Infomedics

Uw tandartspraktijk

Een goudmijn voor internetcriminelen

Wat gaan we doen?

De digitale data-explosie

Nieuwe privacywetgeving (a giant leap for mankind)

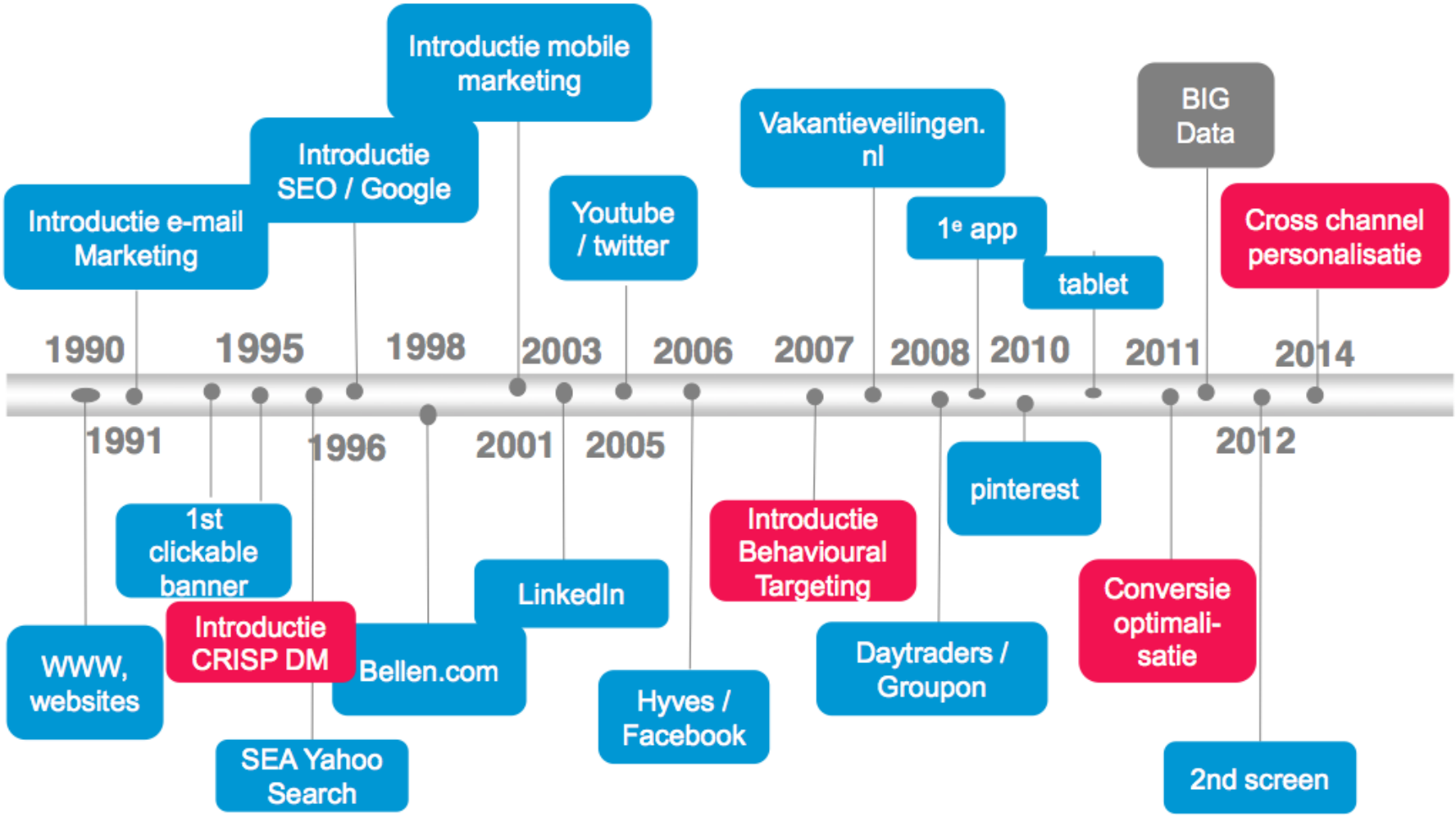
Wat wilt u onze hacker vragen?

Help! Uw praktijk ligt onder vuur!

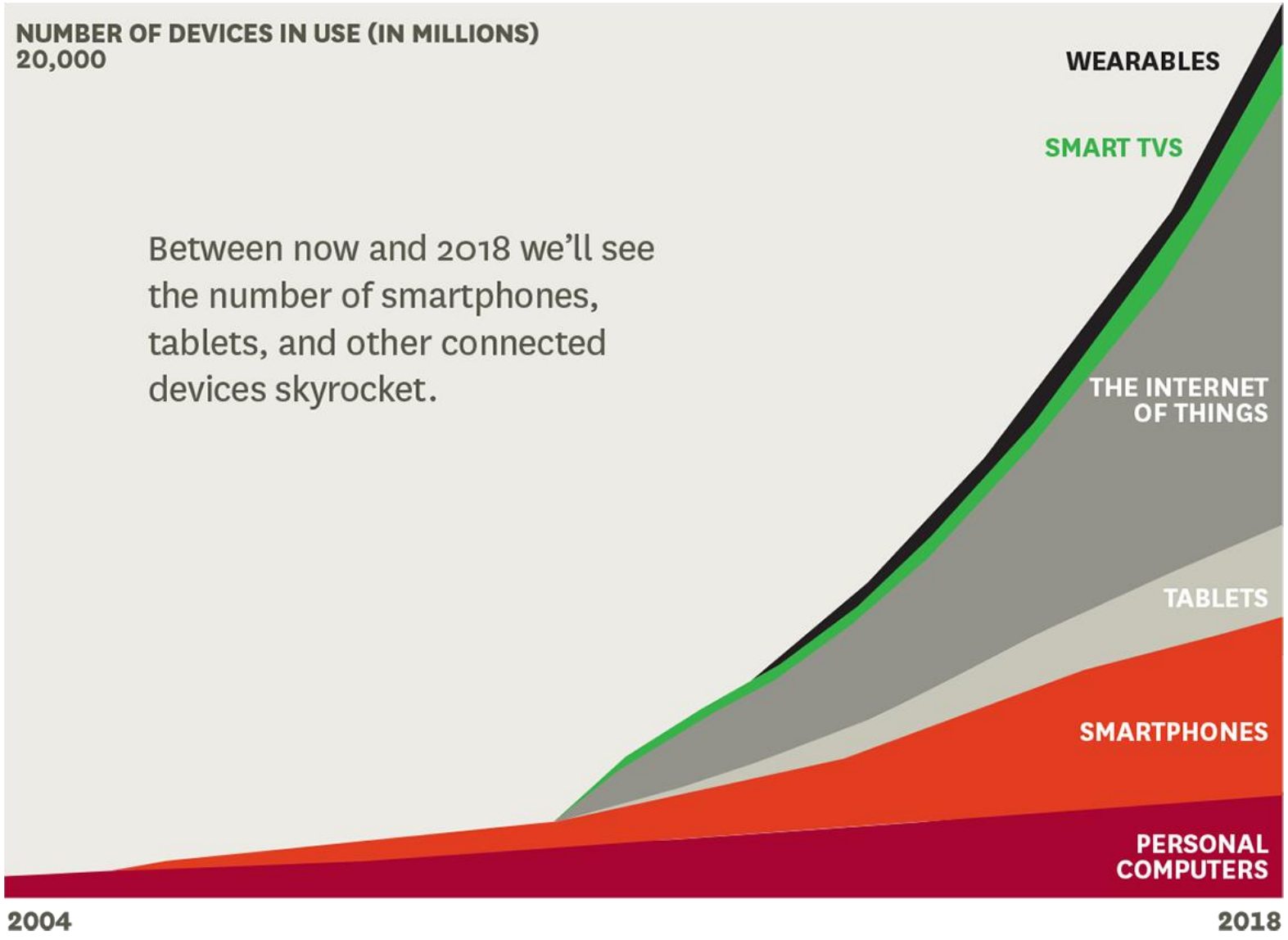
Hoe heeft Infomedics uw informatieveiligheid georganiseerd?

Wat kunt (moet?) u zelf doen?

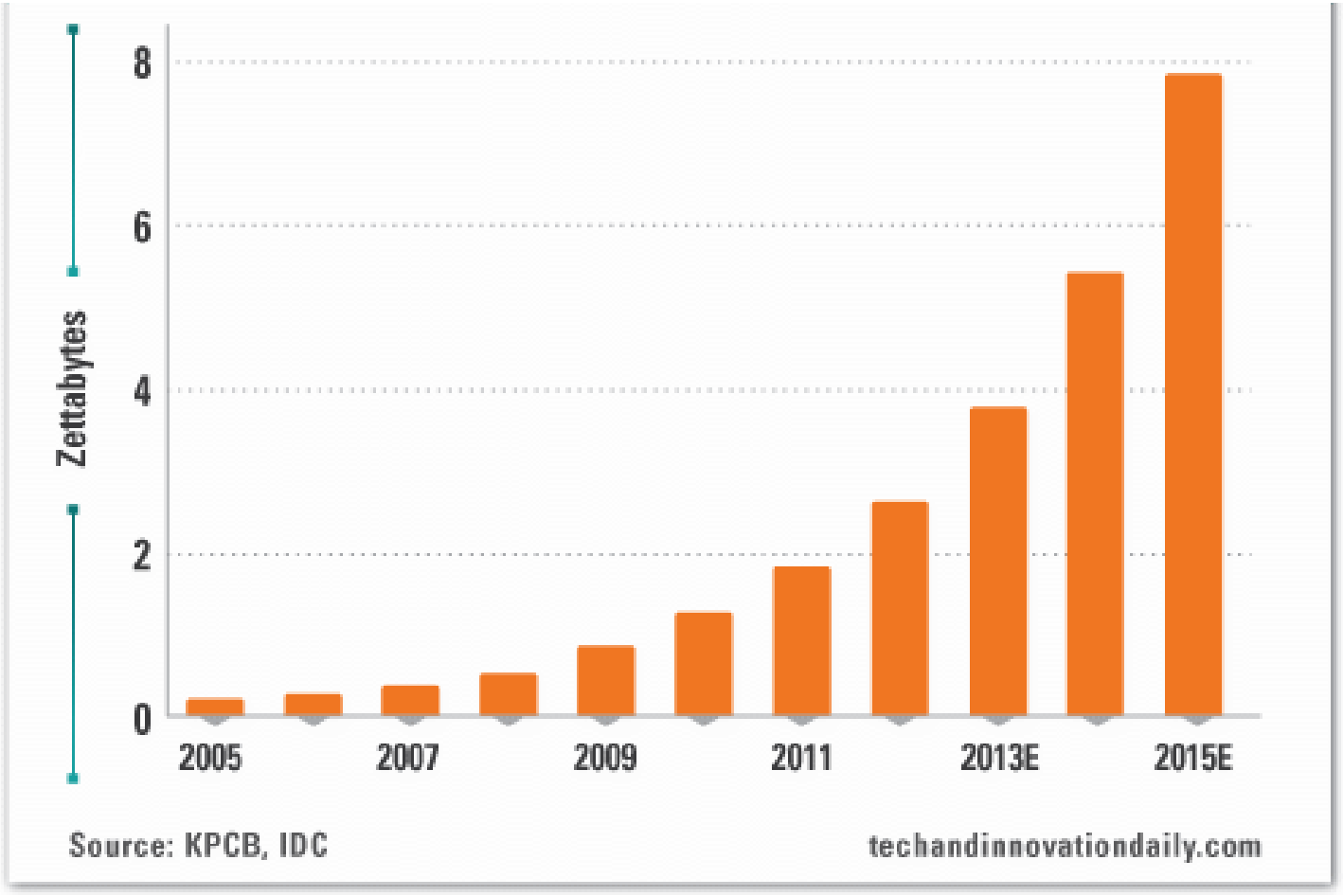
De digitale data-explosie



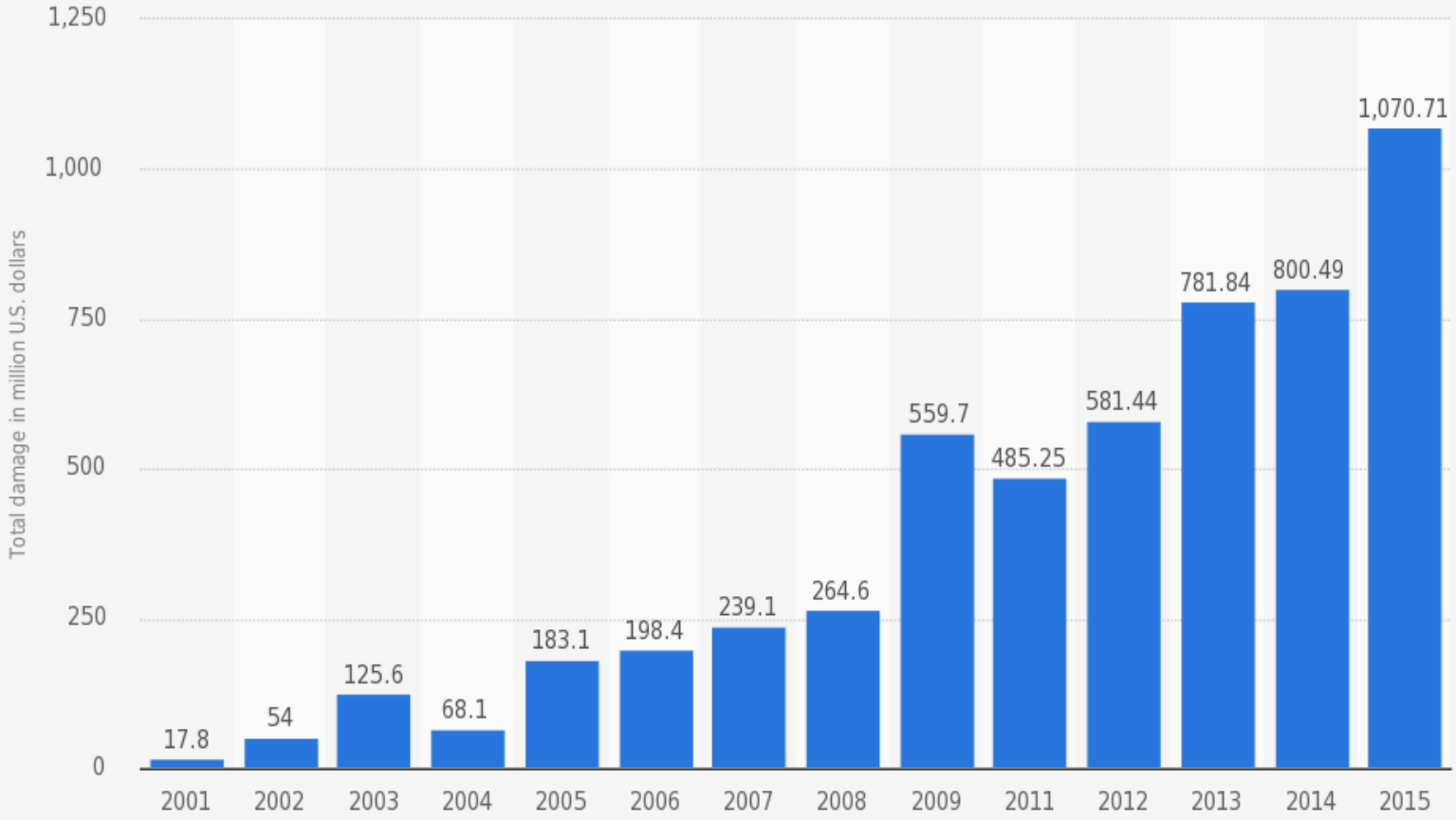
Ontwikkeling datagebruik



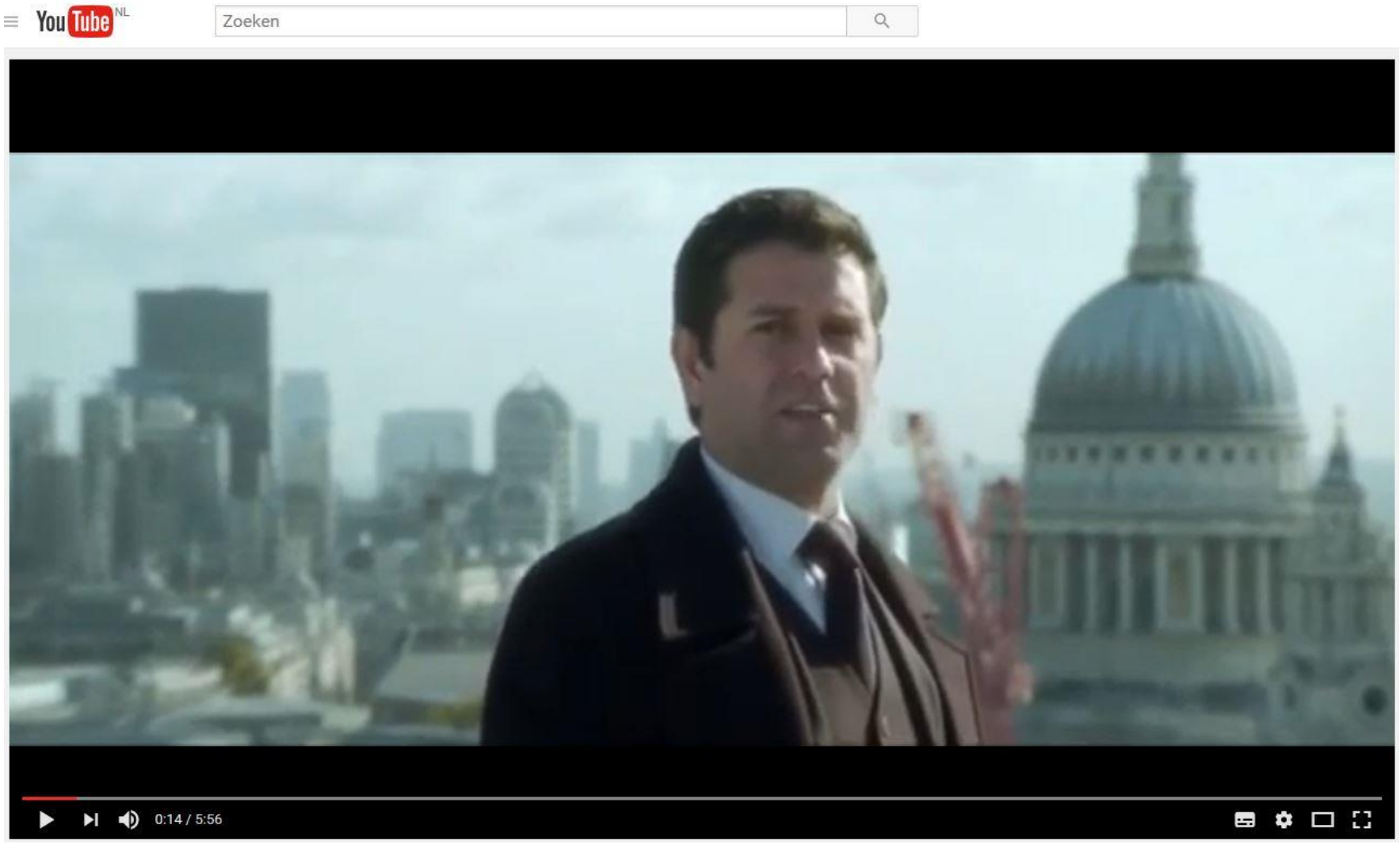
De digitale data-explosie



Ontwikkeling van datamisbruik



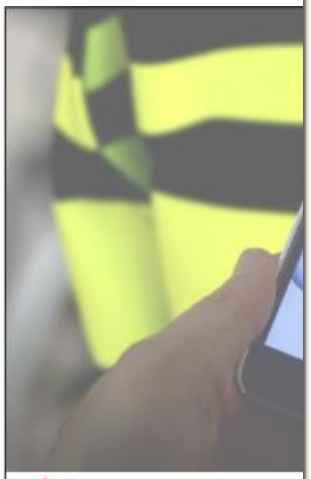
Hacken doe je zo …



https://www.youtube.com/watch?v=3WpLT059MZk

Infomedics

Hacks in het nieuws…



© anp

Instagram-h… ondoordacht…

Maandag werd bekend dat er… misbruiken van instagramac… na die hacks bedrijven name… verkopen, en gingen er verv… nu eigenlijk als je zomaar ge… tussenpersoon advertenties… experts.

Karolien Koolhof 14-03-16, 15:5…

f 0 0

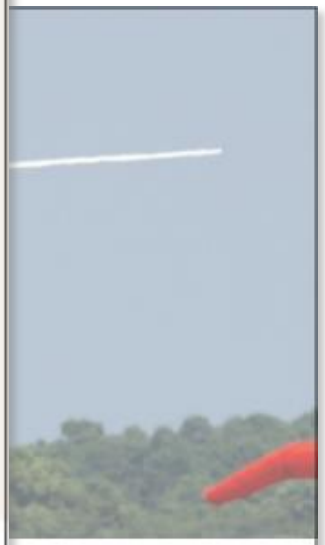
© Thinkstock

Hacker steelt miljoenen Amerikaanse 'sofinummers'

Een hacker is erin geslaagd om 3,6 miljoen social security numbers (de Amerikaanse versie van sofinummers) te bemachtigen uit een database in de Amerikaanse staat South Carolina.

Door: Thomas van der Kolk 27-10-12, 18:35 Laatste update: 18-02-16, 08:38

f 0 0 0



…ang tot…

…is aan Anonymous, …n. Ook zouden zij een …gehackt. NASA ontkent

…e: 09-05-16, 18:33

Data is het nieuwe goud

- Data is overal
- De waarde van data is groot (vooral van complete datasets)
- Data is relatief eenvoudig te stelen, hackers zijn sluw, brutaal en vindingrijk
- De pakkans bij cyber crime is klein
- Transport van de buit is eenvoudig, smokkelen is niet nodig
- Data hotspots zijn kwetsbaar
- Voor een hacker is uw praktijk EEN PROJECT

Wetgeving in historisch perspectief

Wetgeving loopt altijd achter op dynamische werkelijkheid, maar met recente wetgeving is er flink gerepareerd.

Wat staat er in de AVG?

- Rechtmatigheid, eerlijkheid en transparantie
- Integriteit en vertrouwelijkheid
- Dataminimalisering
- Afbakening van het doel
- Afbakening van de opslag
- Nauwkeurigheid
- Verantwoording door de controller

- Geen ondersteunende wetgeving nodig
- Autoriteit Persoonsgegevens kan en zal handhaven
- Hogere boetes

Autoriteit Persoonsgegevens

Onze missie

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

- Voorheen College Bescherming Persoonsgegevens (CPB)
- Belangrijke toezichthouder want privacy is een grondrecht
- Meer gewicht dan bijvoorbeeld de Nza
- Wet niet correct nageleefd > bindende aanwijzing
- Fout niet hersteld > boete van 10% van jaaromzet of max EUR 810.000

Onderzoek Qfast tandartspraktijken

Onderzoeksopzet

- Forensische meting en verkeersanalyse 26 tandartspraktijken
- Scan op malafide IP-adressen, bekende exploits en digitaal gedrag systemen
- Onderzoeksperiode beslaat 5 maanden (2015/2016)

Conclusies

- Gemiddeld 6.000.000 aanvallen per maand (= 230.000 per praktijk)
- Technische beveiliging (firewall, antivirus) is vaak onder de maat
- Software is vaak niet up-to-date
- IT wordt niet of slecht beheerd, beheer vindt plaats op afroep en is reactief
- IT-beheer vindt niet plaats door echte professionals
- Veel menselijke fouten (onbeheerde werkstations, passwords op prikbord)

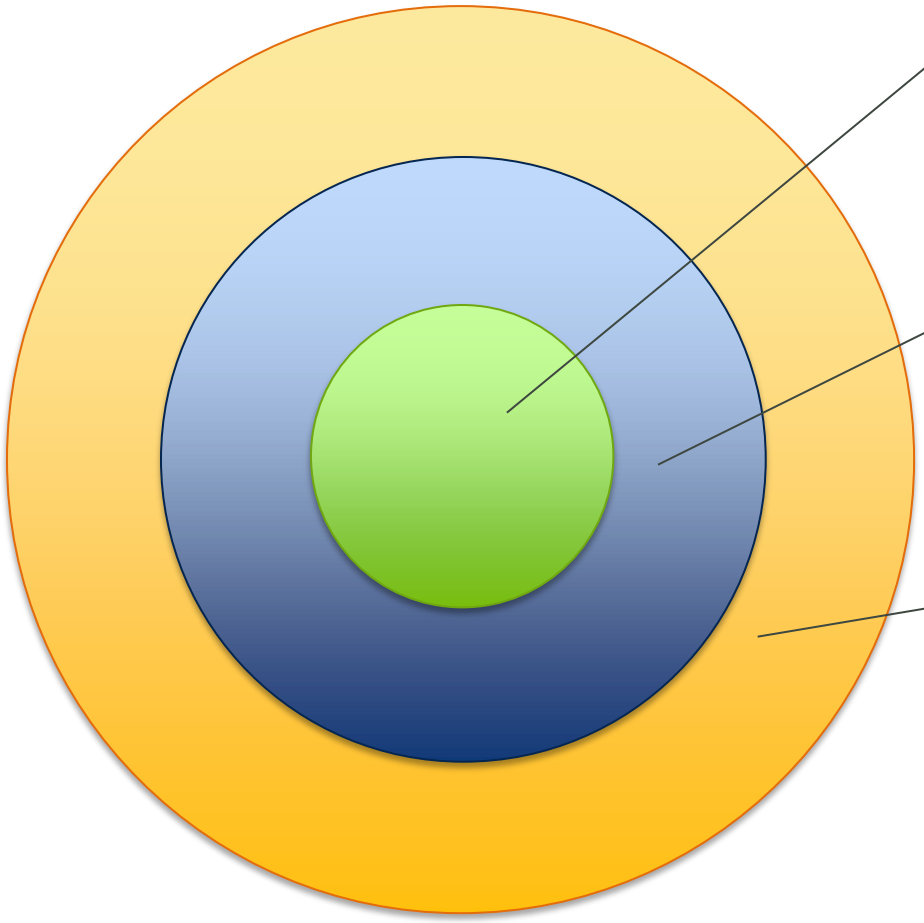
Informatieveiligheid bij Infomedics

- Factoringsysteem (software) > gebouwd onder ‘privacy by design’ principe
- ISO 27001 certificering > internationaal erkende norm
- Ketencertificering en –toezicht > alle ketenpartners ISO27001
- Geregistreerd bij AP als Verantwoordelijke
- Lid van Centrum voor Informatiebeveiliging en Privacybescherming

Wat betekent dit concreet?

Informatiebeveiligingsbeleid – Jaarlijkse ISO 27001 audit – Jaarlijkse hacktest - Opleiding en training medewerkers – Control framework van 114 normen – Systeem van incidentmeldingen – Structuur voor melding datalekken aan AP – Privacy Officer en Security Officer – Uitwisseling persoonlijke gegevens alleen via beveiligde verbindingen – Controle op de hele keten

Safety scope voor de praktijk



<u>Uw praktijk</u>
- techniek
- fysieke inrichting
- gedrag van mensen

<u>Uw partners/leveranciers</u>
- bewerkersovereenkomst
- ISO27001 certificering
- controle op naleving

<u>Partners van uw partners</u>
- ketencertificering
- ISO 27001 en niets minder!
- controle op naleving

Vijf dingen om direct te doen

1. Betrek een specialist bij veiligheid in de eerste ring (uw eigen praktijk). Vaak biedt een safety scan u snel inzicht tegen lage kosten.
2. Werk alleen met gegevensbewerkers die ISO27001 gecertificeerd zijn! NEN7510 certificering alleen is niet genoeg.
3. Controleer de afspraken die uw partners/leveranciers gemaakt hebben met hun partners/leveranciers. En sluit bewerkersovereenkomsten af.
4. Zet een informatiebeveiligingsbeleid op samen met de medewerkers binnen uw praktijk. Dit zorgt voor bewustwording.
5. Maak een simpel protocol voor het melden van datalekken (https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken).

Infomedics

Afsluiting