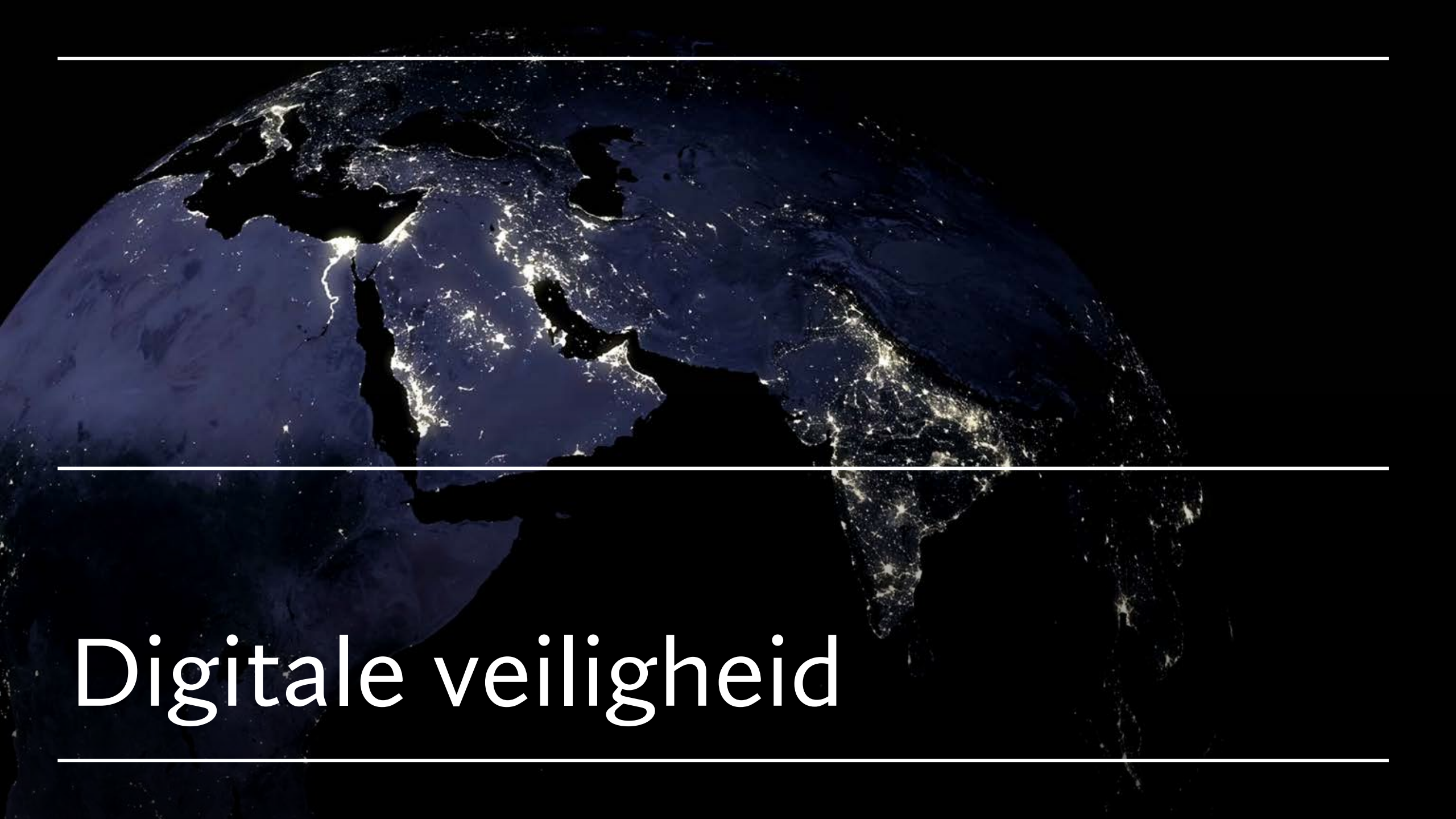
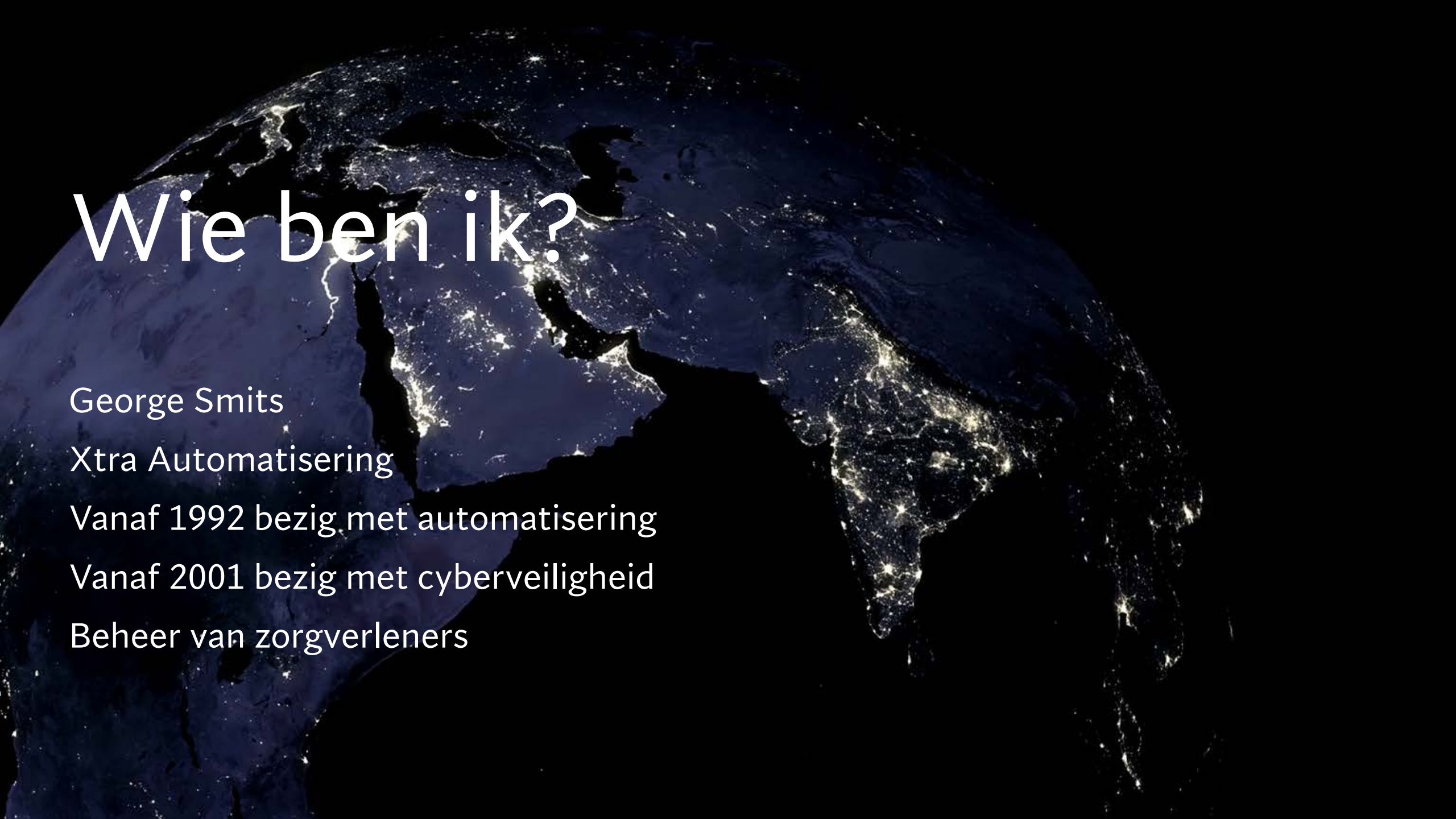


Digitale veiligheid



Wie ben ik?

George Smits

Xtra Automatisering

Vanaf 1992 bezig met automatisering

Vanaf 2001 bezig met cyberveiligheid

Beheer van zorgverleners

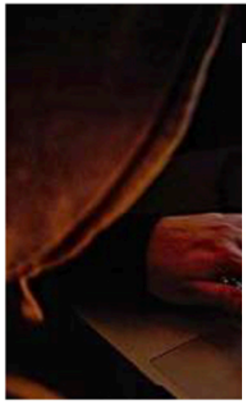
Wat gebeurt er in de wereld?

KASSA'S WERKTEN NIET

Alle Deense 7-Elevens dicht na hackaanval

De Amerikaanse supermarktketen 7-Eleven moest maandag al zijn winkels in Denemarken sluiten na een vermoedelijke hackaanval. Winkelpersoneel kon daardoor niet langer gebruikmaken van de kassa's.

Directeur van de supermarktketen in Denemarken Jesper Ostergaard gaf bij het Deense televisiestation DR aan dat het incident plotseling gebeurde. „De kassa's werkten ineens niet meer en medewerkers begonnen meldingen te doen. Dat is nog nooit gebeurd." 7-Eleven heeft in totaal 175 winkels in Denemarken.



LOSGELD NA

Tandarts voor cyb

OOSTERHOUT • Cy de computersyste um Dental aangeva standen werden d waardoor alle aan ten. De aanvallers dat betaald. „Allee deze korte termij minimaliseren en weer herstellen", drijf zegt niet hoe

Colosseum Dent praktijken in Europa, waarvan ruim 130 in Nederland en België. De tandartsen behandelen jaarlijks ongeveer 600.000 mensen, aldus het bedrijf.

Universiteit Maastricht betaalde 197.000

Fonds

De bitcoins zijn op het moment een stuk meer waard, waardoor de universiteit nu zo'n half miljoen euro terugkrijgt. Het geld is al omgezet van crypto- naar gewone valuta, aldus de universiteitswoordvoerder, maar er moet juridisch nog een en ander geregeld worden voor het op de rekening van het instituut staat.

Ondanks dat de Universiteit Maastricht meer geld terugkrijgt dan ze aan losgeld betaalde, benadrukt de woordvoerder dat er geen sprake is van winst. "De totale schade was flink hoger dan wat er nu terugkomt." Zo moest er onder meer een ICT-bedrijf worden ingehuurd. "Niettemin zijn we hier erg blij mee."

Het geld zal worden ondergebracht in een fonds voor studenten met financiële problemen. "Tijdens die cyberaanval - maar vooral tijdens de coronapandemie daarna - hebben we gezien hoe kwetsbaar studenten zijn."

e ton aan losgeld betaald
utersystemen kort voor

emaakt tijdens een
anval. Het gijzelvirus legde
lam. De universiteit zag
dan te betalen.

De cyberaanval gebeurde met ransomware. Daarbij worden bestanden gegijzeld, die in ruil voor losgeld pas weer beschikbaar komen.

Wat moet je regelen?

1. Zorg voor een goed betaald beveiligingsproduct. Antivirus is niet voldoende. Let op de Nederlandse ondersteuning. Advies: ESET Internet Security.
2. Updates meteen uitvoeren, liefst automatisch. Herstart direct, stel niet uit.
3. Back-up jouw data. Liefst online met goede retentieperiode. Voor foto's is Google een prima partner.
4. Overal een ander onleesbaar wachtwoord van minimaal 10 tekens met hoofd- en kleine letters, cijfers en speciale tekens. Gebruik een wachtwoordkluis. Advies: Lastpass.
5. Wijzig het wachtwoord voor de instellingen van jouw wifi. Gebruik een psk (zie 4). Zet gasttoegang uit indien niet nodig.
6. Versleutel de gegevens van de laptop. Advies: ESET Smart Security Premium.
7. Gebruik waar mogelijk twee factor authenticatie (wachtwoord + wat je hebt).
8. Gebruik een betaalde VPN bij het surfen. Advies: NordVPN

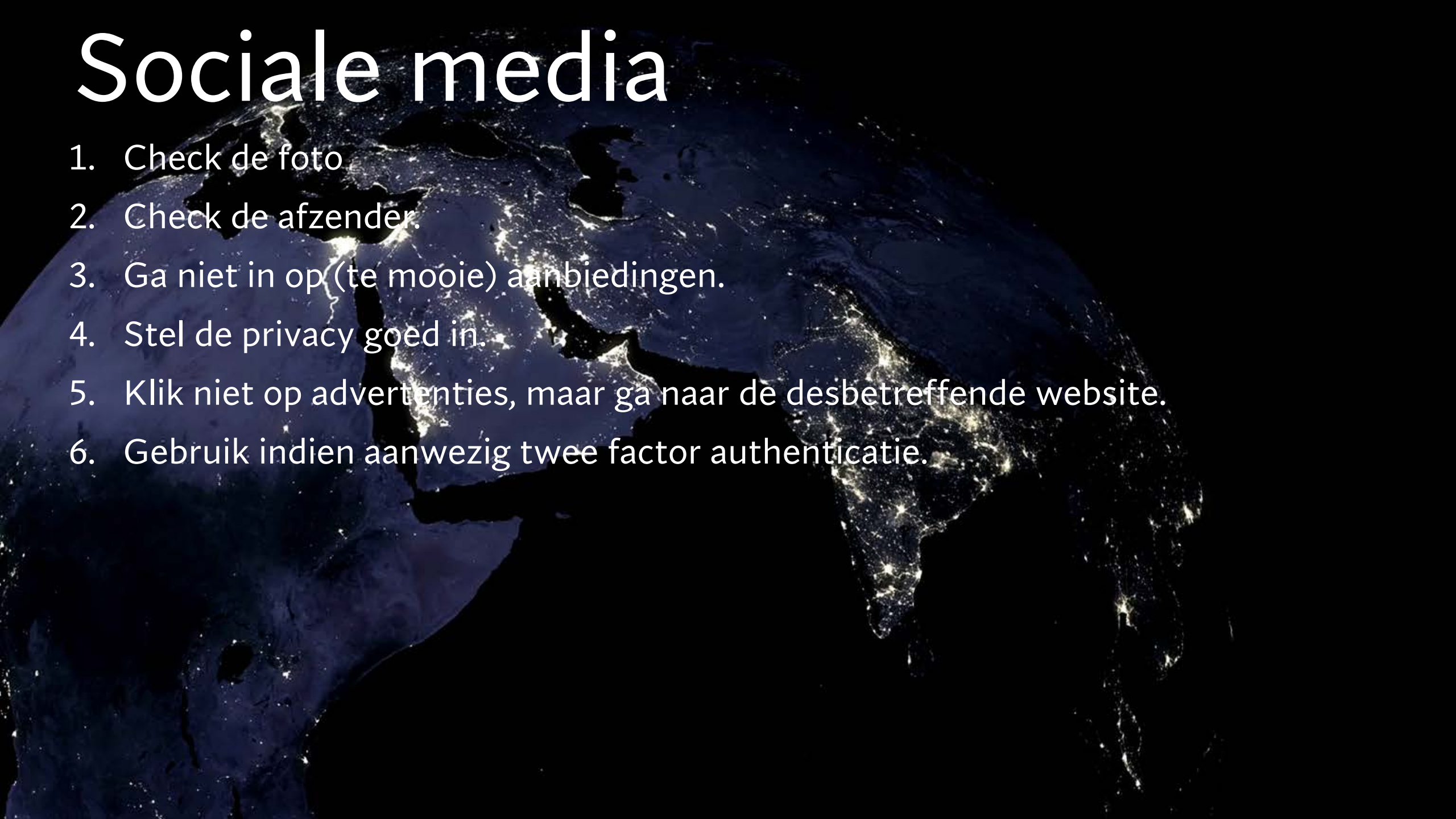
Hoe te surfen?

1. Verwijder onbetrouwbare of niet gebruikte plug-ins uit je browser.
2. Update meteen van de browser en plug-ins uitvoeren, liefst automatisch.
3. Surf alleen naar beveiligde websites (https).
4. Download alleen van betrouwbare websites.
5. Klik niet op advertenties, maar ga naar de desbetreffende website.
6. Gebruik indien aanwezig twee factor authenticatie.
7. Gebruik een VPN (zie vorige dia punt 8).
8. Let op de privacyinstellingen van de browser (geschiedenis, cookies, etc.)
9. Gebruik een op privacy gerichte zoekmachine zoals DuckDuckGo.
10. Gebruik incognito surfen.

Mail

1. Controleer de afzender.
2. Ook al klopt de afzender, vertrouw niet de mail zomaar.
3. Klik niet zo maar op een link of plaatje, maar ga direct naar de juiste website.
4. Open niet zomaar de bijlagen.
5. Er is geen enkele bank die jou via een link naar de bank lokt om in te loggen.
6. Let op valse betaalverzoeken en facturen van de CJIB, Belastingdienst, etc.
7. Er is geen rijke tante in Congo of een weldoener die jou € 5.000.000,00 schenkt en waar je eerst geld naar moet overmaken.
8. Er zijn geen bewijzen van kinderporno op jouw computer.
9. Er zijn geen comprimerende beelden van jou achter je computer.

Sociale media

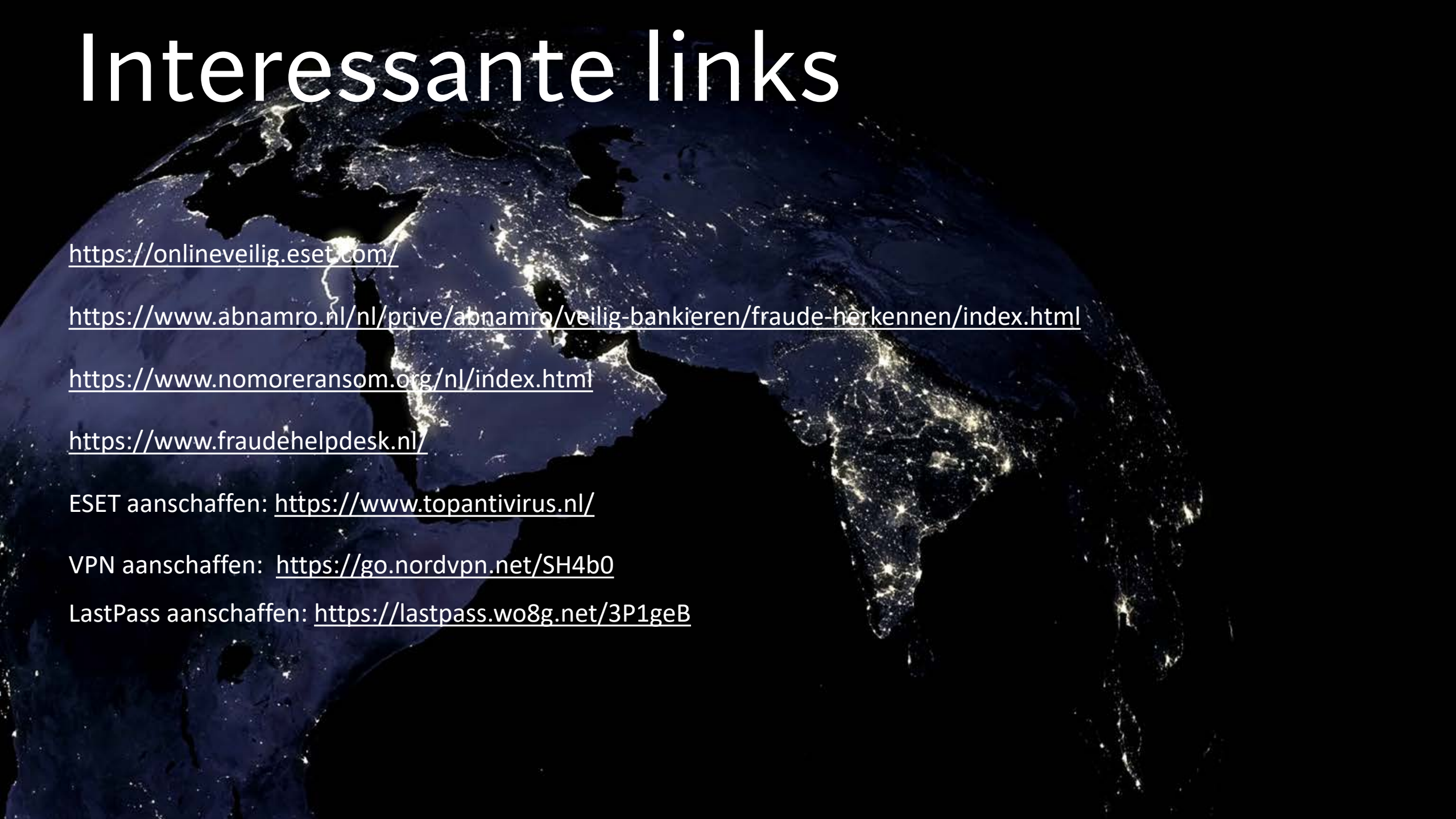


1. Check de foto
2. Check de afzender.
3. Ga niet in op (te mooie) aanbiedingen.
4. Stel de privacy goed in.
5. Klik niet op advertenties, maar ga naar de desbetreffende website.
6. Gebruik indien aanwezig twee factor authenticatie.

Aanvulling

1. Betaal nooit aan de afperser.
2. Er is software om ransomware te verwijderen
3. Zet een schuifje voor de cam.
4. Gebruik nooit een gevonden USB stick.
5. Geef niet zo maar (fysieke) toegang tot jouw computer.
6. QR codes worden ook gebruikt en deze zijn niet te controleren. Dus alleen gebruiken van een betrouwbare bron.
7. Let ook op telefonische oplichting.
8. Microsoft belt jou echt niet op om te helpen om door hun ontdekte malware bij jou te verwijderen.
9. Blijf alert en kritisch.

Interessante links



https://onlineveilig.eset.com/

https://www.abnamro.nl/nl/prive/abnamro/veilig-bankieren/fraude-herkennen/index.html

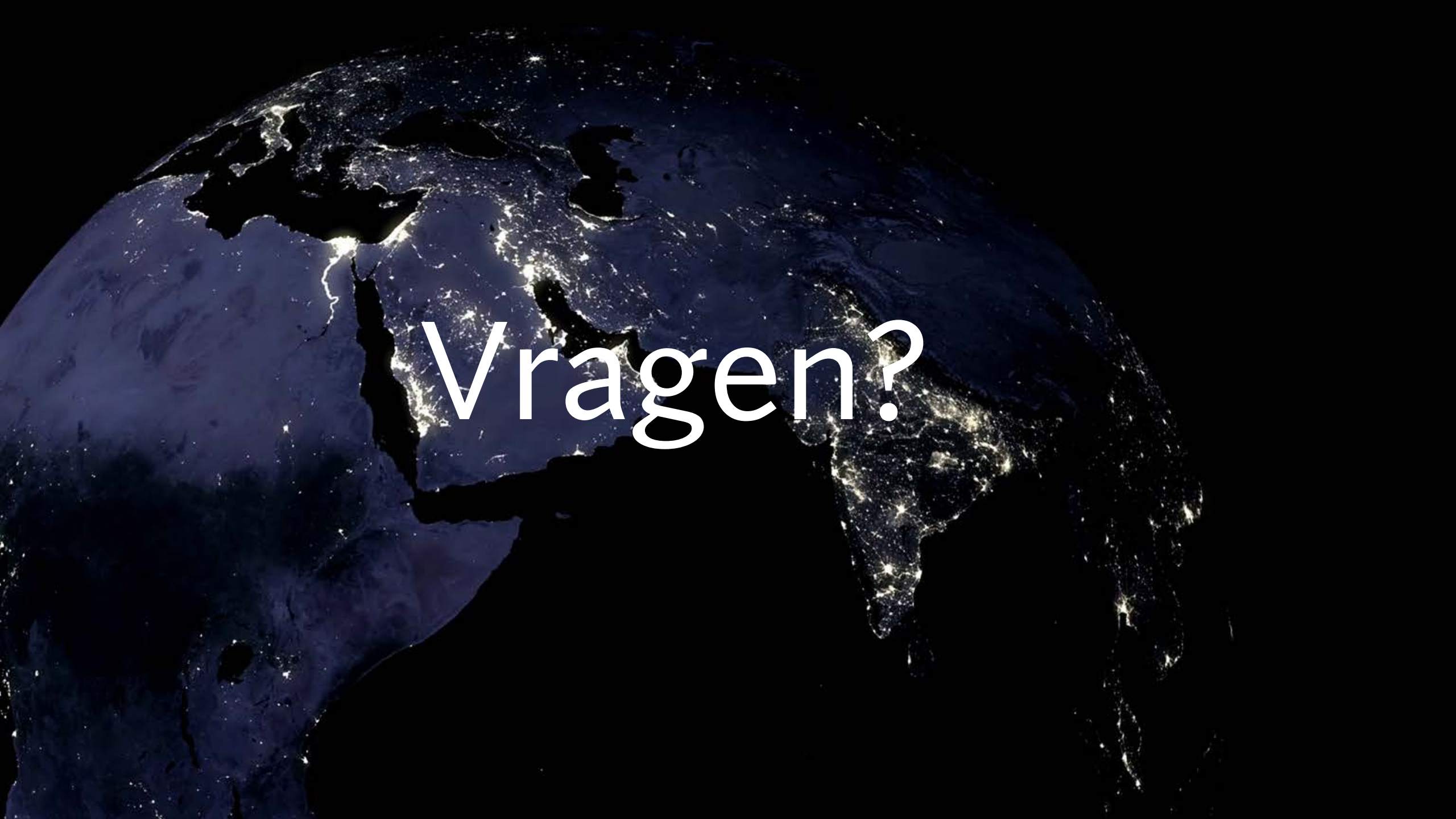
https://www.nomoreransom.org/nl/index.html

https://www.fraudehelpdesk.nl/

ESET aanschaffen: https://www.topantivirus.nl/

VPN aanschaffen: https://go.nordvpn.net/SH4b0

LastPass aanschaffen: https://lastpass.wo8g.net/3P1geB


Vragen?