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.

KLACHT OF AANGIFTE?

Dringend? BEL 101

MAAK EEN

AFSPRAAK

www.politiedeinzezultelievegem.be

of bel **09 244 24 00** !

Stadionlaan 22/A, 9800 Deinze
PZ.DeinzeZulteLievegem@police.belgium.eu
www.politiedeinzezultelievegem.be
x.com/PolitiezoneDZL
facebook.com/PZDeinzeZulteLievegem
instagram.com/politiedeinzezultelievegem

Politie

Deinze-Zulte-Lievegem