

Kindvriendelijk internet



SURFSLEUTEL

Voorwoord brochure 22	3
Inleiding	4
Wat de redactie opviel	7
Je smartphone schoonmaken?	12
Goede foute link	15
Taal tip!	17
MediaMasters	18
Hoe herken ik een nepmail?	21
Nepnieuws Boominktvis	23
Wat is een adblocker?	27
Telefoon beveiligen	28
Organisaties op het gebied van Internetveiligheid en mediawijsheid	32
Kinderinternet de surfsleutel	34
Brochure kinderinternet de Surfsleutel	35
Colofon	36



Voorwoord brochure 22



Het blijft belangrijk en er is nog steeds veel over te melden:

Hoe gaan we veilig om met informatie op het internet? Het blijkt dat nepmails, nepnieuws en nepwebsites voor kinderen nog steeds heel lastig te onderscheiden zijn van echte. Daarom in deze brochure weer volop aandacht voor veilig op internet.

Maar niet alleen met de beveiliging en informatie van je computer of tablet moet je nauwkeurig omgaan. Ook de beveiliging van je telefoon moet je niet vergeten. Tips voor de beveiliging van je smartphone komen in deze brochure ook aan bod.

Heb jij er eigenlijk wel eens bij stil gestaan om je telefoon een keertje schoon te maken? Als je er even over nadenkt en bedenkt hoe vies je telefoon kan zijn ga je gauw met onze schoonmaak tips aan de slag.

Chanine Hameetman heeft weer een leuke Taal tip voor in de brochure gemaakt. Meer taal- en rekentips van Chanine staan op kinderinternet de Surfsleutel onder LEREN en dan taal of rekenen.

Zijn er verder nog onderwerpen over internet of sociale media waar je meer over zou willen weten, laat het ons dan even weten via redactie @surf-sleutel.nl. Dan kijken wij of we er de volgende keer iets over in de brochure kunnen plaatsen.



Namens de redactie veel kindvriendelijk Surfsleutel plezier!

Paula Lagerwerf



“Kinderen hebben recht op een veilige speelplaats op internet. Als deze er niet is, moet deze gecreëerd worden.”

Mediaopvoeding betekent je kind leren om kritisch en bewust te gamen, internetten, lezen en tv te kijken.

De officiële omschrijving is: mediaopvoeding is dat deel van de opvoeding dat erop is gericht om kinderen bewust en selectief met media te laten omgaan

Veel opvoedvragen gaan over het mediagebruik van kinderen. De grootste uitdaging voor ouders is om een goede balans te vinden. Naast digitale media, moet er ook tijd zijn om buiten te spelen, te sporten, te lezen, voldoende te slapen en met elkaar te praten en te lachen. Hoe kun je je kind daarbij helpen?

Kies goede apps, games en websites

Een belangrijke rol heb je als opvoeder in de keuze voor media. Kies daarom voor kwalitatief goede en uitdagende games, apps en YouTube-filmpjes. Onze dossiers over apps en games helpen je hierbij verder.

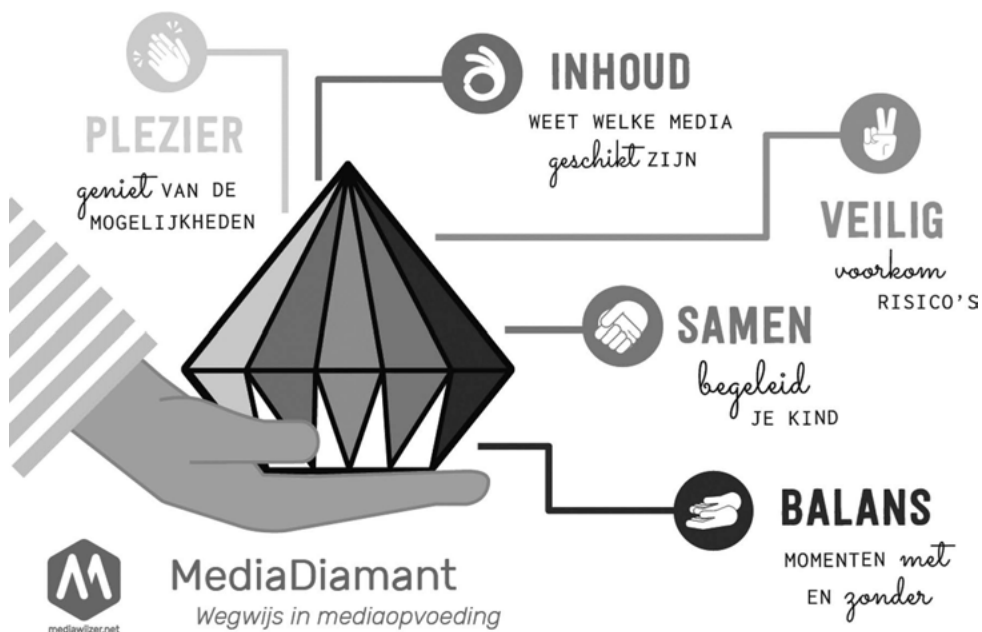
Wegwijs in mediaopvoeding met de MediaDiamant

Veel opvoedvragen van ouders gaan over het mediagebruik van kinderen. Je wil je kind goed begeleiden maar weet niet altijd hoe. De MediaDiamant is een handige wegwijzer met tips voor ouders om kinderen van 0 tot en met 18 jaar mediawijs op te laten groeien.

De MediaDiamant is opgebouwd uit vijf kanten die samen de belangrijkste onderdelen van mediaopvoeding vormen: Plezier, Veilig, Samen, Inhoud en Balans. Bij iedere kant geeft de MediaDiamant praktische tips en informatie en word je verwezen naar websites waar je er meer over kunt lezen. Zo kunnen ouders hun kind helpen om – van kleins af aan – gezonde mediagewoontes te ontwikkelen.

Meer over de mediadiamant:

<https://www.mediawijsheid.nl/mediadiamantv/>



Het actief verbeteren van de veiligheid van kinderen op het internet en het vergroten van hun mediawijsheid (en die van hun ouders) is de basis van alle activiteiten van de redactie van de Surfsleutel. Kern hiervan is Kinderinternet de Surfsleutel, een website waarbinnen ruim 7000 creatieve, ontspannende en educatieve webpagina's zijn opgenomen die door onze web-redactie dagelijks up to date worden gehouden. Een duidelijke indeling in leeftijdscategorieën en rubrieken garandeert de gebruiksvriendelijkheid van de Surfsleutel. De Surfsleutel is kosteloos voor iedereen beschikbaar.

Daarnaast geeft de redactie van de Surfsleutel in samenwerking met DNB Groep B.V. ieder kwartaal een Surfsleutel brochure uit vol informatie en tips op het gebied van veilig internet en mediawijsheid. Deze brochure wordt mogelijk gemaakt door regionale adverteerders en in dezelfde regio verspreid op verschillende basisscholen. U kunt een aantal van deze brochures ook terugvinden in de voetnoot onderaan www.surfsleutel.nl.





IS GROEN SLOTJE IN BROWSER GARANTIE VEILIG INTERNET?

“Een beveiligde website herken je aan een (groen) slotje links bovenaan de pagina en voor het webadres staat https en niet http”. Het is jarenlang gebruikt als herinnering aan internetters om ze te behoeden voor frauduleuze praktijken op het internet. Bijvoorbeeld voor partijen die zich voordoen als financiële instelling. Maar wat zegt dat slotje nu wel en wat niet als blijkt dat je zonder veel probleem een site kunt maken die lijkt op bijvoorbeeld die van een bank en daarvoor ook een certificaat inclusief dat slotje op je site kunt krijgen?

“Er heerst het idee dat het slotje in de internetbrowser absolute veiligheid garandeert. Dat doet het niet en dat heeft het ook nooit gedaan. Gebruikers moeten zelf met gepaste voorzichtigheid beoordelen of zij een website vertrouwen of niet. Want ook via veilige verbindingen worden mensen

opgelicht”, aldus cyber security specialist Richard Kerkdijk.



VEILIGE VERBINDING

Het slotje in de internetbrowser garandeert een versleutelde verbinding met de website die niet door derden kan worden afgeluisterd. Dit wordt mogelijk gemaakt door een SSL (“Secure Sockets Layer”) certificaat, een set digitale sleutels die wordt gekoppeld aan het betreffende internetadres. Zo’n certificaat wordt uitgegeven door een speciale instantie, een certificaat autoriteit.



Bij uitgifte van een certificaat wordt de organisatie achter een website in meer of mindere mate gevalideerd. Er zijn certificaten waarvoor een KvK check is gedaan of om persoonlijke legitimatie is gevraagd, maar er zijn ook certificaten waarbij dergelijke controles niet zijn gedaan. De meeste gebruikers zijn zich niet bewust van de verschillende vertrouwensniveaus die certificaten kunnen hebben en de minieme verschillen in de adresbalk van de browser waaraan je deze kunt herkennen. Het helpt ook niet dat elke browser deze verschillen op een andere manier presenteert.

VOORLICHTING, TECHNIEK EN GEDRAG

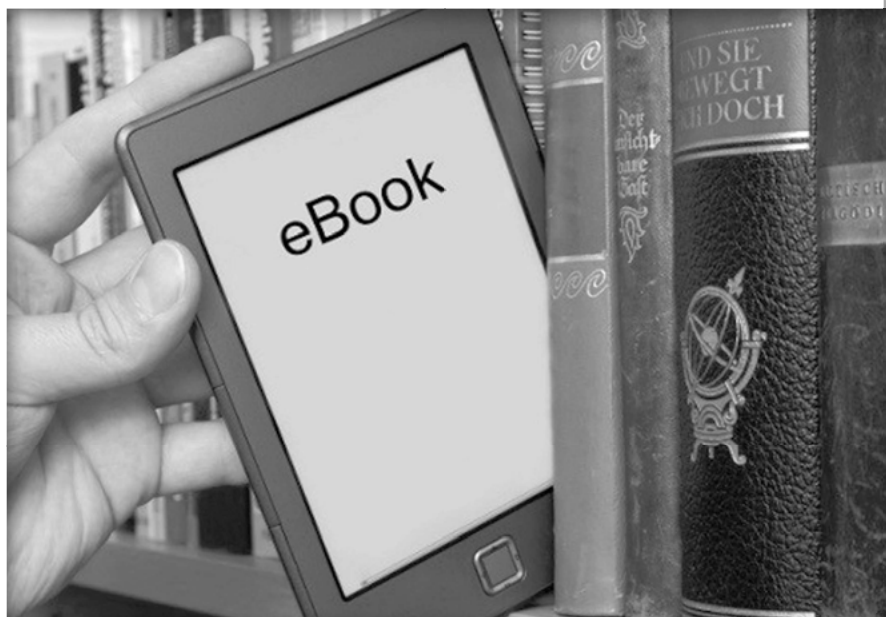
Het slotje in de browser garandeert een veilige verbinding maar zegt niets over de betrouwbaarheid van de achterliggende organisatie. Het biedt ook geen zekerheid dat de website zelf volkomen veilig is en niet bijvoorbeeld met malware is geïnfecteerd. Richard Kerkdijk adviseert een gezonde mate van oplettendheid. “Een organisatie die je niet kent kun je niet puur en alleen vanwege het slotje in de browser vertrouwen. En bij een organisatie die je wel kent moet je je altijd afvragen of het internetadres dat je ziet ook het adres is dat je bij die organisatie verwacht.”

Volgens Richard Kerkdijk zou het publiek beter voorgelicht moeten worden over wat ze wel en niet van het slotje in de browser kunnen verwachten. “Er ligt ook een uitdaging voor de ontwikkelaars van internetbrowsers om intuïtieve security oplossingen te ontwikkelen die veilig en verantwoord gedrag stimuleren.”

TOT SLOT

Het internet is een omgeving die niet altijd veilig is en daar komt ook geen absolute oplossing voor. Https (het slotje in de browser) is een nuttige en betrouwbare techniek maar beschermt niet tegen alle mogelijke risico's. Het is een schakel in de internetbeveiliging die samen met andere maatregelen en verstandig gedrag van eindgebruikers voor een veilige digitale omgeving moet zorgen.

Bron: TNO.nl



Sterke groei in aantal mensen dat gebruikmaakt van digitale bibliotheek

De landelijke digitale bibliotheek heeft in 2017 in totaal 5,4 miljoen e-books uitgeleend. Dat is een stijging van 41 procent in twee jaar tijd.

Het totale aantal uitgeleende digitale producten, naast e-books gaat het daarbij ook om luisterboeken en cursussen, betrof vorig jaar 6,4 miljoen stuks. Dat is 58 procent meer dan in 2015.

In de afgelopen twee jaar groeide het aantal gebruikersaccounts met 144 procent. De landelijke bibliotheek telt nu 602.000 accounts, waarvan 77 procent wordt gebruikt voor het lenen van e-books. Dat blijkt vrijdag uit onderzoek van de Koninklijke Bibliotheek en het Centraal Bureau voor de Statistiek (CBS).

Bron: <http://bit.ly/surfsleutelbibliotheek>



Big Data

Het internet bevat enorm veel gegevens (data). Tweets, video's, foto's, zoekresultaten en profielen op sociale media. Maar ook klantenbestanden en aankoopgegevens.



Dit maakt het voor bedrijven steeds makkelijker om jouw gedrag te voorspellen en te beïnvloeden. Hoe zorg je ervoor dat je controle houdt over jouw gegevens?

Wat is big data?

De hoeveelheid data die we met z'n allen produceren groeit explosief, omdat alles en iedereen online is. Die enorme berg digitale gegevens noemen we big data.

Voordelen van big data

De voordelen voor commerciële bedrijven zijn evident: zij krijgen meer inzicht in het (koop)gedrag van hun klanten. Deze bedrijven noemen het analyseren van grote databestanden ook wel business intelligence.

Ook voor consumenten heeft big data voordelen: zorg op maat, onderwijs op maat, aanbiedingen op maat. Big data maakt het je makkelijk.

Risico's van big data

Big data kan de privacy schaden. Veel mensen weten niet dat hun gegevens worden doorverkocht aan andere bedrijven. Bovendien heeft big data meestal meer dan één eigenaar. Big data wordt samengesteld uit verschillende bronnen en komt van verschillende leveranciers. Interpretatie van gegevens buiten de originele context, kunnen leiden tot verkeerde conclusies.

Bron: <https://www.mediawijsheid.nl/big-data/>





Je smartphone schoonmaken?

Je smartphone kijkt tegenwoordig niet meer van je zijde. Ook tijdens het eten of – laten we eerlijk zijn – op het toilet is je smartphone erbij. Hoe kan je jouw smartphone schoonmaken zonder iets te beschadigen? Met deze tips! (En we hebben dé tip voor een blinkend, krasvrij scherm.)

Broeinest van bacteriën

Je bent verknocht aan je smartphone en hij mag overal mee naartoe. Je pakt 'm niet alleen de hele dag met je handen, je legt je telefoon ook op allerlei publieke plekken neer. Er is een onderzoek gedaan naar de hygiëne van je smartphone en de uitslag was niet al te best.

67% van de Nederlanders neemt hun telefoon mee naar het toilet, en helaas maakt 31% hun telefoon hooguit één keer per halfjaar schoon. En dan alleen als hij zichtbaar vies is.

Omdat je smartphone zo'n vertrouwde metgezel is, wil je misschien niks weten van bacteriën op je lievelingsapparaat. Toch bevatten smartphones zo'n 18% meer bacteriën

dan deuren en doorspoelknoppen van openbare toiletten. En na het aanraken daarvan wil je normaal wel graag je handen wassen toch? Laat staan dat je ze tegen je oor of dichtbij je mond zou houden...

Wat kun je doen tegen een vieze smartphone?

Als jij ook een beetje gruwelt van bovenstaande informatie – zo niet, dan kun je onderstaande tips met een gerust hart overslaan – dan is het hoog tijd voor de Grote Smartphone Schoonmaak. Hoe ga je te werk?

Stap 1: verwijder eerst stoffjes, zand en kruimels

In het gat van je oplader- of koptelefoonaansluiting hopen stoffjes, zand en kruimels zich makkelijk op. Verwijder deze eerst, zodat ze geen krassen kunnen maken op je telefoon zodra je verder gaat met schoonmaken. Hoe? Als er niet al te veel vuil zit, kun je een paar keer heel hard blazen in de gaten. Wil je het grondiger aanpakken? Dan maak je zelf makkelijk een schoonmaak-tool. Namelijk zo: pak een paperclip en buig deze



recht. Rol om het uiteinde een aantal laagjes plakband, met de plakkende kant naar buiten. En voilà: je hebt een mini stoffer voor je smartphone. Wel voorzichtig te werk gaan, zodat je niks beschadigt.

Stap 2: kies het juiste doekje en schoonmaakmiddel

Pak hierna een doekje dat geen krassen achterlaat op je smartphone, zoals een microvezeldoek (en dus geen ruwe theedoek, handdoek of papieren tissue). Deze kun je meestal vinden tussen de andere schoonmaakspullen in de supermarkt of huishoudwinkel. Gebruik géén hygiënische doekjes met alcohol of ammoniak. De bacteriën gaan dan wel dood, maar je loopt ook het risico dat je het touchscreen van je telefoon beschadigt. Om vette vingers

te verwijderen, of etensresten, kun je het doekje een klein beetje vochtig maken. Verder is het een kwestie van flink boenen, met ronde bewegingen. Om je smartphone echt hygiënisch schoon te krijgen kun je daarna het beste een speciale spray pakken. Zoals een alcoholvrije spray voor smart-TV's. Spray niet rechtstreeks op je telefoon, maar eerst op het doekje. Je kunt je telefoon ook schoonmaken met een brillendoekje.





Stap 3: een schone smartphone begint bij jezelf...

Truttig maar waar: een schone smartphone begint met schone handen. Regelmatig je handen wassen helpt om je telefoon, en andere apparaten, schoon te houden. Dus na een toilet-bezoek, een reisje met het openbaar vervoer of een flinke niesaanval is het een goed idee om éven je handen te wassen. Een hoesje om je smartphone is ook nooit weg, zo voorkom je dat er veel stofjes in je telefoon komen.

Wacht, dit is dé tip voor een blinkend scherm

Om een krasvrij en blinkend scherm te krijgen, moet je even in je badkamerkastje duiken. Pardon? Ja, want daarvoor ga je namelijk tandpasta gebruiken! Doe een kleine beetje tandpasta (ter grootte van een boon)

op je scherm, pak een zacht doekje en wrijf zachtjes uit terwijl je ronde bewegingen maakt. Veeg na met een licht vochtig microvezeldoekje en je scherm ziet er weer uit als nieuw.

Een lapje voor je laptop

Nu je weet hoe vies een smartphone kan zijn, kijk je misschien ook bedenkelijk naar je laptop, toetsenbord, muis of tablet. Juist, ook deze apparaten zijn een broeinest voor bacteriën. Geef daarom andere elektronische apparaten waar je veel mee werkt ook wekelijks een lapje. Je kunt voor bijna alle apparaten handige tips online vinden.

Maak jij je smartphone weleens schoon? Of denk je daar nooit aan?

Bron: Simyo

Goede foute link

VERTEL
DOOR


HEB JIJ VOOR JOUW SURFSLEUTEL EEN LEUKE,
MOOIE, GRAPPIGE OF COOLE WEBSITE?
LAAT HET ONS WETEN

VERSTUUR



ZIE JIJ IN DE SURFSLEUTEL EEN ENGE, VIEZE,
GEMENE OF ONEERLIJKE WEBSITE?
LAAT HET ONS WETEN!

VERSTUUR

De inhoud van de Surfsleutel wordt voortdurend onderhouden door een deskundige webredactie. Ook de gebruikers kunnen hieraan een bijdrage leveren. Door middel van een klik op Surfie kan direct een goede nieuwe link worden doorgegeven. Ook een link die door veranderingen door de eigenaar nu foute inhoud bevat kan via deze weg worden gemeld waarna de webredactie meteen in actie komt.

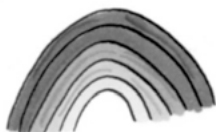


Taal tip

het
bijvoeglijk
naamwoord
zegt iets over
het zelfstandig naamwoord



het lekkere
ijsje



de mooie
regenboog



het gestreepte
t-shirt

Chanine
Hameetman



Hi, ik ben Chanine!

Ik maak onderwijsposters en illustraties.

Mijn taal en reken tips staan op

Kinderinternet de Surfsleutel onder

LEREN > taal en rekenen. Meer weten:

www.chaninehameetman.com



WAT IS MEDIA MASTERS ?

Speel MediaMasters en ontdek de wereld van de mediawijsheid!

MediaMasters is een spannende serious game over de kansen en gevaren van (digitale) media, speciaal voor groep 7 en 8. Door het spelen van de game bouwen leerlingen basis-kennis op over mediawijsheid. Hoe ga je mediawijs om met WhatsApp, privacy en nepnieuws? Leerlingen



gaan samen in de klas én thuis het avontuur aan en bundelen hun media-wijze krachten om MediaMissies te volbrengen. Durft jouw klas het aan?

MediaMasters kan vanaf oktober het hele schooljaar worden gespeeld, met als hoogtepunt de landelijke wedstrijd tijdens de Week van de Mediawijsheid in November.

Speel MediaMasters het hele jaar door

Na de Week van de Mediawijsheid gaat MediaMasters door! Scoorde jouw klas minder op privacy? Wil je meer aandacht besteden aan online omgangsvormen of cyberpesten? Ga dan aan de slag met thematische MediaMissies. Deze zijn het hele jaar, op ieder moment beschikbaar. De drie klassen die op 1 juni 2019 de meeste punten gescoord hebben, winnen een mooie prijs.

Zijn jullie te laat voor dit jaar? Geef jouw klas gauw op voor 2019/2020.

<https://www.mediamasters.nl/>

'Lossen' haken

Wat heb je nodig?

- Bolletje haakkatoen
- Haaknaald

Wat ga je doen?

- Een opzetlus maken
- 'Lossen' haken

Een haakwerk begin je bijna altijd door een aantal 'lossen' te haken. Op de 'lossen' ga je verder werken met andere haaksteken ('vasten' en 'stokjes'). Die leer je later.

De opzetlus:

- Maak aan het begin van de draad een lus. Dat kan om je vinger of door de lus op tafel te leggen. Haal de lange kant van de draad door de lus met je vinger of de haaknaald.
- Nu trek je voorzichtig aan de lange draad en de lus sluit zich om de haaknaald. Doe dit niet te strak.

De 'lossen':

- Vanaf nu houd je de haaknaald in je ene hand en houd je de draad vast met je andere hand, zodat die niet wegglijdt.
- Pak nu steeds met de haaknaald de draad op en trek hem door de lus. Weer voorzichtig en niet te strak aantrekken.
- Zo maak je een ketting van 'lossen'.



SURFSLEUTEL



Hoe herken ik een nepmail?



Soms zie je direct dat een e-mail niet betrouwbaar is, soms is het een stuk lastiger te zien. Omdat je de afzender kent bijvoorbeeld. Criminelen worden ook steeds beter in het maken van e-mails zonder taal- en spellingsfouten. Daardoor zijn de e-mails nauwelijks nog van echt te onderscheiden. Toch moet je altijd kritisch zijn. Hoe herken je nepmail? En wat moet je er vervolgens mee doen?

Direct doen (of laten):

- Een nepmail of telefoontje herkennen

Hieronder wordt uitgelegd hoe je een nepmail (stap 1) en een neptelefoontje (stap 2) kunt herkennen.

Stap 1: Een nepmail herkennen

o Afzender

Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres vaag of het lijkt op een echte bedrijfsnaam of de naam van een instantie, maar is het net niet hetzelfde. Is het adres vaag of onduidelijk? Dan heb je waarschijnlijk met phishing te maken.



o Aanhef

Word je met hele algemene termen, zoals 'Geachte heer/mevrouw' of 'Beste klant', aangesproken, let dan op. Bedrijven en instanties waar je klant bent, gebruiken meestal in ieder geval je achternaam in een e-mail of weten of je een man of een vrouw bent.

o Vragen naar persoonsgegevens

In veel nepmails staat het verzoek om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Je moet dan op een link klikken om dit te doen. Doe dit nooit zomaar. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit op deze manier naar persoonsgegevens. Bel het bedrijf of de instantie liever eerst op om te controleren of ze de e-mail wel zelf hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

o Taalgebruik en vormgeving

De huidige generatie nepmails staan allang niet meer bol van de taal- en spelfouten. Ook de gebruikte logo's en foto's worden steeds professioneler. Lees en bekijk de e-mail goed om te zien of je toch geen onregelmatigheden tegenkomt. Je kunt ook een eerdere mail van een bedrijf of instantie ernaast leggen ter vergelijking.

o Links

Links in nepmails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd of dat je naar een valse website wordt geleid. Klik dus nooit zomaar op de links in e-een e-mail die je niet vertrouwt. Controleer het adres van de link door, zonder erop te klikken, de cursor van je muis op de link te zetten en te kijken welk adres er verschijnt.

o Bijlage

Een bijlage in een nepmail kan ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd. Open dus nooit zomaar een bijlage van een e-mail die je niet vertrouwt. Een zip-bestand is altijd verdacht aangezien bijvoorbeeld facturen en aanmaningen nooit op deze manier worden verstuurd. Verwacht je toch een bestand? Neem dan contact op met de afzender om te vragen wat en hoe ze iets precies verstuurd hebben. Gebruik ook hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

<http://bit.ly/surfsleutelnepnieuws>



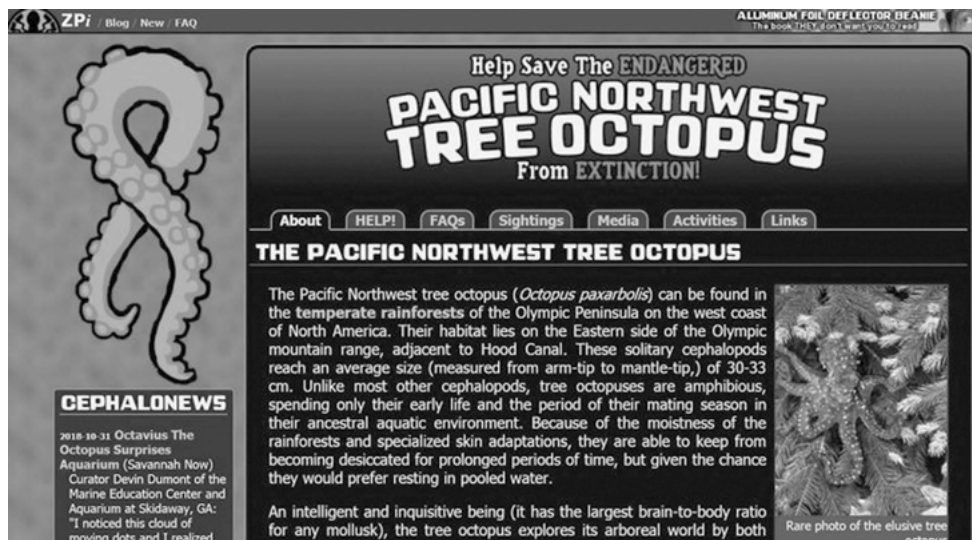
NEPNIEUWS BOOMINKTVIS

Onderzoek wijst uit dat basisschoolkinderen massaal in nepnieuws trappen

Veel basisschoolkinderen zien het verschil niet tussen nepnieuws en echt nieuws. Dat constateren onderzoekers van de universiteiten van Utrecht en Connecticut. Leraren moeten de leerlingen daarin beter trainen, vinden ze.

Bron: Mieke Zijlmans

Help! De Noord-West Pacifische boominktvij wordt met uitsterven bedreigd – tenminste: dat beweert de Amerikaanse nepwebsite. Maar dat beest bestaat helemaal niet en dus kan het ook niet met uitsterven bedreigd worden. Donald Leu, hoogleraar geletterdheid en technologie aan de universiteit van Connecticut, gebruikte de site in 2007 om te onderzoeken of 57 schoolkinderen doorhadden dat het hier gaat om nepnieuws.



Screenshot van de website met het nepnieuws. Beeld Zapatopi



Slechts zes Amerikaanse kinderen snaptten dat de boominktvís een hoax was. Eugène Loos, onderzoeker nieuwe media van de Universiteit Utrecht, herhaalde het onderzoek in 2017 met 27 Nederlandse basisschoolkinderen uit groep 8. Slechts twee Nederlandse kinderen begrepen dat ze keken naar een nepsite. De onderzoekers hebben hun resultaten gepubliceerd in het online tijdschrift Information and Learning Science.

Wat wilden jullie weten?

‘Of schoolkinderen kritisch zijn op de informatie die ze op internet aantreffen.’



De ‘boominktvís’ Beeld Zapatopi

Hoe hebben jullie dat getest?

‘We hebben ze de website over de boominktvís laten openen en een stel vragen gesteld. Wat is het probleem volgens die site? Begrijp je wat er staat? En tenslotte: is je nog iets opgevallen aan de site? Je kunt namelijk niet rechtstreeks vragen naar de betrouwbaarheid van die site, want dan breng je ze op een idee.’

Waarom trappen kinderen hier in?

‘Het gaat om een dier en dat is in gevaar: twee aspecten die inspelen op de emotie. Daardoor komt dit nepverhaal extra binnen.’

Waarom herkenden de Nederlandse kinderen die het door hadden het nepnieuws?

‘Dat waren twee meisjes, die reageerden op de vraag ‘is je nog iets opgevallen aan de site’. Het ene meisje vertelde dat ze met ‘gewoon haar gezonde verstand’ had besloten dat dat niet kan: een inktvis die in een boom woont, want inktvissen leven in het water.

‘Het tweede meisje was ‘verder gaan zoeken op internet’: zij vond het maar een raar beest, met een raar verhaal. De boominktvís stond niet op de lijst van bedreigde diersoorten; en toen ze zocht naar méér bronnen over het beest, kon ze het nergens vinden. Er zitten overigens allerlei hints in die site waaraan je kunt zien dat het verhaal

NIEUWS of NONSENS

een hoax is: hij verwijst naar een niet-bestaande universiteit en er zitten onzin-links in.'

Hoe kun je zorgen dat schoolkinderen verdacht zijn op nepnieuws?

'We zouden ze daarin willen trainen. Ze confronteren met een nepsite. Pas in tweede aanleg vertellen we dat het gaat om nepnieuws. Daarmee veroorzaken we een shockeffect. De bedoeling is daar ze daardoor in de toekomst alerter worden. Kinderen moeten kritisch naar nieuws leren kijken: wat staat er precies? Wie is de schrijver? Zijn de foto's misschien gefotoshopt?'

Waarom is het zo belangrijk juist kinderen te leren alert te zijn op nepnieuws?

'In deze gedigitaliseerde maatschappij is het belangrijk al jong een basis te leggen voor 'mediawijsheid': hoe om te gaan met informatie. Want mij valt op dat studenten van 18 tot 22 jaar weliswaar handig zijn met een smartphone en met gamen, maar dat ze moeite hebben met het vinden en verifiëren van informatie. Dat mag eerder en jonger getraind worden.

Bron: <http://bit.ly/surfsleutelonderzoeknepnieuws>



Wat is een adblocker?



AdBlock

Een adblocker blokkeert het downloaden van advertenties in webbrowsers en bijvoorbeeld commerciële videoboodschappen in Youtube. Een adblocker kan een programma of app zijn.

Voordelen:

- Adblockers zijn goed voor je privacy. Een adblocker blokkeert namelijk ook veel tracking cookies en scripts die marketingbedrijven gebruiken om jou te 'volgen' op internet. Daarmee tonen ze op basis van je surfgedrag gerichte advertenties, of maken een uitgebreider profiel van je.
- Adblockers maken het surfen sneller omdat je geen advertenties hoeft te downloaden.
- Een adblocker vermindert je data-verbruik: gemiddeld tussen de 30% en 40%. Als je surft via een mobiel netwerk (3G of 4G) ben je minder snel door je databundel heen en kun je mogelijk een kleinere, goedkopere internetbundel nemen.
- Met een adblocker loop je minder kans op malware via malafide advertenties.
- Op sommige websites nemen 'agressieve' banners het hele scherm over en/of maken geluid. Een adblocker maakt zulke websites weer bruikbaar.

Nadelen:

- Door adblockers hebben websites met reclamebanners minder inkomsten. Daarmee komen de budgetten voor journalistieke producties en andere kostenposten onder druk te staan. De website maakt daardoor minder (goede) content, of moet zelfs stoppen.
- Alternatieve reclamevormen - die geen last hebben van adblockers - nemen toe. Denk aan advertorials binnen de redactionele pagina's, zoals Nu.nl al volop doet.
- Soms word je met een adblocker simpelweg geweerd van een website: 'zet je adblocker uit anders kom je er niet op'. Dat is hinderlijk.
- Een adblocker zorgt er soms voor dat een webpagina of bepaalde content (teksten, plaatjes, video's) niet juist wordt getoond in de browser. Om zo'n website toch goed te kunnen gebruiken, kun je hem aan de uitzonderingslijst van de adblocker toevoegen.

Wil je meer weten over adblockers kijk dan op:

<http://bit.ly/surfsleuteladblock>

Geschreven door:

Peter Kulche expert Elektronika



Telefoon beveiligen

Zo bescherm je de gegevens op je mobiele telefoon



Op je mobiele telefoon staat vaak persoonlijke informatie. Denk maar aan persoonlijke mails en de informatie in je mobiel bankieren-app. Je kunt op verschillende manieren je telefoon beveiligen om deze gegevens te beschermen. En het mooie is: dit is zo gebeurd!

Risico's van een onbeveiligde telefoon

Allereerst is het goed om te weten waarom je een telefoon goed moet beveiligen. Vreemden kunnen op twee manieren toegang krijgen tot een slecht beveiligde mobiele telefoon. Rechtstreeks als ze de telefoon in handen hebben of van buitenaf via internet.

Op beide manieren kunnen ze dan eenvoudig vertrouwelijke informatie bekijken. Vreemden hebben niet veel tijd nodig om een onveilige app te installeren of om vertrouwelijke informatie op je telefoon te vinden. Door je telefoon en apps goed te beveiligen, bescherm je jouw gegevens.



Telefoon beveiligen: zo doe je dat!

Je kunt je telefoon in een paar stappen goed beveiligen.

Gebruik altijd schermvergrendeling

Thuis doe je waarschijnlijk altijd de deur op slot als je weggaat. Waarom zou je dat ook niet met je telefoon doen? Het is verstandig om deze 'op slot' te doen als je 'm niet gebruikt. Hij is moeilijker te ontgrendelen als hij beveiligd is met een wachtwoord, pincode, veegpatroon of vingerafdruk. Hierdoor is het voor telefoondieven lastiger om persoonlijke gegevens te bekijken.

Schermsgrendeling instellen op Android

Open het instellingenmenu;

- Druk op 'Schermsgrend. en beveilig.';
- Druk op 'Type schermvergrendeling';
- Typ je toegangscode in om toegang te krijgen;
- Je stelt hier het type schermvergrendeling in.

Schermsgrendeling instellen op de iPhone

- Open de 'Instellingen'-app;
- Druk op 'Touch ID en toegangscode';
- Voer je toegangscode in;
- Je stelt hier het type schermvergrendeling in.



Goede en verschillende wachtwoorden: net zo belangrijk!

Je maakt het hackers ook een stuk lastiger door goede én verschillende wachtwoorden te gebruiken. Gebruik dus niet voor elke app of dienst hetzelfde wachtwoord.



Sla je wachtwoorden niet op in je telefoon of in je mail. Voor een hacker is het dan makkelijk om toegang te krijgen tot meerdere accounts.

Het is net zo belangrijk om lange én sterke wachtwoorden te gebruiken. Een langer wachtwoord is moeilijker te kraken voor dieven of nieuwsgierige vrienden. Een sterk wachtwoord heeft veel verschillende letters, cijfers en tekens. Hierdoor is je wachtwoord vrijwel onmogelijk te raden.

- Naast een langer wachtwoord zijn er nog een paar extra tips: Gebruik geen geboortedatum, trouwdag of namen van jezelf of familieleden;
- Verander je wachtwoorden om de zoveel tijd.

Ben je bang dat je door deze tips je wachtwoord gaat vergeten? Dan raden we je aan om een ezelsbruggetje te gebruiken. Bedenk bijvoorbeeld een zin en gebruik van elk woord de eerste letter voor je wachtwoord. Je maakt het wachtwoord sterker door af en toe een hoofdletter toe te voegen.

Bijvoorbeeld: Mijn wachtwoord is het sterkste van allemaal! ('Mwihsva!')

Tweestapsverificatie: accounts met persoonlijke info nóg beter beveiligd



Je telefoon beveiligen: ook populaire apps en diensten helpen daaraan mee. Steeds meer diensten, zoals Dropbox en Google, bieden als extra beveiliging tweestapsverificatie. Dit is een extra beveiligingsmaatregel tegen hackers die op afstand proberen in het toestel te komen. Je moet dan niet alleen het wachtwoord invoeren, maar ook nog een extra code die per sms wordt opgestuurd. Deze code kan alleen als sms op je mobiele telefoon binnenkomen. Zo kan alleen de eigenaar van het toestel inloggen. Om tweestapsverificatie in te schakelen, geef je van tevoren je telefoonnummer door via de website van de dienst.

Telefoon beveiligen: daar blijf je aan werken

De beveiliging van je telefoon is iets waar je aan moet blijven werken. Pas wachtwoorden regelmatig aan. Een ontgrendelingscode kan eenvoudig worden afgekeken. Het is daarom een goed idee om je code regelmatig te veranderen. Iemand hoeft maar één keer af te kijken om je telefoon te kunnen ontgrendelen.



Blijf je telefoon updaten

Zorg dat de software en apps van je telefoon up to date zijn. Ook dit is onderdeel van je telefoon beveiligen. Apps geven regelmatig zelf aan dat er een update klaar staat. Wacht daar niet mee, installeer deze meteen via wifi. Het is mogelijk dat de maker van de app een veiligheidslek heeft ontdekt en die met een update wil verhelpen. Daarom is het belangrijk om meteen op zo'n update in te gaan. Gelukkig is het maar een kleine moeite en kan het tegenwoordig ook automatisch via wifi. Je verbruikt dan geen MB's van je Sim Only internetbundel.

Checken voor updates op Android

- Open de 'Play Store'-app;
- Druk linksboven op de drie streepjes;
- Druk, in het menu dat verschijnt, op 'Mijn apps en games';
- Druk op 'Alles updaten', om al je apps te updaten. Zorg er dan wél voor dat je telefoon is verbonden met een wifi-netwerk.

Checken voor updates op de iPhone

- Open de 'App Store'-app;
- Druk rechtsonder op 'Updates';
- Druk rechtsboven op 'Werk alle bij' om al je apps te updaten. Zorg er dan wél voor dat je bent verbonden met een wifi-netwerk.

Apps: downloaden ze alleen uit een officiële app store

Download apps alleen uit een officiële app store. Deze apps zijn van tevoren gekeurd en zijn daardoor veiliger dan apps die niet in een officiële app store staan. Op de iPhone kun je alleen apps downloaden uit de officiële Apple App Store.



Organisaties op het gebied van Internetveiligheid en mediawijsheid

www.mediawijzer.net is hét online loket voor iedereen die (professioneel) te maken heeft met of meer wil weten over mediawijsheid. Mediawijzer.net is opgezet door het Mediawijsheid Expertisecentrum, op initiatief van de ministeries van OCW en Jeugd en Gezin. In de dossiers vindt u de informatie overzichtelijk op thema gerangschikt.

Media spelen een steeds belangrijkere rol in onze samenleving. Media zijn overal en hun maatschappelijke impact is groot. Op deze site vindt u allerlei informatie op het gebied van mediawijsheid; het vinden en begrijpen en maken van media in een door media gedomineerde samenleving

Postadres:
Mediawijzer.net
Postbus 778
2700 AT Zoetermeer

Bezoekadres:
Paletsingel 32
2718 NT Zoetermeer



Kleurplaat: Surfie carnaval



Sociale en maatschappelijke doelstelling

Kinderinternet de Surfsleutel heeft een sociale en maatschappelijk doelstelling. Wij vinden het belangrijk dat kinderen over een gratis veiligere en kindvriendelijke internetomgeving kunnen beschikken, waar ze geen zaken in tegen komen waar ze niet mee geconfronteerd behoren te worden.

Vanaf januari 2018 heeft de redactie van de Surfsleutel besloten haar maatschappelijk verantwoordelijkheid verder op te pakken door haar redactie open te stellen voor mensen

die uit een sociaal isolement willen komen of een afstand tot de arbeidsmarkt hebben. Mensen die graag zinvol bezig willen zijn. Voor wie het weer krijgen van een dag/ arbeidsritme of het opdoen van sociale -en/of arbeidsvaardigheden belangrijk is.

We gebruiken onze redactie als plaats waar men op eigen tempo kan werken aan een stukje persoonlijke ontwikkeling en vaardigheden. Wij vinden het belangrijk dat men het gevoel heeft zinvol bezig te zijn en dat dit gewaardeerd wordt. Ieder mens is waardevol en kan op zijn eigen manier van alles bereiken!

*Vrijwilligers Nicolette en Daisy
maken samen pepernoten
voor het vernieuwde recept
op de Surfsleutel.*



Brochure kinderinternet de Surfsleutel

In samenwerking met DNB Groep B.V. wordt elk kwartaal een Surfsleutel brochure uitgegeven. Deze brochure wordt mogelijk gemaakt door regionale adverteerders en in 18 regio's aangeboden aan 25 verschillende basisscholen. Iedere basisschool ontvangt in eerste instantie gratis 25 exemplaren en kan naar wens meer exemplaren kosteloos aanvragen.

Met het verspreiden van deze brochure hopen we de naamsbekendheid van Kinderinternet de Surfsleutel te vergroten en verwerven we de middelen om de Surfsleutel online te houden.

De brochure bevat naast informatie over onze kinderwebsite www.surfsleutel.nl vooral veel tips en informatie voor kinderen, hun ouders en begeleiders over hoe je veiliger en kindvriendelijker op het internet kunt surfen. Daarnaast spelen we in op actuele onderwerpen zoals het gebruik van sociale media.

Een aantal van deze brochures is nu ook van deze website te downloaden.

Wenst u de brochure ook gratis te ontvangen dan kunt u deze bij bestellen via:

DNB Groep B.V., telefoonnummer 0598-398800 of email: receptie@dnbgroep.nl



Kinderinternet de Surfsleutel
Pastoor van Kessellaan 3
Unit 3 A
4761 BH Zevenbergen

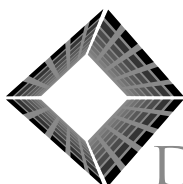
Bezoekadres:
Pastoor van Kessellaan 3
Unit 3 A
4761 BH Zevenbergen
T: 0168-329051
(op werkdagen bereikbaar tussen 9.00 en 13.00 uur)

E: info@surfsleutel.nl
W: www.surfsleutel.nl

De redactie van de Surfsleutel is te bereiken via:
E: redactie@surfsleutel.nl



Uitgever:



DNB GROEP
SOCIALE EN MAATSCHAPPELIJKE PUBLICATIES

WWW.DNBGROEP.NL

DE UITGEVER EN DE SURFSLEUTEL ZIJN NIET VERANTWOORDELIJK VOOR DE INHOUD VAN DE ADVERTENTIES. NIETS UIT DEZE UITGAVE MAG WORDEN GEKOPIEERD EN/OF VERSPREID ZONDER SCHRIFTELIJKE TOESTEMMING VAN DE UITGEVER EN/OF DE SURFSLEUTEL.