

Communicatietoolkit

Ministerie van Economische Zaken en Klimaat

**‘Doe je updates’**

*Januari 2020*

**Inleiding**

Onze levens zijn steeds vaker verbonden met het internet. Niet alleen door de laptop, tablet of mobiele telefoon, maar ook door bijvoorbeeld smart tv’s, slimme thermostaten en draadloze printers. Fijn, want ze maken ons dagelijks leven makkelijker. Maar ook kwetsbaarder. Via apparaten die met internet verbonden zijn, kunnen criminelen digitaal bij je inbreken. En zo je gezin begluren, je privégegevens inzien of je apparaat kapot maken. Tegelijkertijd is dit simpel te voorkomen. Regelmatig checken of er updates klaarstaan voor je apparaten en deze installeren, zorgt ervoor dat je apparaten veilig blijven. En dat criminelen moeilijker digitaal bij je kunnen inbreken.

Om mensen aan te zetten tot het regelmatig updaten van hun slimme apparaten, vervolgt het ministerie van Economische Zaken en Klimaat (EZK) vanaf dinsdag 4 februari 2020 de publiekscampagne ‘Doe je updates’[[1]](#footnote-1). Tijdens de campagne worden online video’s van verschillende lengtes, banners en social ads ingezet op diverse online en social kanalen. Ook wordt een radiocommercial uitgezonden en search ingezet en wordt via PR aandacht gevraagd voor het onderwerp. In deze toolkit vindt u een campagneplanning van deze middelen.

Deze toolkit helpt u, als convenantpartner, om uw klanten, gebruikers en andere stakeholders via uw eigen kanalen informeren over de noodzaak van het updaten van slimme apparaten én tips te geven over hoe dat te doen.

De toolkit bestaat uit de volgende onderdelen:

1. Nieuwsbericht naar aanleiding van de flitspeiling (onder embargo tot 4 februari, start van de campagne)
2. Flitspeiling januari 2020
3. Flyer met tips over het beveiligen van slimme apparaten
4. Mediaoverzicht van alle ingezette middelen in de kanalen en de timing
5. Artikel: Zo herken je een slim apparaat
6. Artikel: Zo update je de software op jouw slimme apparaten
7. Artikel: Zo kun jij je slimme apparaten beter beschermen
8. Voorbeelden social posts

Voor alle campagnematerialen kunt u vanaf 3 februari terecht op [www.campagnetoolkits.nl/doejeupdates](http://www.campagnetoolkits.nl/doejeupdates). Hier vindt u de online video’s, radiospots en andere middelen die tijdens de campagne worden ingezet.

Notabene: er rusten beeldrechten op de campagnevideo’s en -foto’s. Beeldmateriaal mag **ALLEEN** online ingezet worden. De maximale gebruiksperiode is 1 jaar vanaf 4 februari 2020.

Bij vragen over deze toolkit of over de campagne ‘Doe je updates’ kijkt u op [www.doejeupdates.nl](http://www.doejeupdates.nl). Daarnaast kunt u contact opnemen met Noura el Farissi, communicatieadviseur bij het ministerie van Economische Zaken en Klimaat via 06 55 49 39 25 of [n.elfarissi@minezk.nl](mailto:n.elfarissi@minezk.nl) of Marion Beishuizen, campagnemanager bij de Dienst Publiek en Communicatie via 06 29 23 02 60 of [m.beishuizen@minaz.nl](mailto:m.beishuizen@minaz.nl).

Voor meer informatie over de ‘Doe je updates’-campagne ga je naar [www.doejeupdates.nl](http://www.doejeupdates.nl).

Bijlage: Onderzoeksrapport (flitspeiling)

**Mediaoverzicht**

In het mediaoverzicht vindt u de middelen die tijdens de Doe je updates-campagne worden ingezet, inclusief de timings en kanalen. Hierin is advertising meegenomen, maar ook PR inzet en berichten die via de eigen kanalen van EZK worden uitgezet. Het media overzicht geeft u informatie over de totaalinzet aan communicatie vanuit EZK. U kunt het mediaoverzicht gebruiken om bijvoorbeeld berichten van EZK te reposten of om in te haken op berichten die verschijnen in de media. De campagnestart is op dinsdag 4 februari 2020 met het persbericht. Dit wordt nagezonden.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Middel** | **Kanaal** | **Februari** | | | | | **Maart** | | | | |
| **Weeknummer** | | | | | | | | | |
| **6** | **7** | **8** | **9** | **10** | | **11** | **12** | **13** | **14** |
| **PR** | | | | | | | | | | | |
| Nieuwsbericht (4 feb) en persbenadering | PR | 4-2 | 11-2 |  |  |  | |  |  |  |  |
| Twee artikelen (smarticle) | NU.nl | TBD | TBD |  |  |  | |  |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |  |
| **AV** | | | | | | | | | | | |
| Pre roll (30 en 15 sec video) | Talpa TV  RTL XL  Rtl.nl | 4-2 |  |  |  |  | | 15-3 |  |  |  |
| Video link ad (6 sec) | Instagram/ Facebook |  |  | 16-2 |  |  | | 15-3 |  |  |  |
| Introductievideo Hans (lange video) | Twitter + Facebook EZK | 4-2 |  | 16-2 |  |  | |  |  |  |  |
| **Radio** | | | | | | | | | | | |
| Radiospot (30 sec) | Radio (alle exploitanten) | 4-2 |  | 23-2 |  |  | |  |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |  |
| **Online** | | | | | | | | | | | |
| Display (banners) | Contextueel | 4-2 |  |  |  |  | |  |  |  | 5-4 |
| Radiospot (20 sec) | Spotify |  |  | 16-2 |  |  | |  | 22-3 |  |  |
| Video | YouTube |  |  | 16-2 |  |  | |  | 22-3 |  |  |
| Display (banners) | Tweakers |  |  | 16-2 |  |  | | 15-3 |  |  |  |
| Zoekwoorden | Search | <6-1 |  |  |  |  | | 15-3 |  |  |  |
|  |  |  |  |  |  |  | |  |  |  |  |

**Artikel: zo herken je een slim apparaat**

*Slimme apparaten zijn verbonden met internet. Maar waaraan kun je een slim apparaat nog meer herkennen? In dit artikel worden tips gegeven hoe je dat doet. Je kunt dit artikel bijvoorbeeld gebruiken voor in een online nieuwsbrief, magazine of op je website.*

*Advies over moment van plaatsing: vanaf 4 februari 2020*

**Zo herken je een slim apparaat**

Wat een slim apparaat slim maakt, is heel simpel. Want: elk apparaat dat verbonden is met internet is een slim apparaat. En dat zijn er meer dan je denkt. Je smart tv bijvoorbeeld, maar mogelijk ook je stofzuiger, thermostaat en vaatwasser. En wat dacht je van babyfoons die je op afstand kunt bedienen, speakers of een slimme deurbel. En de router natuurlijk, want dat is de toegangspoort tot het internet in jouw huis.

Om te checken of je te maken hebt met een slim apparaat, beantwoord je vijf simpele vragen.

1. Maakt het apparaat verbinding met WiFi of Bluetooth?
2. Kan ik het apparaat bedienen met mijn smartphone?
3. Toont mijn apparaat actuele informatie, zoals het weer op de plek waar je bent?
4. Praat het apparaat terug?
5. Herkent het apparaat personen of hun naam?

Als je op de meeste vragen ‘ja’ antwoordt, heb je waarschijnlijk te maken met een slim apparaat.

**Slimme apparaten vereisen updates**

Nu je weet dat je een slim apparaat hebt, weet je ook dat je dit apparaat moet updaten. Slimme apparaten maken het leven makkelijk, maar ook kwetsbaarder. Via slimme apparaten kunnen criminelen digitaal bij je inbreken. En zo je gezin begluren, privégegevens stelen, of je apparaat kapotmaken. Je voorkomt dit door de software van je slimme apparaten regelmatig te updaten. Doe dus je updates en blijf veilig.

Meer tips? Ga naar [www.doejeupdates.nl](http://www.doejeupdates.nl).

**Artikel: Zo update je de software op jouw slimme apparaten**

*Slimme apparaten maken het leven makkelijker. Bijvoorbeeld door informatie te geven over het weer op je locatie of doordat ze op afstand te bedienen zijn. Slimme apparaten maken het leven ook kwetsbaarder, doordat criminelen via internet bij je kunnen inbreken. In dit artikel geven we tips over het updaten van je slimme apparaten. Je kunt dit artikel bijvoorbeeld gebruiken voor in een nieuwsbrief, magazine of op je website.*

*Advies over moment van plaatsing: dinsdag 11 februari 2020*

**Zo update je de software op jouw slimme apparaten**

Onze levens zijn steeds meer verbonden met het internet. Via je smart tv bijvoorbeeld, maar ook via een slimme thermostaat of draadloze printer. Dat is fijn, want slimme apparaten maken het leven makkelijker. Tegelijkertijd maken ze je leven ook kwetsbaarder. Want doordat deze apparaten verbonden zijn met internet kunnen criminelen digitaal bij je inbreken. Zo kunnen ze je gezin begluren, je privégegevens stelen of je apparaat kapot maken. Gelukkig is een digitale inbraak simpel te voorkomen door software-updates voor je apparaten uit te voeren. Update daarom regelmatig je software en bescherm jezelf en je gezin voor een digitale inbraak.

Je slimme apparaat updaten is heel makkelijk. Volg onderstaande stappen en je bent zo weer veilig en verbonden.

1. Zoek online naar de juiste software-update. Typ het merk, het soort apparaat en ‘update’ in de zoekbalk.
2. Volg de instructies van de fabrikant. Schakel waar mogelijk automatische updates in.
3. Kom je er niet uit? Neem contact op met de fabrikant.

Vaak vind je in het instellingenmenu van je slimme apparaat een optie ‘Controleren op updates’. Doe dit regelmatig, zodat je er zeker van bent dat je slimme apparaten geen risico vormen.

**De risico’s van slimme apparaten**

Als je de beschikbare updates niet installeert, raakt de software op je slimme apparaten verouderd. Dat weten internetcriminelen. Daarom zoeken zij naar kwetsbaarheden in oude software. Met alle gevolgen van dien. Want hebben criminelen eenmaal toegang tot één slim apparaat, dan kunnen zij via je thuisnetwerk ook bij je andere apparaten. Zo kunnen ze bij je desktop of laptop en krijgen ze toegang tot je informatie en foto’s. Check dus direct of er updates beschikbaar zijn, want ze bevatten naast nieuwe functionaliteiten ook belangrijke beveiligingsoplossingen.

Ga voor meer tips naar [www.doejeupdates.nl](http://www.doejeupdates.nl).

**Artikel: Zo kun jij je slimme apparaten beter beschermen**

*Naast het updaten van je slimme apparaten zijn er meer dingen die mensen kunnen doen om zichzelf en hun gezin te beschermen tegen een digitale inbraak. In dit artikel geven we tips hoe mensen hun slimme apparaten nóg beter kunnen beschermen. Je kunt dit artikel bijvoorbeeld gebruiken voor in een nieuwsbrief, magazine of op je website.*

*Advies over moment van plaatsing: dinsdag 18 februari 2020*

**Zo kun jij je slimme apparaten beter beschermen**

Je hebt je slimme apparaten beveiligd om te voorkomen dat criminelen niet meer digitaal bij je inbreken. Lekker bezig. Toch kun je meer doen om je apparaten en daarmee jezelf beter te beschermen. Hieronder geven wij je 4 tips:

1. Schakel, als dat kan, automatische updates in. Als je automatische updates inschakelt, heb je geen omkijken meer naar de software-updates op je slimme apparaten. Ze worden geüpdatet als je ze even niet gebruikt.
2. Kan dat niet? Zet een periodieke herinnering in je smartphone om jezelf aan het updaten van je slimme apparaten te herinneren.
3. Verander het standaardwachtwoord van je apparaat in een nieuw, sterk wachtwoord dat je alleen voor dit apparaat gebruikt. Waar een sterk wachtwoord aan moet voldoen, lees je op [www.veiliginternetten.nl/wachtwoorden/](http://www.veiliginternetten.nl/wachtwoorden/).
4. Stel jezelf de vraag of het echt nodig is om je apparaat te verbinden met het internet. Als je niet alle slimme functies gebruikt, kan het misschien ook wel zonder.
5. Update regelmatig de router waarmee je het apparaat met het internet verbindt.

**Slim apparaat kopen? Check eerst dit!**

Bij de aanschaf van een slim apparaat kun je al rekening houden met de veiligheid. Controleer bijvoorbeeld of je bij de fabrikant of leverancier terecht kunt voor vragen, of je het apparaat makkelijk (automatisch) kunt updaten en hoe lang het apparaat nog wordt ondersteund met software-updates. Welk apparaat je ook in huis haalt, weet dat je deze moet aansluiten op je WiFi-netwerk. Dus wees slim, en check de veiligheid van het slimme apparaat voor je het koopt.

Meer weten? Ga naar [www.doejeupdates.nl](http://www.doejeupdates.nl).

**Voorbeelden social posts**

*Deze social posts kunnen als leidraad dienen voor gebruik op eigen sociale kanalen. Gebruik bij posts over de ‘Doe je updates’-campagne de campagnehashtag #doejeupdates. Daarnaast worden vanuit het ministerie van Economische Zaken online video’s, banners en social posts als advertising ingezet. Deze kunnen gedeeld worden of ingezet worden in de eigen online en social kanalen. Zie voor meer informatie over welk middel wanneer geplaatst wordt het mediaoverzicht.*

Voor alle campagnematerialen kunt u vanaf 3 februari terecht op [www.campagnetoolkits.nl/doejeupdates](http://www.campagnetoolkits.nl/doejeupdates). Hier vindt u de online video’s, radiocommercials en andere middelen die tijdens de campagne worden ingezet.

Notabene: er rusten beeldrechten op de campagnevideo’s en -foto’s. Beeldmateriaal mag **ALLEEN** online gebruikt worden. De maximale gebruiksperiode is 1 jaar vanaf 4 februari 2020.

**Start campagne op 4 februari**

* Wij zijn partner van de Doe je updates-campagne die vandaag start. Want slimme apparaten zijn leuk zolang ze veilig zijn. Update daarom regelmatig je software en kijk voor beveiligingstips op doejeupdates.nl. #doejeupdates
* Slimme apparaten in huis? Update ze regelmatig en zorg ervoor dat je jezelf en je gezin beschermt tegen een digitale inbraak. Kijk op doejeupdates.nl voor tips. #doejeupdates

**Tijdens de campagne (4 februari 2020 – 13 maart 2020)**

* Wij vragen samen met het ministerie van Economische Zaken en Klimaat aandacht voor het beveiligen van je slimme apparaten. Software-updates zorgen ervoor dat je apparaten veilig blijven. Update ze daarom regelmatig. Kijk voor meer tips op doejeupdates.nl #doejeupdates
* Jezelf beschermen tegen een digitale inbraak is simpel: update je slimme apparaten! Ga naar doejeupdates.nl voor tips en #doejeupdates.
* Slim apparaat op het oog? Informeer bij de fabrikant hoe het zit met updates en kijk op doejeupdates.nl voor meer tips. #doejeupdates.
* Meer dan de helft van de Nederlanders stelt updates voor slimme apparaten uit of vergeet die uit te voeren. Dat geeft criminelen de kans digitaal bij je in te breken. Ga naar doejeupdates.nl en #doejeupdates
* Heb jij een slim apparaat? Vier op de tien Nederlanders hebben een of meer slimme apparaten in huis. Populairst zijn smart tv, printer en smartwatch. Beveilig ze met de tips op doejeupdates.nl. #doejeupdates

1. In de uitingen van de campagne ‘Doe je updates’ van het ministerie van Economische Zaken en Klimaat is een (hobby)hacker te zien. Deze hacker is zelf een acteur, maar hij staat symbool voor een (ethische) hacker die kennis deelt over kwetsbaarheden in producten of diensten met organisaties en fabrikanten. Dit gebeurt naar aanleiding van de leidraad Coordinated Vulnerability Disclosure (CVD) welke als doel heeft om bij te dragen aan de veiligheid van ICT-systemen. De vinder kan door Coordinated Vulnerability Disclosure de eigenaren van die producten of diensten op de hoogte stellen of de fabrikant informeren. Eigenaren en fabrikanten kunnen dan maatregelen nemen voordat de kwetsbaarheden actief misbruikt zullen worden door derden. [↑](#footnote-ref-1)