

Filters en controlesystemen

Om kinderen te beschermen tegen ongepaste inhoud op het internet lijkt het een goed idee om een filter te installeren. En toch ... Filters zijn niet altijd betrouwbaar en ze zijn niet echt de ideale oplossing. Want hoewel ze pornografische websites relatief doeltreffend blokkeren, scoren ze maar ondermaats waar het andere twijfelachtige inhoud betreft...

Hoe werken die filters?



Filtersoftware doet het volgende:

- ofwel de toegang verhinderen tot websites die op een 'zwarte lijst' staan, opgesteld door de uitgever van de software of de gebruiker zelf
- ofwel adressen of inhoud blokkeren die ongewenste woorden bevatten (filtering op basis van trefwoorden)
- ofwel geven ze enkel toegang tot bepaalde websites die de gebruiker heeft gekozen, volgens het omgekeerde principe van de zwarte lijst: de 'witte lijst' die de opgegeven websites toelaat. Natuurlijk beperkt deze optie de toegang tot het internet aanzienlijk.

Deze software kan worden gebruikt in besturingssystemen (OS, Windows, Linux,...), maar ook in de browsers

(Explorer, Chrome, Safari, Firefox,...).

Filtersystemen zitten nu trouwens ook in software en andere apparaten dan de computer (tablets, smartphones, gameconsoles, digitale tv,...).

Werken ze echt?

Hoewel je met filters ongewenste inhoud zoals reclame kunt blokkeren, zijn ze nooit 100% doeltreffend. Er is geen enkele technische barrière die kan voorkomen dat kinderen op ongepaste inhoud stuiten. Op het internet, terwijl ze profielen aanmaken of films downloaden, kunnen jongeren pornografische, racistische of gewelddadige inhoud tegenkomen. Een goede begeleiding is dus essentieel. Ook surfen kinderen tegenwoordig overal: op school, in de bibliotheek, bij de grootouders, in de openbare ruimte, via hun smartphone of tablet, op het openbaar vervoer... Kortom, echt overal! De toestellen die ze gebruiken zijn niet noodzakelijk uitgerust met filters. Er is ook geen enkele filter die interacties tussen internetgebruikers kan controleren, blokkeren of beperken. Denk maar aan gesprekken in een chatbox, nieuwe ontmoetingen en de publicatie van filmpjes. Filters zijn tot slot geen onoverkomelijke obstakels. Je kunt ze ook probleemloos verwijderen. Op dat vlak is de creativiteit van sommige jongeren werkelijk grenzeloos.

Filtersystemen op school, jeugdhuis of bibliotheek,...?

Het computerpark van de organisatie wordt intensief gebruikt en moet dus goed zijn beschermd. De machines moeten om te beginnen worden voorzien van sterke anti-spamssoftware en firewalls. En dan stelt zich onvermijdelijk de vraag van filtersystemen. De computers worden immers gebruikt door jonge mensen, in een vrijetijds- of schoolcontext. Het al dan niet installeren van filters moet het resultaat zijn van een beslissing binnen de organisatie, en moet deel uitmaken van de globale visie van de organisatie op de webmedia.

Wat zijn de alternatieven?

In sommige gevallen kan een filter een oplossing bieden voor jonge kinderen om hen te beschermen tegen toevallige pornografische of gewelddadige beelden. Maar geen enkele filter kan het vertrouwen, de opvoeding en de dialoog tussen kinderen en ouders vervangen. De ultieme internetfilter start met de band tussen volwassenen en kinderen. De bestaande internetfilters, ook wel Content-Control Systems genoemd, zijn enkel software-gereedschap en vervangen het ouderlijk toezicht niet.

Wat zijn dan de alternatieve of aanvullende oplossingen? Zorg om te beginnen dat je pc een plaatsje krijgt in een gemeenschappelijke ruimte én zorg daarnaast ook voor de nodige interesse in de internetactiviteiten van uw kroost. Aangezien kinderen zo goed als overal en via verschillende media online kunnen, is de regel van de gemeenschappelijke ruimte op lange termijn niet houdbaar. Ook omdat ze al vlug wat ouder worden en meer nood zullen hebben aan wat privacy. Op dat moment is het belangrijk om duidelijke afspraken te maken en een open dialoog te stimuleren.

Samengevat

Leg uit aan je kind(eren) wat de bedoeling is van dergelijke 'internet'filters. Wijs hen erop dat het gebruik ervan belangrijk is om bepaalde online content te vermijden. Leg uit dat je dit doet om te vermijden dat ze bepaalde informatie of beelden te zien krijgen. Men mag het niet zien als een soort van 'straf', maar als een constructieve stap in het vertrouwensproces.

Natuurlijk kan je via je eigen computer ook op eenvoudig niveau een bescherming instellen. Via je microsoftmenu heb je de keuze om ouderlijk toezicht in te stellen:



Zorg er ook steeds voor dat je kinderen een afzonderlijke account hebben op je eigen pc. Op deze manier kunnen ze niet aan je persoonlijke documenten, mappen, wachtwoorden en gegevens. Stel deze account altijd in als 'gastaccount' met beperkte rechten. De wizard van windows helpt je hierbij stap voor stap.

Via deze website van de Europese Unie kom je alles te weten <http://www.sipbench.eu/>

Wil je een veilige internetbrowser voor jonge kinderen dan kan je altijd mybee eens proberen: <http://www.mybee.nl/>

Meer info en tips op: <https://veiliginternetten.nl/themes/kinderen-online/> en www.clicksafe.be