

Kindvriendelijk internet



**SURF
SLEUTEL**

Brochure "De Surfsleutel"

jaargang 9

nummer 30

SURF SLEUTEL

Voorwoord brochure	30	3
Inleiding		4
Wat de redactie opviel		7
Wat is de app Tiktok?		8
Goede foute link		11
Phishing		13
Eerst checken dan klikken		15
Hoe stop je online inbrekers?		18
Wat is een Filterbubbel?		19
Firefox krijgt HTTPS-Only Mode die standaard alleen https-sites laadt		25
Wat is een sterk wachtwoord?		26
Vouw jouw MediaDiamant		28
Organisaties op het gebied van Internetveiligheid en mediawijsheid		31
Brochure kinderinternet de Surfsleutel		34
Kinderinternet de Surfsleutel		35
Colofon		36



Voorwoord brochure 30



De redactie van kinderinternet de Surfsleutel is weer heel wat interessants tegen gekomen op het internet. Verbaas jij je ook nog dagelijks over wat je nu weer leest of kan doen op en met jouw devices en het internet?

Post jij foto's op Instagram of filmpjes op TikTok? Weet jij als ouder wat TikTok eigenlijk is? We hebben een korte uitleg van wat het is en waar je beter op kan letten.

Deze keer weer aandacht voor internet veiligheid in verschillende uitvoeringen. Denk aan je Cookies! Maar klik ook niet zomaar overal op! Tips om online inbrekers tegen te houden. Aandacht voor het gebruik

van je wachtwoord en natuurlijk weer phishing!

We kunnen je niet vaak genoeg waarschuwen.

Heb jij trouwens wel eens van een filterbubbel gehoord? Lees verderop wat dit inhoudt. Natuurlijk in deze brochure ook weer wat leuke voorbeelden uit de Surfsleutel waar je lekker mee aan de slag kunt.

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@surfsleutel.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

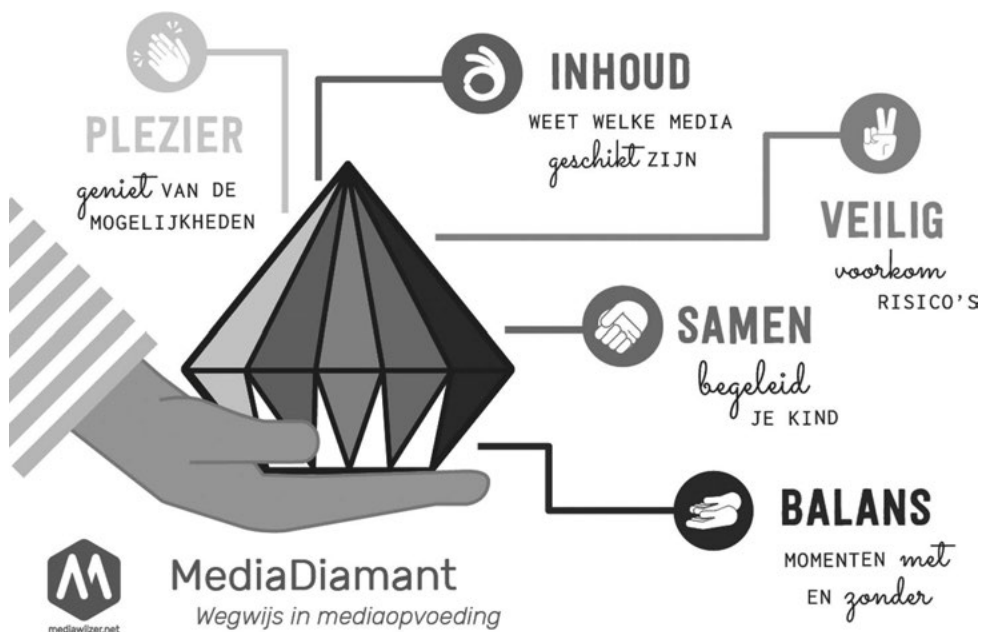
Een belangrijke rol heb je als opvoeder in de keuze voor media. Kies daarom voor kwalitatief goede en uitdagende games, apps en YouTube-filmpjes. Onze dossiers over apps en games helpen je hierbij verder.

Wegwijs in mediaopvoeding met de MediaDiamant

Veel opvoedvragen van ouders gaan over het mediagebruik van kinderen. Je wilt 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/mediadiamant/>



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 gebruiksvriendelijke website waarbinnen ruim 3500 creatieve en educatieve webpagina's zijn opgenomen die door onze web-redactie dagelijks up to date worden gehouden. 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.



Cookies verwijderen: stappenplan

Bedrijven gebruiken cookies om te registreren welke sites jij bezoekt. Gelukkig kun je deze bestanden weggooien of automatisch blokkeren. Lees hoe je dit goed regelt.

Bron: Peter Kulche



Meer lezen: <https://bit.ly/surfsleutelcookies>

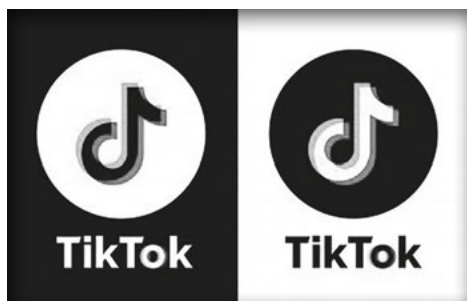
Hoe maak ik veilig gebruik van openbare wifi-netwerken?

Een openbaar wifi-netwerk gebruiken van bijvoorbeeld een café, hotel, camping, vliegveld, trein of bus is nooit veilig, of je nu een wachtwoord gebruikt of niet. Zodra je inlogt op een openbaar wifi-netwerk, kan een hacker toegang krijgen tot je apparaat en daardoor tot je persoonlijke en belangrijke gegevens. Deze gegevens kan hij gebruiken voor identiteitsfraude, om in te loggen op je e-mail of Facebook-account, voor het onderscheppen van DigiD-accounts. Je kunt de risico's beperken.

Bron: veiliginternetten.nl



Wat is de app TikTok?



TikTok is een mobiele app waarmee gebruikers in de vorm van een korte video (15-60 sec.) een bericht kunnen maken over van alles en nog wat en delen met vrienden, familie of de hele wereld. Door het toepassen van speciale effecten zoals muziek in de achtergrond, snelheid, traagheid, verschillende filters, dansen en zingen kun je je video aantrekkelijker maken.

TikTok taal: als "tiktokker" ben je ook bekend met deze woordjes:

- **Feed:** lijst van alle nieuwe filmpjes;
- **For you:** TikTok stuurt jou video's waarvan ze denken dat je die leuk vindt;
- **Challenge:** met #challenge word je uitgedaagd om een filmpje na te doen;
- **Likes:** Als je een filmpje leuk vindt klik je op een hartje. Hoe meer likes hoe populairder het filmpje wordt;

- **Follower:** Vind je een gebruiker leuk dan kun je hem volgen. ???Meer followers is meer video's van de gebruiker;
- **Nieuw Family Pairing:** hiermee kunnen ouders hun TikTok-account koppelen aan dat van hun tienerkind om zo meer beveiligings- en privacy instellingen mogelijk te maken.

<https://bit.ly/Surfsleuteltiktok>

De uitgebreide Family Pairing functie omvat nu:

- **Reacties [NIEUW]:** bepaal wie mag reageren op de video's van uw tienerkind: iedereen, vrienden, niemand;
- **Vindbaarheid [NIEUW]:** bepaal of het account van uw tienerkind privé is. De tiener bepaalt wie zijn inhoud kan zien. Als hij de inhoud openbaar zet kan iedereen deze inhoud bezoeken en bekijken;
- **Video's die ik leuk vind [NIEUW]:** veel gebruikers vinden het leuk om nieuwe video's te vinden die anderen die zij volgen ook leuk vinden. Deze functie stelt gezinnen in staat te beslissen of anderen de lijst met video's kunnen zien die uw tienerkind leuk vindt;

- **Direct Messaging:** Beperk wie berichten naar uw tienerkind kan sturen of schakel directe berichten volledig uit.

Bron: <https://www.emerce.nl/wire/nieuwe-tools-gezinnen-tiktok>

Wat zijn de nadelen van de app?

- TikTok verzamelt persoonlijke gegevens;
- Het is verstandig om de app-machtigingen door te lopen want sommige apps gebruiken je microfoon, camera en opslag terwijl de app niet gebruikt wordt. Zo weten de app bouwers al snel veel data van jou. Zoals je locatie, IP-adres, welke telefoon je hebt en zelfs welke apps je op je telefoon geïnstalleerd hebt.
- TikTok kan heel verslavend zijn;
- Het maken en bewerken van video's neemt veel tijd in beslag;
- TikTok mag jouw filmpjes inzetten voor marketingdoeleinden.

Voor de Ouder

Zitten je kinderen op TikTok? Hier moet je op letten!

Gaat je kind akkoord met de algemene voorwaarden van de app?
Dan gaan ze akkoord met:

- Persoonlijke filmpjes staan standaard openbaar;
- Je profiel staat standaard openbaar, inclusief naam en locatie;
- Jouw filmpjes mogen op andere sociale media gebruikt worden.

Hoe kun je voorkomen dat jij als kind vervelende reacties van vreemde krijgt?

- Praat over onlinepesten;
- Je account instellen op privé en alleen zichtbaar zijn voor vrienden en familie;
- Voeg geen vreemden toe;
- Wissen van gebruikers die onbekend zijn;
- Melden van misbruikers.





zoek



SPELEN

WETEN

HOME

WETEN

SPELEN

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.



Brochure "De Surfsleutel"

11

1.



2.



3.



4.



5.



6.



OLAF the
Snowman



SURF SLEUTEL

©Mae van Aarsen

Phishing



Phishing is een vorm van internet-fraude. Gebruikers worden naar een website gelokt. Deze website is een kopie van de echte site. Daar wordt gevraagd om een inlognaam en wachtwoord of om een betaling te doen. Zo komen criminelen achter je privé-gegevens of hebben ze toegang tot je bankrekening.

Een bank vraagt nooit om die gegevens via de mail, WhatsApp of telefoon. Bij twijfel: bel je bank!

Met de campagne 'Eerst checken, dan klikken' wil de overheid weerbaarheid tegen phishing vergroten. Ga gelijk aan de slag met de tips. Phishing? Zo herken je het!

Op veiliginternetten.nl staat uitgelegd hoe je een phishingmail of telefoontje herkent.

Phishing vindt plaats via e-mail, WhatsApp, sms en/of telefonisch, bijvoorbeeld:

- We zijn bezig met een veiligheidsupdate, controleer uw gegevens
- Ik werk bij uw bank, mag ik uw gegevens controleren?
- U heeft een prijs gewonnen
- U heeft nog een openstaande rekening
- Uw rekening is geblokkeerd
- We zien dat er op dit moment fraude wordt gepleegd met uw creditcard
- Uw instellingen voor internet-bankieren staan niet goed
- U krijgt een erfenis van een oudoom die u niet kent
- Maak geld over en verdien zo nog meer geld
- Stuur dit bericht door naar zoveel mogelijk mensen

Blijf altijd kritisch. Laat je niet ompraten en intimideren. Verbreek bij twijfel de verbinding en check bij de bank of het bedrijf of ze je echt hebben benaderd.

Open nooit zomaar een bijlage en check altijd de link voordat je erop klikt. Dat kan bijvoorbeeld op **Checkjelinkje.nl**.

Bron: mediawijsheid.nl/phishing/





Eerst checken, dan klikken

Bescherm jezelf tegen phishing

Een e-mail, tekstbericht of betaalverzoek met een foute link erin is een veelgebruikte manier om je gegevens te achterhalen of je over te halen om geld over te maken. Dit heet phishing. Met die gegevens, zoals wachtwoorden of toegangscode's, kunnen internetcriminelen je veel geld afhandig maken. Het is dus belangrijk om alert te zijn. Als je phishing kunt herkennen, en niet op linkjes en bijlagen klikt, snijdt je internetcriminelen flink de pas af.

Weet jij wanneer je te maken kan hebben met phishing?

Weet je wanneer je moet opletten?

Er wordt je gevraagd om geld over te maken.

Er wordt je gevraagd om in te loggen of om je persoonsgegevens te mailen. Er is haast bij.

Als dit het geval is weet je voortaan wat je te doen staat! Eerst checken, dan klikken! Klik niet zomaar op een link.

Weet je wat je moet checken?

- Check de URL (het adres) van een link door er met je muis op te gaan staan (niet klikken natuurlijk!). Kijk goed of je vreemde dingen (rare tekens, vreemde woorden) in de URL ziet staan.
- Check het e-mailadres van de afzender.
- Krijg je een onverwacht betaalverzoek van een bekende? Bel op en vraag of het klopt.



- Krijg je een betaalverzoek van een bedrijf? Bel het bedrijf op om te vragen of het klopt.
- Twijfel je aan de juistheid van een link? Ga naar checkjelinkje.nl

Momenteel zijn er drie meest voorkomende methodes van phishing:

1. **E-mail:** Check de aanhef, de afzender en de bijlagen. Is deze vaag, onherkenbaar, of heeft de e-mail een bijlage met .exe. Wordt er gevraagd om geld, moet je heel snel betalen? Grote kans dat je te maken hebt met phishing.
2. **WhatsApp/SMS:** Ken je de persoon of organisatie maar vertrouw je het bericht niet? Neem zelf contact op!
3. **Betaalverzoek:** Is het logisch dat je dat betaalverzoek krijgt? Ken je diegene? Neem zelf contact op als je het niet vertrouwt.

Wat weet jij van phishing?

Heb je toch geklikt zonder te checken?

Gelijk doen:

Verander je wachtwoorden via een andere computer;

Doe aangifte bij de politie;

Doe een virusscan;

Meld het nepbericht bij de zogenaamde verzender;

Meld het nepbericht bij

Fraudehulpdesk

Ben je slachtoffer geworden van phishing en ben je op zoek naar ondersteuning of advies dan kun je contact opnemen met Slachtofferhulp Nederland. Zij bieden emotionele hulp, hulp bij schadevergoeding en hulp bij een eventueel strafproces.

Vijf simpele stappen tegen internetcriminaliteit:

1. Eerst checken, dan klikken;
2. Gebruik verschillende sterke wachtwoorden;
3. Voer software updates uit;
4. Gebruik altijd een virusscanner;
5. Maak regelmatig een back-up.

Onthoud:

- Eerst checken, dan klikken!
- Je bank, creditcardmaatschappij, verzekering, telefoonmaatschappij en internetprovider vragen NOOIT om een betaling of naar persoonsgegevens of inlogcodes in een e-mail, WhatsApp of SMS.
- De overheid vraagt NOOIT om een betaling of naar persoonsgegevens of inlogcodes in een e-mail, WhatsApp of SMS.
- Als je via je vertrouwde app inlogt of zelf de website correct intypt, is de kans op phishing heel klein.

Bron: veiliginternetten.nl



SURFSLEUTEL

©Surfsleutel



Brochure "De Surfsleutel"

Hoe stop je online inbrekers?

Inbreken in je account of computer-systeem noemen we ook wel 'hacken'. Gevoelige informatie, zoals pikante foto's of bankgegevens, kan zo in verkeerde handen vallen en misbruikt worden.

Een paar tips om hackers tegen te houden:

- Zorg dat je updates direct installeert of zet automatische updates aan. Zo heb je altijd de meest veilige versie;
- Maak zo min mogelijk gebruik van openbare wifi, dat is vaak slecht beveiligd. Als je het toch doet: gebruik een VPN-verbinding;
- Versleutel de data op je apparaten;
- Voorkom dat hackers mee kunnen kijken en luisteren tijdens het computeren. Zet de microfoon uit en dek de webcam af;
- Meer tips vind je in de handleiding 'Laat Je Niet Hack Maken'. www.laatjenienethackmaken.nl

Zorg ervoor dat je wachtwoord niet geraden of gekraakt kan worden:

- Gebruik sterke wachtwoorden. Deze vormen een slot op je accounts en apparaten. Doe de Wachtwoord-test en lees de tips

voor een sterk wachtwoord;

- Stel tweestapsverificatie in. Mocht je wachtwoord toch gestolen zijn, dan vormt dit een extra slot;
- Gebruik overal verschillende wachtwoorden. Moeite met onthouden? Gebruik een wachtwoordmanager;
- Geef nooit je wachtwoord aan een ander.

Wat je nog meer moet weten over hacken

Wist je dat...

... hackers vaak voor de grap inbreken in computers? Uit onderzoek van Veiliginternetten.nl blijkt dat 5 procent van de Nederlandse jongeren weleens heeft gehackt. Ook geeft bijna de helft van de jongeren die nog nooit gehackt hebben aan dit wel eens te willen proberen.

... hackers ook kunnen helpen om de veiligheid te vergroten? Met de campagne Hacktalent? Doe er iets goeds mee wil Veiliginternetten.nl hackende jongeren laten zien dat zij deze vaardigheden juist op een positieve manier in kunnen zetten. Bijvoorbeeld als ethisch hacker.

... hackers ook grote bedrijven en overheden aanvallen? Dat doen ze bijvoorbeeld met een DDoS-aanval, waarmee een systeem plat wordt gelegd. Ze vragen vaak om geld om het systeem weer werkend te krijgen.

... criminelen met visueel hacken vertrouwelijke informatie verzamelen door naar het scherm van een ander te kijken? Dit wordt ook schouder-surfen genoemd. Visueel hacken is een groeiend probleem, omdat pc's en laptops steeds vaker in openbare ruimtes gebruikt worden.

Wat is een Filterbubbel?



Filterbubbel (filter bubbel) of informatieluchtbel. Tijdens het surfen wordt er een profiel van je gemaakt. Dat gebeurt o.a. op basis van je zoekgeschiedenis, e-mailverkeer, koopgedrag en berichten op sociale media. In dat profiel staat kortweg wie je bent en wat je voorkeuren en interesses zijn.

Hoe werkt het?

Als je ouders op internet zoeken op het woord Egypte krijgen zij waarschijnlijk informatie over reizen naar Egypte. Bijvoorbeeld over hotels en vliegtickets, maar als jij zoekt op het woord Egypte herkent de zoekmachine dat je nog op school zit en krijg je waarschijnlijk informatie voor een werkstuk.



De zoekmachine zoekt naar het beste antwoord op jouw zoekvraag, en laat andere informatie weg. Dit gebeurt ook op sociale media, zoals Instagram en YouTube. Je ziet daar vooral berichten die passen bij jouw interesses.

Sociale media zoals Facebook maken gebruik van algoritmes om te bepalen wat je het liefst ziet en door middel door cookies bepalen ze welke zoekresultaten en posts jij te zien krijgt.

Waarom kan een filterbubbel gevaarlijk zijn?

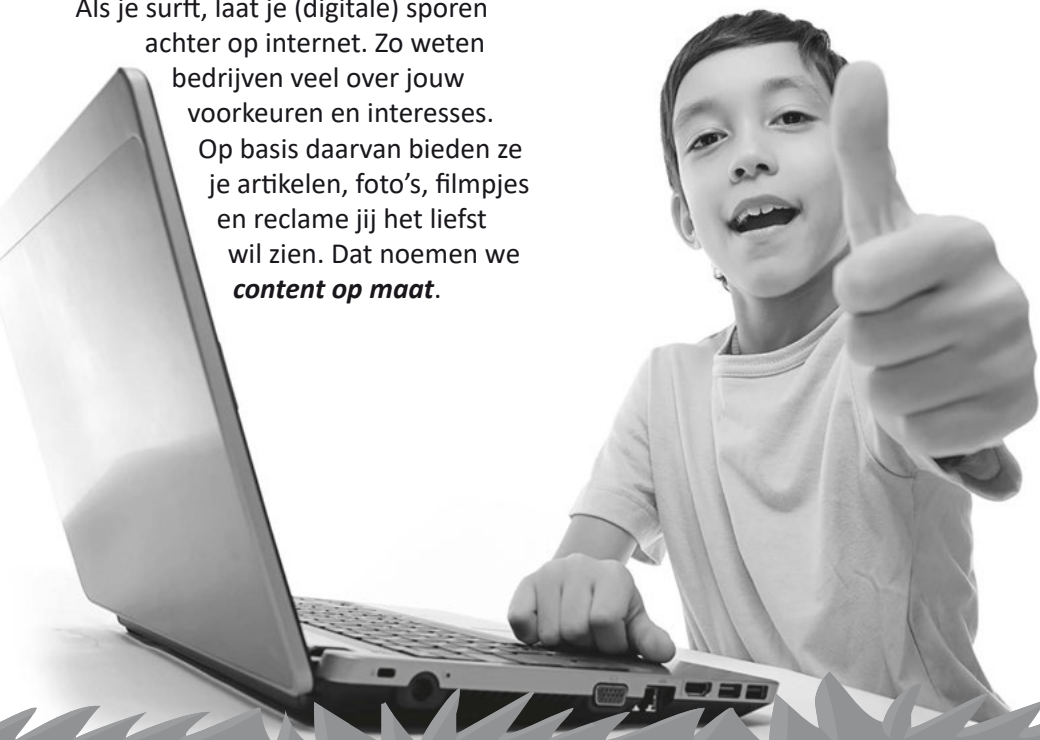
Een filterbubbel is erg handig, maar het kan ook nadelen hebben.

Als je surft, laat je (digitale) sporen achter op internet. Zo weten bedrijven veel over jouw voorkeuren en interesses. Op basis daarvan bieden ze je artikelen, foto's, filmpjes en reclame die jij het liefst wil zien. Dat noemen we **content op maat**.

Content op maat vraagt om media-wijze consumenten. Het kan onduidelijk zijn waar bepaalde content vandaan komt, hoe deze tot stand komt en met welke intenties de makers de content aanbieden. Ook kan het zorgen voor minder diversiteit in de content die je te zien krijgt.

Liever geen filterbubbel?

- Verwijder je cookie;
- Surf anoniem, bijvoorbeeld met zoekmachine DuckDuckGo;
- Leer kinderen informatievaardigheden. Deze vaardigheden helpen bij het zoeken, vinden en beoordelen van informatie;
- Gebruik veel verschillende bronnen en websites.



Halloween-knutsel

Pompoen potje



Wat heb je nodig?

- glazen pot
- schaar
- lijm
- zwart papier
- oranje tissue- of crêpepapier



Hoe maak je het?

- Knip in het tissue- of crêpepapier vormpjes. Op het voorbeeld zie je driehoekjes, maar je kunt ook kiezen voor iets anders.
- Plak het tissue- of crêpepapier om het glazen potje.
- Knip uit het zwarte papier 3 driehoekjes. Dit zijn de ogen en de neus.
- Knip uit het zwarte papier een mond.
- Knip uit de mond een hoekje (zie voorbeeld!).
- Plak de ogen, neus en mond op het glazen potje.
- Stop nu nog een waxinelichtje in het potje en steek deze aan. Vraag altijd papa of mama erbij! In het donker ziet dit er heel erg spannend uit.

SURFSLEUTEL



Kerst- knutsel
Kerstboom op stok



SURF SLEUTEL

Wat heb je nodig?

- stokje
- schaar
- vilt voor boom
- lijn
- borduurgaren
- vulling bv. watjes
- naald met groot oog
- versiersels



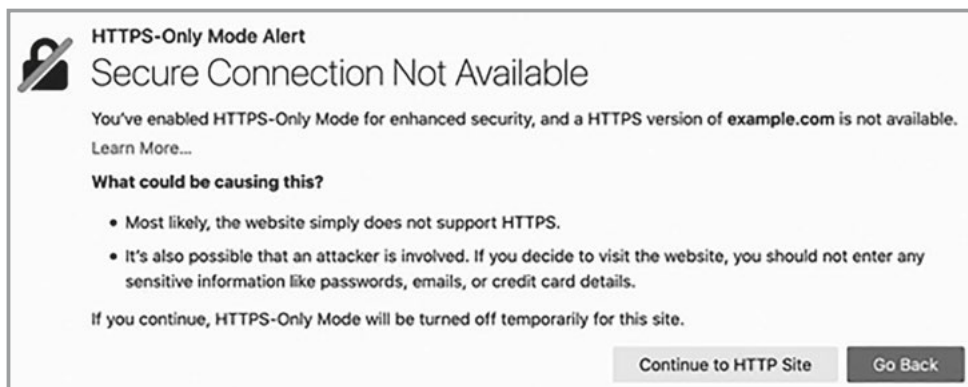
Hoe maak je het?

- Teken zelf een kerstboom op papier en teken deze 2x over op het vilt.
- Knip de kerstbomen uit en leg ze op elkaar.
- Naai de twee kerstbomen op elkaar. De steek die wij gebruiken hebben gaat zo: Steek van achter de naald naar voren toe in het vilt en sla de draad naar voren om de naald. Haal nu de naald helemaal door en doe dit nog een keer je krijgt zo een liggend draadje op de rand van het vilt.
- Ga zo bijna helemaal rond.
- Laat een gaatje over om de boom te vullen,
- vul de boom met bv. watten.
- Maak ook het gaatje dicht.
- versier de boom zoals jij wilt.
- Steek het stokje erdoor. Je kunt de kerstboom nu in een kerststukje of potje zetten.

SURFSLEUTEL



Firefox krijgt HTTPS-Only Mode die standaard alleen https-sites laadt



HTTPS-Only Mode Alert
Secure Connection Not Available

You've enabled HTTPS-Only Mode for enhanced security, and a HTTPS version of **example.com** is not available.
[Learn More...](#)

What could be causing this?

- Most likely, the website simply does not support HTTPS.
- It's also possible that an attacker is involved. If you decide to visit the website, you should not enter any sensitive information like passwords, emails, or credit card details.

If you continue, HTTPS-Only Mode will be turned off temporarily for this site.

[Continue to HTTP Site](#) [Go Back](#)

- Met de HTTPS-Only Mode zal Firefox geen onbeveiligde verbindingen met websites meer opzetten tenzij de gebruiker dit toestaat. Ook wanneer de gebruiker http in de adresbalk tikt of op een http-link klikt zal Firefox bij deze mode er standaard https van maken. Wanneer een website geen https aanbiedt toont de browser een foutmelding en legt het beveiligingsrisico uit. Vervolgens kan de gebruiker ervoor kiezen om de website wel of niet te bezoeken.
- In het geval van 'mixed-content', waarbij de website van https gebruikmaakt, maar bijvoorbeeld afbeeldingen, advertenties of filmpjes via http laadt, kan

HTTPS-Only ervoor zorgen dat de website niet goed wordt weergegeven. In deze situaties is het mogelijk om de beveiligingsfeature tijdelijk voor de betreffende website uit te schakelen.

Mozilla stelt dat als het gebruik van https verder toeneemt browsers de ondersteuning van http volledig kunnen uitschakelen en https voor elke website kunnen verplichten. Volgens cijfers van Let's Encrypt wordt zo'n 84 procent van de websites die Firefox-gebruikers bezoeken via https geladen. De HTTPS Only Mode is beschikbaar in Firefox 83. Gebruikers moeten de optie wel zelf inschakelen.

Bron: www.security.nl



Wat is een sterk wachtwoord?

Met een wachtwoord bescherm je persoonlijke en belangrijke gegevens op je computer, tablet en smartphone. Maar ook voor bijvoorbeeld je e-mail-account, sociale media, zoals Facebook, Twitter en LinkedIn, en data in de cloud gebruik je een wachtwoord. Want je wilt voorkomen dat een vreemde je vakantiefoto's bekijkt, je klantgegevens kopieert of via je smartphone je Facebook-vrienden een ongepast bericht stuurt. Of dat een hacker je BSN steelt en identiteitsfraude pleegt.

Antwoord

Sterk wachtwoord: moeilijk te raden of kraken

Het meest gebruikte wachtwoord is 123456. Dat weet elke hacker. Daarom is dit het minst verstandige wachtwoord om te gebruiken. Je loopt namelijk het risico dat een hacker hiermee toegang krijgt tot je persoonlijke bestanden. Kies een sterk wachtwoord.

Je kunt een wachtwoord voor de veiligheid af en toe veranderen, maar het risico bestaat dat je wachtwoord daardoor minder sterk wordt, bijvoorbeeld als je maar één teken verandert. Het allerbelangrijkste is dat je een sterk wachtwoord kiest.

Sterk

Een sterk wachtwoord is niet te raden door een hacker en moeilijk te kraken door een computer. Tips:

- o Bedenk een wachtwoord zonder voor de hand liggende woorden.
- o Maak een wachtwoord van minimaal 12 karakters. Hoe langer, hoe beter.
- o Gebruik bijvoorbeeld een gezegde, zin uit een liedje of andere zin die je goed kunt onthouden en die lastig te raden of kraken is. Bijvoorbeeld: Liever U2 dan de 6e van Beethoven! Of: Wil ik een kat of 10 honden? Hanteert de website een maximum aantal wachtwoordkarakters, dan kun je bijvoorbeeld de eerste letters van elk woord instellen als je wachtwoord. Bij de eerste zin wordt het: LUdd6vB! Bij de tweede: Wieko10h? Je kunt ook de eerste 2 letters van elk woord uit je zin gebruiken. Dat wordt: LiU2dade6evaBe! En: Wiikeekaof10ho? Of plak alle woorden aan elkaar en gebruik voor elk nieuw woord een hoofdletter: LieverU2DanDe6eVanBeethoven! En: WillkEenKatOf10Honden?

- o Gebruik voor elk account een ander wachtwoord, want ook de website waar je je account hebt, kan gehackt worden, en internet-criminelen proberen een gestolen wachtwoord vaak uit op zoveel mogelijk verschillende internet-diensten. Krijgen criminelen één wachtwoord van jou in handen, dan hebben ze niet direct toegang tot al je accounts.
- o Wijzig je wachtwoord als iemand (mogelijk) toegang heeft of toegang kan krijgen tot jouw account, bijvoorbeeld als je van anderen hoort dat ze vreemde berichtjes uit jouw naam krijgen. Verander je wachtwoord ook als de dienst waar je het account hebt, te maken heeft met een datalek. Daarmee voorkom je dat degene die toegang heeft gekregen tot de dienst ook jouw accountgegevens kan gebruiken. Je kunt bij de dienst Have I Been Pwned? en bij de politie controleren of je e-mail-adres in een gelekte database voorkomt.
- o Vind je het best lastig om je wachtwoorden te onthouden, gebruik dan een wachtwoordmanager.

- o Bij sommige accounts kun je kiezen voor extra veiligheid met tweestapsverificatie.

Zwak en dus snel gehackt:

- o Nienke1984' (als je partner of kind zo heet, kies geen wachtwoord met daarin persoonlijke informatie)
- o 123456
- o qwerty
- o welkom01
- o voetbal123 (of een ander bestaand woord uit het woordenboek met een paar cijfers erachter)
- o 'Facebook01! of 'F@c3B0oK' (of een ander woord dat te herleiden is tot de dienst)



MediaDiamant

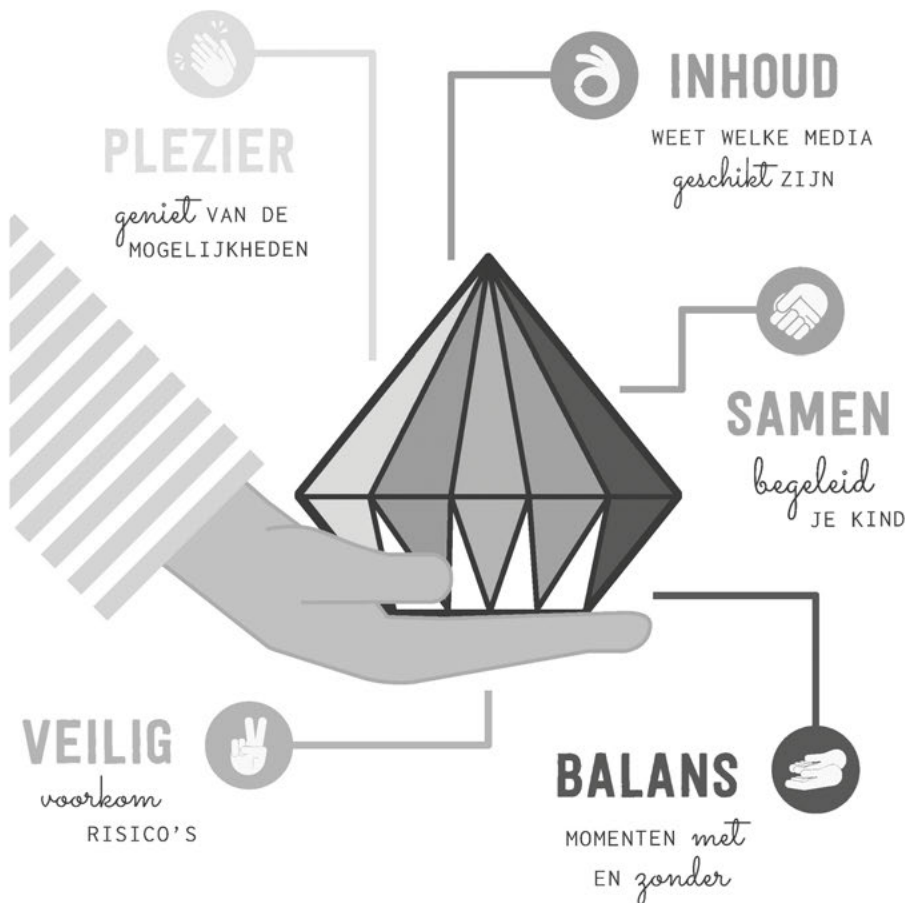
Wegwijs in mediaopvoeding

Op mediawijsheid.nl/mediadiamant vind je concrete tips hoe je de MediaDiamant kunt gebruiken.



*Zelf aan
de slag?*

DRAAI DIT VEL
OM EN VOUW JOUW
MEDIADIAMANT!



BEELD & GELUID



Platform voor de
InformatieGerandag

Kennisnet



KB

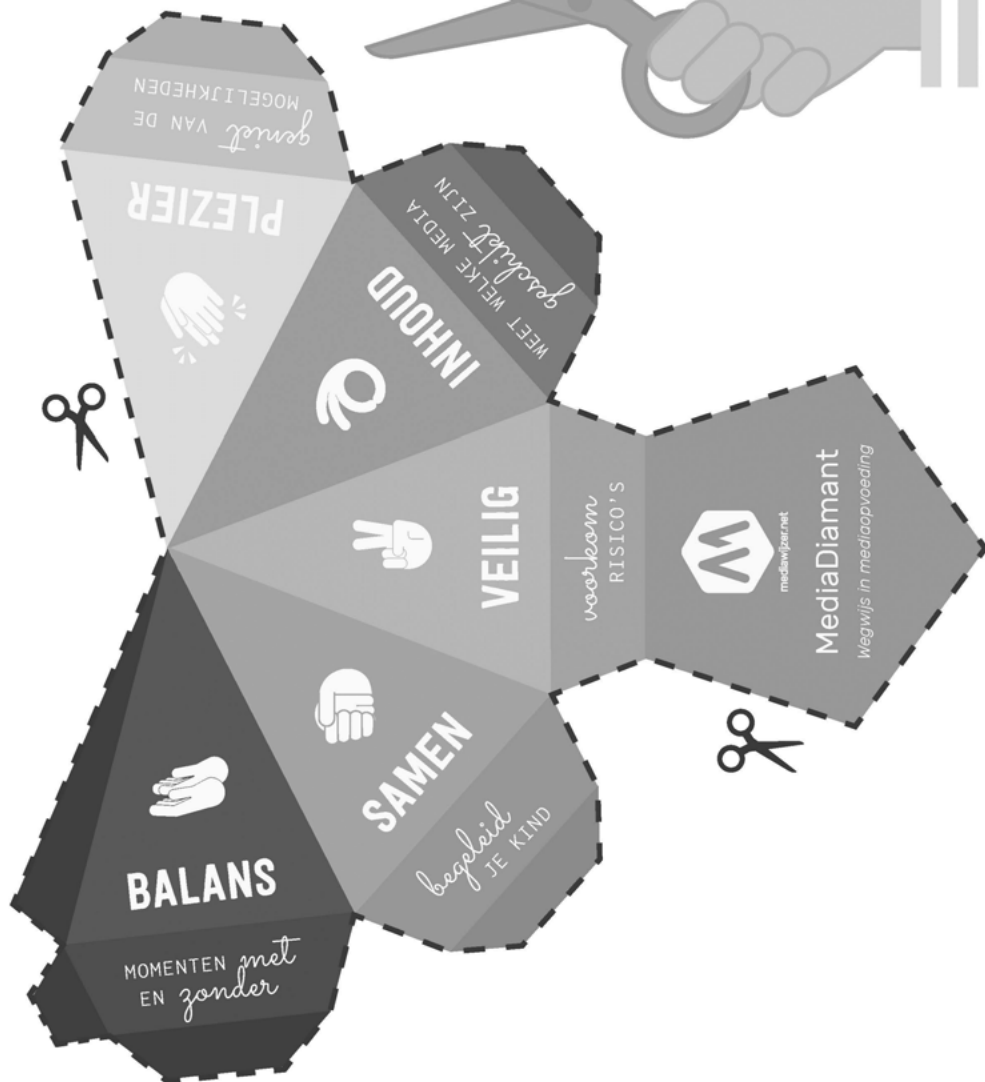
Koninklijke Bibliotheek
Nationale bibliotheek van Nederland



HOUD HET *zelf* IN DE HAND!

KNIP, VOUW & PLAK

JOUW *eigen* MEDIADIAMANT.



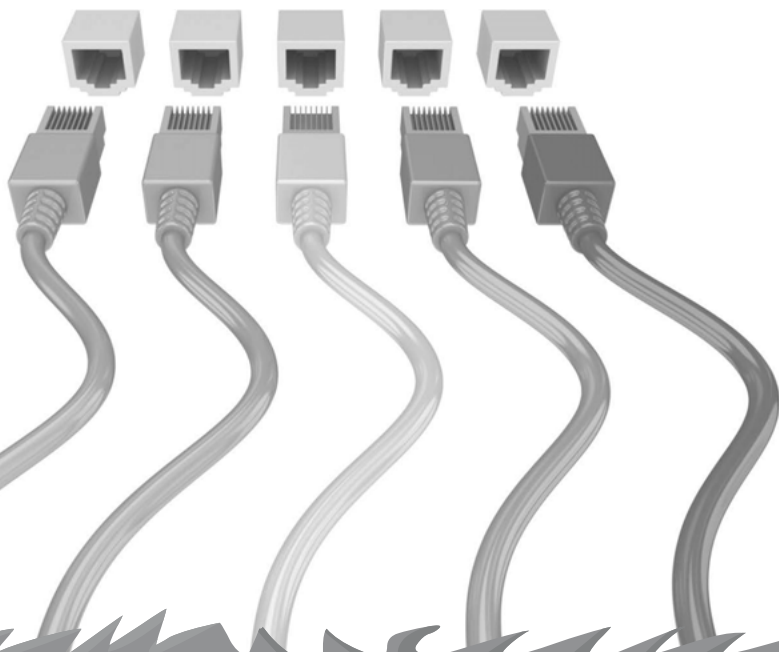
Organisaties op het gebied van Internetveiligheid en mediawijsheid

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



Pizza kerst boom

VRAAG ALTIJD
OF JE MAG GAAN
KOKEN!

Wat heb je nodig?

1 pak bladerdeeg

geraspte kaas

Groene paprika, in
dunne reepjes

Dun salami worstje

1 pot Bolognese saus

Bakpapier

Schaar

Potlood

Liniaal



Hoe maak je het klaar?

- Teken met een liniaal 10 kerstbomen op het bakpapier. Knip de kerstbomen uit.
- Leg op alle bladerdeegplakken de vorm van de kerstboom.
- Snij nu de kerstboom voorzichtig uit.
- verwarm de oven voor op 200 graden.
- Snij alle ingrediënten.
- Smeer de saus over de kerstbomen.
- Beleg naar eigen idee. En bestrooi met kaas.
- Bak de kerstbomen in ongeveer 15 a 20 minuten af.

SUR SLEUTEL

Bron: ah.nl



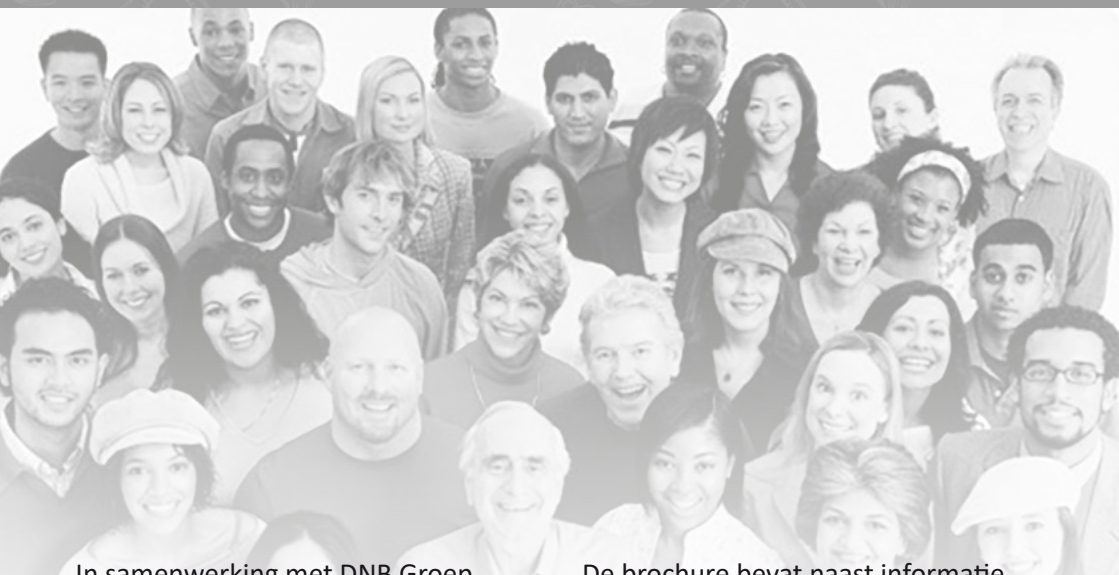
SURFSLEUTEL

Bron: ah.nl



Brochure "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 e-mail: receptie@dnbgroep.nl

Kinderinternet de Surfsleutel

Sociale en maatschappelijke doelstelling

Kinderinternet de Surfsleutel heeft een sociale en maatschappelijke 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 maatschappelijke 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 zij op eigen tempo kunnen 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! Zie ook www.sleutelenaanjetekomst.nl

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



Kinderinternet de Surfsleutel

Noordhaven 98
4761 DC Zevenbergen

Bezoekadres:
Noordhaven 98
4761 DC Zevenbergen

M: 06-48467697
(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.



jaargang 9 nummer 30