Slim
Alert
Sterk
Aardig
Moedig

De Internet Helden.

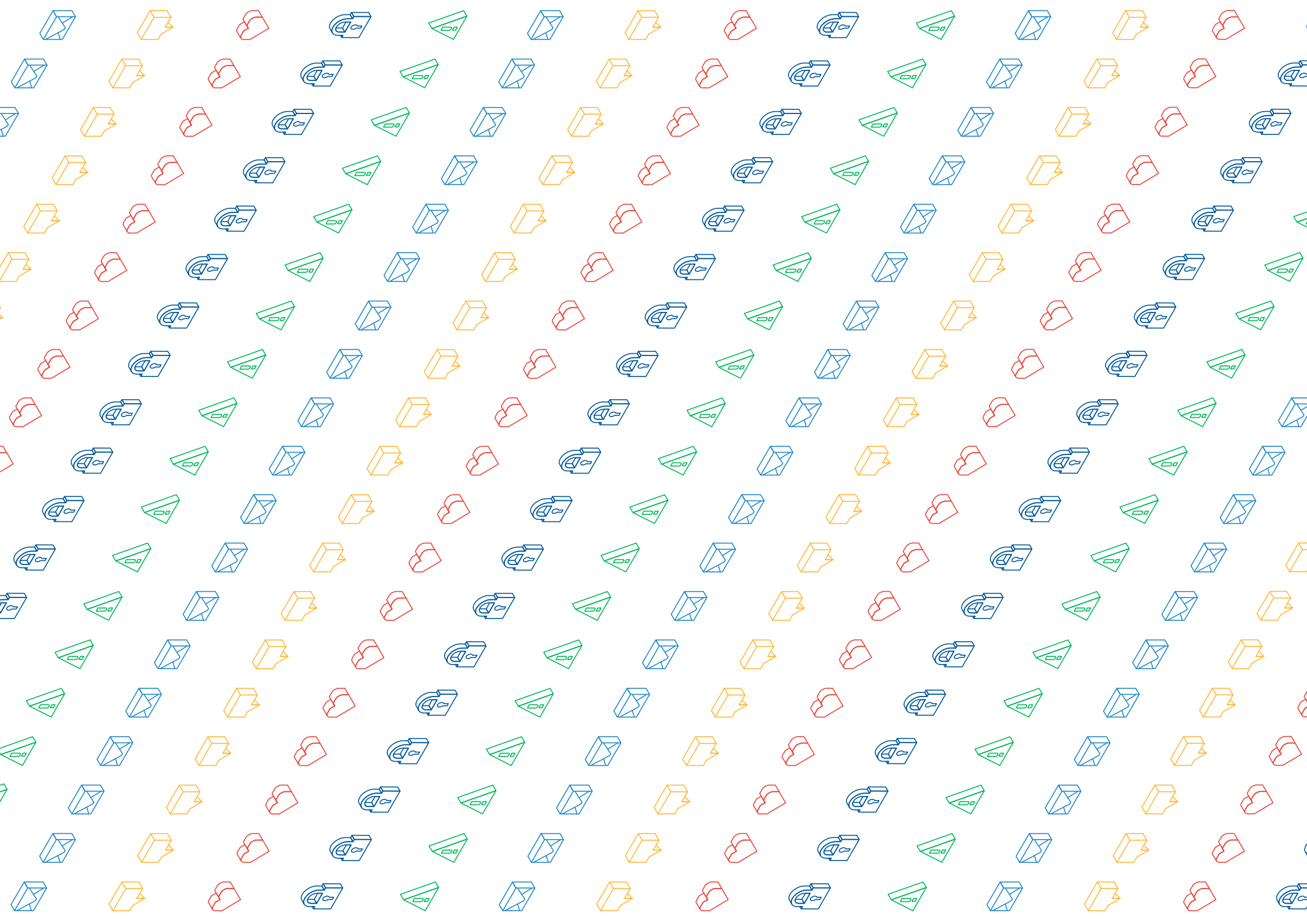
Een samenwerking van:

Bureau Jeugd & Media

SIC Nederland

Google

Toolkit voor ouders over online veiligheid en digitaal burgerschap



Inhoudsopgave

De InternetHelden is een programma voor online veiligheid en digitaal burgerschap, bedoeld voor jongeren. De inhoud is samengesteld door Bureau Jeugd & Media, Safer Internet Centre Nederland en Google, en wordt onderschreven door EOKM, Helpwanted.nl, Ouders & Onderwijs en Veiliginternetten.nl.

Deze toolkit voor ouders is bedoeld om uw kinderen veilig online te laten gaan, en ze positieve ervaringen te laten opdoen. Hij bevat een familiegids met leuke activiteiten voor het hele gezin en een EHBO-kit voor online ongelukken.

Familiegids

Dit zijn de vijf uitgangspunten (en tevens de thema's voor uw gezinsactiviteiten):

Eerst denken, dan delen
Leer wat je beter wel en niet online kunt delen.

Controleer of het waar is
Leer waarop je moet letten om echt van nep te onderscheiden, en om fraude en bedrog te leren herkennen.

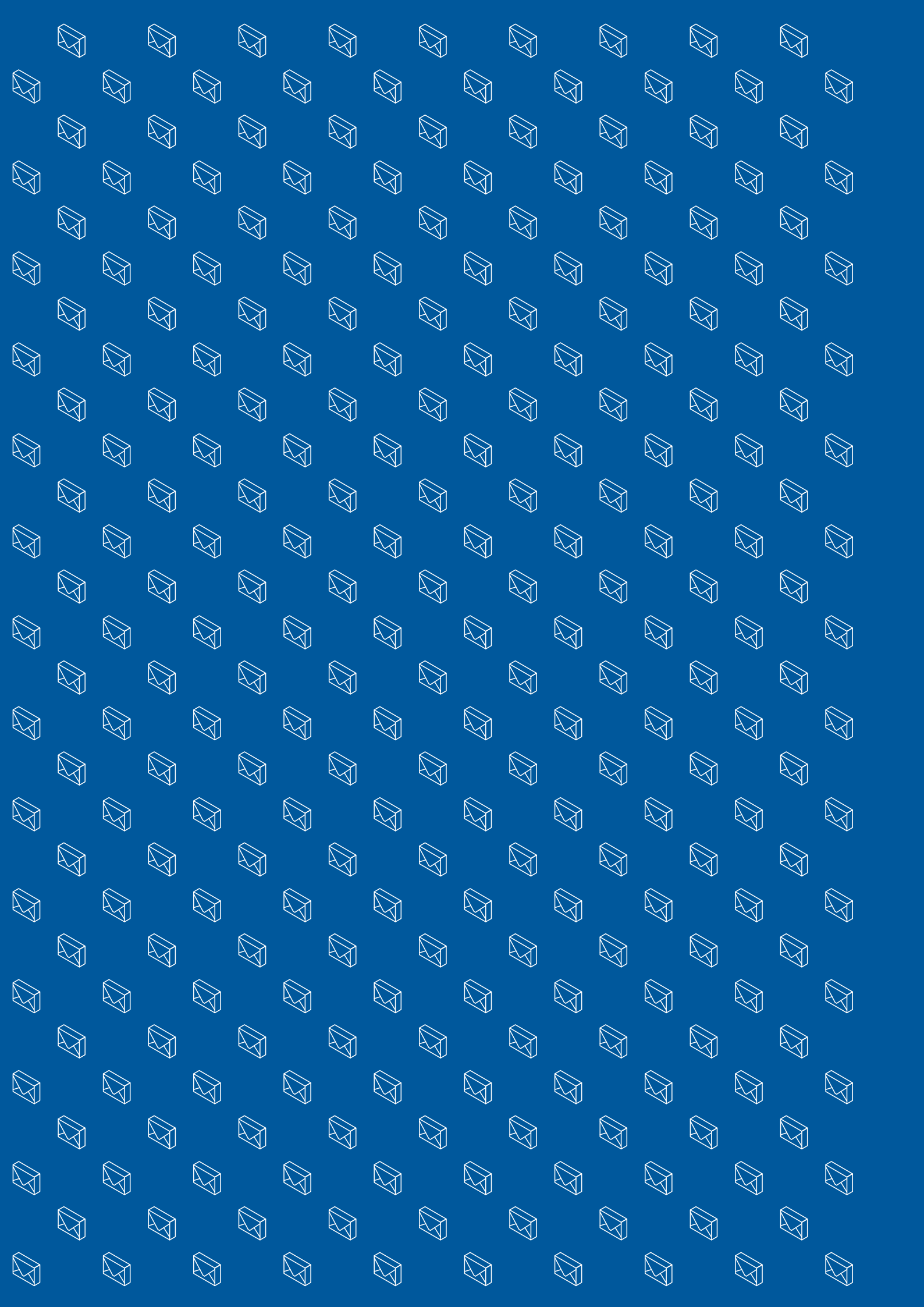
Bewaak wat van jezelf is
Leer hoe je je gegevens kunt beschermen, onder andere met slim wachtwoordgebruik.

Wie goed doet, goed ontmoet
Leer dat het loont om aardig te zijn; dan zijn anderen ook aardig tegen jou. Het respecteren van andermans privacy hoort daarbij.

Bij twijfel: praat erover
Weet dat je niet alleen bent en dat je altijd hulp kunt vragen, bijvoorbeeld bij je ouders, de mentor op school, een oudere broer of zus, of hulpdiensten zoals de Kindertelefoon of Meldknop.nl.
Let op: bij dit laatste uitgangspunt hoort geen aparte gezinsactiviteit. Maak het uw kinderen voortdurend duidelijk, en vertel ze over de ***hulpdiensten*** *waar ze terechtkunnen (zie p. 33).*

Even spieken – Bij elke opdracht staan 'oplossingen' die het startpunt voor een gesprek kunnen vormen. En als u een woord of begrip niet kent: aan het eind staat een verklarende woordenlijst.

Samen aan de slag – De onderstaande gezinsactiviteiten, en uw eigen betrokkenheid daarbij, helpen uw kinderen om de nodige vaardigheden op te doen en veiliger online te gaan. Uit onderzoek is gebleken dat kinderen en jongeren zich minder risicovol gaan gedragen naarmate er thuis meer gepraat wordt over wat er allemaal kan gebeuren.



Eerst denken, dan delen

Jongeren vinden het leuk om dingen online te zetten, variërend van kattenfilmpjes tot foto's van zichzelf of anderen. Maar vaak realiseren ze zich niet goed dat alles wat je online zet, eindeloos zichtbaar kan blijven, met alle gevolgen van dien. En ook niet dat je sommige dingen beter voor jezelf kunt houden.

Eerst denken, dan delen

De onderstaande activiteit helpt jullie om na te denken over de dingen die je online deelt met anderen.

Activiteit

Oké, niet oké of hangt ervan af

Lees elke situatie hardop voor. Vraag elk gezinslid om een oordeel te geven:

- **oké** (delen is prima)
- **niet oké** (nooit doen)
- **hangt ervan af** (soms wel, soms niet)

Vraag steeds om uit te leggen waarom dat oordeel wordt gegeven.

1. Het posten van een foto op social media van je beste vriend of vriendin die een rare bek trekt.
2. Het posten van een video waarin een nare grap met iemand wordt uitgehaald. Zelf moet je er wel om lachen, maar eigenlijk is het best gemeen wat daar gebeurt.
3. Een onbekende vraagt bij het online gamen om je telefoonnummer en je adres.
4. Een klasgenoot die op je slaapfeestje zal komen, vraagt online om je adres, omdat hij (of zij) dat niet weet of vergeten is.
5. Je hebt per ongeluk nét iets te veel informatie over jezelf gegeven aan iemand die je niet kent, en nu maak je je daar zorgen over. Bespreek je dat probleem met iemand anders?
6. Het posten van een grappig kattenfilmpje (van je eigen kat) in een besloten groep.
7. Het posten van een foto van jezelf, met jouw school op de achtergrond, waarbij de naam van de school in grote letters op de gevel zichtbaar is.
8. Het posten van je adres (woonplaats, straat en huisnummer) in een groep met mensen die je nog nooit eerder in het echt hebt gezien.

Eerst denken, dan delen

Even spieken

1. Rare foto van een vriend of vriendin posten
Jongeren realiseren zich vaak niet dat wat ze zélf heel grappig vinden, hun vriendjes of vriendinnetjes wel eens heel vervelend zouden kunnen vinden. Die staan dan voor gek. Leer uw kinderen dat ze altijd eerst om toestemming moeten vragen voor ze een foto van iemand anders posten.

2. 'Grappige' video posten (die anderen niet zo grappig vinden)
Hetzelfde als hiervoor: wat jij grappig vindt, vinden anderen misschien helemaal niet grappig, of zelfs kwetsend. Zeker wanneer het om kinderen gaat die jonger zijn dan jezelf, of kinderen met een probleem of een handicap. Stimuleer uw kinderen om zich altijd in te leven in anderen. Hoe zouden die het vinden? Je kunt het ook omdraaien: hoe zou jíj het vinden als je belachelijk wordt gemaakt? Hoe voelt dat?

3. Een onbekende gamer die om je gegevens vraagt
Bedenk dat je de chatfunctie in online games ook gewoon kunt uitschakelen. Dan heb je nergens meer last van. Controleer of uw kinderen dat weten. Als je het uitschakelen van de chatfunctie te ver vindt gaan, omdat je nog wilt blijven communiceren met anderen, kun je specifieke personen blokkeren. Of bij de beheerder van de game melden dat je vervelende berichten hebt gekregen.

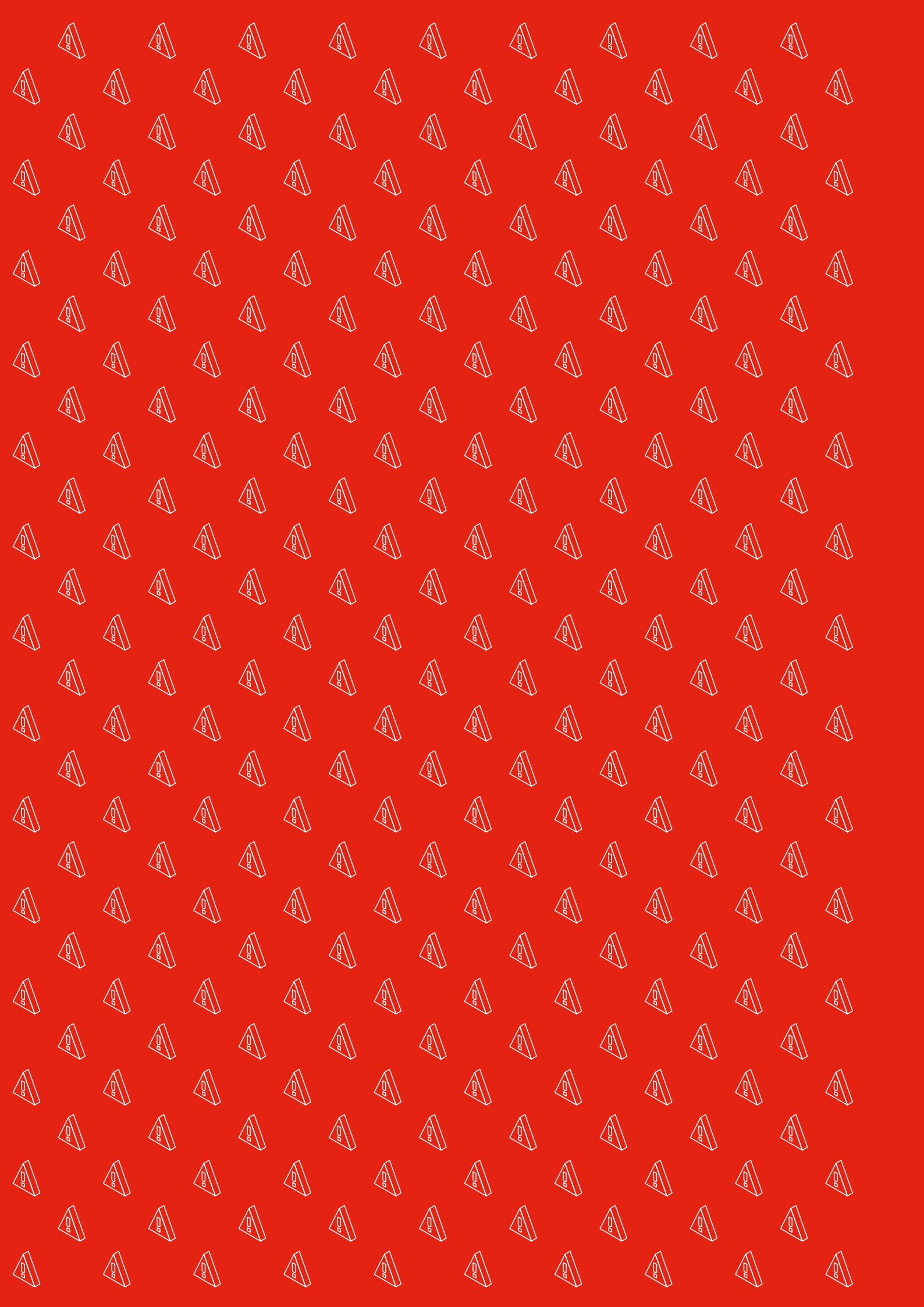
4. Een bekende die om je adres vraagt voor een slaapfeestje
Vrienden en bekenden mogen natuurlijk best je adres weten, maar je moet altijd voorzichtig blijven met het online (via internet) verzenden van je persoonlijke gegevens. Zet je adres in ieder geval niet in een whatsappgroep omdat anderen die gegevens dan ook kunnen zien. Deel persoonlijke gegevens, zoals adresgegevens en wachtwoorden, liever via een privébericht of door te bellen. Nog beter: dat je ouders even bellen met de ouders van degene die komt slapen.

5. Per ongeluk te veel informatie weggegeven. Bespreken met iemand anders?
Per ongeluk te veel informatie van jezelf weggeven is natuurlijk niet oké, maar erover praten met iemand anders wel. Vertel uw kind dat het altijd goed is om naar u (of een ander vertrouwd persoon) te stappen wanneer er dingen mis zijn gegaan. Hoe eerder hoe beter, dus niet te lang blijven tobben. Samen kun je dan actie ondernemen, zoals blocken, wissen of rapporteren.

6. Het posten van een grappig kattenfilmpje (van je eigen kat) in een besloten groep
Praat met uw kinderen over dingen die leuk zijn om te delen zonder dat iemand daar last van heeft. Laat ze zelf een paar van dat soort dingen verzinnen en bespreek hun voorbeelden. Het idee achter deze opdracht is dat het belangrijk (en effectief) is om niet alleen de risico's en gevaren te benoemen, maar vooral ook de leuke en positieve dingen.

7. Het posten van een foto van jezelf, die toont op welke school je zit
Als zo'n foto gepost wordt in een besloten groep, bijvoorbeeld in een groepsapp van je klas, is het natuurlijk geen probleem. Maar doe het liever niet als er ook onbekenden kunnen meekijken. Laat uw kinderen zelf bedenken waarom dat gevaarlijk kan zijn. (Hint: dit is hetzelfde probleem als je woonadres online zetten. Mensen met slechte bedoelingen kunnen je zo persoonlijk benaderen. Of doen alsof ze je kennen en dan nog meer informatie lospeuteren.)

8. Het posten van je adres in een groep met mensen die je nog nooit gezien hebt
Soms wil je wel eens thuis afspreken met een paar gamers die je kent via de chat, of met een paar anderen die je kent van een fansite. Dat kan heel leuk zijn, om elkaar in het echt te ontmoeten. Of het kan tegenvallen, maar niet geschoten is altijd mis. Het is echter onverstandig om je woonadres open en bloot online te zetten (zie ook situatie 4 en 7). Wissel adressen liever uit per mail of per telefoon en laat je ouders eerst contact opnemen met de ouders van die andere kinderen.



Controleer of het waar is

Niet alles wat je online tegenkomt, is waar of betrouwbaar. Maar hoe zie je het verschil tussen nep en betrouwbaar? Dat is nog niet zo makkelijk. Toch zijn er wel dingen waarop je kunt letten.

Controleer of het waar is

Deze activiteit helpt uw kinderen om na te denken over waar en onwaar.

Activiteit

Zoek, controleer, en beoordeel

Zoeken

1. Ga bij elkaar zitten met een tablet, laptop of telefoon, open een browser, en start jullie favoriete zoekmachine.
2. Controleer of 'Veilig zoeken' aan staat. Dat is het filter op de zoekresultaten, zodat die geschikt zijn voor jonge kinderen. Beslist aan te raden voor kinderen tot 12 jaar.
3. Kies een onderwerp dat uw kinderen interessant (of leuk of spannend) vinden, of waar ze al veel van weten, zoals hun favoriete sport of sportclub, hun favoriete muziek of artiest, het dorp of de stad waar jullie wonen, etc. Tik dit onderwerp in het zoekveld in.
4. Klik op een aantal resultaten, zowel bovenaan als een paar pagina's verder.
5. Kijk bij het onderdeel 'Controleren' hieronder, om te zien of jullie al wat aanwijzingen hebben voor de kwaliteit van de zoekresultaten. Echt of nep? Waar of onwaar? Betrouwbaar of onbetrouwbaar?

Controleren

• Is deze website van een organisatie die algemeen bekend en vertrouwd is? Zoals de Rijksoverheid (rijksoverheid.nl), de Kindertelefoon (kindertelefoon.nl) of een landelijk dagblad (zoals De Telegraaf, de Volkskrant, het Algemeen Dagblad of Trouw)?
- **Zo ja,** dan kun je de informatie van deze site redelijk vertrouwen. Kijk wel even of er 'https' in de adresbalk staat, met een slotje, en klik zo nodig even op het slotje om het certificaat te controleren.
- **Zo nee,** ga verder met je onderzoek.

• Heeft deze website een 'About'-/'Over ons'-pagina, een colofon of contactgegevens?
- **Zo ja,** puntje erbij voor de betrouwbaarheid. Maar het geeft nog geen 100% garantie. Ga verder met je onderzoek.
- **Zo nee,** dan is deze website twijfelachtig.

• Staat erbij wie de tekst geschreven heeft (de naam van de auteur)?
- **Zo ja,** puntje erbij voor de betrouwbaarheid. Maar het geeft nog geen 100% garantie. Ga verder met je onderzoek.
- **Zo nee,** twijfelachtig.

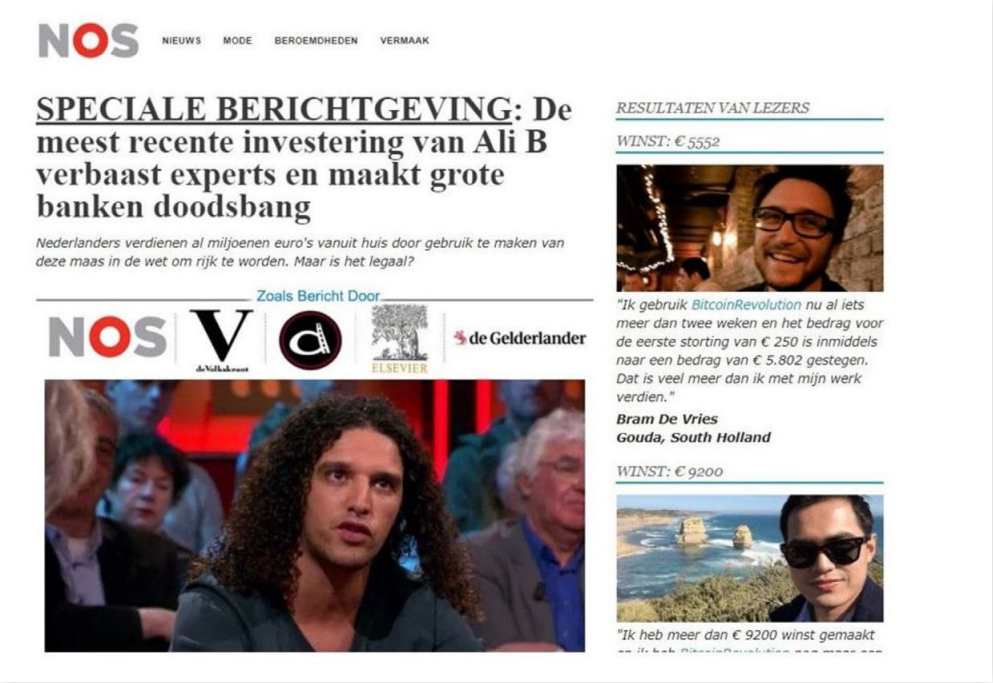
• Staat er de naam van een bekende Nederlander (BN'er) bij?
- Dat klinkt betrouwbaar, maar dat hoeft het niet per se te zijn. De BN'er kan betaald zijn om iets aan te prijzen (denk ook aan influencers), waardoor het dus meer reclame is dan betrouwbare informatie. Of de naam van de BN'er is er gewoon bij verzonnen, zoals bijvoorbeeld in de Bitcoinreclame uit Afbeelding 1.

• Is de site afkomstig van een bedrijf of wordt de site gesponsord? Dat is soms moeilijk te controleren, maar probeer het wel. Je kunt controleren via SIDN door wie de .nl-domeinnaam is geregistreerd en dan zelf nagaan of dat een PR- of reclamebureau is.
- **Zo ja,** dan zal de informatie niet echt neutraal zijn, en vaak alleen maar positief.
- Als je het niet weet, geef dan een 1 (onbetrouwbaar) of een 2 (weet ik nog niet).

Controleer of het waar is

• Is het een fansite?
  - **Zo ja,** dan zal de informatie alleen maar positief zijn, en maar één kant van het onderwerp belichten.

• Is het informatie van een persoon of organisatie die iets wil aanprijzen of juist wil bestrijden?
  - **Zo ja,** dan is die informatie meestal eenzijdig.



Afbeelding 1 (bron: 1media.online)

Beoordelen

Geef elk zoekresultaat een oplopende score van 1 (onbetrouwbaar) tot 3 (redelijk betrouwbaar).

1 = onbetrouwbaar

2 = weet ik nog niet (misschien nog even controleren met mijn ouders erbij)

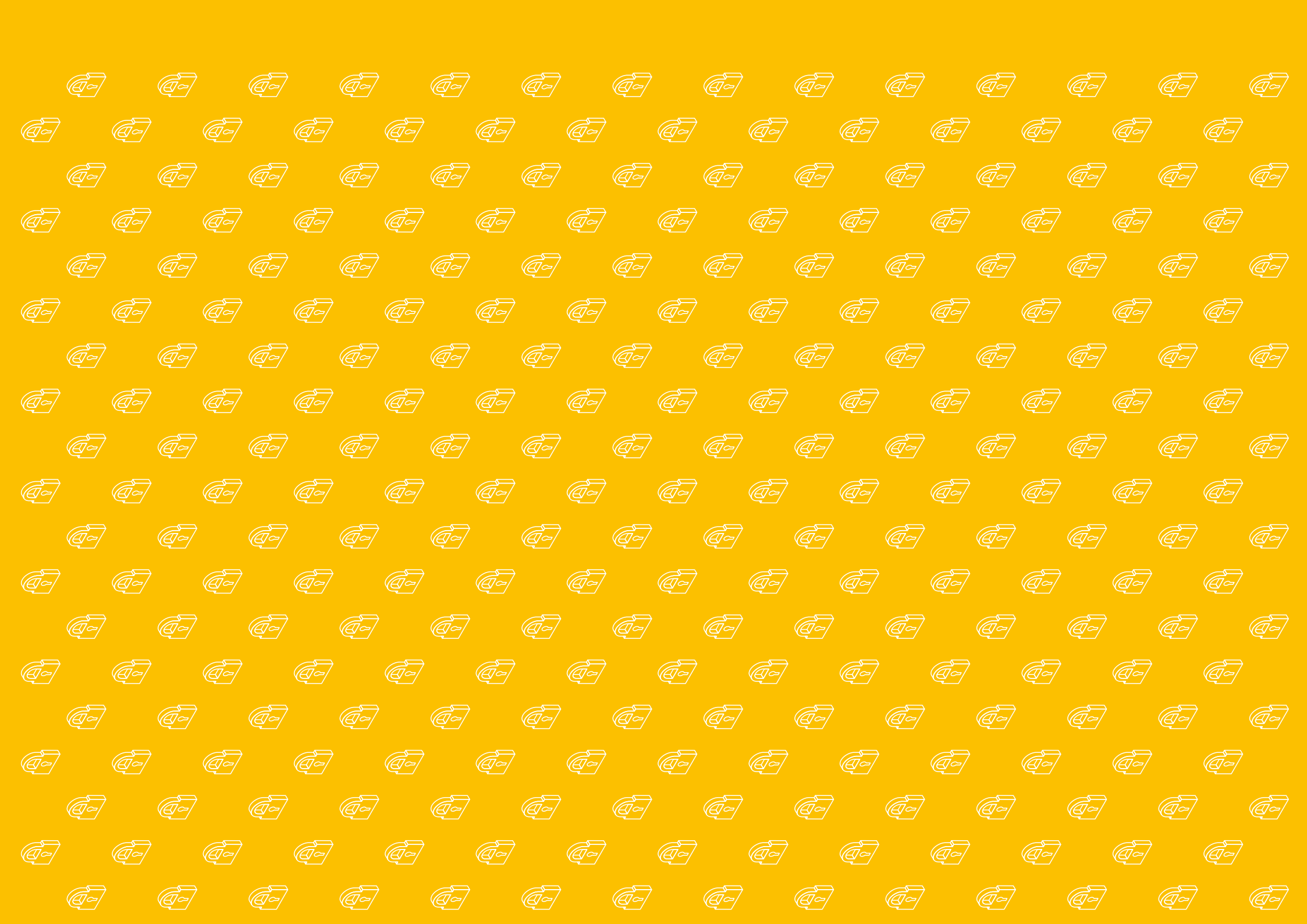
3 = redelijk betrouwbaar

Controleer of het waar is

Even spieken

- Bekijk de zoekresultaten en bespreek ze aan de hand van ‘Controleren’ hierboven. Wat hebben jullie ontdekt?
- Stimuleer uw kinderen om ze te laten vertellen over de websites, weblogs, forums, etc. die ze tegenkwamen. Hoe beoordelen ze de waarde daarvan? Welke waren het betrouwbaarst?
- Kunnen ze de signalen van goede en slechte informatie herkennen? Letten ze bijvoorbeeld op ‘https’ en het slotje in de adresbalk?
- Praat met uw kinderen over het belang dat mensen kunnen hebben bij het publiceren van informatie. Waaróm doen ze dat? Om geld te verdienen? Of om aandacht te krijgen? Of om een andere reden?

Notities



Bewaak wat van jezelf is

Wij, als volwassenen, weten wel dat je bepaalde dingen beter voor jezelf kunt houden. Maar kinderen hebben daar vaak nog moeite mee. Die vinden het bijvoorbeeld geen enkel probleem om hun wachtwoorden te delen met klasgenoten. (Nooit doen.) Maar hoe maak je eigenlijk een goed wachtwoord? En hoe ga je er het beste mee om?

Controleer of het waar is

Deze activiteit helpt uw kinderen om zichzelf beter te beschermen.

Activiteit

Zo word je een wachtwoord-expert

Doe met z'n allen de wachtwoordkraaktest op Veiliginternetten.nl.

Even spieken

Tips voor wachtwoordgebruik[1]

Tips voor een sterk wachtwoord

- Gebruik nooit **123456**. Dat is het meest gebruikte wachtwoord, en dus gemakkelijk te raden.
- Bedenk een wachtwoord zonder voor de hand liggende woorden (zoals je eigen naam of de naam van je school).
- Maak een wachtwoord van minstens 12 tekens. Hoe langer, hoe beter.
- Gebruik het liefst een wachtwoordzin. Dat kan een gezegde zijn, een zin uit een liedje, of een andere zin die je goed kunt onthouden en die lastig te raden of te kraken is. Bijvoorbeeld: **Liever Enzo Knol dan Dylan Haegens!** Of: **Wil ik een kat of 10 honden?**
- Kun je je wachtwoordzin niet invoeren, omdat het account geen lange wachtwoorden toestaat, dan kun je de eerste letters van elk woord gebruiken. Bij de zin hierboven over huisdieren wordt het dan: **Wieko10h?**
- Je kunt ook de eerste twéé letters van elk woord uit je zin gebruiken. Dan wordt het: **Wiikeekaof10ho?**

Zwak en dus snel gehackt

- **Nienke2008** – Je naam plus je geboortejaar. Kies nooit een wachtwoord met persoonlijke informatie.
- **123456** – De eerste cijfers op je toetsenbord.
- **qwerty** – De eerste letters op je toetsenbord.
- **welkom01** – Suggestie overgenomen van de dienst waar je een account aanmaakt.
- **voetbal123** – Of een ander bestaand woord met een paar cijfers erachter.
- **GeertGroote** – De naam van je school.

Om te onthouden

- Deel je wachtwoorden met niemand! (Behalve misschien met je ouders.)
- Je kunt een wachtwoord af en toe veranderen, maar het gevaar bestaat dat je wachtwoord daardoor minder sterk wordt. Bijvoorbeeld als je maar één teken verandert; vooral als je volgnummers gebruikt. Het allerbelangrijkst is dat je altijd een sterk wachtwoord kiest.
- Gebruik voor elk account een ander wachtwoord. Want als criminelen één wachtwoord van jou in handen krijgen (bijvoorbeeld via een datalek), dan kunnen ze ook toegang krijgen tot andere accounts.
- Verander je wachtwoord bij vreemde gebeurtenissen. Bijvoorbeeld als je van anderen hoort dat ze rare berichtjes uit jouw naam krijgen.
- Verander je wachtwoord ook als een dienst waar je zelf een account hebt (of had), een datalek heeft gehad. Zulke gebeurtenissen komen waarschijnlijk wel in het nieuws.
- Bij Have I Been Pwned? (haveibeenpwned.com) kun je controleren of je e-mailadres (dat vaak als inlognaam gebruikt wordt) in een gelekte database voorkomt.
- Vind je het lastig om je wachtwoorden te onthouden, gebruik dan een wachtwoordmanager.
- Bij sommige accounts kun je kiezen voor extra veiligheid met tweestapsverificatie.

[1] Veiliginternetten.nl. Wachtwoordtips.

Notities

Wie goed doet, goed ontmoet

Kinderen beseffen vaak niet dat sommige van hun berichten anders begrepen kunnen worden dan ze bedoeld waren. Wat bijvoorbeeld grappig bedoeld was, kan soms opgevat worden als pesten. Dat wil je natuurlijk niet laten gebeuren.

Wie goed doet, goed ontmoet

Deze activiteit leert uw kinderen het nut van (online) aardig zijn en aardig doen.

Activiteit

Wat zou jij doen?

Lees de onderstaande situaties hardop voor en vraag telkens aan elk gezinslid wat hij of zij zou doen in zo'n geval.

1. Een vriend(in) voelt zich rot omdat iemand hem/haar vervelende berichtjes stuurt.

2. Je ziet dat er vervelende of pesterige reacties geplaatst worden onder de foto's die je vriend(in) gepost heeft.

3. Je speelt een online game en ziet (of hoort) dat iemand steeds flauwe grappen maakt en dingen zegt waar jij niet goed van wordt.

4. Een vriend(in) stuurt je een zogenaamd grappige video van een klasgenoot die gepest wordt op het schoolplein. Jij vindt dat helemaal niet grappig en je vindt het eigenlijk heel naar om te zien.

5. Een vriend(in) is net naar de kapper geweest en jij post een bericht waarin je zegt dat diegene er nu wel 'heel anders' uitziet. Je bedoelde er niets vervelends mee, maar je vriend(in) blijkt er behoorlijk van geschrokken te zijn.

Wie goed doet, goed ontmoet

Even spieken

Er is nooit één goed antwoord. Iedereen kan z'n eigen ideeën over de beschreven situaties hebben en dat is prima. Wel is het belangrijk om gezamenlijk te praten over elkaars oplossingen en reacties. Misschien is de ene toch net iets beter dan de andere.

Om te onthouden:

- Als je niet goed weet wat je moet doen, bespreek het dan met anderen, bijvoorbeeld met je ouders, de mentor op school, een oudere broer of zus, de Kindertelefoon of Meldknop.nl.
- Het is altijd goed om op te komen voor jezelf en voor anderen. Meld het wanneer je iets vervelends ziet. Maar bedenk wel dat klikken of iemand verraden (snitchen) ervoor kan zorgen dat je de hele klas of een hele vriendengroep tegen je krijgt. Dan moet je afwegen wat het zwaarste weegt. Bij twijfel: bespreek het met je ouders, je mentor of de Kindertelefoon.
- Houd er rekening mee dat dingen anders opgevat kunnen worden dan je ze bedoeld had. Zeker online kan dat gemakkelijk gebeuren omdat je de ander niet ziet. Als iemand gekwetst blijkt te zijn, praat het zo snel mogelijk uit!

Belangrijke begrippen

Eerst denken, dan delen

Digitale voetafdruk (digital footprint): alles wat er online over jou te vinden is, zoals profielgegevens, foto's, video- en audio-opnamen, blogs, likes en postings (topicstarters en reacties).

Persoonlijke informatie: dingen die je voor jezelf (privé) wilt houden en 'persoonsgegevens' (zie hieronder).

Persoonsgegevens: alle gegevens waarmee je direct of indirect kunt bepalen wie iemand is. Bijvoorbeeld: je naam, adres, telefoonnummer, e-mailadres of BSN (tevens het leerlingnummer op school). Zelfs je IP-adres (van je smartphone of computer) kan persoonsgebonden zijn. Extra gevoelige persoonsgegevens heten 'bijzondere persoonsgegevens'. Zoals: je geloof (religie), je land van herkomst, je seksuele geaardheid en je medische gegevens. Denk altijd goed na voor je dit soort informatie – gewone persoonsgegevens en vooral bijzondere persoonsgegevens – online deelt.

Privacy-instellingen: de plek (o.a. op socialmediaplatforms, maar ook op websites en in apps) waar je kunt bepalen wat je met wie wilt delen.

Controleer of het waar is

Malware: een samentrekking van *malicious software* oftewel kwaadaardige software, bijvoorbeeld een virus.

Phishing: iemand verleiden om zijn of haar persoonsgegevens (zoals naam, adres, telefoonnummer, wachtwoorden, bankgegevens, etc.) te delen. Meestal door middel van een e-mail of via een nagebootste website (van bijvoorbeeld een bank).

Scam: een aanbieding die te mooi is om waar te zijn. Bijvoorbeeld: aanbiedingen om veel geld te verdienen met weinig werk. Een 'scammer' is dus een oplichter.

Spearphishing: een speciale vorm van phishing waarbij iemand jou persoonlijk aanspreekt en dingen van je lijkt te weten, zoals de namen van je ouders, de naam van je hond of de namen van je broers en zusjes, wat een betrouwbare indruk maakt.

Versleutelen: gegevens – zoals teksten, berichten, of je harde schijf – onleesbaar of ontoegankelijk maken door ze te coderen. Vervolgens kun je ze weer óntsleutelen (ontcijferen, decoderen) om ze weer leesbaar of toegankelijk te maken. Soms vinden versleuteling en ontsleuteling automatisch plaats, zonder dat je er wat van merkt, zoals bij websites die met 'https' werken (zichtbaar aan het slotje in je browser). In andere gevallen, zoals bij het beveiligen van een Word-document, moet je zelf een sleutel (wachtwoord) invoeren.

Bewaak wat van jezelf is

Hacken: de controle overnemen, bijvoorbeeld de controle over een computer of een account. Dus als jij je eigen socialmedia-account niet meer in kunt omdat het overgenomen is door iemand anders, ben je gehackt.
Let op: meestal wordt bij hacken gedacht aan technisch hacken (zoals het kraken van wachtwoorden), maar de laatste tijd wordt sociaal hacken steeds belangrijker. Daarbij zoekt de hacker niet naar de zwakke plekken van systemen (hardware of software), maar naar de zwakke plekken van mensen. Bijvoorbeeld om ze hun wachtwoorden te ontfutselen door er gewoon – met een smoes – naar te vragen.

Hacker: iemand die hackt. Er bestaan zowel goedaardige hackers die de beveiliging van computersystemen testen (ook wel ethisch hackers of 'white hat'-hackers genoemd) als kwaadaardige hackers die daadwerkelijk inbreken in systemen (malafide of 'black hat'-hackers).

Privacy: zélf bepalen welke gegevens je met wie (en in welke context) wilt delen. Kinderen en jongeren zijn extra kwetsbaar omdat ze hun hele verdere leven achtervolgd kunnen worden door uitgelekte of ten onrechte gedeelde gegevens.

Scammer: oplichter.

Security: beveiliging. Je treft beveiligingsmaatregelen om je privégegevens te beschermen, net zoals je je huis op slot doet om je spullen te beschermen tegen diefstal.

Tweestapsverificatie (of 'tweetrapsverificatie'): een beveiligingsproces waarbij inloggen twee stappen vereist. Eerst 'gewoon' inloggen met je gebruikersnaam en wachtwoord en daarna nog een extra code invoeren die je ontvangt per sms of via een speciale app, of een fysieke beveiligingssleutel in de USB-poort steken. Voor meer informatie, zie de pagina *Wat is tweestapsverificatie?* op Veiliginternetten.nl.

Wie goed doet, goed ontmoet

Blocken (ook: 'blokkeren'): zorgen dat iemand geen contact meer met jou kan maken, zodat die persoon geen toegang meer heeft tot je profiel, jou geen berichten meer kan sturen en je postings niet meer kan bekijken. Soms kun je dit zelf regelen (in je socialmedia-account) en soms moet je een moderator of admin (van een forum of andere online dienst) vragen om het te doen. Onwelkome e-mails kun je niet blokkeren, maar wel met (zelf gedefinieerde) filters naar je spambox verwijzen.

Intimideren (harassing): iemand bang maken met dreigende taal of onaangenaam gedrag.

Omstanders: degenen die betrokken zijn (of toekijken) bij pesten. Ze weten wat er gebeurt, maar ze doen er niets aan.

Snitchen (straattaal): klikken, verraden.

EHBO-kit voor ouders

EHBO-kit voor ouders

Vuistregels

Regel 1: word nooit boos

Word nooit boos, maar geef uw kind gelegenheid om zijn of haar verhaal te doen. Luister aandachtig en stel zo nodig vragen ter verduidelijking. Wél boos worden heeft het risico dat uw kind in het vervolg (als er misschien iets nóg ernstigers is gebeurd) niet meer naar u toe zal komen. Dan ben je nog veel verder van huis.

Let op: boosheid tonen is *nooit* verstandig. Niet wanneer uw kind zelf iets fout heeft gedaan, maar ook niet wanneer iemand anders uw kind iets heeft aangedaan. In het laatste geval is het heel begrijpelijk dat u boos wordt. Misschien denkt u zelfs dat u uw kind steunt door uw boosheid te tonen. Maar in noodsituaties hebben kinderen vooral behoefte aan veiligheid en rust. Iets als 'rechtvaardigheid' is dan veel minder belangrijk. Zie ook regel 2.

Regel 2: houd het hoofd koel en raak niet in paniek

Uw kind is misschien erg geschrokken en overstuur geraakt. Ga daar niet in mee. Hoe rustiger u als ouder blijft, hoe beter u het kind helpt. Uw kind wil namelijk vooral zijn gevoel van veiligheid weer terugkrijgen. Dat gaat het best met een rustige ouder die alles onder controle lijkt te hebben.

Daarnaast moet u natuurlijk uw hoofd erbij houden om verstandige acties te kunnen ondernemen, zoals screenshots maken van de dingen die fout zijn gegaan.

Regel 3: denk goed na over 'aangifte doen'

Soms bent u zó boos, dat u aangifte zou willen doen bij de politie. Dat is heel begrijpelijk, maar houd wel rekening met de praktijk:

- Verzamel zo veel mogelijk gegevens op papier, vooral ook screenshots. Met alleen een verhaal komt u niet veel verder.
- Als u aangifte doet, moet u alle details vermelden. Dat kan soms heel pijnlijk zijn.
- Soms is een *melding* ('aangifte light') handiger dan een echte *aangifte*. Bespreek dit met de baliemedewerker van het politiebureau.
- Soms wordt er niets gedaan met de aangifte of wordt er besloten niet tot vervolging over te gaan. Dan is het mogelijk om middels een 'Artikel 12 Sv'-procedure een formele klacht in te dienen.

Wat te doen als er online dingen mis zijn gegaan?

Mijn kind is slachtoffer geworden van shame-sexting

Als 'gewone' sextingbeelden (waar beide partijen zich goed bij voelden) zonder toestemming van de maker verder doorgestuurd worden, bijvoorbeeld als een relatie uit is geraakt, spreek je van 'shame-sexting'.

Nooit doen:

- Zeggen dat het de eigen schuld is van je kind ("Had je maar geen naaktbeelden van jezelf moeten versturen"). Ten eerste past sexting bij de seksuele ontwikkeling, en ten tweede zou het een vorm van blaming the victim zijn, oftewel het slachtoffer de schuld geven. Degene die de beelden ongevraagd heeft doorgezonden, dát is degene die fout zit.

Let op: het verzenden van seksueel getinte beelden van kinderen onder de 18 (dus ook van jezelf als je nog geen 18 bent) is officieel wel strafbaar, omdat dat onder kinderporno valt. Het Openbaar Ministerie (OM) hanteert echter de richtlijn dat sexting niet in alle gevallen vervolgd hoeft te worden. Simpel samengevat: als er geen probleem is, is er geen probleem.

Wel doen:

- Zit de dader op dezelfde school als uw eigen kind? Meld het dan aan school, en zorg dat deze het stappenplan van Soa Aids Nederland en Bureau Jeugd & Media volgt.
- Zit de dader op een andere school (of op een onbekende plek), neem dan contact op met Helpwanted.nl voor nader advies.

Mijn kind is dader van shame-sexting

Het kan natuurlijk gebeuren dat uw éigen kind seksueel getinte foto's en filmpjes heeft doorgestuurd naar anderen. Wat dan?

- Praat erover met uw kind (over grenzen, seks en mediagebruik) en leg uit dat dit echt niet kan.
- Zorg dat uw kind excuses maakt tegenover degene van wie hij of zij het vertrouwen geschonden heeft.
- Zorg dat uw kind deze beelden van zijn of haar eigen telefoon, laptop, etc. verwijdert, en dat hij of zij zich inspant om dat ook te laten doen bij degenen waar die beelden mogelijk terecht zijn gekomen.
- Bespreek het probleem indien nodig met school.
- Neem indien nodig contact op met Helpwanted.nl voor nader advies.

Mijn kind is slachtoffer van online pesten

- Ga eerst goed na of er écht sprake is van pesten. Vaak gaat het om 'grapjes' die helemaal niet vervelend bedoeld waren. Of om neutrale berichten die alleen maar verkeerd gevallen zijn. Online kunnen er snel misverstanden ontstaan. Bespreek dit uitvoerig met uw kind en kijk goed wat er nu werkelijk aan de hand is.
- Als het om een verkeerd begrepen bericht gaat, stimuleer uw kind dan om dit te zeggen tegen de 'pester' en om het onderling uit te praten.
- Als het echt om pesten gaat, dan moet daar natuurlijk wat aan gedaan worden. Zit de dader op dezelfde school als uw eigen kind? Meld het dan aan school en zorg dat deze actie onderneemt.
- Zit de dader op een andere school (of op een onbekende plek), neem dan contact op met Pestweb.nl (van Stichting School & Veiligheid) voor nader overleg.

Mijn kind is dader van online pesten

Het kan natuurlijk gebeuren dat uw éigen kind online gaat pesten. Wat dan?

- Praat met uw kind over zijn of haar gedrag.
- Stel vragen om hem of haar aan het denken te zetten: waarom deed je het? Wat was het probleem? Wat loste het op om te gaan pesten? Hoe zou het voelen als jou dit overkwam? En hoe ga je het stoppen?
- Zorg dat uw kind zijn excuses maakt aan degene die hij of zij aan het pesten was.
- Bespreek het probleem indien nodig met school.
- Neem indien nodig contact op met Pestweb.nl voor nader overleg.

Mijn kind is slachtoffer van oplichting

Er zijn talloze manieren waarop iemand het slachtoffer van (online) oplichting kan worden. Bij een vermoeden van oplichting of fraude kunt u contact opnemen met Fraudehelpdesk.nl.

Mijn kind heeft in-app-aankopen gedaan

Het kan zijn dat uw kind zonder uw toestemming te veel geld heeft uitgegeven aan in-app-aankopen (bijvoorbeeld om extra levens of credits voor een game te kopen). U kunt dan proberen het geld terug te vragen bij de ontvanger, en contact opnemen met Consuwijzer.nl.

EHBO-kit voor ouders

Waar kun je terecht bij narigheid op social media?

Facebook

- Voor het melden van nepaccounts, gehackte accounts, misbruik, pesterij, en aanstootgevende berichten, zie de pagina *Foto's of video's die je privacy schenden*.

Instagram

- Spam en ongepaste postings kunnen gemeld worden via het icoon met de drie puntjes (rechts van de auteursnaam bij elk bericht), gevolgd door 'Rapporteren'.
- Gehackte accounts kunnen gemeld worden bij Instagram, inclusief een verzoek om het account op te heffen. Dat kan via de pagina *Schending van onze communityrichtlijnen rapporteren* op het Helpcentrum.

MovieStarPlanet (MSP)

- Als je account gehackt is, zie de pagina *Wat kan ik doen als iemand mijn account heeft gestolen?*
- Voor overige vragen en problemen, zie *Een aanvraag indienen*.

Snapchat

- Eventuele problemen kun je melden door 'Een veiligheidsprobleem melden' aan te klikken op de pagina *Neem contact met ons op*. Voorlopig kan dat alleen nog in het Engels.

TikTok (voorheen Musical.ly)

- Voor het blokkeren van vervelende personen, zie de pagina *Block an accoun*t.
- Voor het melden van spam en ander misbruik, zie de pagina *Report inappropriate content*.
- Als je account gehackt is, zie de pagina *Hacked account*.

Twitter

- Als je denkt dat je account gehackt is, zoek dan naar 'Beveiliging en gehackte accounts' in het Helpcentrum om de pagina's te vinden die je verder kunnen helpen.
- Voor alle overige problemen, ga naar *Een ticket indienen*.

WhatsApp

- Voor technische ondersteuning: mail naar support@whatsapp.com.
- Voor overige problemen (juridisch, sociaal, etc.): ga naar www.meldknop.nl.

YouTube

- Zie de communityrichtlijnen van YouTube voor praktische tips en informatie over spam, misleidende praktijken, en gevoelige of gewelddadige content.
- Als je content tegenkomt die volgens jou deze richtlijnen schendt, dan kun je content markeren om deze te laten beoordelen door YouTube-medewerkers.

Voor alle sites en toepassingen die hierboven niet genoemd zijn

- Ga naar www.meldknop.nl.

EHBO-kit voor ouders

Verslaafd geraakt?

Je denkt al snel: “Mijn kind is verslaafd aan gamen” (of aan zijn of haar telefoon). Maar met het woord ‘verslaving’ moet je ontzettend oppassen. Het is een begrip uit de psychiatrie, waar duidelijke criteria voor zijn. Bij gamen wordt meestal niet voldaan aan die criteria. Bij ‘veel op je telefoon zitten’ nog minder. Gelukkig maar, want je wilt je kind natuurlijk niet meteen op therapie sturen of laten opnemen in een kliniek.

Toch kunnen kinderen en jongeren wel heel veel tijd besteden aan gamen en social media. Of er dan ook sprake is van *problematisch gamen*, kun je nagaan met Test je gamegedrag van het Trimbos-instituut. Voor *problematisch smartphone- of socialmediagebruik* bestaat zo’n soort test nog niet (omdat er nog te weinig onderzoek naar is gedaan).

Problematisch gamen is vaak een symptoom van een diepliggender probleem. Het komt bijvoorbeeld regelmatig voor bij kinderen en jongeren met een stoornis in het autistisch spectrum. Het kan ook voorkomen bij gewone (niet-autistische) jongeren die vluchten uit de werkelijkheid omdat ze die niet goed aankunnen. Het gamen kan dan een symptoom zijn van een depressie. Of omdat ze gepest worden[2].

Wanneer mediagebruik tot problemen leidt, moeten die problemen worden aangepakt. Of je het nu verslaving noemt of niet. Vanzelfsprekend kan autisme niet genezen worden. Maar als daar sprake van is, moet dáár de aandacht op gericht worden, en niet op het gamen an sich.

[2] Trimbos-instituut (2016). Problematisch gamen: aanbevelingen voor preventie.

Notities

De Internet Helden.

Hulpdiensten

Meldknop.nl

Dit is dé centrale plek voor kinderen en jongeren om nare dingen te melden en advies te vragen. Je kunt online (via de website), telefonisch, door te chatten of door te mailen een melding doen over alle denkbare onderwerpen, van online pesten tot nare filmpjes, en van shame-sexting tot identiteitsfraude, problematische challenges en nepmodellenbureaus. Meldknop.nl is een samenwerkingsverband van meerdere partijen, waaronder de Kindertelefoon en de politie. Tijden waarop je kunt bellen en chatten zijn afhankelijk van de instantie waarnaar je doorverwezen wordt.

Let op: je kunt ook de bijbehorende 'echte meldknop' toevoegen aan je browser, zodat je deze altijd bij de hand hebt. Deze plug-in is alleen beschikbaar voor Internet Explorer, Firefox en Chrome. De makers van de plug-in hebben voorlopig nog geen plannen deze ook beschikbaar te maken voor andere browsers, zoals Edge en Safari.

Kindertelefoon.nl

De Kindertelefoon is bedoeld als luisterend oor voor kinderen én jongeren. Je kunt praten over alles wat je dwarszit. Melden is anoniem.

Hulp vragen via ...	Hoe?	Openingstijden
Telefoon	0800 - 0432	11:00-21:00 (elke dag)
Chat	Op website	11:00-21:00 (elke dag)
Forum	Op website	n.v.t.

Helpwanted.nl

Meld- en adviespunt voor seksueel misbruik via internet. De medewerkers zijn allemaal professionals met kennis over online seksueel misbruik en wat je kunt doen als je ermee te maken hebt. Melden is anoniem, maar als je advies wilt, is er een e-mailadres nodig.

Hulp vragen via ...	Hoe?	Openingstijden
Chat	Op website	15:00-19:00 (ma t/m vrij)
Vragenlijst	Op website	n.v.t.
Contactformulier	Op website	n.v.t.

Vraaghetdepolitie.nl

Voor alle vragen over veiligheid en criminaliteit. De chat is anoniem.

Hulp vragen via ...	Hoe?	Openingstijden
Chat	Op website	19:00-21:00 (di, wo & do)
Contactformulier	Op website	n.v.t.

Je bent een

InternetHeld.

HEEFT HET INTERNETHELDEN-CERTIFICAAT VERDIEND

Jij bent:

Slim: je denkt na over wat je deelt en met wie, en weet hoe je je privacy kunt beschermen.

Alert: je kunt beoordelen of online informatie waar of betrouwbaar is.

Sterk: je weet wat je kunt doen om je persoonlijke gegevens te beschermen.

Aardig: je hebt een positief effect op anderen door aardig te zijn en goed om te gaan met cyberpesten.

Moedig: je weet dat je hulp kunt inschakelen als je online een situatie tegenkomt die je niet vertrouwt.

Je kunt de online wereld nu veilig en met vertrouwen verkennen.

DATUM

HANDTEKENING

g.co/DeInternetHelden

De Internet Helden.

Een internetheld zijn betekent dat je online slim, alert, sterk, aardig en moedig bent. Wij beloven met het hele gezin om ons aan de volgende principes te houden:

Verstandig delen

We denken goed na over wat we delen en met wie. We gaan na welke impact dingen kunnen hebben op onszelf en anderen, en weten hoe we onze eigen privacy kunnen beschermen.

Val niet voor vals

We zijn ons ervan bewust dat mensen, situaties en informatie die we online tegenkomen, niet altijd zijn wat ze lijken.

Beveilig je geheimen

We nemen de verantwoordelijkheid om belangrijke informatie te beschermen. Dit doen we onder andere door het bedenken van veilige wachtwoorden en het instellen van authenticatie in twee stappen.

Met aardig doen kom je verder

We leren om te gaan met de positieve en negatieve ervaringen bij online vriendschappen. We begrijpen wanneer een bericht kwetsend kan zijn en dat er verschillende manieren zijn om online op iemand te reageren.

Blijf er niet mee zitten

We komen voor onszelf en anderen op als we vervelend en ongepast gedrag online zien. We weten wat voor mogelijkheden er zijn om hulp in te roepen als we ons ergens zorgen over maken.

Dit is wat er nodig is om veilig en zelfverzekerd online te zijn.

Was getekend,

g.co/DeInternetHelden

Een samenwerking van:

Bureau Jeugd & Media

SIC NEDERLAND
SAFER INTERNET CENTRE

Google

Onderschreven door:

EOKM
Expertisecentrum Online Kindermisbruik

HELPWANTED.NL
advies bij online seksueel misbruik

Ouders & Onderwijs.
Punt voor ouders

Veilig internetten.nl

De Internet Helden.