

Samen voor Jongeren

A M S T E R D A M



Combiwel, DOCK, Dynamo, perMens, Swazoom en The Mall
werken Samen voor Jongeren in Amsterdam



Themakaart
Veilig internetten



Online weerbaarheid & Veilig internetten

Online veiligheid is niet het eerste onderwerp waar jongeren op aanslaan. Vaak denken ze beter te weten dan de meeste volwassenen hoe ze zich online moeten beveiligen. Totdat er iets misgaat.

Als iemand gehackt of online opgelicht wordt, wordt online veiligheid al snel een belangrijk thema. En dat gebeurt steeds vaker, ook bij jongeren. Online criminaliteit en fraude nemen toe. Het is daarom belangrijk dat jongeren weten hoe ze zichzelf kunnen beveiligen. Jongerenwerkers en straathoekwerkers kunnen hierin een voorbeeld zijn en ondersteunen.

Jongeren vaker slachtoffer van online criminaliteit

In 2021 is één op de vijf 15- tot 25-jarigen slachtoffer geweest van online criminaliteit. Ter vergelijking: van de 65-plussers, die online vaak als kwetsbare groep worden gezien, is dat minder dan één op de acht. Jongeren hebben vooral vaker met online bedreiging en intimidatie te maken dan ouderen. Maar jongeren zijn ook vaker het slachtoffer van hackers. Van aankoopfraude en fraude in het betalingsverkeer werden 25- tot 65-jarigen juist het vaakst slachtoffer. Phishing treft 65-plussers het vaakst.

Bron CBS



Waarom online weerbaarheid?

Het kenmerk van internet en sociale media is dat de gebruikers zelf content maken en onderling communiceren. Er is over het algemeen geen moderatie. En ook al hebben platformen wel gebruikersvoorwaarden die grenzen aangeven van wat toelaatbaar is, er vindt weinig toezicht en handhaving plaats. Je bent voor bescherming en veiligheid dus vooral op jezelf aangewezen.

Er zijn online veel situaties denkbaar die om weerbaarheid vragen, omdat ze risico op schade met zich meebrengen. Ze zijn alleen niet altijd makkelijk te herkennen als onveilig, gevaarlijk, ongezond of onwenselijk. De verschijningsvorm wijkt vaak af van wat we kennen en verandert bovendien voortdurend. Situaties voelen daardoor vaak niet als risicovol, waardoor gebruikers minder alert en voorzichtig zijn.

Jongeren die online weerbaar zijn, komen minder snel in een onveilige situatie terecht. En áls dat gebeurt, herkennen zij dit sneller en weten ze beter wat ze moeten doen om te voorkomen dat het (verder) uit de hand loopt. Dat klinkt makkelijker dan het is. Online veiligheid is immers niet alleen het afschermen van je wachtwoord of weten dat je niet zomaar op een linkje in een mail moet klikken. Het gaat ook over groepsdruk, je grenzen kennen en weten welke afzender betrouwbaar is en welke niet. Het gaat zegge maar om het ontwikkelen van een alarmbelletje dat afgaat als iets online niet in orde is.

Online weerbaarheid verschilt niet van 'gewoon' weerbaar zijn. Je eigen grenzen kennen, aangeven en bewaken als die onder druk komen te staan, bijvoorbeeld wanneer de ander die niet respecteert. Daarvoor is het nodig dat je onveilige situaties kunt herkennen, weet wat je kunt doen om jezelf te beschermen en daarnaar durft te handelen.

Wat kunnen jongeren leren?

Om veilig online te kunnen zijn is het belangrijk om je grenzen te weten, zowel van jezelf als van anderen. Je kunt gewoon aangeven wat je (niet) wilt, ook aan familie en vrienden. Je hoeft geen wachtwoord met iemand te delen (doe dat sowieso niet). Je hoeft niet toe te staan dat iemand foto's van je maakt. Je hoeft het niet oké te vinden dat iemand je foto/informatie zonder jouw toestemming plaatst, doorstuurt of bewerkt.

Hanteer basisregels voor je veiligheid

- Deel geen persoonlijke gegevens met mensen die je niet in real life kent.
- Geef geen informatie aan onbekenden of vage kennissen (bijvoorbeeld over wanneer je van huis bent).
- Als je online iemand ontmoet die je aardig vindt, zorg dan dat je zeker weet dat diegene echt is wie hij/zij zegt te zijn, voordat je persoonlijke informatie deelt. Persoonlijke informatie betreft gegevens over jezelf of over je naasten, gevoelens en/of intieme beelden.
- Geef geen informatie aan onbekenden of vage kennissen (bijvoorbeeld over wanneer je van huis bent).
- Denk na over wat het gevolg kan zijn van wat je online wilt plaatsen en hoe anderen kunnen reageren.
- Wees ook voorzichtig met gegevens van een ander. Geef bijvoorbeeld nooit iemands nummer of andere gegevens aan een ander zonder toestemming te vragen.
- Klik nooit zomaar op linkjes die je opgestuurd krijgt: soms is dat een middel om je te hacken. Op www.checkjelinkje.nl kun je de betrouwbaarheid checken.
- Alle instellingen van alle apps staan automatisch op openbaar. Als je een app installeert, 'installeer' dan ook je instellingen: bepaal wie wat van jou mag zien.
- Let op de locatie-instellingen in apps, zo kunnen mensen met een Snapchat-abonnement anderen volgen via de SnapMap. Niet bepaald privé. Scherm jezelf af in zulke apps en met de locatie instellingen van je mobiel.
- Check na een update van je telefoon je instellingen. Soms worden ze gereset.
- Deel nooit wachtwoorden met iemand, ook niet met je allerbeste vriend.
- Klik nooit op linkjes die je krijgt van mensen die je niet kent.
- Wees extra alert op linkjes van de bank, post et cetera Dat is vaak phishing.
- Als iemand je chanteert of onder druk zet om gebruik van je persoonsgegevens te maken, dan is diegene op dat moment strafbaar. Als je je gegevens deelt en die ander maakt er misbruik van, ben jij te traceren en strafbaar voor de acties die de ander via jou onderneemt.

Geldezels

Jongeren kunnen te maken krijgen met het misbruiken van hun bankgegevens door intimidatie of misleiding. Slachtoffers hiervan worden geldezels genoemd. Jongeren worden benaderd om hun bankgegevens, pincode en rekeningnummer te delen in ruil voor een financiële beloning. Ook kunnen ze worden gedwongen onder dreiging van geweld of chantage. Daders gebruiken de rekening om er frauduleus verkregen geld op te laten storten en over te laten maken naar (buitenlandse) rekeningen. Op dat moment is de geldezel strafbaar. Er staat immers gestolen/illegaal geld op zijn/haar rekening.

- Pas op voor 'nieuwe beste vrienden', die je onder druk zetten
- Pas op voor mensen met een zielig verhaal die je pas willen gebruiken
- Pas op voor mensen die je rekening willen gebruiken.
- Pas op voor mensen die je een cadeau willen geven zoals een telefoon/Playstation in ruil voor je pincode/rekening



Let op!

Als er gezegd wordt dat ze iets over je bekend maken, tenzij je hen je pincode of bankrekening laat gebruiken, word je gechanteerd. Op dat moment is die ander strafbaar. Vanaf het moment dat jij meewerkt aan het doorsluizen van geld, ben jij ook strafbaar én (in tegenstelling tot diegene die je heeft gechanteerd) makkelijk te vinden en te vervolgen

De pakkans voor de geldezel is 100% en de gevolgen zijn enorm. De jongere draait op voor alle schade en wordt bovendien strafrechtelijk vervolgd. Met als gevolg een forse schuld en een strafblad. Ook komen deze jongeren acht jaar lang op een zwarte lijst bij banken te staan. Ze kunnen dan geen bankrekening openen om salaris op te ontvangen en betalingen te doen. Ook kunnen zij geen lening krijgen. Dat alles heeft uiteraard flinke consequenties voor het opbouwen van een zelfstandig bestaan.



Tips!

Kijk dit filmpje over geldezels (2021): youtu.be/629OWlqnq2c

Kijk dit filmpje over WhatsApp fraude: youtu.be/H0xEw1cBUY0

Wat kun je als jongerenwerker of straathoekwerker doen?

▶▶ Besteed aandacht aan online veiligheid

Neem online veiligheid serieus en praat er met jongeren over. Wijs ze op de risico's en wat ze kunnen doen om zichzelf te beschermen. Veel jongeren hebben het idee dat ze niets te verbergen hebben en dus veilig zijn. Maar online heeft iedereen wel iets te beschermen: je privacy, je persoonsgegevens, je imago etc.

Tip!


In de toolkit bij de e-learning vind je kant-en-klare online content waarmee je via sociale media jongeren informatie kunt aanreiken.

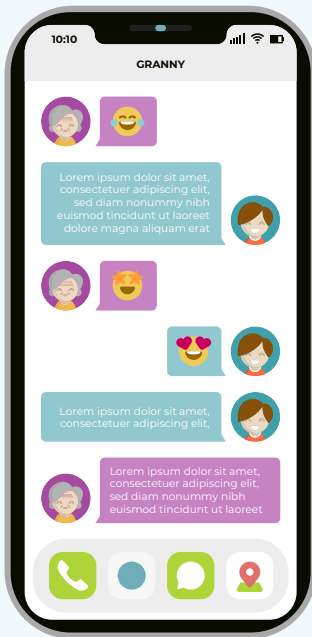
▶▶ Geef het goede voorbeeld

Jongeren zien jou als een rolmodel. Hoe heb je zelf je eigen veiligheid en privacy geborgd? Wat doe jij persoonlijk om veilig te internetten? En de organisatie? Hoe goed is bijvoorbeeld de Wifi in de buurthuizen beveiligd? Is het een openbaar netwerk? Zorg daarom ook dat je je veiligheidsinstellingen op orde hebt.

Als je met jongeren via WhatsApp communiceert, kijk dan samen eens naar het instellen van tweestapsverificatie. WhatsApp kan namelijk heel makkelijk gehackt worden als je dat niet doet en misbruikt worden. Ook zonder dat je het merkt.

1. Ga naar instellingen
2. Kies account
3. Kies verificatie in twee stappen
4. Kies pincode in toetsen

 *p.s.: Beveilig ook je voicemail met een eigen code, anders doen hackers dat en kom je er lastig zelf bij*



En als je dan toch bezig bent, kijk dan ook eens naar de instelling waarmee anderen je niet zomaar aan groepen kunnen toevoegen, maar het eerst moeten vragen. Hiermee voorkom je dat je in onbekende groepen terecht komt en dat onbekenden jouw nummer hebben.

1. Ga naar instellingen
2. Kies account
3. Kies privacy
4. Kies groepen
5. Selecteer 'contacten' ipv iedereen

- Deel deze instellingen met jongeren en vertel waarom je hiervoor kiest. Adviseer ook veiligheidsinstellingen voor andere chatkanalen.

▶▶ **Maak met de jongeren afspraken over online veiligheid**

Bespreek veelvoorkomende situaties en ga met jongeren in gesprek om tot afspraken te komen. Denk aan:

- Privacy: Wat deel je wel en niet van jezelf en over elkaar? Wat verwacht je van anderen als het om het respecteren van jouw privacy gaat? Hoe doe je dat zelf met die van anderen?
- Beeldmateriaal: Wat wel en wat niet delen? Vraag je toestemming aan anderen en hoe? Wat als je iets gedeeld hebt waar anderen opstaan en ze vragen je dat te verwijderen?



▶▶ **Wees je bewust van eventueel ouderschap onder de jongeren met wie je werkt. In de groep waarmee je werkt kunnen zich zowel slachtoffers als daders bevinden.**

▶▶ Weet wat de gevolgen zijn voor jongeren

De gevolgen van online criminaliteit voor slachtoffers kunnen groot zijn. Het kan dan gaan om emotionele of psychische problemen, of om financiële problemen. Dat geldt voor online bedreiging en intimidatie, maar ook voor online oplichting, fraude, hacken en andere online delicten. Al deze situaties kunnen slachtoffers emotionele schade bezorgen, maar ook financiële problemen.



Tip! www.joinhackshield.nl

HackShield is een gratis game die kinderen tussen de 8 en 12 jaar oud weerbaar maakt tegen cybercriminaliteit. Kinderen worden opgeleid tot Cyber Agents die zichzelf en hun omgeving kunnen beschermen tegen online gevaar. Ze leren er van alles over onderwerpen als sterke wachtwoorden, hacken, phishing, geldezels, online pesten.

Met wie kun je samenwerken?

● **Wijkagent/politie:**

www.vraaghetdepolitie.nl/privacy/gegevensmisbruik/wat-zijn-de-10-belangrijkste-tips-voor-veilig-internet-van-de-politie.html

● **Bureau Halt:**

www.halt.nl/index.php/halt-op-school



Waar vind je meer informatie?

- Overheid: Maak het ze niet te makkelijk:
www.maakhetzeniettemakkelijk.nl/online-veiligheid
- CBS, Online criminaliteit
www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021/5-online-criminaliteit
- Consumentenbond: Veilig internetten: waar let je op?
www.consumentenbond.nl/veilig-internetten
- NPO kennis: Hoe blijf je veilig op internet?
npokennis.nl/longread/7719/hoe-blijf-je-veilig-op-internet
- VPN Gids, veilig online in 9 simpele stappen
www.vpngids.nl/veilig-internet/surfen/veilig-online-in-8-stappen

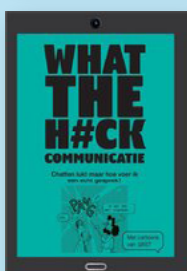
Boeken

- Gratis boek over geldezels, oplichting, misbruik, Veilig Internetten.nl
www.geldlessen.nl/bibliotheek/lesmateriaal/manual/Lesmateriaal-Lessonup/handleiding-lessonup-geldezels.pdf



Boek en luisterboek:

Daniel Verlaan, Ik weet je wachtwoord:
ikweetjewachtwoord.nl



Maria Genova:

- Snel geleerd, slim gedaan
- Komt een vrouw bij de h@cker
- What the h@ck!

mariagenova.nl/boeken/





Colofon

Themakaarten Online weerbaarheid

©Samen voor jongeren Amsterdam

www.samenvoorjongerenamsterdam.nl
mei 2023

Teksten: Martine Borgdorff, Solange Jacobsen, Jacqueline Kleijer

Eindredactie: Martine Borgdorff

Coördinatie: Solange Jacobsen

Vormgeving: Somethingllse

Beeldmateriaal: Freepik, Envato elements

Met dank aan: Oussama Aakouk, Desta Deekman, Erol Esef, Laya Leysner, Carlos Lowijs, Fatiha Majdoub, Marleen Oostenbrink, Clemens Streng, Valérie Wallenburg

De themakaarten Online Weerbaarheid maken deel uit van het project Online Weerbaarheid van Samen voor jongeren Amsterdam. Dit project richt zich op het ontwikkelen en verspreiden van kennis en vaardigheden voor jongeren- en straathoekwerkers, zodat zij voor en met kwetsbare kinderen en jongeren kunnen werken aan het vergroten van online weerbaarheid. Samen voor jongeren Amsterdam is een stedelijke samenwerking van Combiwel, DOCK, Dynamo Amsterdam, perMens, the Mall de Baarsjes en Venzo&Swazoom Welzijn.

Niets uit deze uitgave mag worden verveelvoudigd, door middel van druk, fotokopieën, geautomatiseerde gegevensbestanden of op welke andere wijze ook zonder voorafgaande schriftelijke toestemming van de uitgever.

**Samen voor
Jongeren**
A M S T E R D A M



*Combiwel, DOCK, Dynamo, perMens, Swazoom en The Mall
werken Samen voor Jongeren in Amsterdam*