Google

Slim
Alert
Sterk
Vriendelijk
Moedig

Cyber Helden

Digitale Veiligheid en Burgerschap Curriculum

Cyber Helden

Welkom bij het Cyber Helden-curriculum, een samenwerking tussen Bibliotheken Zonder Grenzen, Test Aankoop, Child Focus en Google. Deze tool maakt deel uit van Cyber Helden, een programma ontworpen om kinderen de vaardigheden aan te leren die ze nodig hebben om veilig en slim om te gaan met het internet.

Het Cyber Helden-programma geeft ouders de tools en methodes die ze nodig hebben om kinderen thuis begrippen als digitale veiligheid en burgerschap bij te brengen.

De vijf pijlers van digitaal burgerschap en veiligheid vormen de Internetcode van de Cyberheld:

- **Denk goed na voor je iets deelt (Wees cyber slim)**
- **Val niet voor vals (Wees cyber alert)**
- **Beveilig je geheimen (Wees cyber sterk)**
- **Vriendelijk zijn is cool (Wees cyber vriendelijk)**
- **Praat erover als je twijfelt (Wees cyber moedig)**

Deze activiteiten komen gedetailleerd aan bod in Interland, een browser-gebaseerd spelletje dat leren over veiligheid en burgerschap leuk en interactief maakt, net als het internet zelf. Door Interland en het bijbehorende werkbladen te gebruiken, kunnen ouders activiteiten uitkiezen die het meest geschikt zijn voor hun kinderen, of de hele reeks doornemen van start tot finish.

Wij geloven dat het programma Cyber Helden een belangrijke stap is in de juiste richting en ervoor zorgt dat onze kinderen de onlinewereld op een veilige manier leren ontdekken.

Dit document valt onder de Creative Commons Naamsvermelding 4.0 Internationale Publieke Licentie.

Inhoud

Thema 01: Denk goed na voor je iets deelt 5

Activiteit 1: **Wanneer je beter niets deelt**
Activiteit 2: **Iets privé houden**
Activiteit 3: **Interland: Berg van Voorzichtigheid**

Thema 02: Val niet voor vals 13

Activiteit 1: **Bijt niet in de phishinghaak!**
Activiteit 2: **Wie ben jij echt?**
Activiteit 3: **Over bots**
Activiteit 4: **Interland: Rivier van de Waarheid**

Thema 03: Beveilig je geheimen 29

Activiteit 1: **Hoe maak je een sterk paswoord**
Activiteit 2: **Hou het voor jezelf**
Activiteit 3: **Interland: Schattentoren**

Thema 04: Vriendelijk zijn is cool 38

Activiteit 1: **Van omstaander naar beschermer**
Activiteit 2: **Een toontje lager**
Activiteit 3: **De daad bij het woord**
Activiteit 4: **Interland: Koninkrijk der Vriendelijkheid**

Thema 05: Praat erover als je twijfelt 48

Activiteit 1: **Wanneer hulp inroepen**
Activiteit 2: **Meld het ook online**

Thema 01: Wees cyber slim

Denk goed na voor je iets deelt

Jezelf en je online reputatie beschermen

Lesoverzicht

Activiteit 1: **Wanneer je beter niets deelt**
Activiteit 2: **Iets privé houden**
Activiteit 3: **Interland: Berg van Voorzichtigheid**

Inleiding

Leerkrachten en ouders begrijpen hoe digitale foutjes iemands reputatie en privacy kunnen schaden en gevoelens kunnen kwetsen. Maar het kan moeilijker zijn om kinderen ervan te overtuigen dat schijnbaar onschuldige posts makkelijk verkeerd kunnen geïnterpreteerd worden door mensen voor wie ze niet waren bestemd. Ook in de toekomst.

Onderstaande activiteiten gebruiken concrete voorbeelden en discussies die aanzetten tot nadenken, om kinderen bij te brengen hoe ze een positieve onlinereputatie onderhouden door hun privacy en persoonlijke informatie zelf te beheren.

Doelstellingen kinderen

- ✓ Een positieve on- en offlinereputatie **creëren en onderhouden**.
- ✓ Andermans grenzen en privacy **respecteren**.
- ✓ Je digitale voetafdruk **begrijpen en beheren**.
- ✓ **Hulp vragen** aan een volwassene in lastige situaties.

Denk goed na voor je iets deelt
Woordenschat

Onlineprivacy: een algemene term die meestal betrekking heeft op het vermogen om te controleren welke informatie je deelt over jezelf online en wie die informatie kan zien en delen.

Digitale voetafdruk (of digitale aanwezigheid): je digitale voetafdruk is alles wat je over jezelf kunt vinden online.Dit zijn onder andere foto's, audio, video's die jij post, maar ook commentaren die je post op profielen van vrienden. Net zoals je voetstappen een afdruk achterlaten wanneer je stapt, laten ook je posts online sporen achter.

Reputatie: de ideeën, meningen, indrukken of overtuigingen die anderen over jou hebben. Je kan niet zeker zijn wat jouw reputatie precies is, maar je hebt wel graag dat ze positief of goed is.

Persoonlijke informatie: informatie over een specifieke persoon. Bijvoorbeeld je naam, straat, woonplaats, telefoonnummer, e-mailadres, enz. Dit noemen we persoonlijke (of gevoelige) informatie. Denk goed na voor je dit soort informatie online deelt.

Oversharing: te veel informatie delen online. Meestal gaat het over te veel persoonlijke informatie delen of te veel over jezelf vertellen in een bepaalde situatie of online gesprek.

Instellingen: het onderdeel binnen een digitaal product, app, website, enz., waarin jij bepaalde voorkeuren kunt regelen. Als het over de instellingen van jouw persoonlijk account gaat, dan kun jij bepalen en aanpassen wat je met wie deelt en hoe je account in elkaar steekt. Ook jouw privacyinstellingen vind je hier terug.

Denk goed na voor je iets deelt: Activiteit 1

Wanneer je beter niets deelt

Vergelijk echte of verzonnen geheimen met je kinderen om ze te laten nadenken over privacyzones.

Doelstellingen

- ✓ **Begrijpen** welke soort informatie best geheim gehouden wordt.
- ✓ **Onthouden** dat iedereen het verdient dat zijn/haar privacybeslissingen gerespecteerd worden.
- ✓ **Identificeren** van andere soorten persoonlijke informatie die je online vindt.

Even praten

Waarom is privacy belangrijk?

Je digitale voetafdruk is wie jij bent online. Dat kan gaan over foto's, audio, video's, teksten, 'likes' en comments die je op profielen van vrienden post. Net zoals het belangrijk is om offline positief aanwezig te zijn (bijvoorbeeld op school), is het belangrijk ook online positief te zijn.

Het internet maakt het makkelijk om te communiceren met familie, vrienden en mensen die dezelfde dingen leuk vinden. We sturen berichtjes, delen foto's en nemen deel aan gesprekken op sociale netwerken. Soms zonder erover na te denken wie er allemaal meekijkt. Een foto of bericht waarvan je denkt dat het vandaag grappig en onschuldig is, kan verkeerd geïnterpreteerd worden door mensen van wie je dacht dat ze het nooit zouden zien, vandaag of in een verre toekomst. Eenmaal iets op het internet staat, is het moelijk om het er weer af te halen. Vergeet niet:

- Zoals alles op het internet is je digitale voetafdruk zichtbaar voor iedereen, ook voor mensen die je nooit hebt ontmoet.
- Zodra iets door of over jou online staat, is het misschien wel voor altijd. Vergelijk het met een alcoholstift: je kunt wat je schrijft niet meer wissen, ook al wilde je iets anders schrijven.

Net daarom is je privacy zo belangrijk. Je kunt je privacy beschermen door enkel de dingen te delen waarvan je zeker bent dat je ze wilt delen. Met andere woorden, wees dus voorzichtig met wat je online post en deelt. Waarom anders zou privacy zo belangrijk kunnen zijn?

Je moet ook weten wanneer je beter helemaal niets post, niet reageert op iemands post, foto of comment, of iets deelt dat niet waar is. "Denk na voor je iets post": iedereen heeft het wel al eens gehoord. Het is dan ook een goed advies.

Je eigen privacy en die van anderen respecteren doe je door na te denken over wat oké is om te posten, wie je post kan zien, welk effect het kan hebben op jezelf en op anderen, en wanneer je best helemaal niets post. Enkele vragen om hierover verder te discussiëren:

- Wanneer is het oké om een foto of video van iemand anders te delen?
- Waarom zijn geheimen zo moeilijk te bewaren?
- Is het soms oké om iemands geheim te verklappen?
- Wat als je om iemand geeft en je merkt dat er iets gepost wordt waardoor je voelt dat die persoon in gevaar is? Als je denkt dat je dat geheim moet delen, zou je die persoon dat dan eerst moeten vertellen? Moeten ze weten dat je bezorgd bent?

Activiteit

1. Vraag je kinderen om een personage te bedenken van ongeveer hun leeftijd. Vraag hen ook om de naam van het personage in het midden van een blad papier te schrijven en eromheen ‘persoonlijke’ informatie over die persoon neer te schrijven of te tekenen.

2. Bekijk nu elk stukje persoonlijke informatie en ga na of het oké is om die informatie online te delen. Welk effect kan delen hebben op de onlinereputatie van het personage?

Lessen

Geheimen zijn slechts één soort persoonlijke informatie die we misschien privé willen houden of enkel delen met familie of vrienden die we vertrouwen. Heb je een geheim gedeeld, dan heb je niet meer helemaal onder controle wat ermee gebeurt. Welke andere soorten informatie moeten we zeker beschermen?

- Je thuisadres en je telefoonnummer
- Je e-mail
- Je paswoorden
- Je gebruikersnamen
- Je schoolwerk en andere documenten die je aanmaakt

Denk goed na voor je iets deelt: Activiteit 2

Iets privé houden

Beoordeel een of enkele van de volgende scenario's met je kinderen en bespreek dan wat de beste privacyoplossing is voor elk scenario.

Doelstellingen

- ✓ **Bekijken** van privacykwesties vanuit verschillende standpunten.
- ✓ **Begrijpen** dat verschillende scenario's verschillende privacyniveaus vragen.

Even praten

Privacyscenario's: Wat moet je doen?

Scenario 1: Een kind dat je kent op school wordt gebeten door een vreemd insect en krijgt lelijke, veelkleurige uitslag op zijn buik. Het wil niet dat iemand anders het te weten komt.

- Hebben andere mensen het recht om dit te weten?
- Moet jij het hen zeggen?

Scenario 2: Iemand schrijft iets in een persoonlijk dagboek. Iemand anders kopieert dat en plaatst het online.

- Was het verkeerd van die andere persoon om dat te posten?
- Hoe zou jij je voelen wanneer iemand dit deed met iets wat je privé wilde houden?

Scenario 3: Iemand post "Geniet van je vakantie" op de socialemediapagina van een vriend.

- Had die vriend publiekelijk aangekondigd dat hij wegging? Wilde hij dat aan iedereen vertellen?
- Bestaan er andere manieren om deze boodschap te delen? Bijvoorbeeld door een rechtstreekse boodschap of bericht te sturen?

Scenario 4: Je weet dat een leerling een vals socialemedia-account heeft aangemaakt om zich op een negatieve manier voor te doen als een andere leerling en hij vermeldt er ook de persoonlijke informatie van die leerling op.

- Heeft de andere leerling het recht om dat te weten?
- Moet iemand dit aan een leerkracht melden of een volwassene die hij vertrouwt? Hoe? En wat kan er gebeuren als niemand dat doet?
- Het is niet duidelijk wie dat account heeft aangemaakt, maar jij weet wie het heeft gedaan. Moet je het vertellen aan een volwassene die je in vertrouwen neemt?

Activiteit

Beoordeel de vier scenario’s met je kinderen en bespreek hoe elk scenario een andere privacyoplossing kan hebben.

Lessen

Andere situaties vragen andere oplossingen. Zowel online als offline.
De privacykeuzes van anderen respecteren is altijd belangrijk, ook al zou jij een andere keuze maken.

Denk goed na voor je iets deelt: Activiteit 3

Interland: Berg van Voorzichtigheid

Het bergachtige stadscentrum van Interland is een plaats waar iedereen andere mensen ontmoet. Maar je moet heel goed opletten wat je deelt en met wie. Informatie verplaatst zich met de snelheid van het licht en er zit een oversharer onder de internauten die je kent.

Open een webbrowser op je desktop en surf naar www.cybersimpel.be/interland en ga naar de Berg van Voorzichtigheid.

Even praten

Nadat de kinderen de Berg van Voorzichtigheid hebben ontdekt, zullen deze vragen ze stimuleren om over de thema's van het spel te praten:

- Welk van alle posts die je gedeeld hebt in het spelletje, zou je in het echte leven het meest delen? Waarom?
- Beschrijf een moment waarop je per ongeluk iets gedeeld hebt dat je beter niet had gedeeld.
- Waarom denk je dat het personage in de Berg van Voorzichtigheid een oversharer wordt genoemd?
- Beschrijf het karakter van de oversharer en hoe zijn acties het spel beïnvloeden.
- Veranderde het spel Berg van Voorzichtigheid de manier waarop je in de toekomst zal nadenken over het delen van informatie?
- Noem één ding dat je anders zal doen nadat je de lessen hebt gevolgd en het spel hebt gespeeld.
- Geef één voorbeeld van een mogelijk negatief gevolg wanneer je iets deelt met het publiek in plaats van enkel met je vrienden.
- Welke stappen kun je ondernemen als je per ongeluk iets persoonlijks hebt gedeeld? Wat als iemand per ongeluk iets te persoonlijks met jou deelt?

Thema 02: Wees cyber alert

Val niet voor vals

Blijf weg van phishing en oplichters

Lesoverzicht

Activiteit 1: **Bijt niet in de Phising-haak!**
Activiteit 2: **Wie ben jij echt?**
Activiteit 3: **Over die bots**
Activiteit 4: **Interland: Rivier van de Waarheid**

Inleiding

Voor kinderen is het belangrijk dat ze begrijpen dat inhoud die ze online vinden niet noodzakelijk waar of betrouwbaar is, en dat sommige websites hun informatie proberen te stelen. Phishing en andere vormen van online oplichting moedigen internetgebruikers van alle leeftijden aan om te reageren op mysterieuze berichten van mensen die ze niet kennen of die zich voordoen als iemand die ze wel kennen.

Doelstellingen kinderen

- ✓ **Beseffen** dat het niet is omdat iets online staat, dat het waar is.
- ✓ **Ontdekken** hoe phishing werkt en waarom het een bedreiging is.
- ✓ **Herkennen** van valse aanbiedingen, prijzen en andere vormen van onlineoplichting.

Val niet voor vals
Woordenschat

Bot: ook wel ‘chatbot’ of ‘virtuele assistent’ genoemd. Dit is software die online werkt of via een netwerk en automatisch vragen beantwoordt, commando’s opvolgt (zoals een routebeschrijving naar het huis van je nieuwe vriend), of eenvoudige taken uitvoert (zoals een liedje afspelen).

Phishing: bij phishing probeert iemand je te misleiden om online persoonlijke informatie te delen. Phishing gebeurt meestal via e-mail, advertenties of websites die lijken op websites die je al eerder gebruikte.

Spearphishing: bij spearphishing is de aanval meer op jou persoonlijk gericht, doordat oplichters jouw persoonlijke informatie gebruiken.

Scam: een oneerlijke poging om geld te verdienen of iets waardevols te verkrijgen door mensen te misleiden.

Betrouwbaar: waarop je kunt vertrouwen om te doen wat juist of nodig is.

Authentiek: echt, oprecht, waar of exact, niet vals of gekopieerd.

Controleerbaar: iets waarvan kan bewezen of aangetoond worden dat het waar of correct is.

Bedrieglijk: bedoeld om iemand te laten geloven dat iets waar is, terwijl het dat eigenlijk niet is.

Manipulatie: iemand die een andere persoon of situatie oneerlijk, onrechtvaardig controleert, beïnvloedt of bedreigt. Ook dingen die je online aantreft kunnen gemanipuleerd zijn, bijvoorbeeld een foto die bewerkt is om je iets te laten geloven dat niet waar is.

Frauduleus: iemand misleiden om iets waardevols van hem te krijgen.

Firewall: een programma dat je computer beschermt tegen de meeste vormen van oplichting en misleiding.

Schadelijk: woorden of acties die bedoeld zijn om wreed of pijnlijk te zijn. Kan ook verwijzen naar schadelijke software die bedoeld is om iemands apparaat, account of persoonlijke informatie schade toe te brengen.

Catfishing: een valse identiteit of account maken op een sociale netwerkdienst om mensen te misleiden om hun persoonlijke informatie te delen, of te laten geloven dat ze met de echte persoon praten, met een authentiek account, profiel of pagina.

Clickbait: manipulatieve online-inhoud, berichten of advertenties die zijn ontworpen om de aandacht van mensen vast te houden en ervoor te zorgen dat ze klikken op een link of webpagina, vaak om views of websiteverkeer te doen stijgen om zo geld te verdienen.

Val niet voor vals: Activiteit 1

Bijt niet in de phishinghaak!

Een spel waarbij kinderen verschillende teksten en e-mails bestuderen en proberen uit te maken welke de echte en valse phishingberichten zijn.

Doelstellingen

- ✓ **De technieken herkennen** die mensen gebruiken om je identiteit te stelen.
- ✓ **Bekijken** hoe je identiteitsdiefstal voorkomt.
- ✓ **Durven** praten met een vertrouwde volwassene als je denkt dat iemand je gegevens heeft gestolen.
- ✓ De tekenen van een phishingpoging **herkennen**.
- ✓ **Voorzichtig** zijn met hoe en met wie je persoonlijke informatie deelt.

Even praten

Wat is phishing nu eigenlijk?

Phishing gebeurt wanneer iemand informatie probeert te stelen (zoals je login- of accountgegevens) door zich in een e-mail, sms of andere onlinecommunicatie voor te doen als iemand die je vertrouwt. Phishing-e-mails kunnen ook virussen op je computer plaatsen die je contactenlijst gebruiken om je vrienden en familie nog meer phishing-e-mails te sturen. Ze doen dit door je naar een onveilige website te sturen of door je downloads en bijlagen te doen openen.

Andere oplichters proberen je te misleiden om malware of ongewenste software te downloaden door je te vertellen dat er iets fout is met je toestel. Let op: een website of advertentie kan onmogelijk zeggen of er iets fout is met je toestel! Sommige phishingaanvallen zijn duidelijk nep. Maar andere kunnen echt lijken en overtuigend zijn. Stuurt een oplichter jou bijvoorbeeld een bericht waarin enkele van je persoonlijke gegevens vermeld staan, dan noemen we dit spearphishing. Misschien trap je er wel in omdat ze je doen denken dat het betrouwbaar is.

Het kan heel moeilijk zijn om dit te herkennen, want door je eigen informatie te gebruiken, kan het lijken alsof ze jou echt kennen. Voor je op een link klikt of je paswoord invoert op een site die je nooit eerder hebt bezocht, is het goed jezelf enkele vragen te stellen over die e-mail of webpagina. Deze vragen kun je jezelf stellen:

- Ziet de site er even professioneel uit als andere websites die je kent en vertrouwt, met het gebruikelijke logo van het product of het bedrijf en met tekst zonder spelfouten?
- Komt de URL van de site overeen met de naam van het product of het bedrijf dat je zoekt? Staan er spelfouten in?
- Zijn er spamachtige pop-ups?
- Begint de URL met https:// met aan de linkerkant een groen hangslotje? (dit betekent dat de verbinding veilig is.)

- Wat staat er in de kleine lettertjes? (Dat is waar het gevaar in schuilt.)
- Biedt de e-mail of site iets aan dat te mooi is om waar te zijn, zoals de kans om veel geld te winnen? (Het is bijna altijd te mooi om waar te zijn.)
- Klinkt de boodschap een beetje vreemd? Alsof ze je kennen, maar je bent toch niet helemaal zeker?

En wat als je toch in de val trapt? Eerst en vooral: geen paniek!

- Vertel het meteen aan een ouder, je leerkracht of een andere volwassene die je vertrouwt. Hoe langer je wacht, hoe erger de dingen kunnen worden.
- Verander de paswoorden van je online-accounts.
- Word je het slachtoffer van oplichters, vertel het dan meteen aan je vrienden en andere contacten, want zij kunnen ook getroffen worden.
- Gebruik de instellingen om het bericht indien mogelijk te melden als spam.

Activiteit

Wat je nodig hebt:

- Hand-out: werkblad "Phishingvoorbeelden"

1. Bestudeer enkele voorbeelden

Laat uw kinderen deze voorbeelden van berichten en websites bestuderen.

2. Geef keuzes aan

Selecteer "Echt" of "Nep" voor elk voorbeeld en zeg daaronder waarom.

3. Bespreek de keuzes

Welke voorbeelden lijken betrouwbaar en welke lijken verdacht?
Hebben sommige antwoorden je verrast?

Antwoorden op het werkblad "Phishingvoorbeelden":

1. **Echt.** De e-mail vraagt de gebruiker naar de website van het bedrijf te surfen en in te loggen op hun account, in plaats van een link te geven in de e-mail of hen te vragen hun paswoord te mailen (links kunnen gebruikers naar twijfelachtige websites leiden).
2. **Nep.** Verdachte en geen beveiligde URL.
3. **Echt.** Let op de https:// in de URL.
4. **Nep.** Verdacht aanbod in ruil voor bankgegevens.
5. **Nep.** Niet veilig en verdachte URL.

4. Verdere discussie

Dit zijn enkele vragen die je jezelf kan stellen bij het beoordelen van berichten en sites die je online vindt:

- **Ziet dit bericht er goed uit?**
  Wat is je eerste indruk? Vallen jou onbetrouwbare aspecten op?

- **Biedt de e-mail jou iets gratis aan?**
  Gratis aanbiedingen zijn meestal niet echt gratis (ook al is het geen phishing).

- **Vraagt het bericht je persoonlijke gegevens?**
  Sommige websites zullen jou persoonlijke informatie vragen, zodat ze jou nog meer bedrieglijke berichten kunnen sturen. Bijvoorbeeld een 'persoonlijkheidstest' waarin je informatie prijsgeeft op basis waarvan ze jouw paswoord of andere geheime informatie makkelijker kunnen raden. De meeste echte bedrijven zullen geen persoonlijke informatie via e-mail vragen.

- **Is het een kettingmail of post op sociale media?**
  E-mails en posts die je vragen iets door te sturen naar iedereen die je kent, kunnen jou en anderen in gevaar brengen. Doe het niet, tenzij je zeker bent van de bron en zeker weet dat je het bericht veilig kan doorgeven.

- **Lees de kleine lettertjes**
  Onderaan de meeste documenten vind je de kleine lettertjes. Deze tekst is klein en bevat vaak de dingen waarvan ze willen dat je ze over het hoofd ziet. Een kop bovenaan de tekst vertelt bijvoorbeeld dat je een gratis telefoon hebt gewonnen, maar in de kleine lettertjes staat dat je dat bedrijf eigenlijk 200 euro per maand moet betalen.

Opmerking: in deze oefening gaan we ervan uit dat 'Internaut Mail' een echte, vertrouwde service is.

Lessen

Ben je online, wees dan altijd op je hoede voor phishingaanvallen in e-mails, sms-berichten en posts. Zorg ervoor dat je de juiste mensen hierover aanspreekt als iemand je voor de gek houdt.

Werkblad: Activiteit 1

Voorbeelden van phishing

1. Is dit echt of nep?

.....

2. Is dit echt of nep?

.....

3. Is dit echt of nep?

.....

4. Is dit echt of nep?

.....

5. Is dit echt of nep?

Val niet voor vals: Activiteit 2

Wie ben jij echt?

In deze activiteit oefenen uw kinderen hun antiphishingvaardigheden door hun vermoedens van – en mogelijke reacties op – verdachte onlineteksten, posts, vriendschapsverzoeken, afbeeldingen en e-mails te bespreken.

Doelstellingen

- ✓ **Erkennen** dat een onlinepubliek misschien groter is dan ze denken.
- ✓ **Bevestigen** dat ze de echte identiteit kennen van de mensen met wie ze online praten.
- ✓ **Eerst nadenken** voordat ze 'vriendschap sluiten' of online contact leggen met iemand.
- ✓ **Opletten** aan wie ze persoonlijke informatie verstrekken en welke dingen ze delen.
- ✓ **Vragen** stellen en/of hulp zoeken bij een volwassene als ze het niet zeker weten.
- ✓ **Een volwassene vertellen** wanneer iemand hen online ongemakkelijk doet voelen.
- ✓ **Eerlijk zijn** in alle onlinecontacten.

Even praten

Hoe weet je dat zij het echt zijn?

Ben je met een vriend aan het bellen, hoe kan je dan zien dat hij het echt is, zonder dat je hem 'ziet'? Je hoort het aan zijn stem, toch? Maar de onlinewereld zit een beetje anders in elkaar. Soms is het moeilijker te achterhalen of iemand is wie hij zegt dat hij is. Soms doen mensen zich voor als andere mensen om iemand te plagen. Anderen bootsen iemand na om persoonlijke informatie te stelen. Dit noemen we Catfishing. Op het internet kunnen vreemden contact met je zoeken. Het veiligste is er niet op ingaan of vertellen aan een ouder of volwassene die je vertrouwt dat iemand contact met je zoekt die je niet kent. Maar als je beslist dat het oké is om erop in te gaan, dan is het ook raadzaam om eerst na te gaan wat je over die personen kunt vinden. Check hun profiel, bekijk wie hun vrienden zijn of zoek andere informatie die bevestigt dat ze zijn wie ze zeggen dat ze zijn. Er zijn verschillende manieren om iemands identiteit na te gaan online. Een paar voorbeelden om ons op weg te helpen.

Opmerking voor de ouder

Misschien kunt u eerst brainstormen over de vraag "Hoe check je iemands identiteit online?" En ga dan verder met deze ideeën om over na te denken.

- **Is hun profielfoto verdacht?**
  Is hun profielfoto wazig of moeilijk te zien? Of is er helemaal geen foto te zien, bijvoorbeeld een bitmoji of een cartoongezicht? Slechte foto's, bitmoji's, afbeeldingen van huisdieren, enz. maken het makkelijk om je identiteit te verbergen op social media. Oplichters stelen meestal ook foto's van een echte persoon om een nepprofiel in te stellen. Vind je meer profielen van de betrokken persoon met dezelfde naam?

- **Bevat hun gebruikersnaam hun eigen naam?**
  Komt hun schermnaam op sociale media bijvoorbeeld overeen met een echte naam? (Bijvoorbeeld: het profiel van de heer x heeft als URL SocialMedia.com/de heer_x.)

- **Hebben ze een bioprofiel?**
  Zo ja, klinkt het alsof het geschreven werd door een echte persoon? Hebben ze een persoonlijke biografie? Zo ja, klinkt die alsof ze is geschreven door een echte persoon? Valse accounts hebben misschien niet veel 'Over Mezelf'-informatie of hebben misschien wat willekeurige informatie bijeengesprokkeld om een nepprofiel te maken. Staat er informatie in hun biografie die je kunt bevestigen als je ze opzoekt?

- **Hoe lang is het account actief geweest?**
  Is het profiel nieuw of vertoont het veel activiteit? Heeft de persoon gemeenschappelijke vrienden met jou, zoals je zou verwachten? Valse accounts hebben meestal niet veel inhoud of vertonen weinig tekenen van mensen die berichten of commentaren plaatsen en sociale contacten hebben.

Activiteit

Wat je nodig hebt:

- Een kopie van het werkblad "Wie ben jij echt?". Phishingspiekbriefje.

Neem een of meer scenario's uit het bakje en bespreek hoe je op deze situatie zou reageren. Ben je met 3 of meer, dan kun je een scenario naspelen (één persoon vertelt, een tweede doet het 'bericht' en een derde beantwoordt het, een vierde legt de redenering uit, ...). Daarna kun je discussiëren terwijl je het spiekbriefje checkt. Verzin gerust andere berichten die volgens jou nog vervelender zijn.

Lessen

Jij bepaalt met wie je praat online. Zorg ervoor dat de mensen met wie je contact hebt, zijn wie ze zeggen dat ze zijn!

Phishingspiekbriefje: Activiteit 2

Wie ben jij echt?

Dit zijn vijf scenario's van berichten die iemand online kan ontvangen of op zijn telefoon. Elk heeft een lijst met de manieren waarop je kunt reageren, sommige zijn goed andere minder. Bekijk of je ze logisch vindt of dat je nog andere antwoorden kunt bedenken. Overkomt een van deze scenario's jou in het echt en ben je niet zeker wat je best doet, dan is het beste antwoord altijd geen antwoord. Je kunt ze altijd negeren of blokkeren. En erover praten met een leerkracht of ouder kan ook nooit kwaad.

Scenario 1

Je krijgt dit bericht van iemand die je niet herkent: "Hé! Je lijkt een leuke persoon om mee om te gaan. Laten we samen wat plezier maken! Kun je me toevoegen aan je vriendenlijst? Groetjes, Daan." Wat zou jij doen?

- **Negeer Daan.** Als je hem niet kent, kan je gewoon besluiten om niet met hem te praten, punt.
- **"Hallo, Daan. Ken ik jou?"** Als je het niet zeker weet, vraag het dan eerst.
- **Blokkeer Daan.** Als je hebt gecontroleerd wie hij is en besloten hebt hem te blokkeren, ontvang je geen berichten meer van hem. Op de meeste socialemediaplatformen zal hij zelfs niet merken dat je hem hebt geblokkeerd.
- **Controleer Daans profiel.** Maar wees voorzichtig - profielen zijn eenvoudig aan te maken! Controleer de vriendenlijst van deze kerel en check met wie hij verbonden is. Zijn vriendenkring kan een andere manier zijn om na te gaan of hij echt is of niet, vooral als je niemand kent die hij kent! Is er niet veel activiteit op zijn pagina, dan is dat ook een teken dat hij niet echt is.
- **Voeg Daan toe aan je vriendenlijst.** Niet aanbevolen, tenzij je hebt gecontroleerd wie hij is en het gecheckt hebt bij een volwassene die je vertrouwt.
- **Geef hem persoonlijke informatie.** Geef nooit persoonlijke informatie aan mensen die je niet kent.

Scenario 2

Je krijgt een bericht op je smartphone van iemand die je niet herkent. "Hé, dit is Jana! Herinner je me van deze zomer?" Hoe reageer je?

- **Blokkeer Jana.** Dit kan onbeleefd zijn als je haar echt kent. Maar als je zeker weet dat je afgelopen zomer niemand hebt ontmoet die Jana heet of als ze jou te veel berichten stuurt, blokkeer haar dan.
- **Negeer Jana.** Zoals gezegd: ken je deze persoon niet, dan kan je er gewoon voor kiezen niet tegen haar praten, punt.
- **"Hallo Jana. Ken ik jou?"** Dit is een veilige optie als je niet zeker weet of je haar hebt ontmoet en wilt uitvissen of het wel zo is, door wat meer info te vragen. Maar vertel Jana niet waar je afgelopen zomer was!

- **“Ik kan je me niet herinneren, maar we kunnen elkaar nog wel een keer ontmoeten.”** Echt geen goed idee, je moet nooit aanbieden om iemand te ontmoeten die je niet kent.

Scenario 3

Je krijgt een bericht van @soccergirl12, iemand die je niet volgt.”Hallo! Ik hou van je berichten, je bent ZO grappig! Geef me je telefoonnummer en dan kunnen we verder praten!” Hoe reageer je?

- **Negeer @soccergirl12.** Je hoeft niet te reageren als je dat niet wilt.
- **Blokkeer @soccergirl12.** Als je deze persoon verdacht vindt, kan je haar blokkeren en nooit meer van haar horen. Tenzij ze een nieuw fake profiel aanmaakt en met jou opnieuw contact zoekt als een andere fake persoon.
- **“Hallo, ken ik je?”** Als je het niet zeker weet, stel dan vragen voordat je persoonlijke gegevens zoals je telefoonnummer opgeeft.
- **“Oké, mijn nummer is…”** Niet doen! Zelfs wanneer je gecheckt hebt wie die persoon is, dan nog is het geen goed idee om persoonlijke informatie vrij te geven op sociale media. Zoek een andere manier om contact te leggen, via ouders, leerkrachten of andere personen die je vertrouwt.

Scenario 4

Je krijgt een chatbericht van iemand die je niet kent. “Ik zag je vandaag in de gang. JE BENT SCHATTIG! Wat is je adres? Ik kan langskomen om elkaar nog eens te zien.” Hoe reageer je?

- **Negeren.** Waarschijnlijk een goede keuze.
- **Blokkeer deze persoon.** Aarzel niet om dat te doen wanneer je een slecht gevoel over iemand krijgt.
- **“Wie ben jij?”** Waarschijnlijk niet de beste keuze. Als het bericht verdacht klinkt, is het misschien beter om het niet te beantwoorden of de persoon gewoonweg te blokkeren.
- **“Ben jij dat Liza? JIJ BENT OOK SCHATTIG! Ik woon in de Stationsstraat 1”.** Dit is geen goed idee, zelfs als je denkt dat je weet wie Liza is. Voordat je iemand je adres of andere persoonlijke informatie geeft, moet je ze eerst controleren, zelfs als je ervan uitgaat dat je ze kent. Spreek nooit met iemand af in het echt die je enkel van onlinecontacten kent.

Scenario 5

Je ontvangt dit bericht: “Hé, ik heb net je vriendin Sam ontmoet! Ze heeft me over jou verteld, zou je graag ontmoeten. Wat is je adres?” Hoe reageer je?

- **Negeren.** Als je deze persoon niet kent, maar je hebt een vriendin met de naam Sam, is de veiligste keuze om Sam de vraag te stellen voordat je op dit bericht reageert.
- **Blokkeren.** Als je deze persoon niet kent en je hebt geen vriendin met de naam Sam, is het waarschijnlijk een goed idee om je instellingen te gebruiken om te voorkomen dat deze persoon contact met je opneemt.
- **“Wie ben jij?”** Waarschijnlijk geen goed idee. Als je de persoon niet kent, kan je beter niet antwoorden, tenminste als je niets van Sam hebt gehoord.

Val niet voor vals: Activiteit 3

Over bots

Kinderen communiceren tegenwoordig met meer en meer niet-menselijke ‘stemmen’ die uit apparaten, apps en sites komen. Meestal gebeurt dit thuis, maar ook steeds vaker op school. Soms worden ze ‘chatbots’ genoemd, soms ‘virtuele assistenten’, vaak kortweg ‘bots’. Deze activiteit is een eenvoudig vraag-en-antwoordspel dat is ontworpen om kinderen samen (of gewoon samen met u) hardop te laten nadenken over interactie met bots.

Opmerking: probeer de discussie open te houden; deze activiteit is bedoeld om kritisch te denken, niet om conclusies te trekken.

Doelstellingen

- ✓ **Leren** over deze interactieve technologie die op steeds meer plaatsen in het leven van kinderen opduikt.
- ✓ **Ervaringen** met bots van verschillende types identificeren.
- ✓ **De impact analyseren** die deze technologieën kunnen hebben op het dagelijks leven, zowel positief als negatief.

Even praten

Meer en meer mensen gebruiken bots tegenwoordig. Heb je dat woord ooit al gehoord? Sommigen noemen ze “chatbots” of “virtuele assistenten”. Ze worden ingezet voor ontelbare doeleinden: om te gamen, het weer te checken, vragen te beantwoorden, instructies te krijgen, te melden wanneer de tijd verstreken is, enz. Soms hebben ze een menselijke naam, soms beschrijven hun namen gewoon wat ze doen, bijvoorbeeld Hond per Dag, een bot die dagelijks een foto van een hond verstuurt. Bots kunnen op mobiele apparaten staan, online, in auto’s, of het kunnen speciale apparaten zijn die mensen in verschillende kamers van hun huis plaatsen. Laten we even praten en nadenken over welke ervaringen uw kinderen al hadden met bots. Deze vragen kunnen we in overweging nemen:

- Weet je wat een bot is?
- Wie van jullie heeft al met een bot gepraat? Op welk soort toestel?
- Wie wil ons vertellen hoe dat is?
- Waarvoor denk je dat bots het meest geschikt zijn (voorbeelden om hen aan het denken te zetten: vragen naar het weerbericht, nieuwsfeiten geven, een spelletje spelen, vragen naar informatie)?
- Bots gebruiken wat we AI of artificiële intelligentie noemen. In zekere zin leert AI uit de dingen die jij vraagt, zodat het jou beter kan helpen. Daarom ‘onthouden’ of nemen bots op wat jij vraagt en zegt. Ga je hierdoor nadenken over wat je een bot vertelt? Zo ja, wat zou je er dan tegen zeggen en welke soort informatie zou je voor jezelf houden?
- Vind je dit hetzelfde als tegen een mens praten? In welk opzicht is het hetzelfde en ook niet hetzelfde?
- Hoe behandelen of praten mensen die je kent met hun bots?
- Hoe zou jij ermee praten? Zou je vriendelijk zijn, of zou er soms tegen roepen?

- Vind je het oké dat mensen roepen tegen bots? Waarom wel of waarom niet? (Is het een soort van interactie?)
- Soms denken heel kleine kinderen dat bots mensen zijn. Wat zou jij je kleine zus, broer, neefjes of nichtjes vertellen zodat ze begrijpen waarmee ze aan het praten zijn?
- Als bots kunnen leren van mensen, kun je dan iets bedenken dat wij niet mogen zeggen omdat je niet wilt dat bots het leren? (Tip: denk even terug aan de activiteiten in “Share with Care” en bespreek hoe ze hiermee samenhangen.)
- Kun je informatie beoordelen als “goed of slecht” of “echt of vals”? Hoe kunnen we deze vragen proberen te beantwoorden?”

Activiteit

Zoek na de discussie op je toestellen thuis naar afbeeldingen van en informatie over bots (inclusief nieuwsverslaggeving). Mogelijke zoekwoorden: “bots”, “chatbots,” “digitale assistenten” of “virtuele assistenten.” Beslis in familieverband of de informatie oké is en schrijf er een samenvatting van één alinea over.

Lessen

Kritisch denken is een van de beste en meest nuttige vaardigheden die we hebben om ons technologiegebruik duurzaam te houden. Het mooie eraan is dat het beter wordt telkens we er gebruik van maken. Hardop nadenken is een krachtige en leuke manier om die vaardigheid te gebruiken en te verbeteren.

Val niet voor vals: Activiteit 4

Interland: Rivier van de Waarheid

In de rivier die door Interland stroomt, lopen feiten en fictie door elkaar. Maar de dingen zijn niet altijd zoals ze lijken. Gebruik je gezond verstand om de stroomversnellingen over te steken en val niet voor de trucjes van de phisher die in deze wateren op de loer ligt!

Open een webbrowser op je desktop en surf naar www.cybersimpel.be/interland en dan naar Reality River.

Even praten

Laat uw kinderen de River van de Waarheid spelen en gebruik onderstaande vragen om te bespreken wat ze geleerd hebben in de game.

- Beschrijf een moment waarop je moest beslissen dat iets echt of nep was op het internet. Welke aanwijzingen heb je gezien?
- Wat is een fisher? Beschrijf zijn gedragingen en hoe die het spel beïnvloeden.
- Heeft het spel Rivier van de Waarheid de manier veranderd waarop je dingen en mensen in de toekomst zal beoordelen? Zo ja, hoe? Noem één ding dat je anders zal doen nadat je de activiteiten hebt gedaan en het spel hebt gespeeld.
- Geef enkele aanwijzingen van iets dat ‘niet oké’ is of akelig in een bepaalde situatie online. Hoe voel je je erbij als je online iets twijfelachtigs tegenkomt?
- Ben je niet zeker of iets echt is, wat moet je dan doen?

Beveilig je geheimen

Wees realistisch over privacy en veiligheid

Lesoverzicht

Activiteit 1: **Hoe maak je een sterk paswoord**
Activiteit 2: **Hou het voor jezelf**
Activiteit 3: **Interland: Schattentoren**

Inleiding

Voor online privacy en beveiligingsproblemen zijn er niet altijd duidelijk goede of slechte oplossingen. Je persoonlijke en privé-informatie beschermen (alle dingen die jou 'jou' maken), betekent dat je de juiste vragen stelt en je eigen slimme antwoorden vindt.

Doelstellingen kinderen

- ✓ **Ontdekken** waarom privacy belangrijk is en hoe het zich verhoudt tot onlineveiligheid.
- ✓ **Oefenen** hoe je sterke paswoorden maakt.
- ✓ **De hulpmiddelen** en instellingen bekijken die je beschermen tegen hackers en andere bedreigingen.

Beveilig je geheimen
Woordenschat

Privacy: bescherming van je persoonlijke gegevens en die van anderen (ook wel gevoelige informatie genoemd).

Veiligheid: bescherming van de toestellen van mensen en de software die zich erop bevindt.

Tweestapsverificatie (ook wel tweefactorverificatie en tweestapsauthenticatie genoemd): een beveiligingsproces waarbij inloggen op een service twee stappen vereist. Je moet bijvoorbeeld je paswoord invoeren én een code invoeren die naar je mobiele telefoon is verzonden of een code van een app.

Paswoord of pascode: een geheime combinatie die wordt gebruikt om toegang te krijgen tot iets. Deze kan verschillende vormen aannemen. Je kunt bijvoorbeeld een viercijferige numerieke code hebben voor je telefoon en een veel complexer paswoord voor je e-mailaccount. Een vuistregel is dat je je paswoorden zo lang en ingewikkeld mogelijk moet maken als je kunt, maar ze nog altijd moet kunnen onthouden.

Versleuteling: het proces waarbij informatie of gegevens worden omgezet in een code waardoor deze onleesbaar en ontoegankelijk wordt.

Complexiteit: de mate waarin je paswoord moeilijk is samengesteld en moeilijk te achterhalen is. Dat is de bedoeling wanneer je een veilig paswoord creëert. Een paswoord is bijvoorbeeld complex als het een mix is van cijfers, speciale tekens (zoals “$” of “&”) en zowel kleine als hoofdletters.

Hacker: een persoon die computers gebruikt om ongeoorloofde toegang te krijgen tot apparaten van andere mensen of organisaties en gegevens.

Beveilig je geheimen: Activiteit 1

Hoe maak je een sterk paswoord?

Kinderen leren hoe je een sterk paswoord maakt en ervoor zorgt dat het geheim blijft.

Doelstellingen

- ✓ **Erkennen** dat het belangrijk is hun paswoorden enkel met de ouders/voogd te delen.
- ✓ **Meer weten** over paswoorden die apparaten en identiteit beschermen.
- ✓ **Begrijpen** hoe je paswoorden kan maken die moeilijk te raden zijn en die je gemakkelijk kunt onthouden.
- ✓ **De juiste beveiliging kiezen** voor aanmeldingsinstellingen en twee-factorverificatie overwegen.

Even praten

Voorkomen is beter dan genezen

Digitale technologie maakt het gemakkelijk om te communiceren met vrienden, klasgenoten, leraren en andere mensen. We kunnen op zo veel manieren contact leggen met de buitenwereld: via e-mail, sms en directe berichtjes, in woorden, via foto's en filmpjes en met behulp van telefoons, tablets en laptops. Hoe leg jij bijvoorbeeld contact met je vrienden?

Maar dezelfde tools die het ons gemakkelijk maken om informatie te delen, maken het ook voor hackers en oplichters eenvoudig om die informatie te stelen en te gebruiken om onze apparaten, onze relaties en onze reputatie te beschadigen.

Beschermen betekent eenvoudige maar slimme dingen doen, zoals schermvergrendeling op onze apparaten gebruiken, voorzichtig zijn met het plaatsen van persoonlijke informatie op apparaten die verloren of gestolen kunnen worden en vooral goede paswoorden kiezen.

- Weet iemand wat de twee meest gebruikte paswoorden zijn? (Antwoord: "1 2 3 4 5 6" en "paswoord".)
- Laten we brainstormen over enkele andere slechte paswoorden. (Voorbeelden: volledige naam, telefoonnummer, het woord 'chocolade'). Wie denkt dat dit sterke paswoorden zijn?

Activiteit

Laten we onze nieuwe vaardigheden oefenen door het paswoordspel te spelen.

1. Creëer paswoorden
Elk gezinslid krijgt 60 seconden om een paswoord te creëren.

2. Vergelijk paswoorden
Schrijf alle paswoorden op papier.

3. Stem!
Stem voor het beste en bespreek welk het sterkst is.

Lessen

Dit is een idee om een extra veilig paswoord te creëren:

- Denk aan een leuke zin die je kan onthouden. Het kan je favoriete songtekst zijn, de titel van een boek, een quote uit een film, enz.
- Kies de eerste letters of de eerste twee letters van elk woord in de zin.
- Verander enkele letters in symbolen of getallen.
- Kies enkele letters in hoofdletters en enkele in kleine letters.

Het is belangrijk en leuk om sterke paswoorden te maken!

Richtlijnen om sterke paswoorden te creëren

Dit zijn enkele tips om paswoorden te creëren waarmee je je persoonlijke info/ geheimen beschermt.

Sterke paswoorden zijn gebaseerd op een beschrijvende zin die gemakkelijk te onthouden is en moeilijk door iemand anders te raden is. Zoals de eerste letters van de woorden van een favoriete titel of lied, de eerste letters van een zin over iets wat je hebt gedaan. Sterke paswoorden bevatten een combinatie van letters, cijfers en symbolen. Een voorbeeld: “Ik ging naar de lagere school in Brussel tot mijn 12 jaar” kan gebruikt worden om een paswoord te creëren: IgNdL$iBXLt12J.

Gewone paswoorden zijn paswoorden die sterk zijn en niet gemakkelijk te raden zijn door slechte software, maar kunnen worden geraden door iemand die jou kent (bijvoorbeeld, Ik ging naar de lagere school in Brussel).

Zwakke paswoorden gebruiken gewoonlijk persoonlijke informatie, zijn gemakkelijk te kraken en kunnen worden geraden door iemand die jou kent (bijvoorbeeld “IkhouvanLisa” of “Ikhouvanchocolade”).

DO’s

- Gebruik een uniek sterk paswoord voor elk van je belangrijkste accounts.
- Gebruik minimaal acht tekens, maar liefst veel meer (zolang je ze maar onthoudt!).
- Gebruik combinaties van letters (hoofdletters en kleine letters), cijfers en symbolen.
- Zorg ervoor dat je je paswoorden kunt onthouden, zodat je ze niet moet opschrijven, wat riskant is.
- Verander je paswoord meteen als je weet of denkt dat iemand anders dan een vertrouwde volwassene het kan weten.
- Gebruik altijd sterke schermbeveiligingen op je apparaten. Stel altijd automatisch vergrendelen in, voor het geval ze in verkeerde handen terechtkomen.
- Overweeg een paswoordbeheerder, bijvoorbeeld een die ingebouwd is in je browser om je paswoorden te onthouden. Zo kun je een uniek paswoord gebruiken voor elk van je accounts en hoef je ze niet allemaal te onthouden.

DON’Ts

- Gebruik geen persoonlijke informatie (naam, adres, e-mail, telefoonnummer, RSZ-nummer, de meisjesnaam van je moeder, geboortedata, enz.) of gewone woorden in je paswoord.
- Gebruik geen paswoord dat makkelijk te raden is zoals je bijnaam, enkel de naam van je school, je favoriete voetbalteam, een cijferreeks (zoals 123456), enz. En gebruik zeker niet het woord “paswoord”!
- Deel je paswoord niet met iemand anders dan je ouders of je voogd.
- Schrijf paswoorden nooit ergens op waar iemand ze kan vinden.

Beveilig je geheimen: Activiteit 2

Hou het voor jezelf

Voor deze activiteit gebruikt u als ouder een thuisapparaat om aan te tonen waar uw kinderen moeten kijken en zoeken wanneer ze hun privacyinstellingen aanpassen.

Doelstellingen

- ✓ **Privacyinstellingen** aanpassen voor de onlinediensten die ze gebruiken.
- ✓ **Beslissingen** nemen over het delen van informatie op de sites en services die ze gebruiken.
- ✓ **Begrijpen** wat tweefactor- en tweestapsverificatie betekenen en wanneer je die moet gebruiken.

Even praten

Privacy staat gelijk aan veiligheid

Onlineprivacy en -beveiliging gaan hand in hand. De meeste apps en software bieden manieren om te bepalen welke informatie we delen en hoe.

Wanneer je een app of website gebruikt, zoek je naar een optie zoals ‘Mijn account’ of ‘Instellingen’. Hier vind je de privacy- en beveiligingsinstellingen waarmee je kan beslissen:

- Welke informatie zichtbaar is op je profiel.
- Wie berichten, foto’s, filmpjes of andere inhoud die je deelt, kan bekijken.

Door deze instellingen te leren gebruiken om je privacy te beschermen en up-to-date te houden, ben je zo veilig mogelijk online.
Het is belangrijk dat je steeds afspreekt met ouders of voogd om deze instellingen aan te passen.

Activiteit

Wat je nodig hebt:

- Een toestel thuis waarmee u een voorbeeld kunt geven van wat geschikt geacht wordt voor kinderen (bijv. uw eigen e-mailaccount of die van uw kinderen).

1. Verificatieopties

Ik heb mijn laptop aangesloten op het projectiescherm. Laten we naar de instellingenpagina van deze app gaan. Hier zie je de keuzemogelijkheden:

- Je paswoord wijzigen
- Waarschuwingen ontvangen als iemand probeert in te loggen bij je account vanaf een onbekend apparaat
- Je onlineprofiel maken, inclusief foto’s en filmpjes, alleen zichtbaar voor de door jou gekozen groepen familieleden en vrienden
- Tweefactorauthenticatie of tweestapsverificatie inschakelen

2. Aanvullende verificatieopties

Laten we het hebben over tweestaps- en tweefactorverificatie.

- Tweestapsverificatie: wanneer je je aanmeldt op je account, zijn er twee stappen nodig. Zo moet je bijvoorbeeld je paswoord invoeren EN ontvang je een code per sms die je binnen de 10 minuten moet invoeren voordat ze vervalt.
- Tweefactorverificatie: dit systeem vereist twee soorten informatie om je aan te melden. Het kan bijvoorbeeld vragen om je normale paswoord en vingerafdruk.

Welke privacy- en beveiligingsinstellingen zijn geschikt voor jou? Dat is iets om te bespreken met je ouder of voogd. Maar vergeet niet dat de belangrijkste beveiligingsinstelling in je hoofd zit: jij neemt de belangrijkste beslissingen over hoeveel, wanneer en met wie je persoonlijke gegevens wilt delen.

Lessen

Een sterk, uniek paswoord voor elk van je belangrijke accounts kiezen, is een goede eerste stap. Nu moet je ze onthouden en ook beveiligen.

Je paswoorden opschrijven is niet per se een slecht idee. Maar doe je dit, laat dan geen papiertje met je paswoorden rondslingeren (bijvoorbeeld op je computer of bureau). Beveilig de lijst en bescherm jezelf door hem ergens te verbergen.

Beveilig je geheimen: Activiteit 3

Interland: Schattentoren

HELEEEEP! De toren is niet op slot, waardoor de waardevolle spullen van de Internaut, zoals persoonlijke informatie en paswoorden, een hoog risico lopen. Ontloop de hacker en bouw bij elke stap een onaantastbaar paswoord... om je geheimen voor eens en voor altijd te beveiligen.

Open een webbrowser op je desktop en surf naar www.cybersimpel.be/interland en ga naar de Schattentoren.

Even praten

Laat uw kinderen de Schattentoren spelen en gebruik onderstaande vragen om te bespreken wat ze geleerd hebben in de game. De meeste kinderen hebben er het meest aan wanneer ze alleen spelen. Het kan ook zinvol zijn voor jonge kinderen om het samen te spelen.

- Wat zijn de elementen van een supersterk paswoord?
- Wanneer is het belangrijk om in het echte leven sterke paswoorden te creëren? Welke tips heb je geleerd over hoe je dit kan doen?
- Wat is een hacker? Beschrijf het gedrag van dit personage en hoe hij het spel beïnvloedt.
- Ga je je gegevens door de Schattentoren anders beschermen in de toekomst?
- Noem iets dat je anders gaat doen nadat je deze lessen hebt geleerd en het spel hebt gespeeld.
- Maak drie oefenpaswoorden die ‘supersterk’ zijn.
- Geef enkele voorbeelden van gevoelige informatie die je moet beschermen.

Thema 04: Wees cyber vriendelijk

Vriendelijk zijn is cool

De kracht van positiviteit op het internet

Lesoverzicht

Activiteit 1: **Van omstaander naar beschermer**
Activiteit 2: **Een toontje lager**
Activiteit 3: **De daad bij het woord**
Activiteit 4: **Interland: Koninkrijk der Vriendelijkheid**

Inleiding

De digitale wereld houdt nieuwe uitdagingen en kansen in voor sociale interactie, zowel voor kinderen als voor ieder van ons. Sociale signalen vang je online niet zo makkelijk op. Voortdurend verbonden zijn, kan zowel een comfortabel gevoel als angst teweegbrengen, en anonimiteit kan een stimulans zijn voor verliefdheid en complimentjes maar kan ook jezelf en anderen kwetsen.

Het is nogal ingewikkeld, maar we weten dat het internet zowel vriendelijkheid als negativiteit kan versterken. Leren vriendelijk zijn en empathie overbrengen is essentieel voor het opbouwen van gezonde relaties en het verkleinen van het gevoel van isolement. Het gevoel van isolement zou soms kunnen leiden tot pesten, depressie, leer- en andere problemen. Daarom is het ook belangrijk te leren hoe je reageert op negativiteit en intimidatie.

Onderzoek toont aan dat, in plaats van simpelweg te zeggen dat kinderen online niet negatief mogen zijn, doeltreffende lessen in online bescherming de onderliggende oorzaken van negatief gedrag aanpakken. Deze activiteiten moedigen kinderen aan om vanaf het begin positief te communiceren en leren hen omgaan met negativiteit wanneer ze ermee in aanraking komen.

Doelstellingen kinderen

- ✓ **Bepalen** wat positief zijn op het internet betekent.
- ✓ **Positiviteit uitdragen** in onlinecommunicatie.
- ✓ **Situaties identificeren** waarin je een vertrouwde volwassene zou moeten aanspreken.

Vriendelijk zijn is cool
Woordenschat

Pesten: doelbewust, gemeen gedrag dat gewoonlijk herhaald wordt. Het doelwit heeft het vaak lastig om zichzelf te verdedigen.

Cyberpesten: pestgedrag online of via digitale apparaten.

Intimidatie: een meer algemene term dan pesten die vele vormen kan aannemen (zoals lastigvallen, ergeren, intimiteren, vernederen, enz.) en ook online kan gebeuren.

Conflict: een argument of meningsverschil dat niet noodzakelijkerwijs wordt herhaald.

Agressor: de persoon die pest of intimideert; ook soms de “pestkop” genoemd, experts in het voorkomen van pestgedrag raden aan mensen nooit zo te noemen.

Doelwit: de persoon die wordt gepest of het slachtoffer is.

Omstaander: iemand die de mogelijkheid heeft om in te grijpen of slecht gedrag te melden, maar niets doet om het te stoppen.

Beschermer: een getuige van intimidatie of pestgedrag die het doelwit privé of openlijk steunt, en soms het incident waarvan hij of zij getuige is probeert te verhinderen en/of melden.

Uitvergroten: Iets luider of sterker laten klinken.

Uitsluiting: Het gevoel dat je niet bij een groep hoort.

Blokkeren: een manier om alle contacten met een andere persoon online te verbreken, door te voorkomen dat die persoon toegang krijgt tot je profiel, jou berichten stuurt, je posts kan bekijken, enz. zonder die persoon daarvan te verwittigen (niet altijd ideaal in een context van pesten waarbij het doelwit wilt weten wat de agressor zegt of wanneer het pesten ophoudt).

Muten: minder definitief dan blokkeren. Muten betekent dat je posts, commentaren, enz. van de ander niet meer ziet in je socialemediafeed wanneer die berichten vervelend worden - zonder dat die persoon op de hoogte wordt gebracht of dat zijn feed wordt gedempt (niet zinvol bij pesten).

Anoniem: een naamloze of onbekende persoon; iemand online van wie je de naam of identiteit niet kent.

Trolling: een bericht of commentaar posten online op een manier die doelbewust wreed, beledigend of provocerend is.

Misbruik melden: onlinehulpmiddelen of -systemen van sociale media gebruiken om intimidatie, pesten, bedreigingen, en andere schadelijke inhoud te melden die doorgaans in strijd is met de servicevoorwaarden of communitystandaarden van de service.

Vriendelijk zijn is cool: Activiteit 1

Van omstaander naar beschermer

Kinderen oefenen in het herkennen van de vier rollen bij pesterijen (de pester, het doelwit van de pester, de omstaander en de beschermer) en wat ze moeten doen als ze een omstaander of doelwit zijn.

Doelstellingen

- ✓ Situaties van intimidatie of pestgedrag online **identificeren**.
- ✓ **Evalueren** wat het betekent om een omstaander of beschermer te zijn online.
- ✓ Specifieke manieren **leren** om te reageren op pesten als je het ziet.
- ✓ **Weten** hoe je je moet gedragen als je je geïntimideerd voelt.

Even praten

Waarom is vriendelijk zijn zo belangrijk?
Soms is het belangrijk om onszelf eraan te herinneren dat er achter elke gebruikersnaam en avatar een echte persoon met echte gevoelens zit, en we moeten hen ook op die manier behandelen. Als pesten of ander ongepast gedrag zich voordoet, zijn er meestal vier soorten mensen bij betrokken:

- De agressor, of de persoon die pestgedrag vertoont.
- Er is ook iemand die wordt gepest. Dat is het doelwit.
- Er zijn getuigen van wat er zich afspeelt, gewoonlijk omstaanders genoemd.
- Er zijn getuigen van wat er zich afspeelt die positief proberen op te treden, vaak beschermers genoemd.

Ben je zelf het doelwit van pesterijen of ander gemeen gedrag online, dan kun je deze dingen doen:

Ben ik het doelwit, dan kan ik…

- Niet antwoorden.
- De persoon blokkeren.
- De persoon melden. Het vertellen aan een ouder, leerkracht, broers of zussen of iemand anders die ik vertrouw en de meldingsprogramma's in de app of service gebruiken om het intimiderende bericht, de reactie of de foto te melden.

Als je jezelf een omstaander vindt bij intimidatie of pesterijen, dan kun je ingrijpen en wreed gedrag melden . Soms proberen omstaanders het pesten niet te stoppen of het doelwit te helpen. Wanneer ze dat wel doen, worden ze een beschermer. Je kunt ervoor kiezen een beschermer te zijn door te beslissen gemeen gedrag niet te steunen en op te komen voor vriendelijkheid en positiviteit. Met een beetje positiviteit kom je online al een heel eind. Het kan gebeuren dat negativiteit zich verspreidt en uitmondt in wreedheid en schade berokkent.

Als ik de omstaander ben, kan ik een beschermer zijn door...

- Een manier te vinden om vriendelijk te zijn of steun te geven aan het doelwit.
- Het gemene gedrag melden in een comment of een reply (denk eraan om het gedrag en de persoon te melden), als je je daar goed bij voelt en denkt dat het veilig is.
- Beslissen de agressor niet te helpen om het pesten te verspreiden of erger te maken door een gemene post of onlinecommentaar te delen.
- Een boel vrienden overtuigen om een 'stapel van vriendelijkheid' te maken door een heleboel vriendelijke berichten te posten over het doelwit (maar niets gemeens over de agressor, omdat jij het goede voorbeeld geeft en geen wraak neemt).
- De intimidatie melden. Het vertellen aan iemand die kan helpen zoals een ouder, een leerkracht of een vertrouwenspersoon op school.

Activiteit

Wat je nodig hebt:

- Hand-out: werkblad "Van omstaanders naar beschermers" werkblad

Antwoorden op het werkblad "Van omstaanders naar beschermers":

Scenario 1: O, B, O (omdat je de situatie niet vooruithelpt), B, B

Scenario 2: B, O, B, B

Scenario 3: B, B, O, O, B

Scenario 4: de antwoorden kwamen helemaal van jou!

1. Lees de scenario's en rangschik de antwoorden

Na het bespreken van de rollen, deelt u het werkblad uit en geeft u uw kinderen 15 minuten de tijd om de drie scenario's te lezen en elk antwoord te rangschikken.

2. Bespreek de antwoorden vóór of na de discussie

Vraag hen of ze u kunnen vertellen waarom het leuk kan zijn beschermers te hebben online en op school.

3. Bespreek de antwoorden die moeilijk te rangschikken waren

Vraag uw kinderen of sommige antwoorden moeilijk te rangschikken waren en waarom. Bespreek dit.

Lessen

Of je nu opkomt voor anderen, iets kwetsend meldt, of iets negeert om te vermijden dat het nog wordt uitvergroot, je kunt uit een aantal strategieën kiezen afhankelijk van de situatie. Met een beetje vriendelijkheid kan iedereen een groot verschil maken om negatieve situaties om te buigen naar positieve situaties.

Werkblad: Activiteit 1

Van Omstaander naar Beschermer

Dus nu weet je dat een omstaander zijn krachten positief kan gebruiken en een beschermer kan zijn door iemand die gepest wordt te helpen. Hieronder staan drie scenario's die voorbeelden zijn van onlinepesten of -intimidatie. Als je wilt, maak je een vierde scenario van iets dat gebeurd is met mensen die je kent en verzin je antwoorden van zowel beschermers als omstaanders. Voor elk van de drie reeds gemaakte scenario's is er een lijst met antwoorden. Lees elk antwoord en beslis of het is wat een omstaander zou doen of wat een beschermer zou doen. Noteer dan een "O" voor "omstaander" of een "B" voor "Beschermer" in het witte vakje naast het antwoord.

Scenario 1

Een vriendin van jou liet haar telefoon vallen aan de drinkwaterfontein bij het voetbalveld van de school. Iemand heeft hem gevonden en een heel gemene boodschap over een andere leerling gestuurd naar een aantal mensen in haar voetbalteam en dan de telefoon teruggelegd aan de drinkwaterfontein. De leerling die het doelwit was, vertelde jouw vriendin dat ze een vreselijk iemand is omdat ze dat bericht heeft verzonden, ook al heeft zij het niet verzonden. Niemand weet wie het gemene bericht heeft gestuurd. Jij…

- ☐ ... voelt je slecht in de plaats van je vriendin, maar je doet niets omdat niemand weet wie haar die loer heeft gedraaid.
- ☐ ... gaat naar het doelwit en vraagt haar hoe ze zich voelt en of je kunt helpen.
- ☐ ... verspreidt het gemene verhaal door het te delen met andere vrienden.
- ☐ ... en je vriendin overtuigen iedereen van het voetbalteam om complimenten te posten over het doelwit.
- ☐ ... en je vriendin melden het incident anoniem aan de directeur, met de boodschap dat iedereen het moet hebben over een goede telefoonbeveiliging en het vergrendelen van hun telefoon.

Scenario 2

Je leerkracht heeft een klasblog gemaakt voor talen, waarop de klas commentaren kan schrijven, bewerken en posten. De volgende dag is de leerkracht ziek en de vervanger merkt niet dat het fout loopt in de klasblog: iemand post echt gemene berichten over een van je medeleerlingen. Jij…

- ☐ ... geeft commentaar op de commentaren door dingen te zeggen als “Dit is niet zo cool” en “Ik ben de vriend van _____ en het is allemaal niet waar.”
- ☐ ... negeert het tot de leerkracht terugkeert.
- ☐ ... overtuigt andere leerlingen om vriendelijke berichten en complimenten te posten over het doelwit.
- ☐ ... vertelt de vervanger dat sommige leerlingen zich gemeen gedragen in de klasblog en dat ze dit misschien aan de leerkracht moet melden.

Scenario 3

Er is een onlinegame die heel wat vrienden van jou spelen. Meestal gaat de chat in de game over wat er in de game gebeurt. Soms gaat het er wat gemeen aan toe, maar doorgaans is dat niet meer dan gezonde rivaliteit onder vrienden. Maar die ene keer begint een speler echt gemene dingen te zeggen over een van je vrienden die ook aan het spelen is en hij wil echt niet stoppen. Ook de volgende dag gaat hij ermee door. Jij…

- ☐ ... belt je vriend op en vertelt hem dat je dit ook helemaal niet leuk vindt en vraagt hem wat hij denkt dat jullie beiden best zouden doen.
- ☐ ... belt iedereen die je kent die met jullie gamet (en je zorgt ervoor dat je vriend weet dat je dit doet) om te zien of iedereen het eens is dat het tijd is om te zeggen dat iemand gemeen doet.
- ☐ ... beslist af te wachten tot dat andere kind stopt en dan misschien iets te ondernemen.
- ☐ ... verlaat de game een tijdje.
- ☐ ... bekijkt de communityregels van de game en als pesten niet is toegestaan, meld je het gemene gedrag via het meldsysteem van de game.

Scenario 4

Creëer een scenario uit het echte leven op basis van een situatie waar een van jullie al over heeft gehoord. Bedenk dan een reactie van zowel een omstaander als van een beschermer om te tonen hoe goed je snapt waar we het nu over hebben!

Vriendelijk zijn is cool: Activiteit 2

Een toontje lager

Kinderen interpreteren de emoties achter sms'jes om kritisch te leren denken en om een verkeerde interpretatie en conflicten bij onlinecommunicatie te voorkomen.

Doelstellingen

- ✓ **De juiste beslissingen nemen** wanneer je kiest hoe en wat je communiceert.
- ✓ **Situaties herkennen** waarin het beter is te wachten tot je oog in oog staat met iemand, dan meteen een tekst of bericht te verzenden dat misschien verkeerd kan geïnterpreteerd worden.

Even praten

Dingen worden al snel verkeerd begrepen
Jongeren gebruiken verschillende communicatievormen door elkaar, maar onlineberichten kunnen anders worden geïnterpreteerd dan face-to-face of via de telefoon.

Ben je ooit verkeerd begrepen geweest online? Heb je bijvoorbeeld ooit een grapje gemaakt en nam je vriend jou serieus of vond hij jou zelfs gemeen?

Heb je zelf iemand anders in een sms of chat ooit verkeerd begrepen? Wat heb je gedaan om de communicatie te verduidelijken? Wat zou je anders kunnen doen?

Activiteit

Wat je nodig hebt:

- Voorbeelden van tekstberichten op het bord geschreven of geprojecteerd

1. Berichten beoordelen
Laten we deze voorbeelden van tekstberichten op het bord bekijken. Uw kinderen hebben vast ook geweldige voorbeelden. Noteer er wat extra om over te praten.

- "Dat is zo cool".
- "Whatever".
- "Ik ben zo kwaad op jou".
- "BEL ME NU".
- "Oké, chill".

2. Lees de berichten hardop
Voor elk bericht gaan we nu één persoon vragen het hardop te lezen op een specifieke toon (😕 🙃 😀). Wat valt je op? Hoe kan dit overkomen bij andere mensen? Hoe kan een 'afzender van berichten' beter communiceren wat hij echt bedoelt?

Lessen

Uit wat iemand schrijft of sms't kan je moeilijk afleiden hoe die persoon zich voelt. Zorg ervoor dat je de juiste manier kiest voor je volgende bericht en ook dat je niet te veel zoekt achter dingen die mensen online tegen je zeggen. Ben je niet zeker wat iemand bedoelde, vraag het die persoon dan persoonlijk of aan de telefoon.

Vriendelijk zijn is cool: Activiteit 3

De daad bij het woord

Kinderen bespreken hoe ze ook het gedrag van volwassenen kunnen beïnvloeden.

Doelstellingen

- ✓ **Nadenken** over onlinegedrag van volwassenen.
- ✓ **Voorspellen** hoe de manier waarop volwassenen reageren het gedrag van de jongere generaties kan vormgeven.

Even praten

Wat kunnen volwassenen leren aan kinderen en wat kunnen kinderen aan volwassenen leren? Het is belangrijk om kinderen vriendelijkheid bij te brengen. Maar het is al even belangrijk om onze lessen in vriendelijkheid vorm te geven. Er zijn een heleboel voorbeelden waaruit blijkt dat pesten en intimidatie niet enkel betrekking hebben op kinderen.

Kijk maar eens hoe volwassenen elkaar online, in nieuwsmedia of in het verkeer behandelen. We hebben al gepraat over hoe belangrijk het is om vriendelijk te zijn tegen je klasgenoten en vrienden on- en offline. Heb je ooit volwassenen gezien die gemeen deden tegen elkaar, in het gewone leven of in de media? Heb je al volwassenen gezien die elkaar pesten? (Je hoeft geen namen te noemen, laten we enkel praten over gedrag.)

Denk je dat jouw generatie een internet kan creëren dat vriendelijker en positiever is dan de omgeving die sommige volwassenen rondom zich hebben gecreëerd? (Veel volwassenen denken waarschijnlijk ook dat jij hier beter in bent dan zij.)

Denk je dat sommige kinderen pestgedrag vertonen of onvriendelijke opmerkingen beginnen te maken omdat ze volwassenen rondom zich of in het nieuws net hetzelfde zien doen? Antwoord je ‘ja’ op al deze vragen? Geef enkele voorbeelden. Wat zou JIJ doen in de plaats? Hoe zou jij een beter rolmodel kunnen zijn voor volwassenen?

Lessen

Hoe jij en je vrienden elkaar online behandelen, zal een grote impact hebben op de digitale wereld die jouw generatie opbouwt en zeker ook op de offlinewereld.

Vriendelijk zijn is cool: Activiteit 4

Interland: Koninkrijk der Vriendelijkheid

Roddels kunnen besmettelijk zijn, zowel positief als negatief.

In de zonnigste hoek van het land lopen cyberpesters rond die overal negativiteit verspreiden. Blokkeer en rapporteer pestkoppen, maar wees wel vriendelijk tegen andere internetgebruikers om de vrede in dit land te herstellen.

Open een webbrowser op je desktop en surf naar www.cybersimpel.be/interland en ga naar het Koninkrijk der Vriendelijkheid.

Even praten

Laat je kinderen het Koninkrijk der Vriendelijkheid spelen en gebruik onderstaande vragen om te bespreken wat ze geleerd hebben in de game.

- Welk scenario in het Koninkrijk der Vriendelijkheid ligt jou het best en waarom?
- Beschrijf een moment waarop je actie hebt ondernomen om vriendelijkheid online te verspreiden.
- In welke situatie zou het gepast zijn iemand online te blokkeren?
- In welke situatie zou het gepast zijn iemands gedrag te melden?
- Waarom denk je dat het personage in het Koninkrijk der Vriendelijkheid een agressor wordt genoemd? Beschrijf de eigenschappen van dit personage en hoe zijn acties het spel beïnvloeden.
- Heeft het spel de manier veranderd waarop jij je in de toekomst tegenover anderen zal gedragen? Zo ja, hoe?

Praat erover als je twijfelt

Moedig gedrag online definiëren en stimuleren

Lesoverzicht

Activiteit 1: **Wanneer hulp inroepen**
Activiteit 2: **Meld het ook online**

Inleiding

Het is belangrijk dat kinderen snappen dat ze niet alleen zijn wanneer ze content online zien waarbij ze zich ongemakkelijk voelen. Vooral wanneer het lijkt alsof ze zelf kunnen gekwetst raken of iemand anders kan gekwetst raken. Ze mogen nooit aarzelen om hulp te vragen aan iemand die ze vertrouwen. Het is ook goed dat ze weten dat er verschillende manieren bestaan om moedig te zijn en actie te ondernemen, van dingen uitpraten online tot het gebruiken van meldingstools online.

Doelstellingen kinderen

- ✓ **Begrijpen** in welk soort situaties je hulp moet inroepen of erover praten met een volwassene die je vertrouwt.
- ✓ **Bedenk** welke mogelijkheden er zijn om moedig te zijn online en waarom volwassenen bij het gesprek betrekken belangrijk is.

Praat erover als je twijfelt
Woordenschat

Dapper: moedig; niet noodzakelijk onverschrokken, want mensen zijn heel moedig wanneer ze bang of nerveus zijn maar ze reageren toch positief.

Gehackte account: een online-account dat door iemand anders is overgenomen, zodat je er zelf geen controle meer over hebt.

Leerlingenbemiddeling: een stap verder dan een leerling die erover praat, is leerlingenbemiddeling, om zaken aan te pakken of te veranderen; ook opkomen voor jezelf en anderen; vaak beschouwd als een essentieel onderdeel van burgerschap.

Vertrouwen: sterke overtuiging dat iets of iemand betrouwbaar, oprecht of bekwaam is.

Praat erover als je twijfelt: Activiteit 1

Wanneer hulp inroepen

Een advies dat steevast terugkeert in alle lessen geldt voor elke online-activiteit: komen kinderen iets tegen waarbij ze zich ongemakkelijk voelen of erger, moedig hen dan aan om erover te praten. Ze moeten moedig zijn en erover praten met iemand die ze vertrouwen en hen kan helpen, ook u, de directeur of een leerkracht. Kinderen moeten natuurlijk ook leren moedig te zijn en om hulp te vragen. Om ze hierbij te helpen stelt deze activiteit een gesprek voor in uw gezin rond het principe “erover praten als je twijfelt”. Hieronder vindt u een lijst met situaties waarin het uitpraten echt kan helpen.

Belangrijke opmerkingen

1. *Kinderen worden al vele generaties lang onderwezen of geconditioneerd niet te ‘verklikken’, zodat dit is uitgegroeid tot een sociale norm. Experts in het voorkomen van pestgedrag hebben hard gewerkt om kinderen het verschil te helpen inzien tussen het ‘vertellen’ en hulp inroepen. Help uw kinderen inzien dat steun zoeken wanneer er online kwetsende dingen gebeuren, niet hetzelfde is als ‘verklikken’. Het gaat om hulp zoeken voor zichzelf of voor klasgenootjes wanneer iemand gekwetst wordt.*

2. *Bevorder open communicatie en herinner kinderen eraan dat u er altijd bent om hen te steunen en om het op de juiste manier te melden.*

3. *In onderstaande discussie moet u ervoor zorgen dat telkens als kinderen iets delen over momenten dat ze hulp van een volwassene hebben gezocht, het gesprek zo verloopt dat ze zich trots voelen en moedig dat ze iets hebben ondernomen.*

Doelstellingen

- ✓ **Erkennen** dat hulp zoeken voor jezelf of anderen een teken is van sterkte.
- ✓ **Hardop nadenken** over situaties waarin erover praten echt kan helpen.

Even praten

Dit is een lijst met situaties waarin je online kan terechtkomen. We kunnen ze misschien niet allemaal bekijken, want ik hoop dat je zal vertellen wanneer iets op die lijst jou doet denken aan een situatie waarin je terechtkwam en wat je toen hebt gedaan. Zo kunnen we samen over die situaties praten.

Even praten

1. **Vraag uw kinderen** om de lijst in stilte te lezen. Terwijl ze dat doen, vraagt u hen om na te denken of een van deze situaties hen ooit is overkomen, of ze hulp zouden vragen als ze in een van deze situaties terechtkwamen en of ze het al dan niet hebben gedaan.
   - Je had het vermoeden dat je account werd gehackt. (Discussiemogelijkheid: wat kun je doen om je account nog beter te beveiligen?)
   - Je had hulp nodig om je paswoord te onthouden.
   - Je wist niet zeker of iets al dan niet oplichting was, of dat je er misschien was ingetrapt. (Discussiemogelijkheid: wat zijn de waarschuwingssignalen?)
   - Iemand probeerde online iets met jou te bespreken waarbij je je ongemakkelijk voelde.
   - Je ontving een akelig bericht of commentaar van een onbekende. (Discussiemogelijkheid: wat maakt iets akelig?)
   - Je wilde iets bespreken dat iemand online vertelde en echt aardig OF echt gemeen was.
   - Je was bezorgd dat je misschien iets had gedeeld online wat niet mocht. Vertel ons enkel wat het was als je je er goed bij voelt om dat te delen, maar als je dat niet doet, vertel ons dan toch maar hoe je erop reageerde.
   - Je stelde vast dat een klasgenoot een andere leerling online kwetste.
   - Je zag dat iemand ermee dreigde te vechten of iemand te kwetsen.
   - Iemand creëerde een fake profiel van een andere leerling.
   - Je was bezorgd over een andere leerling door iets wat gepost of ge-sms't werd. (Discussiemogelijkheid: soms is het moeilijk en dreig je je vriend boos te maken, maar is zijn veiligheid en welzijn niet belangrijker?)

2. **Vraag uw kinderen** om te vertellen wat ze (niet) deden en waarom.

3. Laat ons over die situaties **praten.**

Lessen

Het lijkt misschien niet altijd zo, maar hulp inroepen als je niet zeker bent is moedig. Als je dat doet om jezelf of anderen te beschermen of te voorkomen dat je zelf of iemand anders gekwetst wordt, dat ben je tegelijk slim en moedig.

Praat erover als je twijfelt: Activiteit 2

Meld het ook online

Door een thuisapparaat te gebruiken om te tonen waar ze ongepaste inhoud en gedrag moeten melden in apps, bekijken u en uw kinderen diverse soorten inhoud, beslissen jullie of het moet gemeld worden en praten jullie over het waarom.

Doelstellingen

- ✓ **Zich bewust zijn** van de onlinetools om misbruik te melden.
- ✓ **Overwegen** wanneer je ze moet gebruiken.
- ✓ **Praten** over waarom en wanneer je misbruik moet melden.

Even praten

Wanneer er online gemene en andere ongepaste zaken opduiken, dan hebben mensen verschillende mogelijkheden om te reageren. In de laatste activiteit hadden we het over de belangrijkste mogelijkheid: erover praten met iemand die je vertrouwt. Een andere mogelijkheid is het melden aan de app of service waar je de inhoud hebt aangetroffen. Dit kan helpen om de inhoud te verwijderen. Het is belangrijk om onlinemeldingstools te leren gebruiken.

Kinderen moeten het gewoon worden om een screenshot te nemen van gesprekken of activiteiten die kwetsend of verdacht zijn alvorens de blokkerings- en meldingstools te gebruiken (anders is de activiteit misschien niet meer zichtbaar). Dit zorgt ervoor dat vertrouwde volwassenen kunnen zien wat er is gebeurd en het probleem kunnen helpen oplossen.

Activiteit

Wat je nodig hebt:

- Hand-out: werkblad “Meld het ook online!”

1. Zoek hoe je een probleem meldt

Neem zo veel mogelijk apparaten waarover je thuis beschikt. Zoek samen de tools in minstens drie thuisgerelateerde accounts om ongepaste inhoud of gedrag te melden.

2. Bekijk de scenario’s

Bekijk zeven situaties op het werkblad.

3. Zou je dit melden?

Vraag kinderen om te vertellen of zij deze inhoud zouden melden. Vraag hen ook om te vertellen waarom ze iets al dan niet zouden melden.

4. Zo ja, waarom?

Er is niet één juiste reactie of aanpak. Zorg ervoor dat kinderen dit weten voor u met hen de discussie start.

Lessen

De meeste apps en apparaten hebben tools om ongepaste inhoud te melden en/of te blokkeren, en het kan de betrokken mensen, hun community en de platformen zelf helpen als we die tools gebruiken. Voor je ongepaste inhoud blokkeert of meldt, is het altijd verstandig om een screenshot te nemen zodat je een bewijs hebt.

Werkblad: Activiteit 2

Meld het ook online

Laat uw kinderen elk van de onderstaande scenario's lezen en vraag hen of ze het zouden melden aan de app of service waarin ze ze hebben aangetroffen. Laat hen voorbereiden en uitleggen waarom ze het al dan niet zouden melden en bespreek daarna die keuzes.

Opmerking: er is niet één juiste keuze en daarom is erover discussiëren zinvol.
Niemand mag zich slecht voelen over de gemaakte keuze. Zelfs volwassenen weten niet altijd wanneer of hoe ze iets moeten melden.

Situatie1	Een leerling post een groepsfoto op een publieke account en jij haat de manier waarop je op de foto staat. Zou je die foto melden of niet? Hoe kun je reageren?
Situatie 2	Iemand maakt een account aan van een leerling en gebruikt diens naam en foto. Die persoon heeft een meme gemaakt van de foto en er een snor en andere vreemde gezichtskenmerken bij getekend, waardoor de foto een grap lijkt. Zou jij de account melden of niet?
Situatie 3	Iemand post een heleboel gemene commentaren over een leerling uit jouw school zonder diens naam te gebruiken, maar jij denkt te weten over wie het gaat. Zou jij die commentaren melden of niet?
Situatie 4	Een leerling creëert een account met de naam van je school in de schermnaam en post foto's van leerlingen met commentaren over iedereen. Sommige zijn complimenten, andere zijn gemeen tegenover leerlingen. Meld je de gemene commentaren, de hele account of beide?
Situatie 5	Op een nacht merk je dat een leerling online een commentaar heeft gepost met de mededeling dat ze de volgende dag gaan vechten met een andere leerling in de eetzaal. Meld je dat onlinecommentaar of niet? Meld je het bij de leerkracht of directeur de volgende dag of niet? Of beide?
Situatie 6	Je bekijkt een cartoonfilmpje en plots verschijnt er vreemde inhoud die duidelijk niet geschikt is voor kinderen en je voelt je er ongemakkelijk bij. Meld je het of niet?
Situatie 7	Je speelt een onlinespel met vrienden en iemand die niet meespeelt, begint met jou te chatten. Die persoon is niet gemeen of zo, maar je kent hem niet. Negeer je die persoon of meld je het?

Dit document valt onder de Creative Commons Naamsvermelding 4.0 Internationale Publieke Licentie.

BONUS

BONUS

5 minuten voorbereidingstijd met volwassenen
1 uur activiteit voor de kinderen

8 tot 14 jaar

Teken de scherm kaart bij jullie thuis

Hoeveel schermen zijn er bij jullie thuis? Hoe worden ze elke dag gebruikt? Via deze eerste activiteit worden jullie bewust van alle digitale apparaten in het huis en van jullie relatie met deze schermen. Zo zetten jullie de eerste stap naar digitaal burgerschap.

Doelstellingen

- **Verken** de verschillende manieren waarop jullie toestellen worden gebruikt.
- **Neem** een kritische houding aan ten opzichte van jullie relatie tot de schermen.
- **Stel** de impact dat technologie heeft op jullie gezondheid en op jullie relatie met anderen in vraag.
- Laat je **creativiteit** de vrije loop.
- **Structuration et vision** de l'espace

Activiteit

Benodigdheden:

- Een zo groot mogelijk blad (A2/A3 of groter) of meerdere A4 bladen om aan elkaar te hangen
- Kladpapier
- Stiften en kleurpotloden
- Lijm en een schaar

1. Begin met het maken van een inventaris

Hoeveel schermen zijn er in huis? Waarvoor dienen deze schermen?
Zie de tabel hieronder ter inspiratie:

Schermen	Voor wie en om wat te doen?
2 pc's	Ouders - om te werken Kind 1 - Om te spelen Kind 2 - Om lessen te volgen ...
1 Tablet	Papa - Om de krant te lezen Kind 1 - Om te spelen...
3 Smartphones (ouders, kind 2)	Iedereen - Communiceren met familie en vrienden (Whatsapp, Instagram...) Kind 2 - Om naar muziek te luisteren
1 Televisie	Iedereen - Ontspanning & informatie ....

Het is uiteraard mogelijk om andere antwoorden in de tabel te schrijven afhankelijk van de verschillende gezinsleden. In dat geval gebruik je best een verschillend kleur voor elk gezinslid. Discussieer vervolgens de verschillende gebruikswijzen van de schermen: sommigen gebruiken de computer enkel om te werken, anderen gebruiken de smartphone enkel om te bellen en met anderen te communiceren en nog anderen enkel om te spelen.
Werden er tijdslimieten bepaald voor sommige schermen? Zijn er momenten waarop het verboden is om de schermen te gebruiken?

Vervolg op de volgende pagina →

2. Maak jullie schermkaart

Teken op het grote blad jullie gezin of huis in het midden. Jullie kunnen er ook een foto opkleven. Teken vervolgens in elke hoek van het blad de verschillende schermen in jullie huis.

Teken of schrijf rond elk scherm je gebruikswijze van de schermen die jullie in de eerste oefening hebben opgelijst. Jullie mogen foto's, smileys, logo's van sociale media of zoekmachines, etc. gebruiken. Wees creatief!

Verbind daarna elk gezinslid met de verschillende schermen die ze gebruiken en de manier waarop ze dat scherm gebruiken. Je kan verschillende kleuren gebruiken per gezinslid.
Jullie kunnen ook de tijdslimiet waarmee een scherm wordt gebruikt erbij zetten en/of zinnetjes over hoe jij je voelt wanneer je een bepaald scherm gebruikt, waar je van houdt of waar je niet van houdt (bvb.: "Ik speel graag op mijn gsm, dat ontspant me", "ik hou niet van een computer, want daar begrijp ik niets van", etc.). Voilà, jullie schermkaart is klaar! Hoe kleurrijker en plezant jullie schermkaart is, hoe liever jullie ze thuis willen ophangen.

Trots op jullie schermkaart? Stuur dan snel een foto door naar cyberhelden@bibzondergrenzen.be of gebruik #cyberhelden op Instagram, Facebook of TikTok