



Bescherm de pc tegen calamiteiten

Bescherm jezelf tegen internet bedreigingen

Samenstelling en presentatie: Rob Kooman

Deze presentatie downloaden?

www.sr-pc-hulp.nl

Presentaties





De pc is zo traag dat u er bij in slaap valt.

De telefoon gaat en u hoort: *“Hello, ik ben een computerspecialist van Microsoft en heb geconstateerd dat uw PC besmet is met een virus waardoor uw pc vermoedelijk erg traag is”*

Wat doet u dan:

- 1- doet een vreugdedansje en smeekt de MS-persoon u te helpen**
- 2- gooit de hoorn op de haak en roept F#\$%\$# off en wacht rustig af totdat windows al zijn updates heeft verwerkt.**

Het grootste veiligheidsrisico.....



Maar met voldoende kennis.....
ben je zelf de beste bescherming

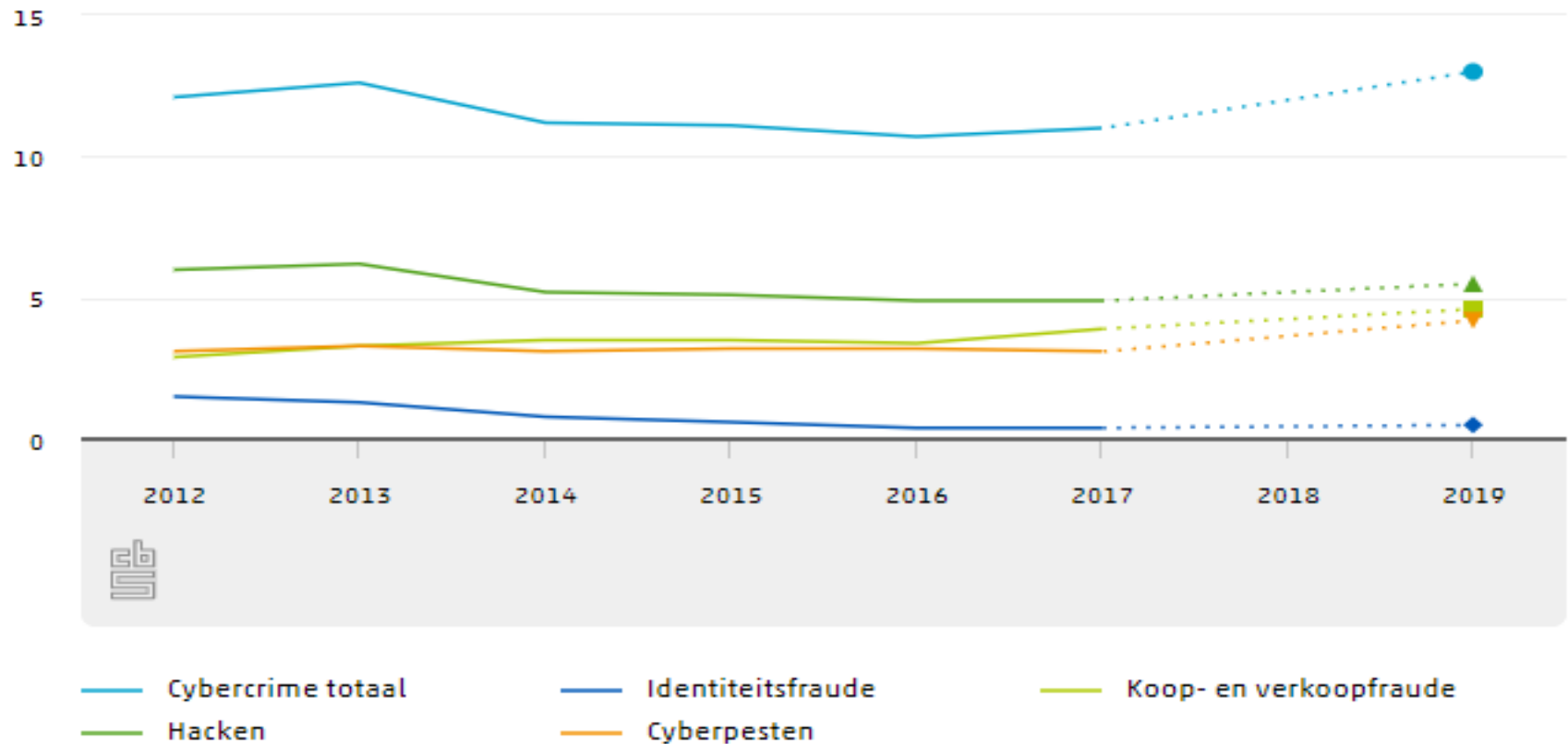
Basis regel om boven het beeldscherm te hangen

**ELKE AANBIEDING VIA E-MAIL
OF TELEFOON IS NEP EN EEN
POGING U GELD AFHANDIG
TE MAKEN**

Elk jaar meer slachtoffers cybercrime

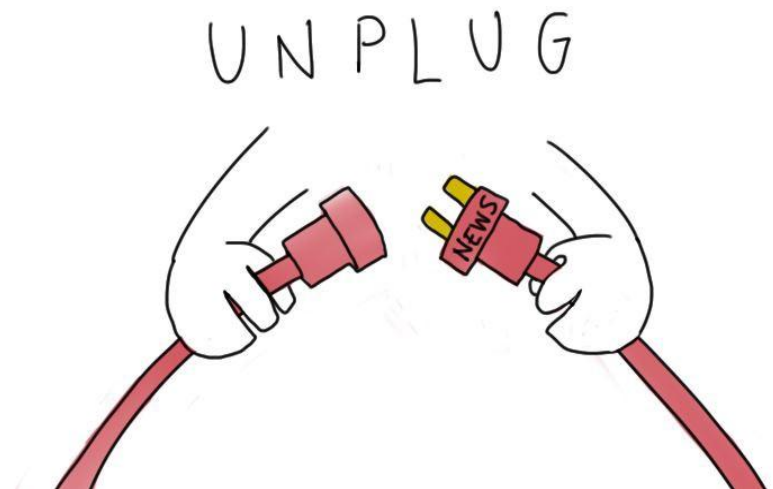
Slachtoffers cybercrime¹⁾

% bevolking 15 jaar of ouder



https://www.youtube.com/watch?v=9HSWenis_Cg&feature=youtu.be

100% beveiliging bestaat niet



Basis ingrediënten van beveiliging



Preventie



Detectie



Herstel

- Kennis en kundigheid
- Hulpmiddelen
- Handelingen

Preventie

- 1- Ken de gevaren, wees op uw hoede
- 2- Gebruik van beschermingssoftware
- 3- De juiste Windows instellingen
- 4- Fysieke splitsing HD/SSD Software en gegevens
- 5- Backups maken

Detectie

- 1- Herken de gevaren en symptomen
- 2- Beschermingssoftware detecteert

Herstel

- 1- Scan/herstel software
- 2- Recente backups terug zetten van software en gegevens

Preventie: Ken de gevaren, wees op uw hoede

Hoe werkt een virus/malware en dus ook gijzelsoftware?



Analyse van dit soort malware:

- 1- het is allemaal **software**
- 2- software moet **op de pc komen** voordat het iets kan doen
- 3- dat kan via een automatisch afspeelbaar medium als een **USB-stick** (of iets dergelijks), of **een link in een E-mail**, of een **download**, of een **website-bezoek**
- 4- eenmaal werkend wordt **alles besmet dat bereikt kan worden**, dus ook in de cloud, in een NAS of een externe HD die gekoppeld staat

Preventie: Ken de gevaren, wees op uw hoede



Oplichters en hackers speculeren op:

Nieuwsgierigheid



Hebzucht



Angst



Dit moet u zien!!

U bent de winnaar

Uw account is gehacked

Meest voorkomende besmettingsbronnen

1. Internet: alles wat gratis is en niet van de makers zelf komt
 - Gratis software (geeft vaak malware) van websites als Softonic
 - Illegale downloads (torrents e.d.)
 - E-mails met aanbiedingen of bedreigingen (en links daarin)
 - Bijlagen van E-mails
2. Groepen die uit zijn op koopjes, aanbiedingen en leuke dingen
 - Scholieren en onderwijsinstellingen in het algemeen
 - Kleinkinderen
3. Nieuwsgierige mensen en argeloze mensen
 - Die elke nieuwe ict-trend willen hebben
 - Die op elke JA-knop drukken
 - Die elke e-mail openen

**Basis regel om boven het
beeldscherm te hangen**

**ELKE AANBIEDING VIA
E-MAIL IS NEP EN EEN
POGING U GELD
AFHANDIG TE MAKEN**

Soorten bedreigingen en calamiteiten



Virussen & Malware



Phising



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Soorten bedreigingen en calamiteiten



Inbraak/diefstal pc



Kapotte hardware



Brand

Ken de gevaren, wees op uw hoede voor **virussen en malware**

Doel van virus/malware besmetting:

- PC infecteren met misdaadsoftware (phishing, fraude, keyloggers, gijzelsoftware, identiteitsdiefstal)
- PC infecteren met hulpsoftware = zombie pc (DOS-aanvallen, ongewenste e-mailing/Spam, kraken van encryptie)
- PC infecteren met ongewenste marketingtools (omleiding naar bepaalde websites, popups, reclameberichten)
- Pesten/stoer doen
- Kijken wat er mogelijk is

Ken de gevaren, wees op uw hoede voor **virussen en malware**

Middelen van virus/malware besmetting:

- E-mail met link naar bepaalde website
- E-mail met bijlage die bij download software installeert
- Alles wat gratis te downloaden valt (software, films, muziek, e-books, etc) en zeker wat niet legaal gratis is
Gratis software altijd van de website van de maker downloaden
- Alle media die automatisch starten, zoals een USB-stick
- Gehackde websites (komt nog al eens voor bij “digibete” websites, zoals kunst en alternatieve zaken)

Voorkom schade door virussen/malware

1. Verwijder onbekende berichten ongeopend
2. Druk NOOIT op een link in een bericht, maar ga zelf naar de betreffende website
3. Gebruik AV-software en bescherming in de browser
4. Download geen illegale software, e-books, muziek, e.d
5. Download gratis producten alleen vanaf de website van de maker
6. Druk niet ongezien op de “JA”-knop, maar lees eerst wat er staat. Bij twijfel niet verder gaan.

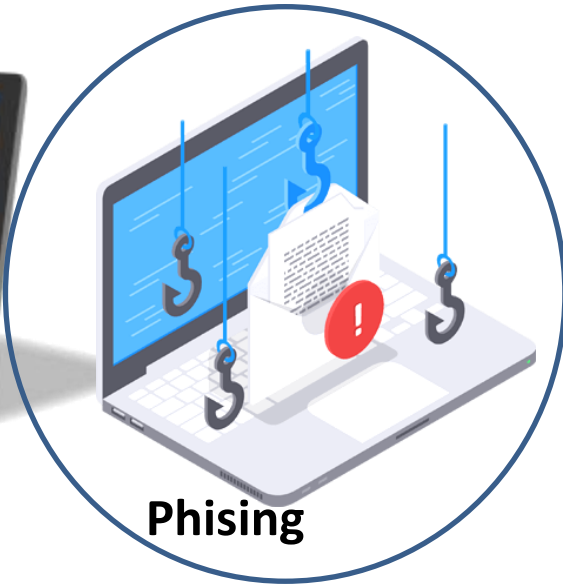
Voorkom schade door virussen/malware (vervolg)

7. Bij installatie van gratis software nooit de standaard/snelle manier doen, maar altijd de detail manier (zelf bepalen wat er wel/niet mee geïnstalleerd wordt).
8. Wees voorzichtig met leuke/mooie/gratis dingen van anderen, met name van de risicogroepen
9. Laat de (klein)kinderen niet op je eigen PC, maar geef ze een aparte PC en zet na afloop de system backup terug
10. Wees voorzichtig met gevonden USB-sticks

Soorten bedreigingen en calamiteiten



Virussen & Malware



Phising



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Ken de gevaren, wees op uw hoede voor **Phishing**



Ken de gevaren, wees op uw hoede voor Phishing

Doel van Phishing:

- Bankgegevens verkrijgen en rekening leeghalen
- Persoonlijke en vertrouwelijke gegevens verkrijgen:
Inloggen, identiteitsdiefstal, spullen kopen, lening
aangaan, creditcard aanvragen
- De verkregen gegevens doorverkopen

Ken de gevaren, wees op uw hoede voor Phishing

Middelen:

- Malware (keyloggers)
- E-mail met link naar bepaalde website
- SMS met link naar bepaalde website
- Telefoon (Nep MS-helpdesk)
- Onveilige wifi-verbinding

De waarde van gestolen gegevens

ISTR Internet Security Threat Report Volume 24 | February 2019 (Symantec)

- Gaming platform accounts: \$0.50-\$12
- Video and music streaming accounts: \$0.10-\$2
- Cloud service accounts: \$5-\$10
- Online banking accounts: 0.5%-10% of the account's value
- Name, social sec number and date of birth: \$0.10-\$1.50
- Medical notes and prescriptions: \$15-\$20
- ID/passport scans or templates: \$1-\$35
- Mobile phone online account: \$15-\$25

Ken de gevaren, wees op uw hoede voor Phishing E-mails

Van: ING bank <ING_bank@live.nl>
Aan:
CC:
Onderwerp: ING Bank N.V.



Geachte heer/mevrouw.



De bank kent uw naam!

We hebben onregelmatige activiteiten ontdekt op uw Mijn ING account. Melding: 82141-40000

Als primaire contactpersoon moet u uw accountactiviteit verifiëren voordat u uw kaart verder kunt gebruiken. Na de verificatie zullen we de op uw account gezette beperkingen opheffen en moet u deze procedure niet opnieuw herhalen. Controleer uw account zo snel mogelijk a.u.b. [klik hier](#), vervolgens logt u in en volgt u de stappen.

Inloggen

Wilt u meer weten?

- ▶ Alle zakelijke spaarproducten
- ▶ Actuele rentepercentages
- ▶ Historische spaarrentes

Heeft u vragen?

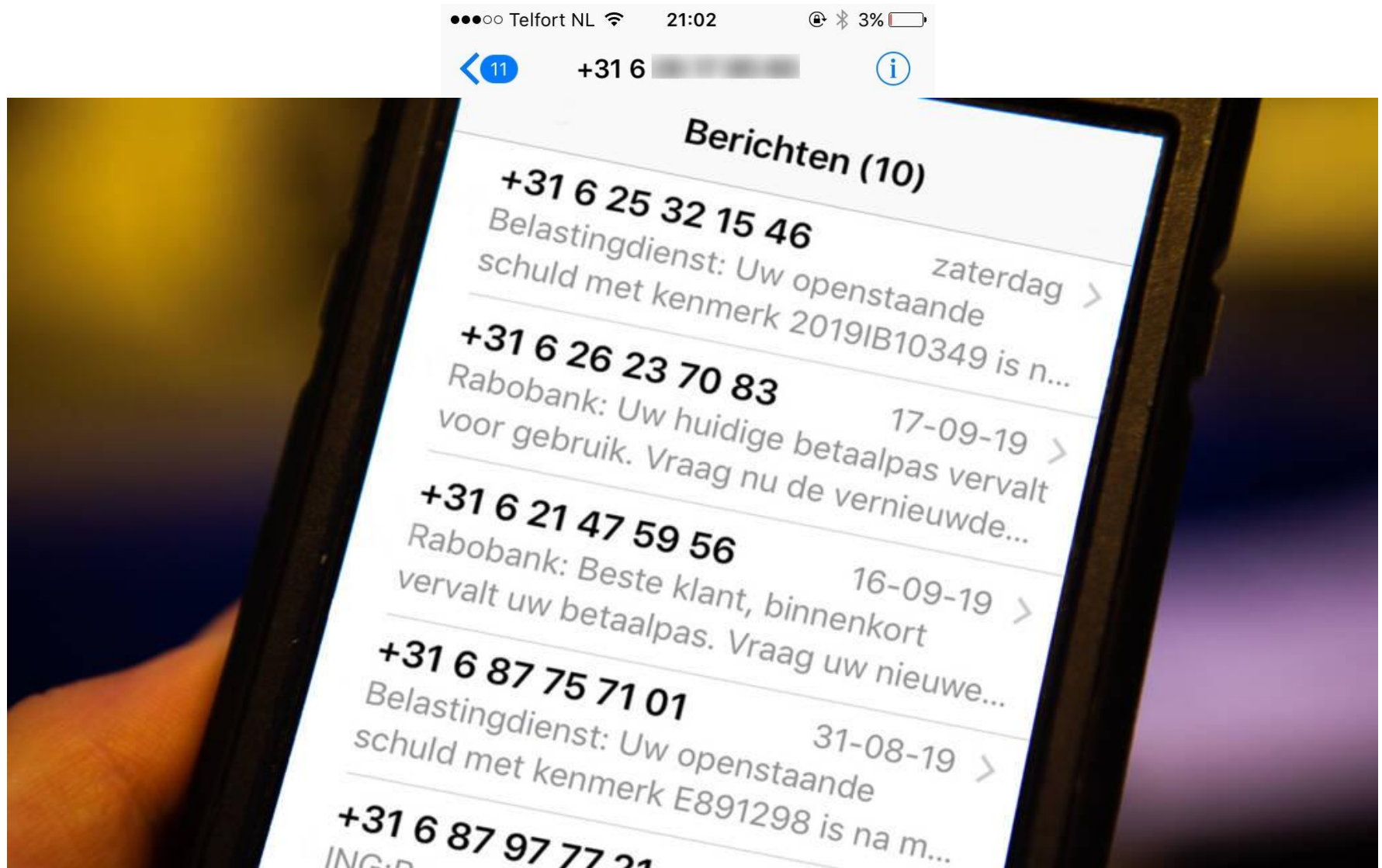
- ▶ Hoe komen rentelaterlven tot stand?
- ▶ Veelgestelde vragen over sparen
- ▶ Neem contact op met de IN

Deze e-mail afkomstig van ING Bank N.V., statutair gevestigd te Amsterdam, Handelsregister nr. 33031431.

**Basis regel om boven het
beeldscherm te hangen**

**ELKE AANBIEDING VIA
E-MAIL IS NEP EN EEN
POGING U GELD
AFHANDIG TE MAKEN**

SMS Phishing



SMS Phishing



Bericht
Vandaag 20:45

Dit is een automatisch SMS-bericht vanuit MijnOverheid namens uw bank.

Uw betaalpas is verouderd en zal overmorgen komen te vervallen.

U kunt direct uw nieuwe betaalpas aanvragen via de DigiD-omgeving:

[Tik om voorvertoning te laden](#)

mijnoverheid-sm... >

ABN AMRO

Beste klant,

Uw betaalpas vervalt binnen 2 dagen. Wees er snel bij en vraag kosteloos een vervangende pas aan.

Voorkom blokkade! Klik hier
x.co/6nUSz

Mvg, ABN AMRO

Uw Rabobank bankpas is wegens overschrijding van onze veiligheidsregels in de quarantaine zone geplaatst.

Uw bankpas wordt vanaf dinsdag [12-03-2019](#) geblokkeerd.

U kunt wel een nieuwe bankpas aanvragen via de volgende link:
<http://x.co/NL>

Wees op tijd met de aanvraag en vermijd blokkade van uw gehele bankrekening.



Bericht



De “oogst” phishing mails van één dag

Mail delivery failed: returning message to sender	• Mail Delivery System	🔥 14-2-20...
Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw account gehackt).	• bliss@box.nl	🔥 14-2-20...
Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw account gehackt).	• aigrets@traveller.cz	🔥 14-2-20...
Undeliverable: Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw ac...	• postmaster@blue-tbd.nl	🔥 14-2-20...
Undeliverable: 1.000.000 Euro	• postmaster@uhk.cz	🔥 14-2-20...
Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw account gehackt).	• kghvp309@amm-komputer.pl	🔥 14-2-20...
Mail delivery failed : returning message to sender	• Mail Delivery System	🔥 09:10
Mail delivery failed : returning message to sender	• Mail Delivery System	🔥 09:10
Mail delivery failed : returning message to sender	• Mail Delivery System	🔥 09:10
Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw account gehackt).	• info@dierenspeciaalzaakxxl.nl	🔥 10:14
Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw account gehackt).	• info@droomdeco.nl	🔥 12:53

Phishing door Nep Microsoft Helpdesk



We hebben een melding binnen gekregen dat er iets mis is met uw pc

Dat kunnen we nu voor u verhelpen.

Wilt u svp naar deze website gaan

Eerst even de windows Assistance aanzetten

Voorkom schade door Phishing

- 1. Verwijder dit soort berichten ongeopend
Toch geopend? Dan NIET op de link drukken**
- 2. Willen weten of het wel/niet zo is?
Ga dan zelf rechtstreeks naar de website van
de bank, Overheid, etc.**
- 3. Microsoft belt nooit zelf, dus gesprek gelijk
beëindigen**
- 4. Gebruik VPN bij openbare Wifi**
- 5. De standaard maatregelen tegen virus/malware**

Soorten bedreigingen en calamiteiten



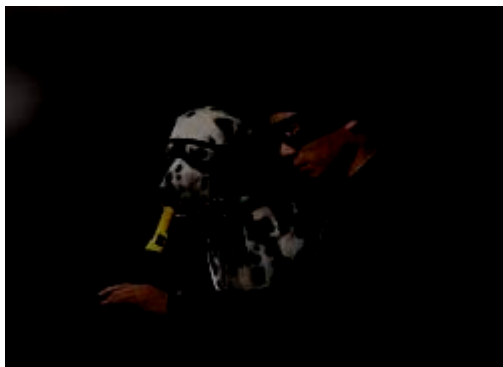
Virussen & Malware



Phising



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Ken de gevaren, wees op uw hoede voor fraude



Ken de gevaren, wees op uw hoede voor **fraude**

Doel van internet fraude:

- Zo veel mogelijk geld afhandig maken

Middelen:

- Telefoon (Nep MS-Helpdesk, Nep bank-bediende)
- Whatsapp (familielid in nood)
- Sociale media & Marktplaats (link met verzoek 1 cent over te maken)
- E-mail (zie Phishing mails) U heeft een prijs gewonnen

Telefoon (Nep MS-Helpdesk)

- Buitenlandse persoon die zich voordoeft als Microsoft. Microsoft zal nooit zelf bellen

Nep-MS-Helpdeks doel:

- Toegang krijgen tot de PC (Teamviewer of Windows Remote assistance)

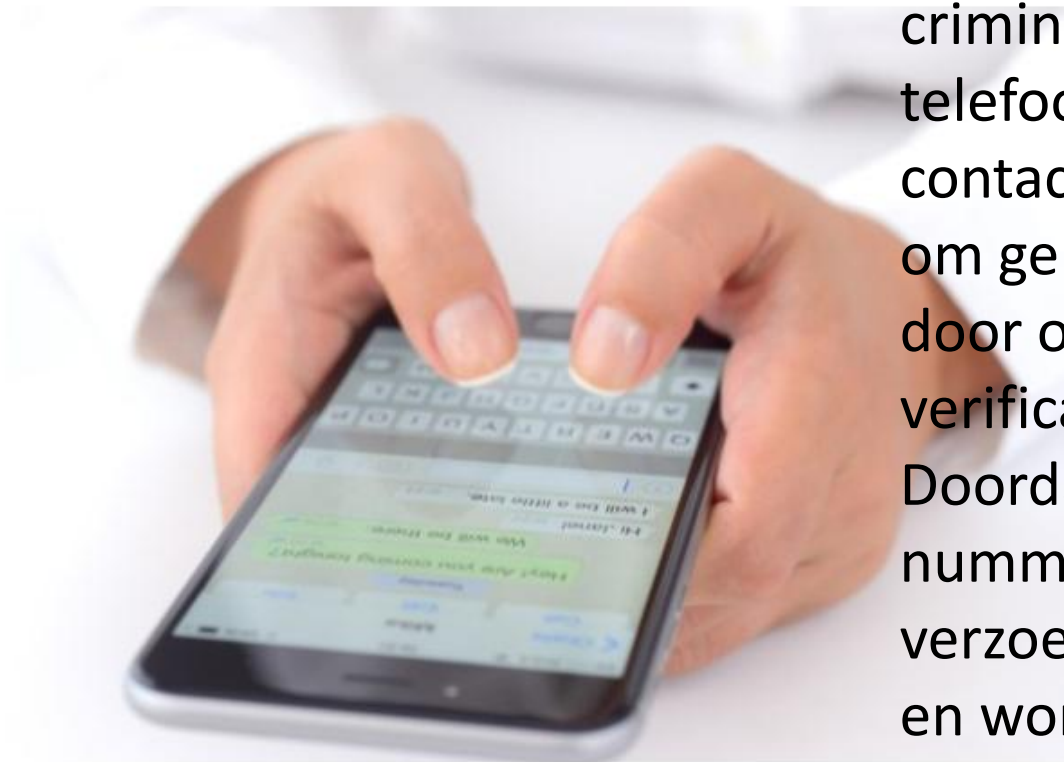
NB! Zet Remote assistance uit

- Malware plaatsen op de PC
- Bankrekening leeghalen

WhatsApp-fraude

Politie Westelijke Mijnstreek waarschuwt voor WhatsApp-fraude

01-02-2019 om 12:45 door Paul Dolhain



*WhatsApp-fraude komt steeds vaker voor.
Afbeelding: Getty Images*

Bij WhatsApp-fraude komen criminelen op slinkse wijze achter telefoonnummers, waarna ze contactpersonen in de telefoon om geld vragen. Bijvoorbeeld door om een WhatsApp-verificatiecode te vragen. Doordat de ontvanger het nummer herkent, komt het verzoek waarheidsgetrouw over en wordt in vele gevallen geld afhandig gemaakt.

Oplichting via Marktplaats

Whatsapp verzoek identiteitsbewijs

<https://opgelicht.avrotros.nl/uitzending/gemist/item/oplichters-opgepakt-voor-marktplaatsfraude/>

Gelijkoversteken-dienst van Marktplaats

<https://www.youtube.com/watch?v=2tJwRFsL5l4>

<https://www.consumentenbond.nl/online-kopen/opgelicht-marktplaats>

Oplichting via Marktplaats

Reactie buiten Marktplaats om (rechtstreeks via e-mail of Whatapp) : altijd weigeren

Geen mobiel nummer vermelden in de advertentie

Verzoek om betaling anders dan “gewone” overschrijving:
altijd weigeren: alleen standaard bankoverschrijving doen
Trap niet in de “1 cent-overmaak-truc” of Tikkiefraude

Verzoek om identificatie (kopie bankpasje en/of
rijbewijs/paspoort): altijd weigeren

Wel betalen, niet leveren: bij voorkeur ophalen en
contant betalen

Afpersing via E-mail



Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw a... • bliss@box.nl



Controleer de integriteit van uw informatie (volgens onze beveiligingsservice is uw a... • aigrets@traveller.cz

Ik ben een professionele hacker die toegang heeft tot uw besturingssysteem. Ik heb ook volledige toegang tot uw account. Bla bla bla

Mijn bitcoin-adres (BTC Wallet):

1GXDt3MAyT5D7Sjwa9MShLCDdPKx9mpDNZ

Na ontvangst van de betaling, zal ik de video verwijderen en je zult me nooit meer horen. Ik geef je 48 uur om te betalen. Zodra u deze e-mail opent, werkt de timer. Ik ontvang onmiddellijk een melding over dit evenement.

Voorkom schade door Fraude

1. Verwijder verdachte berichten ongeopend
Toch geopend?
Druk dan NOOIT op de link in het bericht
2. Marktplaats bij voorkeur contant anders
standaard bankoverschrijving met pc (niet mobiel)
- Contact via Marktplaats-(E-mail)communicatie.
NOOIT kopieën id/pas/rijbewijs opsturen
3. Verzoek om financiële hulp van een familielid?
Bel het familielid op, of vraag haar/hem jou te bellen
4. Wantrouw aanbiedingen die te mooi zijn om waar
te zijn; ze zijn meestal niet waar

Soorten bedreigingen en calamiteiten



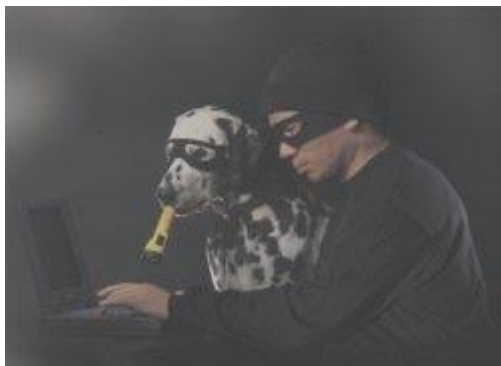
Virussen & Malware



Phising



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Ken de gevaren, wees op uw hoede voor ransomsoftware =gijzelsoftware



Ken de gevaren, wees op uw hoede voor ransomsoftware =gijzelsoftware (losgeldsoftware)

Doel van gijzelsoftware:

Afpersing door het onleesbaar maken van de gegevens en de sleutel verschaffen tegen betaling met bitcoins

Nieuwste vorm van ransom software: alle informatie wordt van de pc, uit de cloud gestolen/gekopieerd en vrijgegeven op internet (als je niet betaald)

Ken de gevaren, wees op uw hoede voor ransomsoftware =gijzelsoftware

Middelen:

Toegang verkrijgen tot computer/netwerk

- Phishing e-mail
- hacken van Remote Desktop Protocol van Windows 10 (Remote Assistance)
- hacken van tooltjes die systemenmanagement-taken uitvoeren (Nep Microsoft Helpdesk)
- vervolgens alle bereikbare gegevens versleutelen (onleesbaar maken) incl. cloud, NAS, aangesloten USB-sticks en aangesloten externe HD

NB! Windows encryptie wordt gebruikt!

Ken de gevaren, wees op uw hoede voor gijzel software

Voorkom schade door gijzelsoftware door zelfde maatregelen als tegen virussen/malware:

1. Verwijder onbekende berichten ongeopend
2. Druk NOOIT op een link in een bericht, maar ga zelf naar de betreffende website
3. Gebruik AV-software en bescherming in de browser
4. Download geen illegale software, e-books, muziek, e.d
5. Download gratis producten alleen vanaf de website van de maker
6. Druk niet ongezien op de “JA”-knop, maar lees eerst wat er staat. Bij twijfel niet verder gaan.

Ken de gevaren, wees op uw hoede voor gijzel software

Voorkom schade door gijzelsoftware door zelfde maatregelen als tegen virussen/malware:

7. Bij installatie van gratis software nooit de standaard/snelle manier doen, maar altijd de detail manier (zelf bepalen wat er wel/niet mee geïnstalleerd wordt).
8. Wees voorzichtig met leuke/mooie/gratis dingen van anderen, met name van de risicogroepen
9. Laat de (klein)kinderen niet op de eigen PC, maar geef ze een aparte PC en zet na afloop de system backup terug
10. Wees voorzichtig met gevonden USB-sticks

Ken de gevaren, wees op uw hoede voor ransomsoftware =gijzelsoftware

Voorkom schade door gijzelsoftware door:

- Zet gevoelige informatie NIET op de pc, of in de cloud, maar op een externe HD of USB-stick en bewaar altijd twee kopieën op twee verschillende media (omdat er 1 kapot kan gaan)
- Zet de remote assistance van windows uit
- Zet de encryptie van windows uit

Soorten bedreigingen en calamiteiten



Virussen & Malware



Phishing



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Ken de gevaren, wees op uw hoede voor hacking

Doel van hacking:

- Plaatsen van malware/gijzelsoftware, etc.
- Overnemen PC voor DOS-aanval
- Stelen van gegevens, geld en/of identiteit
- Omdat het kan (studenten, nerds)
- Opscheppen

Ken de gevaren, wees op uw hoede voor hacking

Middelen:

Zelfde als voor Virussen/Malware en Phishing
M.n. onbeschermd wifi thuis en in openbare ruimte

Voorkom schade door:

- Zelfde als voor Virussen/Malware en Phishing
- Let met name op E-mails en Nep-MS-Helpdesk
- Gebruik VPN bij openbare Wifi
- Geef router een andere naam (SSID) dan standaard en Gebruikersnaam en wachtwoord

Soorten bedreigingen en calamiteiten



Virussen & Malware



Phising



Fraude



Hacking



Gijzelsoftware



**(Persoons)gegevens/identiteit
diefstal**

Ken de gevaren, wees op uw hoede voor Identiteitsdiefstal

Doel van identiteitsdiefstal:

Kopen van spullen op andermans rekening

Gebruik van creditcard/betaalpas

Aanvragen van subsidie

Inloggen op beveiligde websites /e-mail

Cyberpesten

Wees op uw hoede voor Identiteitsdiefstal

Middelen:

- inbraak van de woning of auto
- stelen van post uit brievenbussen
- kopiëren van kaartgegevens bij kaartgebruik in winkel of geldautomaat (Skimmen)
- kopiëren van bestanden met persoonsgegevens van klanten (door medewerkers van bedrijven)
- hacken van computersystemen/e-mail-systemen
- informatie in afval- en prullenbakken
- **phishing/ E-mails en Facebook << meest voorkomend**
- plaatsen van een valse vacature om zodoende c.v.'s te 'oogsten'.
- Telefonisch achterhalen van de gebruikersnaam en het wachtwoord
- Googelen (facebook en andere sociale media)

Ken de gevaren, wees op uw hoede voor gegevensdiefstal **via E-mail**

**Gevoelige informatie verstuur je toch ook niet
via een ansichtkaart?**



Iedereen die
weet hoe dat
moet kan uw
e-mails lezen.
Verstuur
NOOIT
vertrouwelijke
informatie via
E-mail

Museum ruziet over aankoop schilderij van 'gehackte' kunsthandelaar

30 januari 2020 23:42

Aangepast: 31 januari 2020 09:21



Neprekening in Hongkong

Die zei daarna dat het niet zijn rekeningnummer was, maar van fraudeurs die zich op een of andere manier hadden binnengedrongen in het e-mailverkeer tussen de twee partijen. Het geld zou zijn terechtgekomen op een neprekening in Hongkong.

Wees op uw hoede voor Identiteitsdiefstal

Voorkom schade door:

Bewaar identiteitsbewijs en gevoelige documenten op een veilige plaats en niet op de PC maar op een aparte USB-stick

Beveilig de brievenbus tegen hengelen (borstel achter de klep)

Geef geen persoonlijke informatie prijs op sociale media

Kijk uit voor babbeltrucs (“bankmedewerker” via telefoon)

Verder alle maatregelen voor virussen/malware/phishing en fraude

Ken de gevaren, wees op uw hoede



10-03-2020

Bescherm de PC tegen calamiteiten
Seniorenacademie Delft

Fysieke bedreigingen en calamiteiten



Inbraak/diefstal pc



Kapotte hardware



Brand

Bescherming tegen fysieke bedreigingen en calamiteiten

Inbraak preventie (Sluit- en hangwerk)

Zet geen “uitnodiging” tot inbraak op sociale media

Wekelijkse backup maken van Systeem en gegevens op externe HD en eens per kwartaal kopie daarvan “buiten”

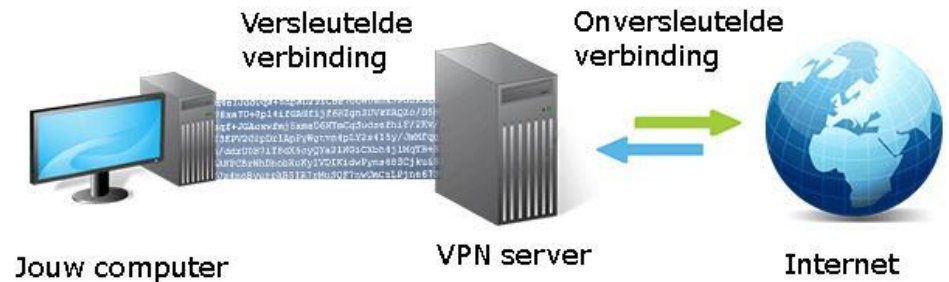
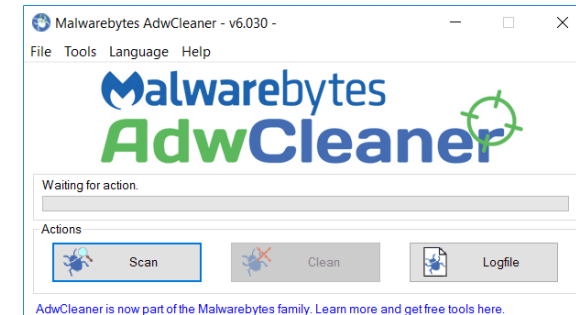
Cloud is een oplossing bij brand een kapotte HD

**Basis regel om boven het
beeldscherm te hangen**

**ELKE AANBIEDING VIA
E-MAIL IS NEP EN EEN
POGING U GELD
AFHANDIG TE MAKEN**

Preventie

2- Beschermingssoftware

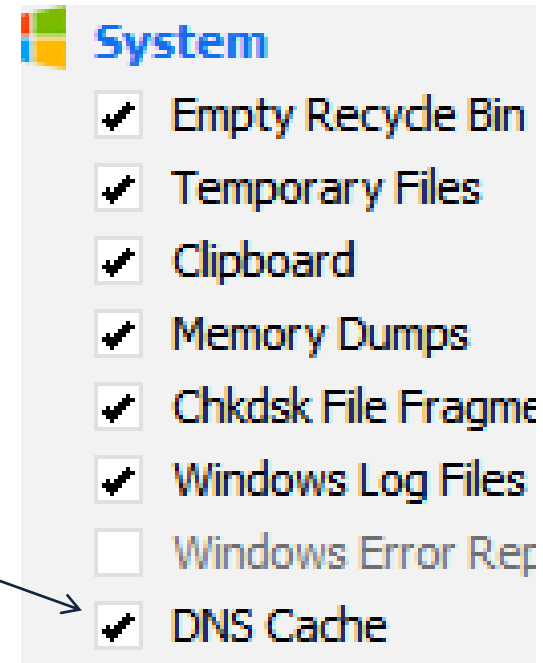


VPN schematisch weergegeven

Preventie

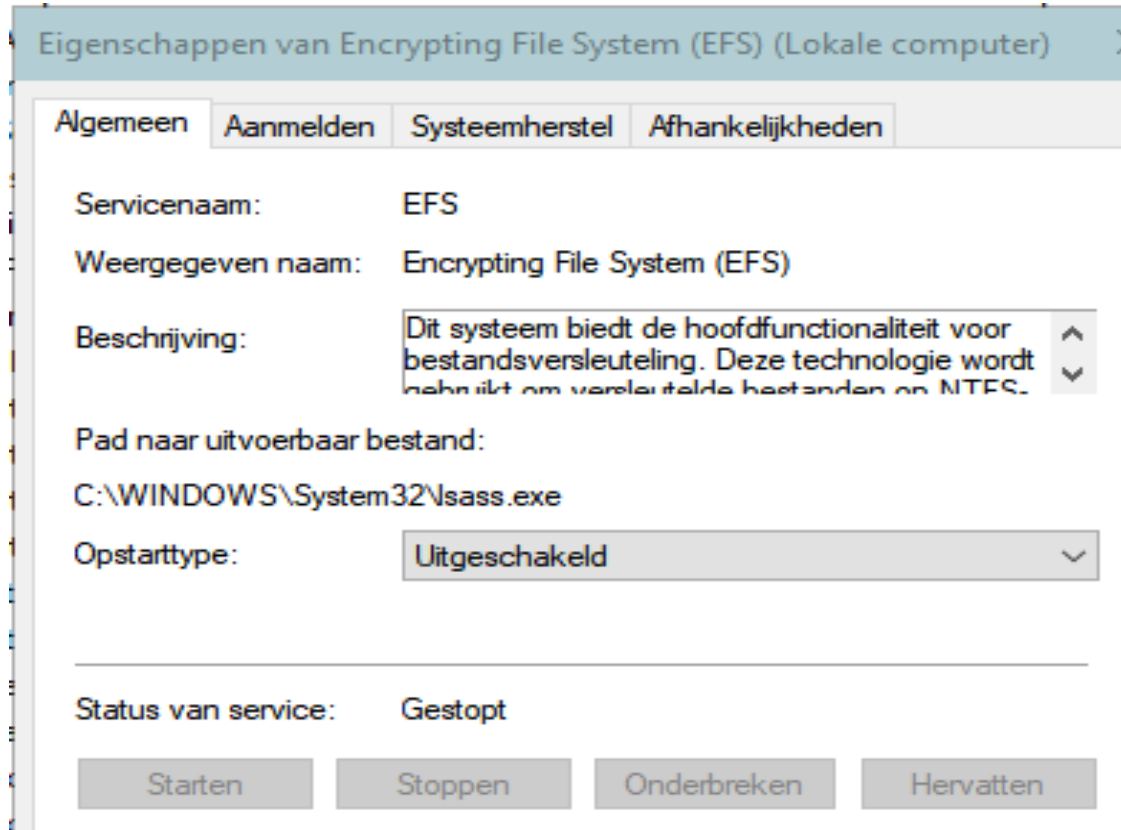
2- Beschermingssoftware

- Houdt de (av)-software actueel
- Voer eens per week extra scan's uit (ook met "off-line" pakketten als Malwarebytes e.d.)
- Eens per maand een volledige scan
- Eens per week een Ccleaner run met DNSCache aangevinkt



Preventie

3- Windows instellingen: Encryptie



Stop Windows
10 Encryptie
service

win-key+R

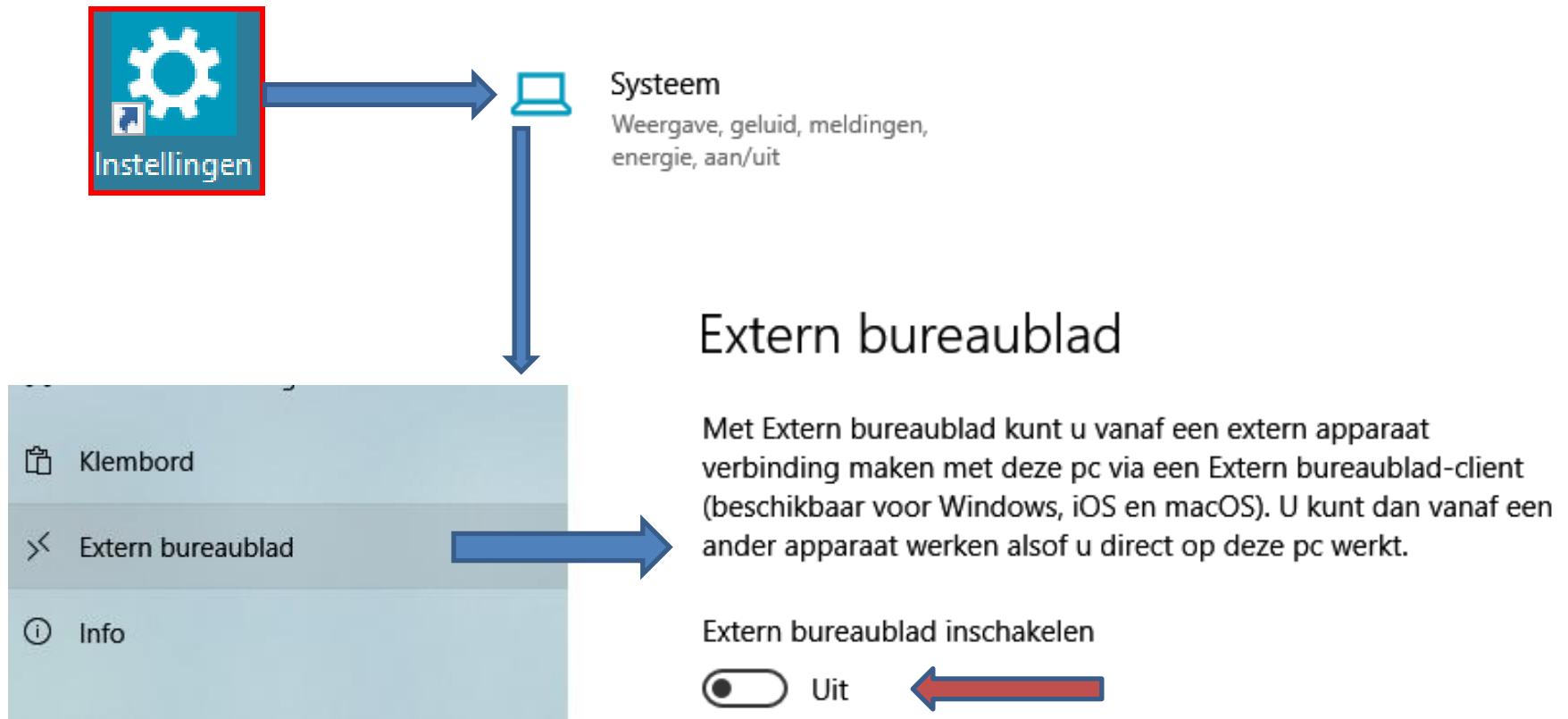
en type dan

fsutil behavior set disableencryption

Preventie

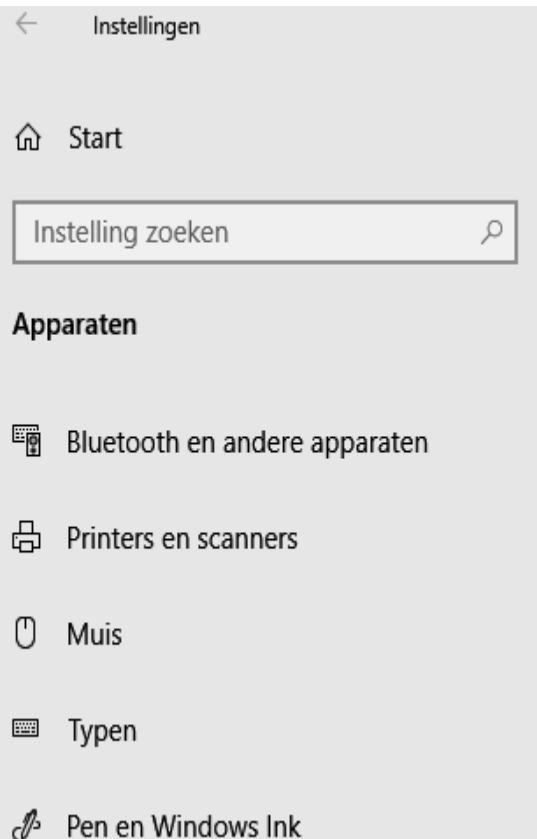
3- Windows instellingen: Remote Assistance

Zet de Windows Remote Assistance uit



Preventie

3- Windows instellingen: automatisch afspelen



Automatisch afspelen

Automatisch afspelen voor alle media en apparaten gebruiken



Aan

Standaardinstellingen voor automatisch afspelen kiezen

Verwisselbaar station

Map en bestanden weergeven (Verkenner)



Geheugenkaart

Map en bestanden weergeven (Verkenner)



Zet
automatisch
afspelen op
“Map en
bestanden
weergeven”

Preventie

3- Windows Defender instellingen



Virus- en
bedreigingsbeveiliging
Geen actie vereist.



Accountbeveiliging
Geen actie vereist.



Firewall- en
netwerkbeveiliging
Geen actie vereist.



App- en browserbeheer
Geen actie vereist.



Apparaatbeveiliging
Status weergeven en beheren
van hardware-
beveiligingsfuncties niet
beschikbaar

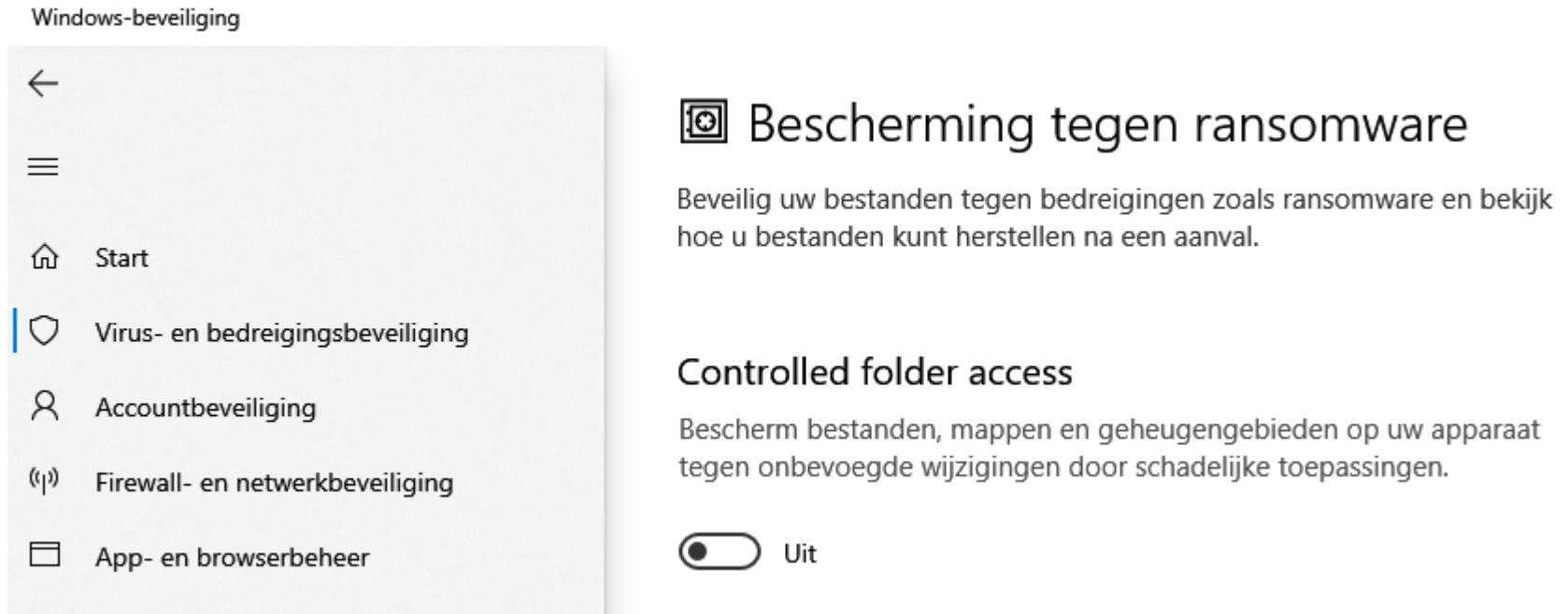


Apparaatprestaties en -
status
Geen actie vereist.

Controleer
regematig of
alle
beveiligings-
onderdelen
aan staan

Preventie

3- Windows Defender instellingen



Bescherming tegen Ransomsoftware (Controlled Folder Access) bij mij geen succes daar bepaalde software niet meer functioneerde.

Preventie

3- Windows Defender instellingen

- Alleen Windows Prof, 64bit
- Geen import fav
- Downloads verboden
- Extensies verboden
- Geen adblocking
- Geen privacy bescherming
- Traag

Browser in een sandbox

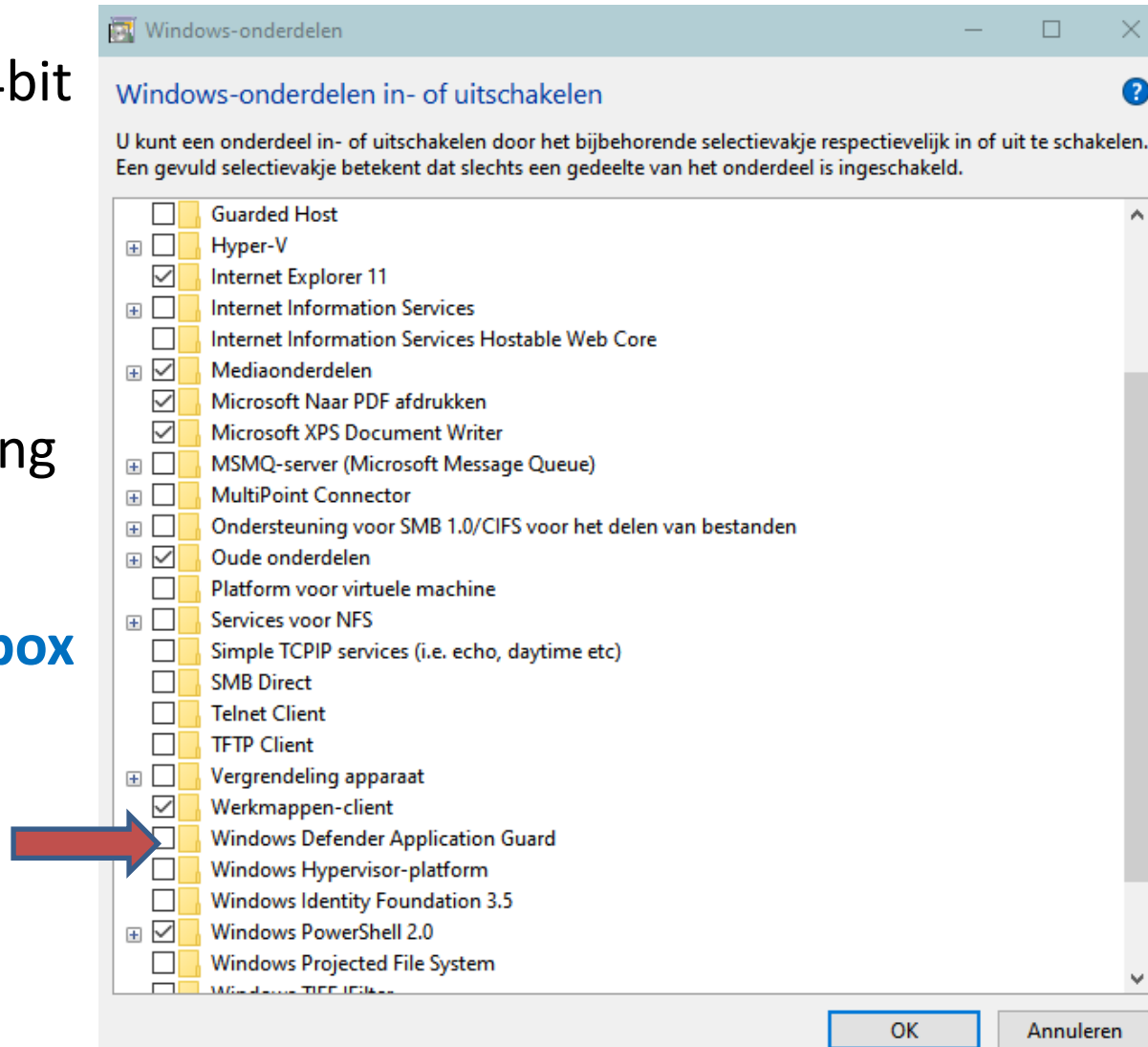
WDAG=

Windows

Defender

Application

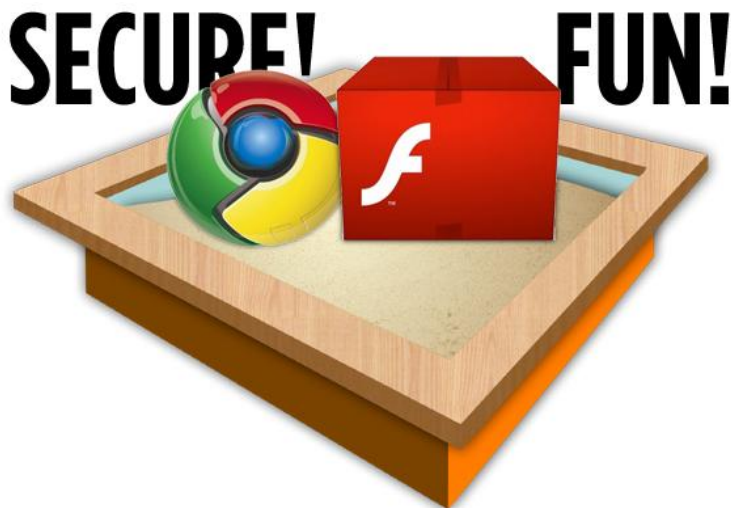
Guard



Preventie

3- Browsen in een Sandbox

- Bitbox
- Bufferzone
- Shade Sandbox → <https://www.shadesandbox.com/download>
- Sanboxie
- Toolziw Time Freeze
- etc.etc



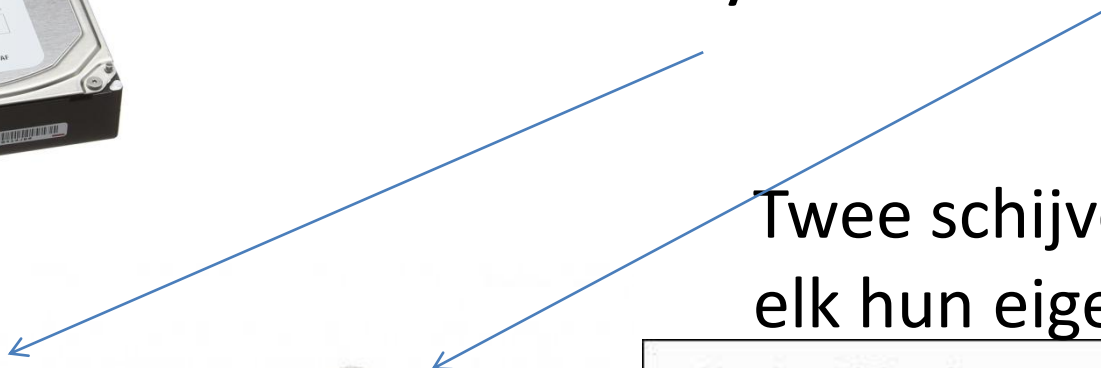
- 1- Download en installeer
- 2- Start ShadeSandbox en sleep de browser in het Shade-windows
- 3- Start de Browser
- 4- Downloads e.d komen in een Virtuele Shade Map
- 5- Sleep testsoftware naar Shade en test het daar zonder gevaar

Preventie

4- Fysieke splitsing HD/SSD Software en gegevens

1 Partitie C: voor systeem en data

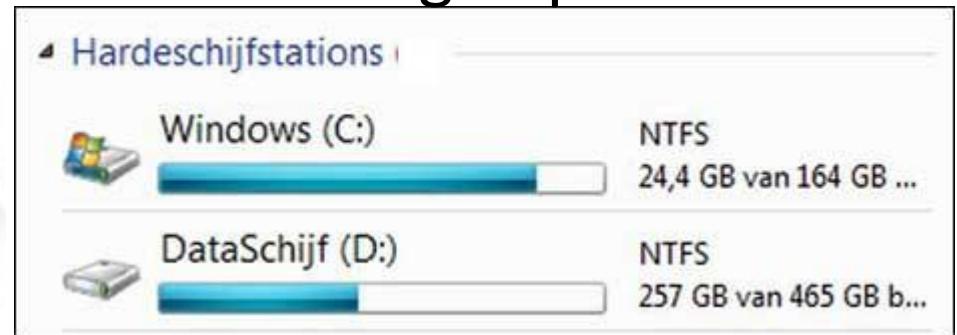
Twee schijven/SSD's met elk hun eigen partitie



C: SYSTEM



D: DATA



Optimale situatie Windows (C:) op SSD en Data (D:) op HDD

Preventie

5- Backups maken naar **Externe HD/SSD**

Uitgaande van twee HD's/SSD met gescheiden System en Data-partitie

Eens per week
Kopie van
Windows/
Systeem



Elke dag
kopie van
gegevens
en e-mail



Preventie

5- Backups maken naar **Externe HD/SSD**



Gevoelige informatie (paspoort, wachtwoorden, persoonsgegevens, etc.) niet op de PC of in cloud maar op een USB-stick/externe HD

NB! Ook kopiëren omdat alles eens kapot gaat

Preventie

- 1- Ken de gevaren, wees op uw hoede
- 2- Beschermingssoftware
- 3- Windows instellingen
- 4- Fysieke splitsing HD/SSD Software en gegevens
- 5- Backups maken

Detectie

- 1- Herken de gevaren en symptomen
- 2- Beschermingssoftware

Herstel

- 1- Scan/herstel software
- 2- Recente backups terug zetten van software en gegevens

Detectie

1- Herken de gevaren en symptomen



PC en/of internet trager dan normaal; maar kan ook Windows update zijn.



Windows en/of toepassingen gedragen zich anders dan normaal



De browser gedraagt zich anders dan normaal, bijv. popups

Detectie

1- Herken de gevaren en **symptomen**

Traag, anders dan normaal gedrag?

Kijk of er updates bezig zijn

(Instellingen – Bijwerken en beveiliging)

Niet het geval, dan

- Diepgaande AV-check uitvoeren met standaard AV-software
- Ook een diepgaande check met extra beveiligingssoftware (bijv. Adwcleaner, Malwarebytes, Emsisoft, etc.

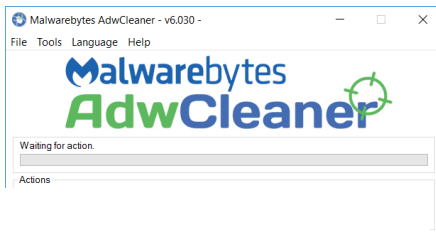
Detectie

2- Beschermingssoftware



AV/Security software, DE belangrijkste vorm van permanente bescherming & detectie

Periodiek uitgebreide scan met permanente bescherming



Malwarebytes



Daarnaast eens per week extra controle met andere beveiligingssoftware dan de permanente bescherming

Preventie

- 1- Ken de gevaren, wees op uw hoede
- 2- Beschermingssoftware
- 3- Windows instellingen
- 4- Fysieke splitsing HD/SSD Software en gegevens
- 5- Backups maken

Detectie

- 1- Herken de gevaren en symptomen
- 2- Beschermingssoftware

Herstel

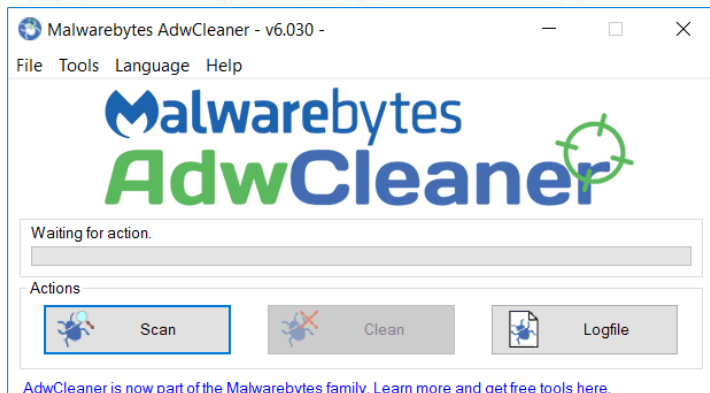
- 1- Scan/herstel software
- 2- Recente backups terug zetten van software en gegevens

Herstel

1- Scan/herstel software



Alle beveiligingssoftware heeft naast de scan-functie een herstel-functie of de optie om de gevonden malware in quarantaine te plaatsen, of te verwijderen.



Malwarebytes



Herstel

2- Recente backups terugzetten van software en gegevens

Als herstel niet lukt, of bij twijfel of alle malware gevonden is

Maar altijd i.g.v. gijzelsoftware

- De systembackup (windows) terug zetten over de C:-partitie heen**
- De gegevensbackup terug zetten over de D:-partitie heen**

Wat ik op mijn eigen PC hier aan doe

- Windows Defender als algemene dagelijkse beveiliging en daarnaast (niet permanent actief):
Malwarebytes, Adwcleaner, ZHPcleaner en Emsisoft
- Browserbescherming (Extenties) - Brave:
 - Ublock Origin tegen advertenties en kwalijke websites
 - Ghostery voor privacy bescherming
- E-mailbescherming:
Spamfilter aan bij provider
Spamfilter in e-mailpakket (Thunderbird)
- Router een andere DSSID en wachtwoord dan standaard
- VPN aan bij “gevoelige” acties en op locatie (wifi)

Wat ik op mijn eigen PC hier aan doe

Wekelijks

- Uitvoeren Malwarebytes, ZHPCleaner, AdwCleaner, Emsisoft Emergencykit , extra scan Defender
- Ccleaner voor legen DNS en Tijdelijke mappen windows en Browsers
- Windows opruiming (overbodige bestanden op C-partitie)
- Volledige kopie System-partitie (3 generaties bewaren)
- Incrementele kopie van partitie met gegevens, e-mail, etc.
- Eens per kwartaal een kopie van backup naar buiten

SAMENVATTING

- (Her)ken de gevaren en de risico's
- Snap hoe het werkt en wees op je hoede
- Onderdruk de nieuwsgierigheid
- E-mail = een ansichtkaart
- Gooi alle financiële mail/sms ongeopend weg
- Druk nooit op een link in een e-mail of sms
maar ga zelf naar de website toe
- Ongevraagde Microsoft helpdesk is nep/fraude
- Geef geen vertrouwelijke informatie prijs op
sociale media

SAMENVATTING (vervolg)

- Als het te mooi is om waar te zijn is het niet waar
- Marktplaatscontact alleen via Marktplaats e-mail (en niet whatsapp e.d.)
- Marktplaatsspullen bij voorkeur contant betalen
- Als contant niet kan, dan alleen via standaard bankoverschrijving op pc (geen Tikkie, mobiel e.d.)
Trap niet in de “1 cent overmaak truc”
- Nooit identiteitsbewijzen of betaalpas kopieën opsturen
- Geef nooit bankgegevens over de telefoon

SAMENVATTING (vervolg)

- Bewaar wachtwoorden en kopieën van pasjes, rijbewijs, paspoort, etc niet op de pc maar op een losse USB-stick
- Geef de router een andere naam en wachtwoord dan de standaard
- Gebruik VPN bij openbare wifi
- Gebruik beveiligingssoftware voor permanente bewaking van de pc-processen en gegevens
- Voer wekelijks een scan uit met meerdere beveiligingspaketten

SAMENVATTING (vervolg)

Bescherm de browser tegen malafide websites
(met bijv. Ublock Origin en Ghostery)

Wellicht later Browsen in een Sandbox

Zet Spam-filter aan bij provider en in eigen
mailpakket

**Maak wekelijks een backup van het systeem en
een backup van de gegevens op een externe HD
en koppel die los**

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

**Basis regel om boven het
beeldscherm te hangen**

**ELKE AANBIEDING VIA
E-MAIL IS NEP EN EEN
POGING U GELD
AFHANDIG TE MAKEN**

Vragen?

