Security technologie

Consultancy

Technical writer

Internet diefstal (cyber crime)

Pierre Janssen woonachtig in Roggel

- Opleiding HBO en Universitair en al meer als 40 jaar ervaring en in beveiliging branche werkzaam, Een Technische achtergrond: computertechnologie, Computernetwerken, Product manager Controls en Communications,

- Werkzaam geweest in Nederland, Brussel, Zweden, en Ierland, Product Manager communications en controls,

- Op moment docent voor de beveiligingsopleidingen in Nederland : gastdocent aan UTC universiteit Brussel, Gastdocent aan Hoogeschool Utrecht.

Presentatie:

De andere kant van het **INTERNET**…….

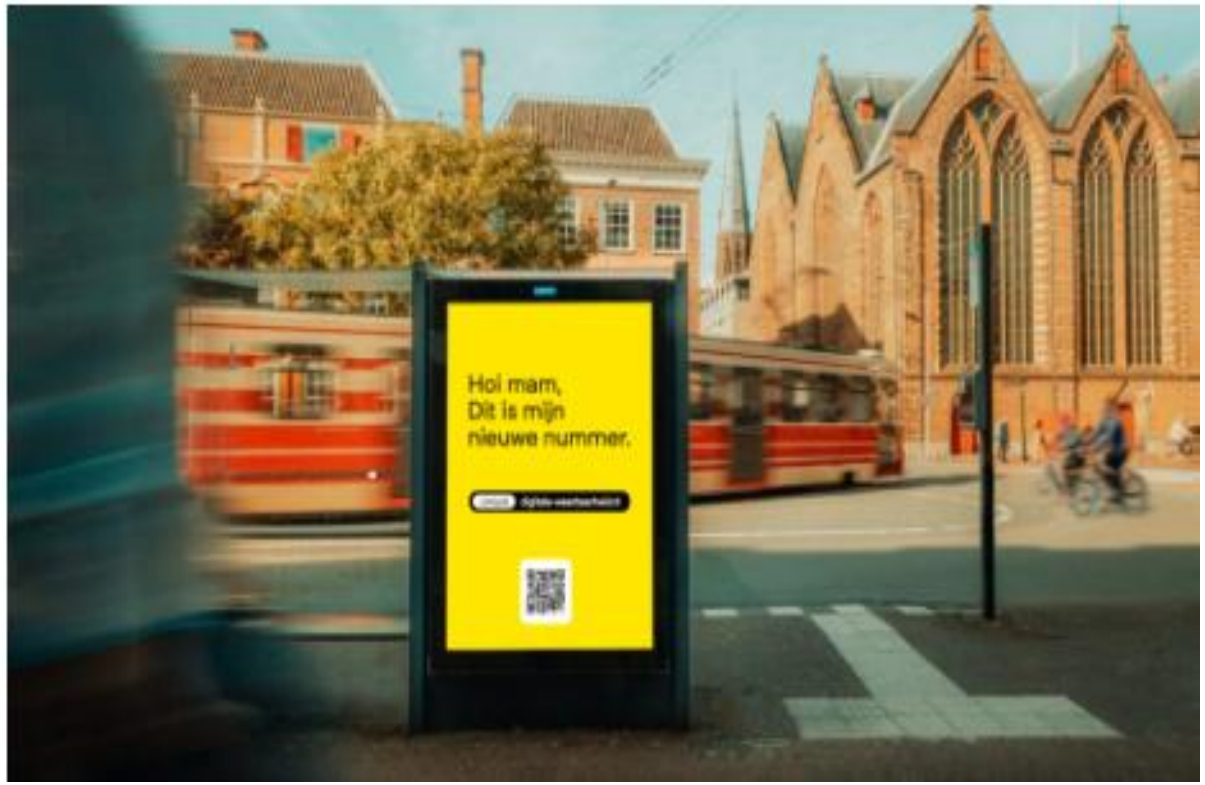
Een <u>informatiebijeenkomst</u> over:

AI – internet fraude – phishing – malware – privacyrisico – ransomware – datalek – cybercrime

<u>Wat is het? Hoe ga je ermee om?</u>

Digitale Weerbaarheid

Kleding kopen, je bankzaken regelen of een aanvraag bij de gemeente, je regelt het allemaal gemakkelijk online. Het internet maakt ons dagelijks leven aangenamer. Tegelijkertijd blijkt uit de Online Veiligheidsmonitor dat slechts één op de drie Nederlanders zich echt veilig voelt online en geeft slechts een kwart aan dat ze over voldoende kennis beschikken om hun online veiligheid te waarborgen.



Schaam je niet, het kan iedereen overkomen

Iedereen kan slachtoffer worden van online oplichting, Ik heb IT’ers gehad die slachtoffer werden van **WhatsApp-fraude** en bankmedewerkers die slachtoffer zijn geworden van beleggingsfraude.”

Van klikken op een valse link of het plaatsen van een bestelling op een malafide webshop: online oplichting zit in een klein hoekje. Ben jij in de val getrapt, wees dan niet bang om hulp te zoeken. Het helpt juist om anderen in vertrouwen te nemen,

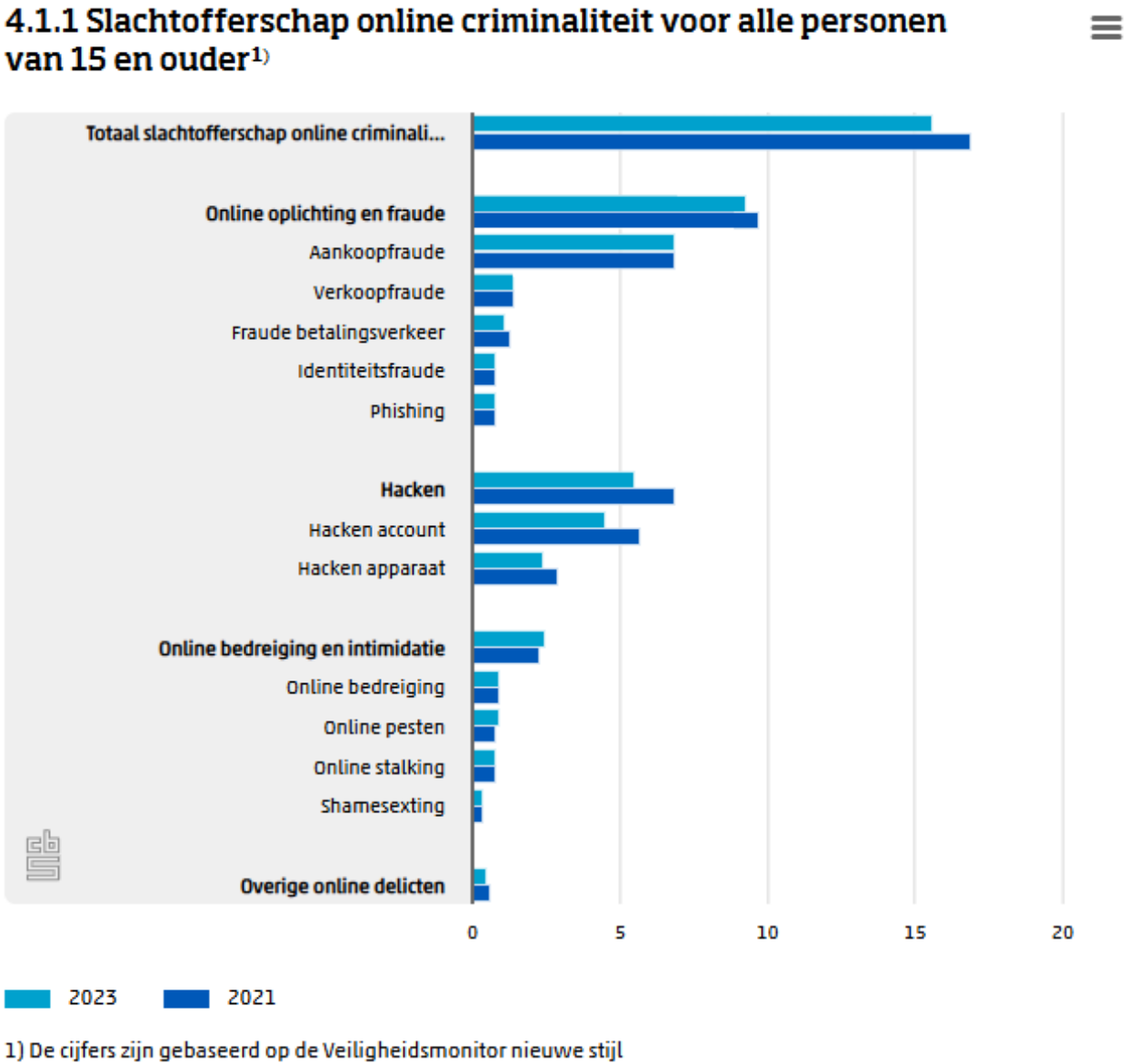
Daders gaan heel geraffineerd te werk en de technieken ontwikkelen zich dagelijks. Een officiële website van bijvoorbeeld een bank, is tegenwoordig nauwelijks te onderscheiden van een nepsite. “Soms kun je als leek denken: ‘Hoe kunnen mensen hier intrappen?’ Maar men realiseert zich niet dat er vaak criminele organisaties achter zitten die 24 uur per dag bezig zijn met het oplichten van mensen.”

cijfers in Nederland van cyber criminaliteit

Het probleem is groot 16% is wel eens slachtoffer geweest

Iedereen doet (onbewust) dingen die kunnen leiden tot een cyberaanval, zowel zakelijk als privé. Bijvoorbeeld als je per ongeluk op een valse link klikt, of persoonlijke gegevens achterlaat op een malafide website. Hoe voorzichtig je ook bent, het kan iedereen overkomen. En als het dan een keer mis gaat, gaat dit vaak gepaard met schaamte.

Cyberschaamte was niet voor niets het cyberwoord van 2024.



Digitale toegankelijkheid

Informatie over hoe **je veilig kan internetten, dit moet voor iedereen beschikbaar en toegankelijk zijn.** Ook als je online gebruik maakt van een hulpprogramma of ondersteuning nodig hebt, omdat je afbeeldingen niet kunt zien of een video niet kunt horen.

We gaan beginnen aan zware werk nu !

Belangrijk is kijk goed voor je klikt liefst 2 maal

Ziet U de verschillen ?

Maybank2u.com
Maybank2u.com

Zijn beide wel/niet het zelfde

Info/verzekeren@Rabobank.com

Info/verzekeren@Rabobank.com

De eerste is correct en de 2e is van een Hacker

De letter ; **a** ; in de URL (internet adres) is van een cyrillic alfabet

Een onoplettende internet gebruiker kan dit over het hoofd zien, zeker als er een link instaat voor te openen en een boodschap over U financiën

Het Internet

Een Revolutie in Communicatie en Technologie

Het internet heeft de manier waarop mensen communiceren, werken, leren en hun leven leiden fundamenteel veranderd. Als een wereldwijd netwerk van netwerken verbindt het miljarden apparaten en gebruikers over de hele wereld.

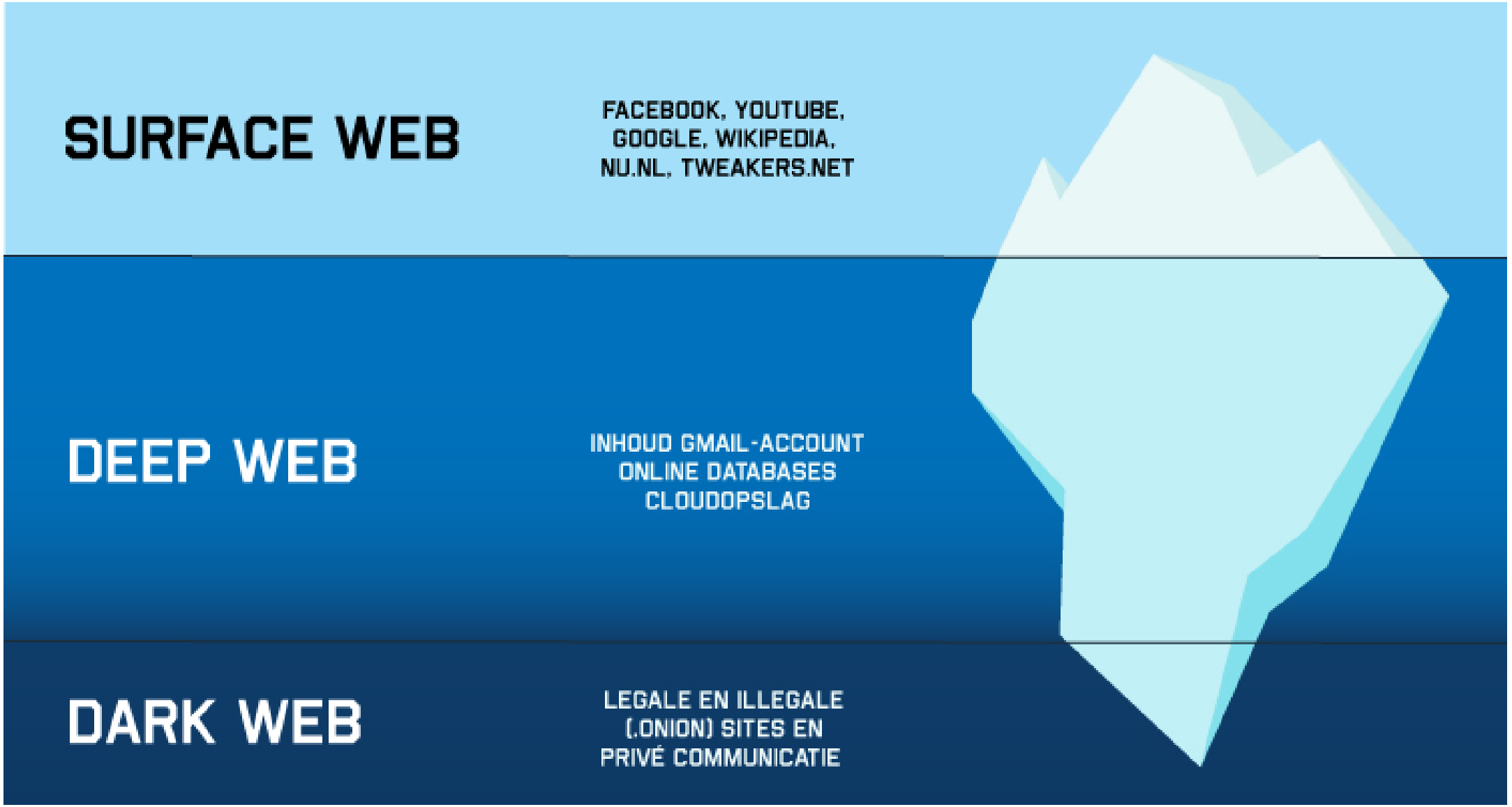
De Geschiedenis van het Internet

De oorsprong van het internet gaat terug tot de jaren 1960, toen het ARPANET werd ontwikkeld door het Amerikaanse ministerie van Defensie. Dit netwerk was ontworpen om onderzoeksinstellingen met elkaar te verbinden en informatie te delen. In de jaren 1980 werd het ARPANET omgevormd tot een meer algemeen netwerk

Het World Wide Web

In 1989 introduceerde Tim Berners-Lee het World Wide Web, een systeem van hypertekst om documenten via het internet te verbinden. Dit maakte het mogelijk om webpagina's te maken en te bekijken met behulp van browsers, wat leidde tot een explosieve groei van internetgebruik in de jaren 1990. Het web veranderde het internet van een netwerk voor wetenschappers en onderzoekers in een platform voor het grote publiek.

Het World Wide Web



Dark web vs. surface web

De verschillen tussen het dark web en het 'normale' surface web dat iedereen dagelijks gebruikt

Surface web	Dark web
Wordt dagelijks door miljarden mensen gebruikt	Onbekend, maar relatief klein aantal gebruikers
Circa 1,7 miljard websites	Onbekend aantal sites
Vindbaar via zoekmachines	Niet geïndexeerd door zoekmachines

Vanwege het gebrek aan regels en de hoge mate van anonimiteit trekt het darkweb veel criminelen aan en vinden er illegale activiteiten plaats, zoals:

- Handel in drugs, wapens, valse identiteiten en gelekte gebruikers gegevens
- Verspreiden van malware, illegale content of kinderporno

Op het dark web wordt zelfs gehandeld in organen. Je kunt het zo gek niet bedenken..

Hoe werkt Internet nu en welke programmering is belangrijk om probleemloos te surfen over het net (in niet te technische uitleg)

- Wanneer u een webadres zoals Google invoert op uw computer en op enter drukt, start een reeks processen die ervoor zorgen dat uw verzoek wordt verwerkt en u de gewenste webpagina te zien krijgt.

- Het proces begint wanneer u een Uniform Resource Locator (URL), zoals www.google.com, invoert in uw browser. De browser begint nu het adres van de server te zoeken die verantwoordelijk is voor de website.

DNS-query

- Het Domain Name System (DNS) speelt een cruciale rol in deze fase. Computers werken met IP-adressen (numerieke identificaties zoals 142.250.74.14) om elkaar te herkennen op het netwerk. Uw computer gebruikt een DNS-server om het door u ingevoerde webadres (zoals www.google.com) om te zetten naar het juiste IP-adres.

Verbindingsopbouw

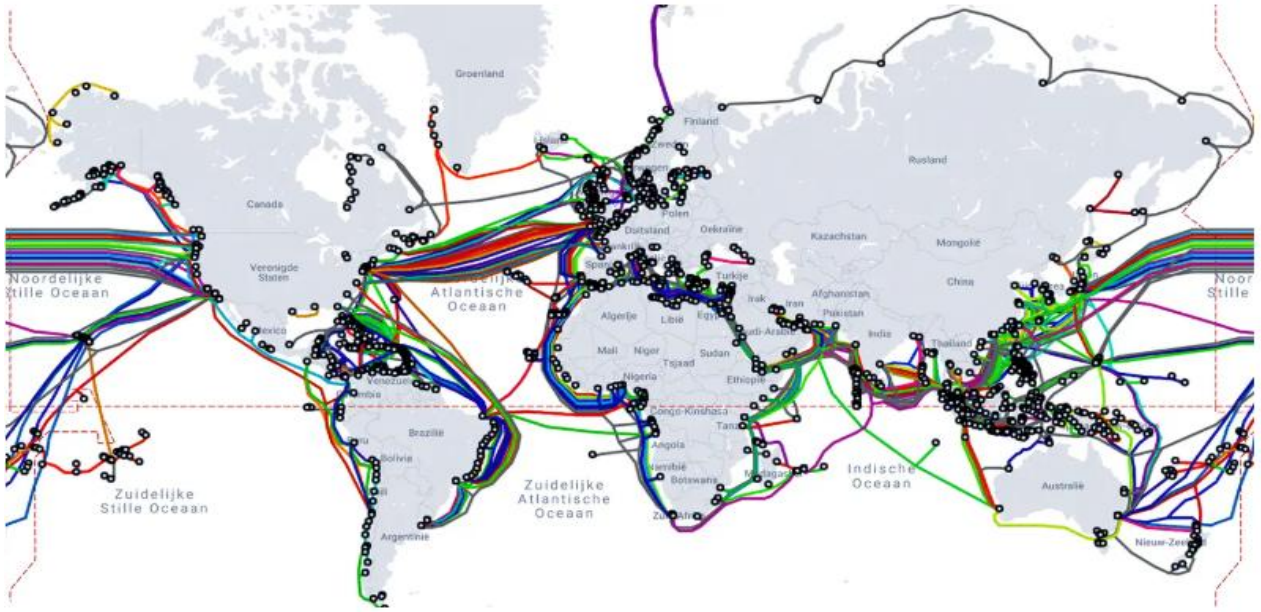
- Na ontvangst van het correcte IP-adres start de browser met het opbouwen van een verbinding. Dit gebeurt via het Transmission Control Protocol (TCP).
- Uw computer initieert een TCP-handshake met de server waarop Google wordt gehost. Dit is een drie-stappenproces waarbij beide apparaten akkoord gaan over hoe te communiceren.
- Naast TCP wordt het HyperText Transfer Protocol Secure **(HTTPS)** gebruikt om ervoor te zorgen dat de communicatie versleuteld is.

De ruggengraat van het internet

- Het internet blijft goed werken door zogeheten *backbones*. Dit is het centrale netwerk van het internet en verbind alle continenten met glasvezelkabels op de bodem van oceaan.

- Glasvezelkabels kunnen over grote afstanden razendsnel informatie versturen via lichtsignalen met een snelheid van 200.000 per seconde.

- Het belangrijkste internetknooppunt in Nederland is de Amsterdam Internet Exchange(AMS-IX). Dit bedrijf regelt het internetverkeer met andere knooppunten in het buitenland en het verkeer voor Nederlandse internetproviders.



Onderzeese glasvezelkabels transporteren het internetverkeer tussen alle continenten

Wat is een IP-adres?

- IP staat voor *Internet Protocol* en bepaalt hoe apparaten op netwerken gegevens met elkaar uitwisselen. Gegevens worden verzonden in kleine pakketten die zijn voorzien van de IP-adressen. Zo weten de pakketten precies waar ze naartoe moeten.

- Je internetprovider geeft je een openbaar IP-adres waarmee je kunt internetten. Providers koppelen dit adres aan je klantgegevens en locatie. In een thuisnetwerk deelt je router IP-adressen uit om het internetverkeer over al je apparaten te verdelen.

- Hoe je IP-adres is opgebouwd, is afhankelijk van het type. Er zijn twee soorten in omloop: IPv4 en IPv6. Een apparaat kan beide tegelijk ondersteunen, zodat er nog steeds verbinding gemaakt kan worden met oudere systemen.

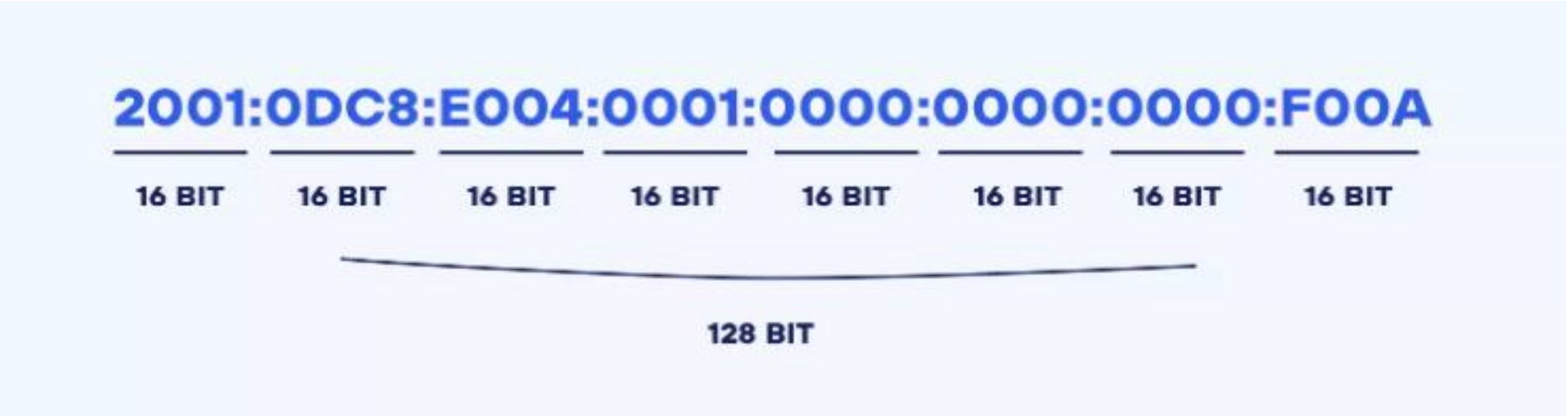
IPv4 was lange tijd de standaard. Deze versie werd in 1983 geïntroduceerd en wordt nog altijd veel gebruikt op het internet. Het is een 32 bits adres, waarbij het adres uit vier delen van 8 bits bestaat. In de praktijk betekent dit dat het adres bestaat uit vier getallen kleiner dan 256, die van elkaar gescheiden worden met een punt. **Zo kan 1.2.3.4 een IP-adres zijn, maar 56.178.93.203 ook**. In totaal kunnen er 4,3 miljard unieke codes met dit systeem gemaakt worden.

Adres Klassen:

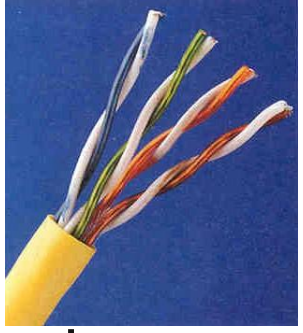
Er zijn 5 verschillende IP adres klasse.
Klasse “A” > voor grote organisatities/bedrijfven (UTC)
klasse “B” > meestal voor universiteiten (Harvard, Cambridge)
Klasse “C”> voor klein bedrijven of interne netwerken
Klasse “D”> wordt gebruikt voor software developers
Klasse “E”> nooit gebruikt

In 2014 waren alle IP (versie 4) adressen vergeven.

Doordat we steeds meer apparaten gebruiken, is er een enorme schaarste aan IP-adressen ontstaan.
Daarom is **IPv6 ontwikkeld**. De samenstelling van deze IP-adressen ziet er iets anders uit. Het is een 128-bits adres en bestaat niet uit vier delen, maar uit acht. Deze delen mogen bovendien uit cijfers en letters bestaan en worden van elkaar gescheiden met een dubbele punt. **Zo is 2a00:d78:0:712:94:198:159:35 een voorbeeld**.
Dankzij deze veel langere code met cijfers en letters zijn er onuitputtelijk veel IPv6-adressen beschikbaar.



Bedraad of draadloze netwerken



Wifi

wordt algemeen gebruikt als de term voor een draadloos netwerk. Eigenlijk is het een vorm van certificatie voor draadloze netwerken die werken volgens de internationale standaard IEEE 802.11 voor draadloze ethernet of wifi. (2,4 Ghz of 5 Ghz)

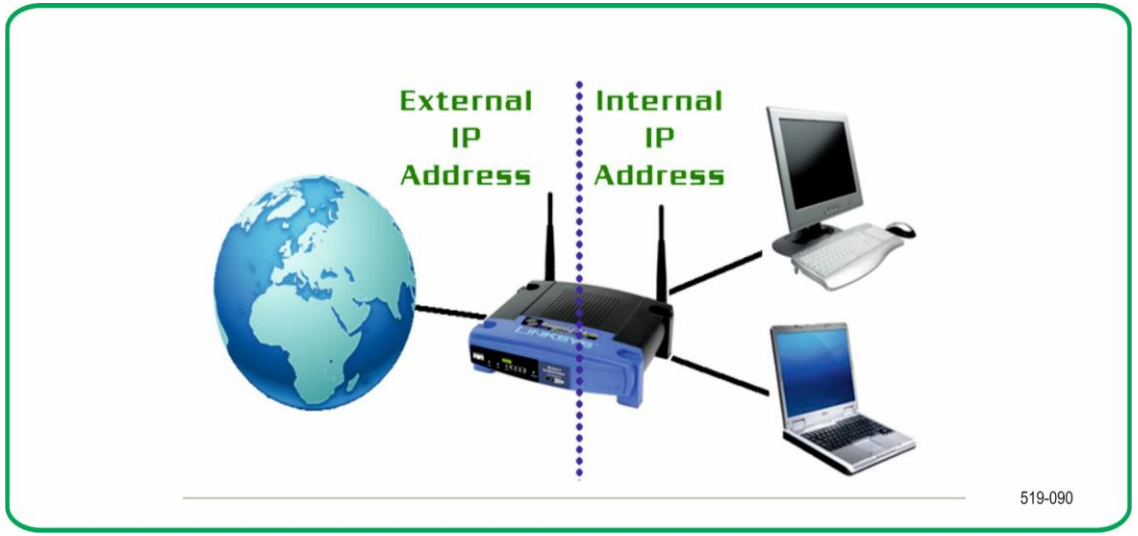
Wifi thuis

Heb je wifi thuis, dan kun je met je computer, laptop, smartphone, tablet via je draadloze netwerk internetten. Erg handig als je in de tuin je e-mail wilt checken of als de kinderen op zolder YouTube-filmpjes op de tablet afspelen. Ook slimme apparaten in huis (Internet of Things) werken via wifi.

Een WEP-sleutel

Wi-Fi Protected Access of WPA

Wat is een openbaar wifi–netwerk?



Dankzij wifi kun je met een computer, tablet of smartphone draadloos internetten. Thuis, maar ook op plekken waar een zogenoemd openbaar wifi-netwerk wordt aangeboden, zoals een café, hotel, camping en vliegveld. Iedereen kan en mag zonder gebruikersnaam of wachtwoord een openbaar wifinetwerk gebruiken.

Het gebruik van *een open wifi-netwerk is nooit veilig*. Soms is het wel van een wachtwoord voorzien, maar dat kan elke bezoeker krijgen. Ook een cybercrimineel. En voor een cybercrimineel is het heel eenvoudig om je smartphone, tablet of computer voor de gek te houden.

draadloze netwerk

Draadloze beveiliging is cruciaal om veilig online te blijven. Verbinding maken met internet via onbeveiligde koppelingen of netwerken is een beveiligingsrisico dat zou kunnen leiden tot gegevensverlies, gelekte accountreferenties en de installatie van **malware** op je netwerk. Het toepassen van de juiste wifibeveiligingsmaatregelen is essentieel, maar het is daarbij belangrijk het verschil te kennen tussen diverse draadloze encryptiestandaarden,

zoals **WEP, WPA, WPA2 en WPA3.**

Wat is WEP? Aangezien draadloze netwerken gegevens verzenden door middel van radiogolven, kunnen gegevens gemakkelijk worden onderschept, tenzij er beveiligingsmaatregelen zijn ingesteld. WEP versleutelt verkeer met een 64- of 128-bits sleutel in hexadecimale notatie. Dit is een statische sleutel, wat inhoudt dat al het verkeer, ongeacht het apparaat, wordt versleuteld met één sleutel.

draadloze netwerk

Wat is WPA?

Daarna kwam WPA, ofwel Wi-Fi Protected Access. Dit protocol werd geïntroduceerd in 2003 en was voor de Wi-Fi Alliance de vervanger van WEP. Het was deels vergelijkbaar met WEP, maar bood verbeteringen in de manier waarop beveiligingssleutels werden verwerkt en gebruikers werden geautoriseerd. Waar WEP aan elk geautoriseerd systeem dezelfde sleutel toekent, maakt WPA gebruik van het Temporal Key Integrity Protocol (TKIP), dat de sleutel die systemen gebruiken dynamisch aanpast. Hiermee wordt voorkomen dat indringers hun eigen encryptiesleutel kunnen maken die overeenkomt met de sleutel die door het beveiligde netwerk wordt gebruikt. De encryptiestandaard TKIP werd later vervangen door de Advanced Encryption Standard (AES).

WPA2 is gebaseerd op het mechanisme van het Robust Security Network (RSN)

draadloze netwerk

Welk type beveiliging heeft mijn wifi?

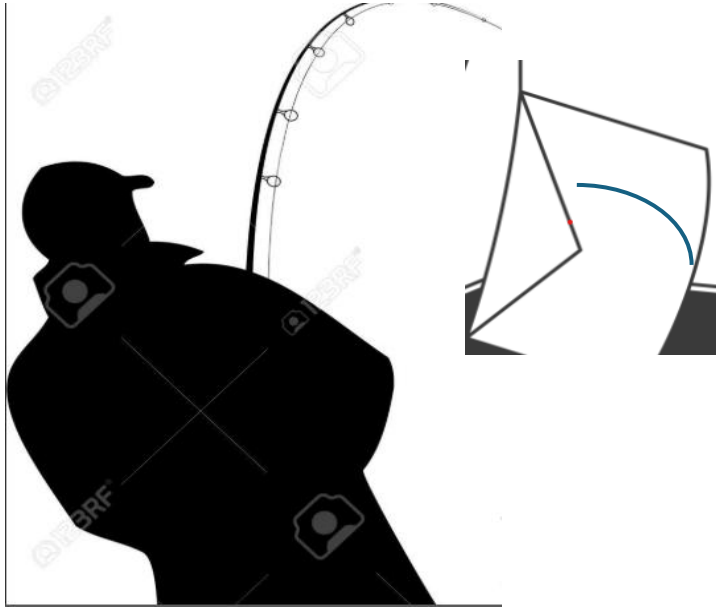
Voor de veiligheid van je netwerk is het belangrijk te weten welk type wifi-encryptie er wordt gebruikt.

Oudere protocollen zijn kwetsbaarder dan nieuwere en kunnen dus eerder ten prooi vallen aan een hackpoging.

Zo ontdek je het beveiligingstype van je wifi: (in Windows)

zoek het pictogram van de wifiverbinding in de taakbalk en klik erop.

- Klik vervolgens op **Eigenschappen** onder je huidige wifiverbinding.
- Scroll omlaag en zoek de wifigegevens onder **Eigenschappen**.



Phishing

Phishing is een vorm van cybercrime waarbij criminelen een e-mail naar je verzenden om te proberen inloggegevens, creditcardinformatie, pincodes of andere persoonlijke gegevens van jou te achterhalen. Vandaar het woord phishing, dat ‘hengelen’ betekent.

Phishing is een van de meest voorkomende vormen van cybercrime. Dat komt ook omdat phishing berichten steeds professioneler worden en bedrieglijk echt lijken. Vroeger stonden ze vol met fouten, maar tegenwoordig kan het lastig zijn om een zo'n vals bericht van een echte te onderscheiden.

Wees alert bij mails of telefoontjes van organisaties zoals je bank.
Al helemaal als er om gegevens of geld wordt gevraagd. Lees hieronder over hoe je een nepmail of neptelefoontje kunt herkennen


TNT-FedEx:
Uw pakket kon niet worden afgeleverd omdat ons systeem onvolledige adresgegevens heeft gedetecteerd. (Pakket is op 28 mei 2025 in het magazijn aangekomen) Bevestig of wijzig uw adres zo snel mogelijk via de onderstaande link om de verzending te versnellen. Indien u uw adres niet op tijd wijzigt, wordt het pakket teruggestuurd naar de afleverlocatie.

https://tnt-fedex-loec.top/nl

(Antwoord "Ja" en open dit bericht opnieuw om op de link te klikken. U kunt de link ook kopiëren en openen in Safari.)

FedEx wenst u een gelukkig leven!

Hoe herken je valse berichten?

- Er is haast bij. Het moet nu of het moet snel.
- Online criminelen spelen in op je emoties: bijvoorbeeld je nieuwsgierigheid, angst, medelijden of zorg om bijvoorbeeld een ouder of een kind.
- Online criminelen doen zich voor als een ander: de overheid, je bank, maar ook je (klein)kind.
- Oplichters doen alsof er een noodgeval is; als je niet snel reageert raak je je geld kwijt.
- De crimineel biedt een buitenkans aan; vaak te mooi om waar te zijn.
- Vaak weten online oplichters iets persoonlijks van je; ze lijken je te kennen omdat ze je wachtwoord weten via een data-lek of omdat ze gegevens over je hebben opgezocht via sociale media.
- Online oplichters blijven altijd heel vriendelijk; ze proberen je vertrouwen te winnen door heel behulpzaam te zijn.

1. Je bank, creditcardmaatschappij, internetprovider of andere organisatie vraagt nooit per e-mail of telefoon om je inlogcodes of wachtwoorden door te geven.

Hieronder wordt uitgelegd hoe je een nepmail en een neptelefoontje kunt herkennen.

Het e-mailadres van de afzender

Via spoofing kan een cybercrimineel je laten denken dat de afzender bijvoorbeeld een bank of webshop is. Controleer het e-mailadres goed. Klik op het e-mail adres, zodat die helemaal zichtbaar is. Criminelen gebruiken vaak e-mailadressen die lijken op die van bekende organisaties.
Het adres kan er bijna hetzelfde uitzien, maar heeft een **vreemd teken of cijfers** in het e-mailadres staan. Let vooral goed op de domeinnaam. **Dat is het deel achter het @-teken**. Soms veranderen criminelen één letter of cijfer in de domeinnaam om deze echt te laten lijken. Ze vervangen bijvoorbeeld de letter ‘o’ door het cijfer 0 of de letter ‘I’ door het cijfer 1. Zoek zelf de website van de afzender op..

•Er is geen persoonlijke aanhef

Bekende personen en organisaties gebruiken meestal je naam in een e-mail. Als je met algemene termen als ‘Geachte heer/mevrouw’ of ‘Beste klant’ wordt aangesproken, let dan extra op.

•Het taalgebruik in de e-mail

Valse e-mails bevatten veel minder taal- en spelfouten dan vroeger. Ook de logo's en foto's die worden gebruikt, zien er steeds professioneler uit. Neem toch de tijd om de e-mail goed door te lezen en te bekijken of je een rare taalfout ontdekt.

•Een link in de e-mail

De link die je ziet in een e-mail, kan er in het echt anders uitzien. Ga met je muis over de link heen **zonder te klikken.** We noemen dat **'hoveren'**. Zo zie je de link waar je naartoe zou gaan als je erop zou klikken. Kijk goed of deze verwijst naar een bekende website.
Je kunt ook de link kopiëren en checken bij **Scamcheck.** blokkeert automatisch websites waarvan deze tool herkent dat ze phishing bevatten. **(rechter muisknop inhouden)**

Als een e-mail in je spambox (ongewenste e-mails) zit, is dit meestal een valse e-mail. Denk je toch dat het de e-mail van een betrouwbare afzender komt? Check dan even goed de stappen hierboven.

Dat is wel even schrikken als je zo brief in mailbox hebt

Wees extra alert op phishing in verband met de laatste NAVO-top bv. Of andere gebeurtenis

Wees in aanloop naar en tijdens een grote gebeurtenis of iets dergelijks extra waakzaam op e-mailberichten die je ontvangt. Kijk goed naar de **domeinnaam** waar de mail vandaan is verzonden en open geen bijlage die je niet vertrouwt.

POLITIE NEDERLAND
Nationaal Cyber Security Centrum
Turfmarkt 147
2511 DP Den Haag

GEWAARMERKT AFSCHRIFT
Juni 2025

Attentie: Aan wie het aanbelangt

In samenwerking met de Minister van Justitie en Veiligheid, Interpol en Europese Unie van Politie Nederland is een gerechtelijke procedure gestart in de vorm van een direct gerechtelijk bevel tegen uw Internet Protocol (IP) adres..

Deze actie is ondernomen op gezag van de Nederlandse Hoofdcommissaris van Politie, Janny Knol, als reactie op het bekijken, verzorgen, verspreiden en in bezit hebben van materiaal waarop minderjarigen te zien zijn die betrokken zijn bij expliciet seksueel gedrag.

De dernièrstralle werd uitgevoerd met behulp van een reeks geavanceerde forensische volgsoftware. Het is aangetoond dat deze tools in staat zijn om internetgebruikers die websites met jeugdporno bezoeken effectief te betrappen.
Het bovenstaande omvat het verwerven en verwerken van digitale beelden, het berekenen van hashwaarden, het terughalen van verwijderde gegevens van harde schijven, de nieuwste besturingssystemen voor mobiele telefoons (Android, IOS en Chinees), servers en draagbare forensische tools voor onderzoek ter plaatse.

Volgens Artikel 248e / 252 van het Nederlandse Wetboek van Strafrecht is het volgende verboden:-

(1) Het produceren, verspreiden, tentoonstellen, verzorgen, importeren, doorsturen, exporteren en in bezit hebben van kinderpornografie is een strafbaar feit, zowel voor persoonlijk gebruik als voor publicatie, en is onderworpen aan wettelijke sancties, waaronder mogelijke gevangenisstraf.

(2) De persoon die het initiatief neemt tot het regelen van een vergadering, door middel van een geautomatiseerd werkproces of door gebruik te maken van een communicatiedienst, met een persoon die hij kent of van wie hij redelijkerwijs moet aannemen dat hij hem kent, is onderworpen aan de volgende bepalingen.

Als een persoon jonger dan zestien jaar betrokken is bij een daad van ontuchtig gedrag met een andere volwassene of afgebeeld wordt in een seksuele handeling, kan de dader juridische gevolgen krijgen. Deze gevolgen kunnen een gevangenisstraf van maximaal twee jaar of een geldboete van de vierde categorie zijn.

Deze mededeling is gebaseerd op de bevindingen die voortvloeien uit de controle van uw Internet Protocol (IP)-adres tijdens gevallen waarin het IP-adres in kwestie werd gebruikt om toegang te krijgen tot online sites die als illegaal worden beschouwd.

Hierbij wordt verzocht om een reactie binnen 24 uur na ontvangst van deze mededeling. Dan kunnen verdere instructies worden gegeven. Als u niet binnen de aangegeven termijn reageert, kan dit leiden tot onmiddellijke juridische stappen.

GEWAARMERKT AFSCHRIFT

Janny Knol
Commissaris Korps Nationale Politie
Nederland

Directeur Nationaal Cyber Security Centrum
(NCSC)

Catherine De Bolle
Directeur

QR-codefraude
trap niet in deze nieuwe manier van oplichting

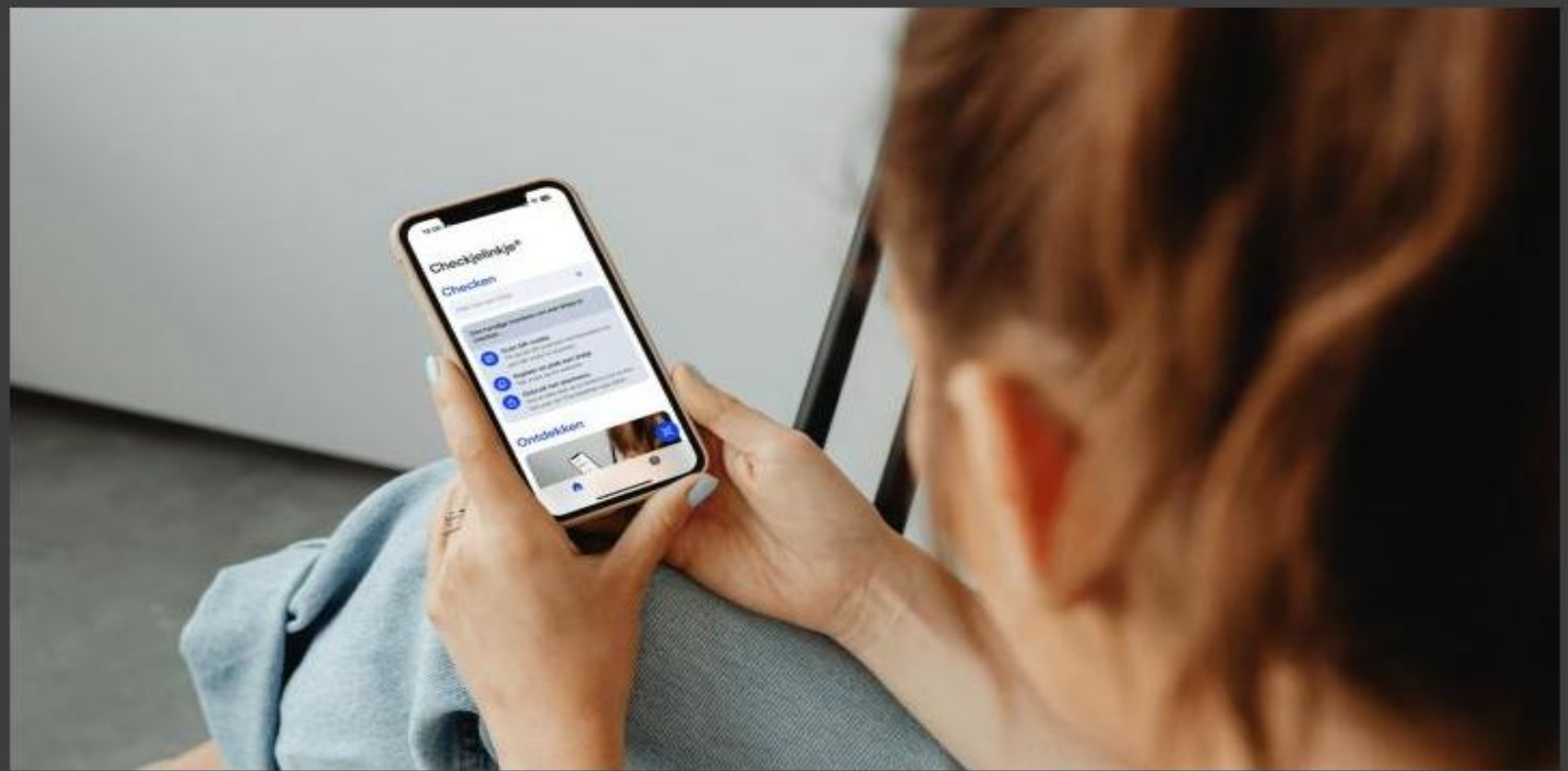
QR-codes zijn al bijna niet meer weg te denken uit het dagelijks leven. We komen ze tegen in winkels, restaurants en online. QR-codes zijn handig en makkelijk om te gebruiken, maar steeds meer criminelen maken er ook gebruik van.

Bij QR-codefraude maken criminelen gebruik van kwaadaardige QR-codes om mensen te misleiden. Kwaadwillende willen je naar een nepwebsite lokken.

Check je (QR) linkje.

Let bij elke QR-code goed op en controleer het webadres net als bij (phishing)berichtjes met linkjes. Check het webadres het liefst bij het scannen, voordat je doorklikt.

Bijvoorbeeld met de app van Checkjelinkje.nl



Scan de QR-code in deze valse brief niet

Sinds begin maart wordt er een brief verspreid die lijkt van DigiD te komen. In de brief staat dat je de gegevens van je DigiD moet beschermen. Dit zou je moeten doen door je DigiD opnieuw te activeren.

De brief roept op om een QR-code te scannen.

Net echt

De brief wordt verstuurd via de gewone post en via social media en ziet er bedrieglijk echt uit. De logo's van DigiD en de Rijksoverheid zijn echt en ook de telefoonnummers kloppen.

Heel belangrijk om te onthouden. De overheid stuurt u geen brieven, e-mails of berichten via social media met een link of QR-code erin. DigiD doet dat ook niet. Krijg je dus een brief, e-mail of tekstbericht met de vraag om een op een link te klikken of een QR-code te scannen, doe dat dan niet.

Ik ben gebeld door mijn bank

Oplichters doen zich voor als medewerkers van U bank en bellen met de mededeling dat Uw bankrekening in gevaar is. Doordat zij gebruikmaken van de techniek “spoofing” ziet U het nummer van uw bank, terwijl de oplichters in werkelijkheid met een ander nummer bellen. Zo proberen zij Uw vertrouwen te winnen, zodat U geld overmaakt of inlog-gegevens afgeeft

Dit kunt U direct doen

Hang op en bel zelf uw bank op met het U bekende nummer. En vraag na of uw bank u inderdaad gebeld heeft.

Ing en de Rabo app voor bankieren hebben een toets voor direct contact met de bank om te controleren of U gebeld word door een bankmedewerker op dat moment

Druk op “hulp” 📖 en dan in 2e menu op “bel” ☎

Deze signalen wijzen op fraude

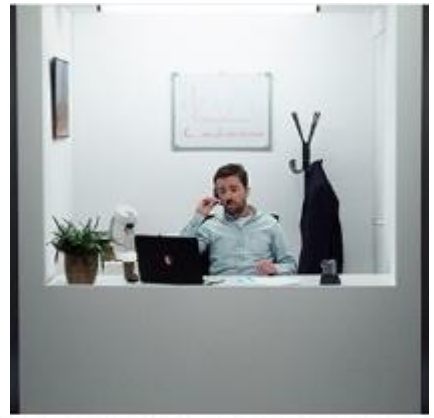
U moet Uw geld overboeken naar een zogenaamde “veilige rekening” omdat er spraken zou zijn van een digitale dreiging of fraude

De oplichters vragen U om in te loggen in Uw bankomgeving of Uw inloggegevens en/of pincode door te geven

Het gebeurt ook dat oplichters iemand naar U toesturen om uw bankpasje en/of waardevolle spullen op te halen en “veilig te stellen”

•Heb je een nieuwe betaalpas ontvangen? Onthoud: knip de chip. Na het doorknippen van de betaalchip (het goudkleurige vierkantje op de pas) kun je je oude pas weggooien bij het restafval. Als je alleen de kaart, maar niet de chip doormidden knipt, kan een oplichter met de doorgeknipte betaalpas (en je pincode) nog steeds geld opnemen bij een geldautomaat.

Ik had contact met een helpdesk ivm computer problemen



Oplichters doen zich voor als medewerkers van de helpdesk van een groot bedrijf. Om u goed te kunnen helpen vragen ze u software te downloaden waarmee ze op afstand problemen met uw computer kunnen oplossen. In werkelijkheid krijgen ze zo toegang tot uw bankomgeving en/of gevoelige informatie.

Dit kunt u direct doen

- Hang direct op wanneer u ongevraagd benaderd wordt door een helpdesk en ga niet in op pop-ups die waarschuwen dat contact met een helpdesk nodig is.
- Download nooit software op verzoek van een onbekende (helpdesk).
- Zoekt u zelf contact met een helpdesk, controleer dan de contactgegevens: oplichters maken namelijk ook gebruik van valse websites waarop ze zich voordoen als de helpdesk van bekende bedrijven.

Gebeld door een Incasso buro of de belastingen

Oplichters doen zich voor als een incassobureau of de Belastingdienst en bellen u over een openstaande factuur of belastingachterstand.

Om beslaglegging te voorkomen, moet de openstaande factuur direct worden betaald. Sommige oplichters vragen meer geld dan het zogenaamd openstaande bedrag. U zou bijvoorbeeld een betalingsachterstand hebben van 300 euro, maar er wordt geadviseerd 3000 euro te betalen. Wat u teveel betaalt wordt later weer teruggestort. In werkelijkheid bent u het geld kwijt.

Advies

Gaat het om een incassobureau, vraag dan eerst om de openstaande factuur en om een bewijs van de overeenkomst. Verbreek vervolgens de verbinding. Krijgt u niets toegestuurd, dan weet u zeker dat het om een niet bestaand incassobureau gaat. Krijgt u wel iets toegestuurd, controleer dan of het om een bestaand en betrouwbaar incassobureau gaat. Dit kan b.v. in het register van de Kamer van Koophandel.

Gaat het om de Belastingdienst, verbreek dan de verbinding en bel zelf terug. Gebruik daarvoor de telefoonnummers uit uw eigen administratie of die op de website van de Belastingdienst en controleer of er daadwerkelijk een achterstand betaald moet worden.

! Wat kunt u doen tegen nepagenten?

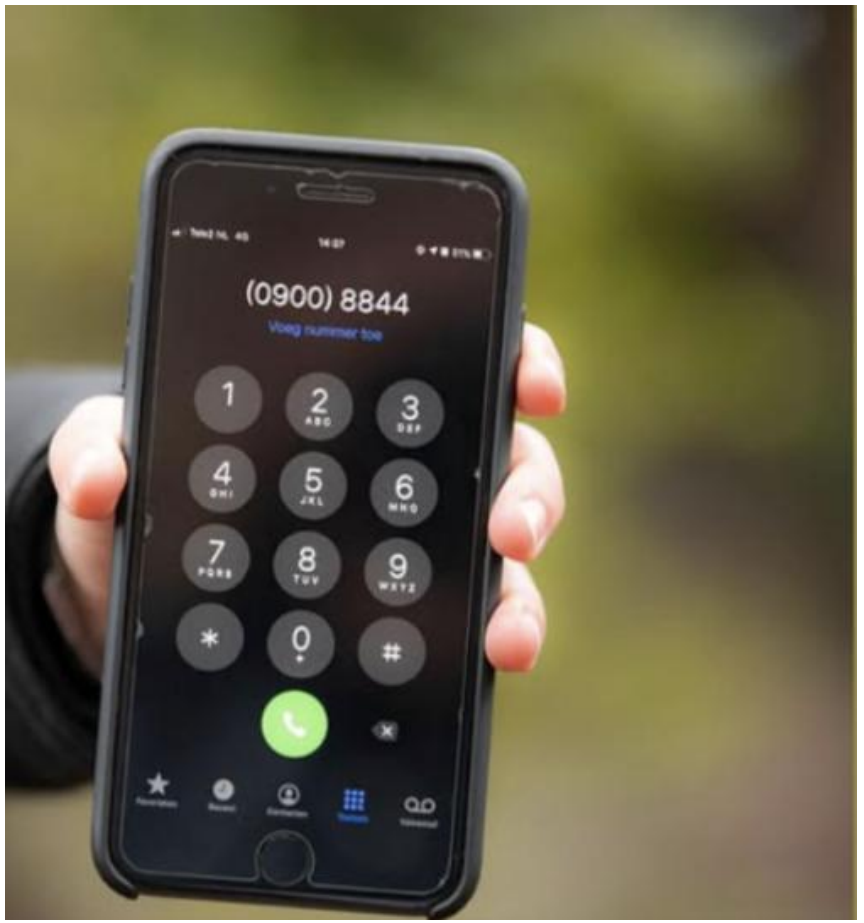
Als u bent gebeld: dat een agent langskomt voor goederen veilig te stellen

- Hang direct op als u wordt gebeld door iemand die zegt van de politie te zijn en die vraagt naar kostbaarheden zoals sieraden of bankgegevens.
- Bel de politie **via 0900-8844** en controleer via hen of u echt gebeld bent door een politiemedewerker.
- Als u informatie heeft doorgegeven: laat niemand binnen.

Politienummer wordt gebruikt voor fraude: 'Trap er niet in'

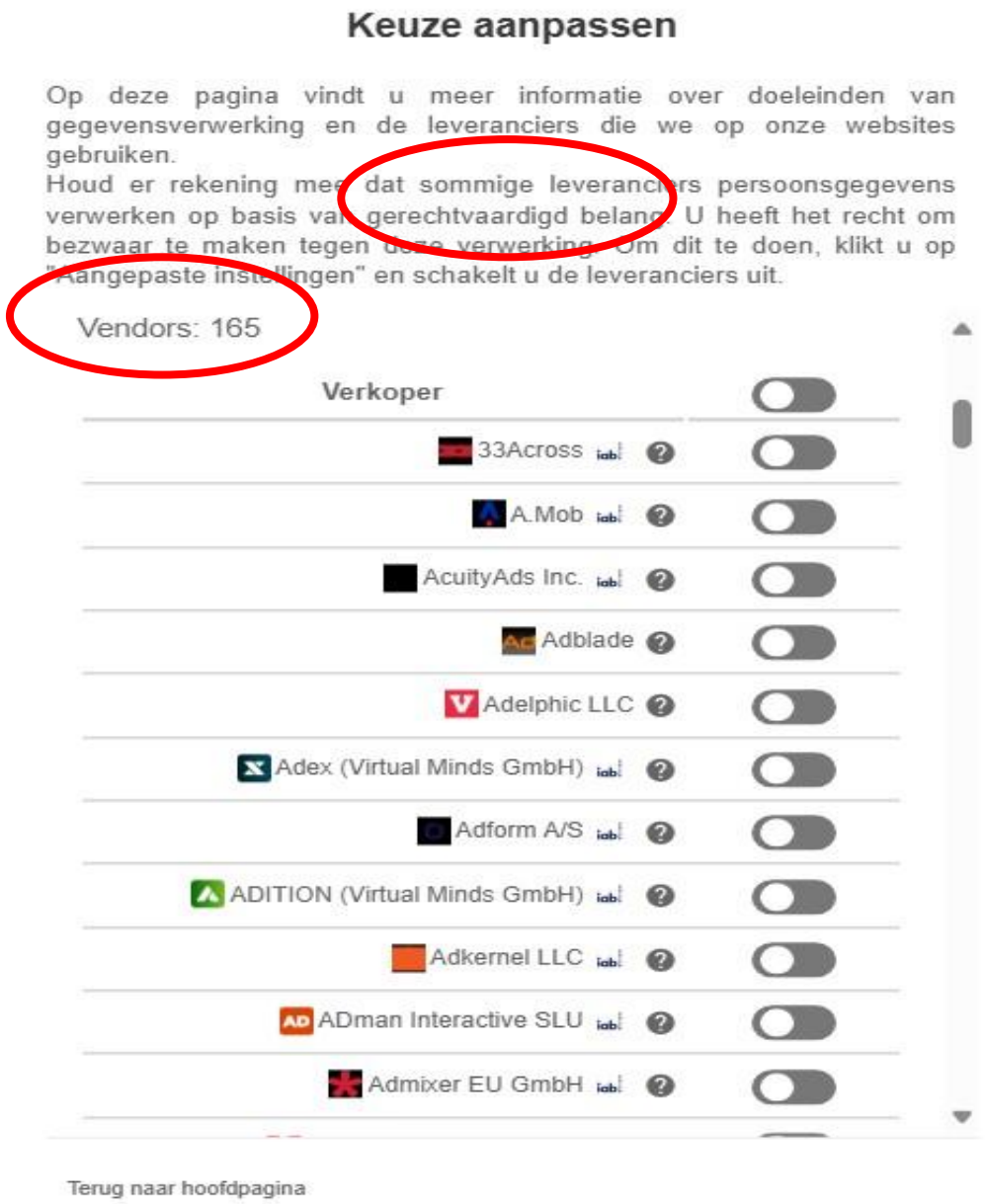
Het landelijke politienummer 0900-8844 wordt misbruikt door oplichters. Ze doen zich aan de telefoon voor als de politie en proberen mensen geld afhandig te maken. De politie waarschuwt: "Wees extra alert."

Op sociale media waarschuwt het Regionaal Service Centrum (RSC) van de politie dat hun nummer wordt misbruikt voor spoofing, dat is een techniek waarbij fraudeurs op het scherm van hun slachtoffer een vals telefoonnummer laten verschijnen. "Je zou daardoor kunnen denken dat je door de politie wordt gebeld. Maar dat is niet zo, de politie belt meestal anoniem", aldus een woordvoerder.



De impact van privacybeleid van grote providers

In onze moderne, digitale wereld is het internet een onmisbaar onderdeel geworden van het dagelijks leven. Van sociale media tot online winkelen, en van onderwijs tot werk, het internet biedt eindeloze mogelijkheden. Echter, zoals met elke innovatie, komen deze mogelijkheden niet zonder risico's. Een van de grootste zorgen is de kwestie **van online privacy** en het beleid van grote providers dat soms de grens tussen gemak en inbreuk op persoonlijke vrijheid doet vervagen. Hoe gevaarlijk is dit en wat kunnen we eraan doen?



Wat zijn cookies?

Cookies zijn kleine bestandjes die een website op je computer, smartphone of tablet plaatst tijdens je bezoek aan de website. Sommige cookies zijn noodzakelijk, sommige niet. Noodzakelijke cookies zorgen dat de website goed werkt en onthouden bijvoorbeeld de voorkeursinstellingen van websitebezoekers.

De meeste websites willen weten wat jij daar doet. Sommige onthouden voor je wat je in je winkelmandje stopt. Andere websites bieden op basis van je zoekgedrag advertenties aan die daarbij passen. Dit kan dankzij cookies.
Er zijn verschillende soorten cookies:

- functionele cookies,
- analytische cookies,
- en tracking cookies.

Alleen voor tracking cookies is het verplicht om jouw toestemming te vragen om deze cookies te plaatsen.

Privacybeleid: een wolf in schaapskleren?

Veel grote providers beschrijven hun privacybeleid in uitgebreide, juridische documenten die voor de gemiddelde gebruiker moeilijk te begrijpen zijn. Vaak bevatten deze documenten clausules die bedrijven toestaan om gegevens te delen met dochterondernemingen, partners of zelfs derden. Hoewel dit vaak wordt gerechtvaardigd als noodzakelijk **voor het verbeteren van diensten**, kan het ook leiden tot een verlies van controle over persoonlijke informatie.

Identiteitsdiefstal

Wanneer persoonlijke gegevens zoals namen, adressen, of financiële informatie in verkeerde handen vallen, kan dit leiden tot identiteitsdiefstal. Hackers kunnen deze gegevens gebruiken om bankrekeningen te openen, leningen aan te vragen of zelfs fraude te plegen onder iemand anders' naam.

Beperk gegevensdeling: Controleer de instellingen van apps en diensten en **schakel onnodige gegevensverzameling altijd uit.**

In April 2025 al gemeld

24 apr 2025 om 12:05
Update: 4 dagen geleden

249 reacties Delen

Mensen die niet willen dat hun gegevens worden gebruikt om de kunstmatige intelligentie (AI) van techbedrijf Meta te trainen, hebben nog tot 27 mei de tijd om daar bezwaar tegen te maken. De Autoriteit Persoonsgegevens (AP) wijst daarop.

Na 27 mei gaat het bedrijf de gegevens van gebruikers van zijn platforms Facebook en Instagram inzetten om de technologie te ontwikkelen. Het gaat om onder meer berichten, foto's en reacties.

Privacywaakhond AP raadt mensen aan om bezwaar te maken tegen het gebruik van hun data als ze zich er niet goed bij voelen. "Het risico is dat je als gebruiker de controle over jouw persoonsgegevens verliest", zegt vicevoorzitter Monique Verdier in een verklaring.

"Je hebt ooit iets op Instagram of Facebook gepost en die gegevens zitten straks in dat AI-model. Zonder dat je precies weet wat daarmee gebeurt. En zitten jouw gegevens eenmaal in het AI-model, dan kun je ze er niet zomaar weer uitkrijgen."

Weer een schending van jouw Privacy door Meta:

Om informatie van gebruikers voor AI te gebruiken een ‘serieuze inbreuk’ op je privacy. „Je verliest de controle over je gegevens.

Hi Pierre,

We're updating our Terms of Service on November 3, 2025. See what's changing. Learn more

Starting on November 3, 2025, we'll also use data from members in your region to improve the content-generating AI that enhances your experience and better connects our members to opportunities. This can help hirers find and reach you more easily, and assist members in creating content such as profile updates, messages, and posts. This could include data like details from your profile and public content you create on LinkedIn; it does not include your private messages. You can opt out anytime in your settings if you'd prefer not to have your data used in this way. If you've already submitted the Data Processing Objection Form, please check your settings to make sure your choice to opt out is shown.

Visit our European Regional Privacy Notice for more information on our reliance on legitimate interest as our legal basis for processing data for training our content-generating AI models used in our products.

You have choices over how LinkedIn uses your data. Learn more in our Help Center.

Thanks for being part of the LinkedIn community — we're glad you're here.

The LinkedIn Team

Deze nieuwe Meta-functie maakt je foto’s 'postwaardiger'

Meta-woordvoerder Mari Melguizo gaf een gedetailleerde toelichting. Ze benadrukte dat de media die door de functie naar de cloud wordt geüpload puur voor het doen van suggesties is, en niet wordt gebruikt om de AI van Meta te verbeteren.

Het is echter niet voor de berichten **die je al hebt geplaatst**, maar voor de parels die nog in je camerarol staan. Als je de functie activeert, zal Meta's AI je camerarol doorzoeken, je ongepubliceerde foto's uploaden naar de cloud van Meta en zogenaamde ‘verborgen parels’ naar boven halen die ‘verloren zijn gegaan tussen schermafbeeldingen, bonnetjes en willekeurige snaps’,

Wat kan ik doen als ik iets heb gekocht in een webwinkel, maar niets ontvangen?

In 2025 heeft bijna de helft van consumenten problemen gehad met online bestellingen

Uit onderzoek van het bedrijf **Klarna** blijkt dat bijna de helft van de consumenten (47 procent) dit jaar te maken heeft gehad met problemen bij online bestellingen. Dit gaat over niet-bezorgde bestellingen of artikelen die niet overeenkwamen met de beschrijving. Deze consumenten zijn waarschijnlijk slachtoffer geworden van **aankoopfraude**.

Als je iets hebt besteld, het niet ontvangt en de klantenservice niet reageert, kan je gebruikmaken van het herroepingsrecht. Het kan ook dat je slachtoffer bent geworden van een nepshop en/ of heb je te maken met aankoopfraude.

webshops betrouwbaar ?

Waar moet je op letten

- **Betaalmethoden**

Veelgebruikte online betaalmethoden zijn iDEAL, Paypal en de creditcard. Een webwinkel moet je ook de keuze geven om (een deel van het bedrag) achteraf te betalen. Bijvoorbeeld met AfterPay of Klarna. Wees voorzichtig als deze mogelijkheid er niet is

- **Scamcheck**

Via **ScamCheck** kun je controleren of een website betrouwbaar is. ScamCheck checkt diverse bronnen om te kijken of een website of link mogelijk malware, phishing of een scam is. Hiervoor wordt input gebruikt van partijen zoals Thuiswinkel.org en Kamer van Koophandel en internationale partijen als Trustpilot (voor reviews), Quad9 (malware), ScamAdviser (scams) en Netsweeper (o.a. phishing). Daarnaast worden technische controles gedaan, zoals de oprichtingsdatum van een website en de domeinnaam. Dat geeft een eindresultaat op basis waarvan ScamCheck aangeeft hoe groot de kans is dat het om een veilige of onveilige website gaat.

Check een url op ScamCheck

ScamCheck is de Nederlandse versie van een tool die ontwikkeld is door ScamAdviser. Deze tool staat op Veiliginternetten.nl en is in Nederland een initiatief van ECP | Platform voor de InformatieSamenleving en Thuiswinkel.org.

Check makkelijk en snel een website

Via ScamCheck kan je controleren of een website of link oplichterij, phishing of betrouwbaar is. Typ de naam van een website in de zoekbalk hiernaast en klik op de button ernaast.

www.example.com

Naar scamcheck →

ScamCheck-extensie

Is een website betrouwbaar of heb je te maken met een phishing-website? Dat is soms lastig te beoordelen. Daarom is er nu de ScamCheck-extensie. Deze extensie waarschuwt je als een website waarschijnlijk onveilig is. Je downloadt de extensie eenvoudig. En daarna krijg je in je scherm een melding als je op een valse website bent terechtgekomen.

Waarborg of keurmerk

Een waarborg of keurmerk kan erop wijzen dat het om een erkende, veilige webwinkel gaat. Een van de bekendste keurmerken in Nederland is het keurmerk Thuiswinkel.org. Kijk voor meer informatie over dit keurmerk op de website van **Thuiswinkel.org*.** Je kunt er bijvoorbeeld lezen hoe je kunt **controleren of een webshop het logo terecht gebruikt*.** Andere keurmerken zijn het **Qshops Keurmerk*** en **WebwinkelKeur*.** Controleer op de website van het keurmerk of deze het keurmerk ook daadwerkelijk aan die webwinkel heeft gegeven. Controleer ook wat de betekenis van het keurmerk is.

Beoordelingen

Via vergelijkingssites, zoals **www.vergelijk.nl*, www.kieskeurig.nl*** of www.beslist.nl* kun je beoordelingen van andere klanten van de webwinkel lezen. Vind je veel positieve beoordelingen, dan kan dit erop wijzen dat de webwinkel veilig is

Doe altijd aangifte bij de politie, of bij de Fraudehelpdesk en check via je betaalmethode of er een kopers bescherming bij zit. In dat geval kan je je geld soms terugkrijgen.

Artificiële intelligentie (AI) verwijst naar systemen of machines die **menselijke intelligentie nabootsen**.

Ze zijn ontworpen om zelfstandig taken uit te voeren, zoals het oplossen van problemen, leren van data en logisch redeneren.

AI omvat een **breed scala aan technologieën en toepassingen**, variërend van chatbots en **virtuele assistenten** tot zelfrijdende auto's en geavanceerde beeldherkenning. Ook in de gezondheidszorg wordt kunstmatige intelligentie ingezet om diagnoses te verbeteren door medische beeldvorming te analyseren.

Verschillende types van Artificiële Intelligentie

Artificiële intelligentie wordt meestal onderverdeeld in **drie hoofdcategorieën**:

Smalle Artificiële Intelligentie (Narrow AI)

Dit is de meest voorkomende vorm van artificial intelligence, ontworpen om **specifieke taken** uit te voeren, zoals gezichtsherkenning of het geven van aanbevelingen op sociale media. Smalle AI is niet in staat om taken buiten zijn programmeerbare doel te volbrengen.

Algemene Artificiële Intelligentie (General AI)

Deze hypothetische vorm van AI zou **menselijke intelligentie volledig kunnen nabootsen**, inclusief creativiteit en sociale vaardigheden. Hoewel er veel onderzoek naar wordt gedaan, is general AI nog niet beschikbaar.

Superintelligente systemen

Deze systemen zouden de **intelligentie van mensen ver overtreffen** en complexe problemen oplossen op manieren die wij ons nog niet kunnen voorstellen. Ook dit type AI bevindt zich nog in de theoretische fase.

Hoe werkt Artificiële Intelligentie?

AI-systemen kunnen **intelligent gedrag vertonen** door patronen te herkennen en op basis daarvan beslissingen te nemen. Ze gebruiken **algoritmes** als fundamentele bouwstenen om enorme hoeveelheden data te analyseren en kunnen zo zelfstandig actie ondernemen.

Deze algoritmes zijn vaak geïntegreerd uit verschillende systemen en sectoren, waar AI wordt toegepast om processen te optimaliseren.

Het proces wordt vaak **aangedreven door machine learning en deep learning**.

- **Machine learning**: Computers leren patronen in data te herkennen en zelfstandig beslissingen te nemen. Een geavanceerde methode binnen machine learning is reinforcement learning, waarbij het systeem zichzelf verbetert door ervaring op te doen en de meest succesvolle strategieën te vinden.
- **Deep learning**: Dit is een meer geavanceerde vorm van machine learning, waarbij neurale netwerken data verwerken, geïnspireerd door het menselijk brein.

Hoewel AI in staat is om patronen te herkennen en zelfstandig actie te ondernemen, ontbreekt het aan echt begrip zoals mensen dat hebben. Het is daarom belangrijk dat gebruikers zich bewust zijn van de beperkingen van AI.

Wat is AI en wat zijn de risico's?

door Meta:

Risico’s van AI

AI brengt ook gevaren en risico’s met zich mee. Zowel op het gebied van (online) veiligheid als privacy. Criminelen kunnen de technologie bijvoorbeeld inzetten om kwaadaardige software te ontwikkelen. Maar AI kan ook misbruikt worden voor het verspreiden van nepnieuws of voor het manipuleren van verkiezingen. Een manier waarop dit wordt gedaan is met ‘**deep fakes**’.

Dit zijn video’s, afbeeldingen of audio-opnamen die echt lijken, maar dit niet zijn. Met behulp van AI kan een filmpje worden gemaakt waarin een bekende politicus bepaalde uitspraken doet.

Experts waarschuwen daarnaast dat AI gebruikt kan worden om persoonlijke data te verzamelen of om privé informatie te delen zonder toestemming. Als je in contact bent met een programma of app dat AI gestuurd is, bijvoorbeeld een chatbot, is het belangrijk dat je weet dat je niet te maken hebt met een mens, maar met een computer.

Wees daarom kritisch op welke (persoonlijke) informatie je deelt.

Wat zijn deepfakes?

Deepfakes zijn beelden die zijn gemaakt met behulp van artificial intelligence (AI) en algoritmen .
In deze beelden worden gezichten en stemmen nagedaan en geïmiteerd.

Deepfakes zijn digitale manipulaties van audio, beeld en video

Ze lijken soms levensecht, maar zijn dit niet. **Deepfakes** worden gemaakt met behulp van artificial intelligence (AI) en algoritmen die kunnen leren om gezichten en stemmen te imiteren. De maker van een deepfake verzamelt bestaande beelden van degene die hij wil namaken, en zet AI in om deze te vervormen.

Deze technologie is volop in ontwikkeling, en deze beelden lijken steeds echter lijken. **Helaas wordt het gebruik ervan daardoor ook steeds interessanter voor cybercriminelen.** Het is daarom belangrijk dat je je ervan bewust bent dat niet alles wat je online ziet of hoort, echt is.

De gevaren van deepfake - sextortion, wraakporno en desinformatie

Deepfakes worden ook ingezet voor het schaden van het imago en de reputatie van personen of organisaties. **Sextortion** en **wraakporno** zijn hierbij de meest voorkomende vormen. Hierbij gebruikt de maker met vervelende bedoelingen deepfake-technieken om het gezicht van een pornoacteur te vervormen tot het gezicht van iemand anders – degene die hij belachelijk wil maken of kwetsen. Maar denk ook aan een deepfake van een directeur van een organisatie die iets zegt wat onhandig of zelfs beledigend is. Je kan je voorstellen dat het hem niet alleen in een kwaad daglicht stelt, maar ook het vertrouwen van zijn personeel en klanten kan kosten.

De gevaren van deepfake - sextortion, wraakporno en desinformatie

Basistips voor je eigen veiligheid/plezier

Cybersecurity is een gedeelde verantwoordelijkheid, en er zijn tal van oplossingen die je zelf kunt toepassen om jezelf te beschermen tegen digitale bedreigingen. Of het nu gaat om het gebruik van een firewall, het inzetten van AI, of het voorkomen van telefoonscans en bankfraude, met een beetje moeite kun je je online veiligheid aanzienlijk verbeteren.

voor je online veiligheid, deze begint eerst bij jezelf

Cybercriminelen proberen op veel verschillende manieren jouw telefoon of computer binnen te komen en schade aan te richten. Denk aan **hacken, phishing of ransomware**. Je kan jezelf daartegen beveiligen.

5 basistips voor je online veiligheid

1. Zorg voor veilige wachtwoorden voor al je apparaten en accounts.
2. Doe altijd direct software-updates van je slimme apparaten.
3. Gebruik een virusscanner of een VPN verbinding
4. Maak regelmatig een back-up.
5. **Eerst checken, dan klikken.**

1 - Tips voor een goed wachtwoord

• Een goed wachtwoord moet eenvoudig genoeg zijn om te onthouden en sterk genoeg om niet makkelijk te kunnen kraken, dus gebruik: hoofdletters, kleine letters, cijfers, tekens en minimaal 10 karakters.

• Maak een verdeling naar de domeinen waarop je werkt: gebruik één wachtwoord voor , zakelijk werk, één voor email, één voor correspondentie met banken en dergelijke, één voor social media, enzovoort.

• Bewaar wachtwoorden in een wachtwoordkluis, zoals Keepass. Of in een beveiligde Excelsheet.

Wachtwoordzin

Het allerbelangrijkste van een wachtwoord is de lengte van het wachtwoord. Daarom adviseren ik ook vaak om een wachtwoordzin te gebruiken. Verzin een wachtwoord(zin) van tenminste 12 tekens. Een wachtwoord wordt sterker als je andere tekens gebruikt (cijfers, leestekens) maar **lengte is altijd belangrijker.** Een wachtwoord van tien kleine letters is meer dan honderd keer sterker dan een wachtwoord van acht tekens waarin ook hoofdletters, cijfers en speciale tekens zijn verwerkt.

Wees creatief

Daarnaast is het belangrijk dat je wachtwoord niet voor de hand ligt: 'Pa$$w0rd' lijkt een sterk wachtwoord, maar is behalve erg kort, ook heel erg voor de hand liggend. Een hacker probeert de eerste 1000 voor de hand liggende wachtwoorden; 'aaaaaaaaaaaaaaaaaaa' is daarom ook geen goede keuze. Het is lastig te kraken, maar makkelijk te raden omdat het bovenaan de lijsten staat met veel voorkomende wachtwoorden. Wees dus creatief en bedenk een originele wachtwoordzin, bijvoorbeeld: Erstonden3grotegrazersindewei! En bedenk, als wachtwoorden gestolen worden, maakt het niets uit of je een sterk wachtwoord hebt. Maar als je accounts verschillende wachtwoorden hebben, kan een hacker niet in één keer bij al je accounts

Zorg er dus voor dat al je accounts een ander wachtwoord hebben!

Wachtwoordmanager

Gebruik een wachtwoordmanager. Dit is een digitale 'kluis' waarin je al je wachtwoorden en gebruikersnamen kunt opslaan. Je hoeft dan alleen het wachtwoord van je wachtwoordmanager te onthouden. En bezoek je een website, dan vult de wachtwoordmanager automatisch je gebruikersnaam en wachtwoord in.

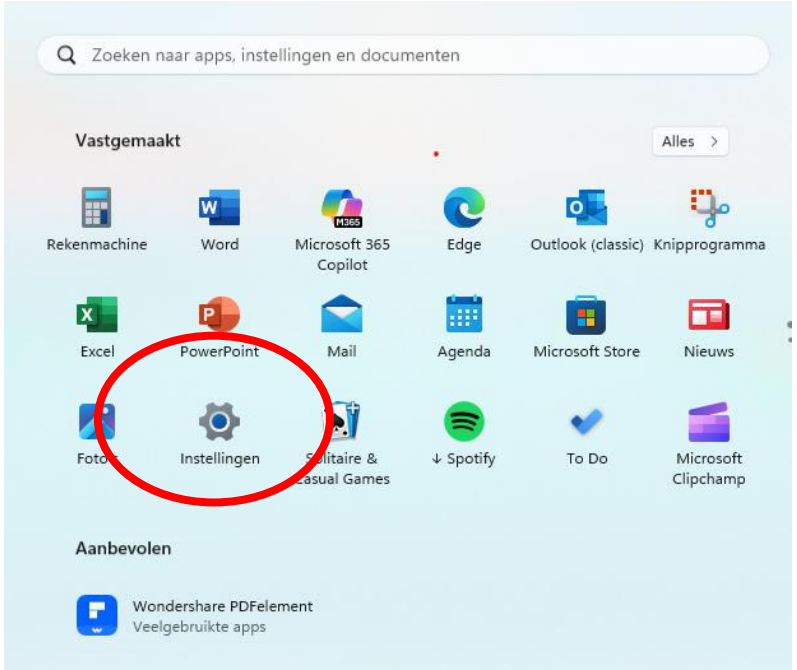
Natuurlijk is het belangrijk om een sterk wachtwoord voor je wachtwoordmanager te kiezen. Een wachtwoordmanager maakt ook automatisch een sterk wachtwoord voor je. Je kunt de meeste wachtwoordmanagers op verschillende apparaten gebruiken, zoals je computer, tablet en smartphone.

Een aantal wachtwoordmanagers op een rij:

- 1Password
- NordPass
- Keeper
- KeePass
- iCloud-sleutelhanger
- LastPass

2 - Maak altijd direct software-updates van je programma's

Installeer updates tegen beveiligingslekken
Fabrikanten brengen updates uit voor hun software om nieuwe functionaliteiten toe te voegen, maar ook om fouten op te lossen en beveiligingslekken te dichten. Dat laatste is heel belangrijk. Het updaten van software kan je behoeden voor grote schade door een cyberaanval met bijvoorbeeld gijzelsoftware. Lees daarom verder wat je kunt **updaten** en doe de test of **automatisch updaten** van je bedrijfssoftware verstandig is.



Maak altijd direct software-updates van je programma’s

- **Besturingssysteem:** De bekendste software updates voor computers en laptops zijn de updates voor het besturingssysteem. Bijvoorbeeld de updates die Microsoft voor Windows en Apple voor MacOS beschikbaar stelt. Deze updates worden vaak automatisch gedownload en geïnstalleerd, maar het is belangrijk om af en toe te controleren of dit ook werkelijk zo is.
- **Applicaties:** Het is belangrijk te beseffen dat de updates die je installeert voor het besturingssysteem, geen updates bevatten voor applicaties die op het apparaat draaien. Denk hier bijvoorbeeld aan internet browsers, tekstverwerkers, foto bewerkers of software die PDF bestanden kan lezen. Juist op dit soort standaardapplicaties kan een beveiligingslek gemakkelijk tot misbruik leiden. Een tijdige update van de applicatie voorkomt dit. Ga daarom na welke applicaties zijn geïnstalleerd en probeer waar mogelijk automatisch updaten in te schakelen. Er bestaan tools die het mogelijk maken om veel van deze applicaties (automatisch) te updaten.
- **BIOS:** Computers en laptops hebben onderliggende software nodig die de verschillende hardware op een lager niveau aanstuurt. Bijvoorbeeld de werking van een toetsenbord of muis. Dit soort software wordt ook wel “firmware” genoemd. De laatste jaren zijn veel kwetsbaarheden ontdekt in bijvoorbeeld processoren. Deze kwetsbaarheden kunnen vaak alleen worden opgelost door updates in de zogenaamde BIOS Firmware van een laptop of computer en kunnen niet automatisch worden geïnstalleerd. Op de website van de fabrikant van je computer of laptop vind je deze updates met de bijbehorende installatie instructies.

Systeem

pierke15
Aspire A517-53
Naam wijzigen

Microsoft 365
Beheren

OneDrive
Beheren

Windows Update
Laatst gecontroleerd: 43 minuten geleden

- **Beeldscherm**
  Monitoren, helderheid, nachtlamp, beeldschermprofiel
- **Geluid**
  Volume niveaus, uitvoer, invoer, geluidsapparaten
- **Meldingen**
  Waarschuwingen van apps en systeem, niet storen
- **Focus**
  Afleidingen verminderen
- **Aan/uit en accu**
  Scherm en slaapstand, batterijgebruik, energiemodus, energiebesparing
- **Opslag**
  Opslagruimte, stations, configuratieregels

Windows Update

Uw pc is bijgewerkt
Laatst gecontroleerd: vandaag, 11:10

Naar updates zoeken

Meer opties

Krijg de nieuwste updates zodra ze beschikbaar zijn
Wees een van de eersten die de meest recente niet-beveiligingsupdates, oplossingen en verbeteringen krijgt zodra ze worden uitgerold. Meer informatie
Aan

Updates onderbreken
Een week pauzeren

Geschiedenis van updates

Geavanceerde opties
Bezorgingsoptimalisatie, optionele updates, actieve uren, andere update-instellingen

Windows Insider-programma
Preview-versies van Windows downloaden om feedback te delen over nieuwe functies en updates

Windows Update zet zich in om de koolstofuitstoot te verminderen. Meer informatie

Verwante ondersteuning

Hulp bij Windows Update

3 - Wat is een virus en hoe bescherm ik mijn apparaten hiertegen?

Een virus is een klein programma dat de werking van je computer verstoort. Het kan bijvoorbeeld gegevens op je computer beschadigen of verwijderen, je e-mail gebruiken om zichzelf te verspreiden of zelfs je hele harde schijf wissen. Bescherm je apparaten hiertegen door een virusscanner te gebruiken,

Een virusscanner is een van de belangrijkste onderdelen van de bescherming van je computer. Bij de keuze voor een virusscanner is een goede afweging tussen prijs, kwaliteit en functionaliteit belangrijk

Let op de volgende aandachtspunten bij de keuze voor een virusscanner.

Tegen welke gevaren

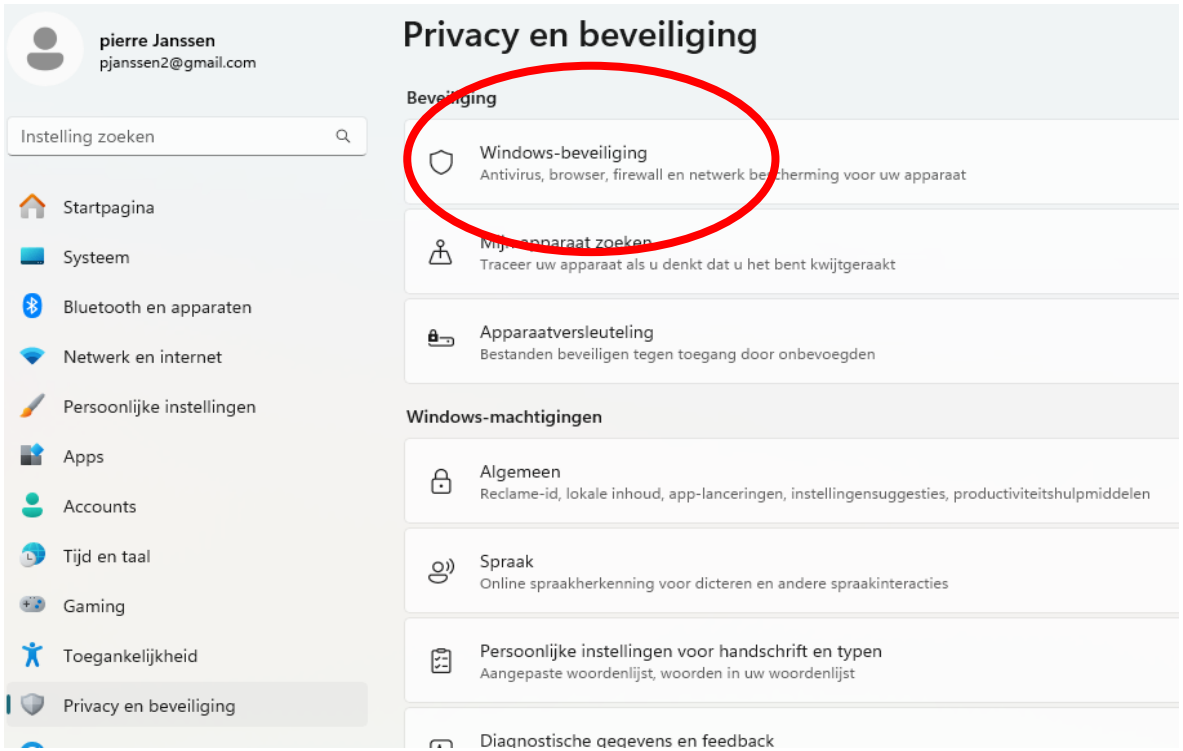
Bepaal tegen welke gevaren het antivirusproduct je computer moet beschermen. Elke virusscanner beschermt je tegen veelvoorkomende virussen, wormen en trojans. Sommige pakketten hebben daarnaast nog extra functies, zoals een firewall, het blokkeren van pop-ups,

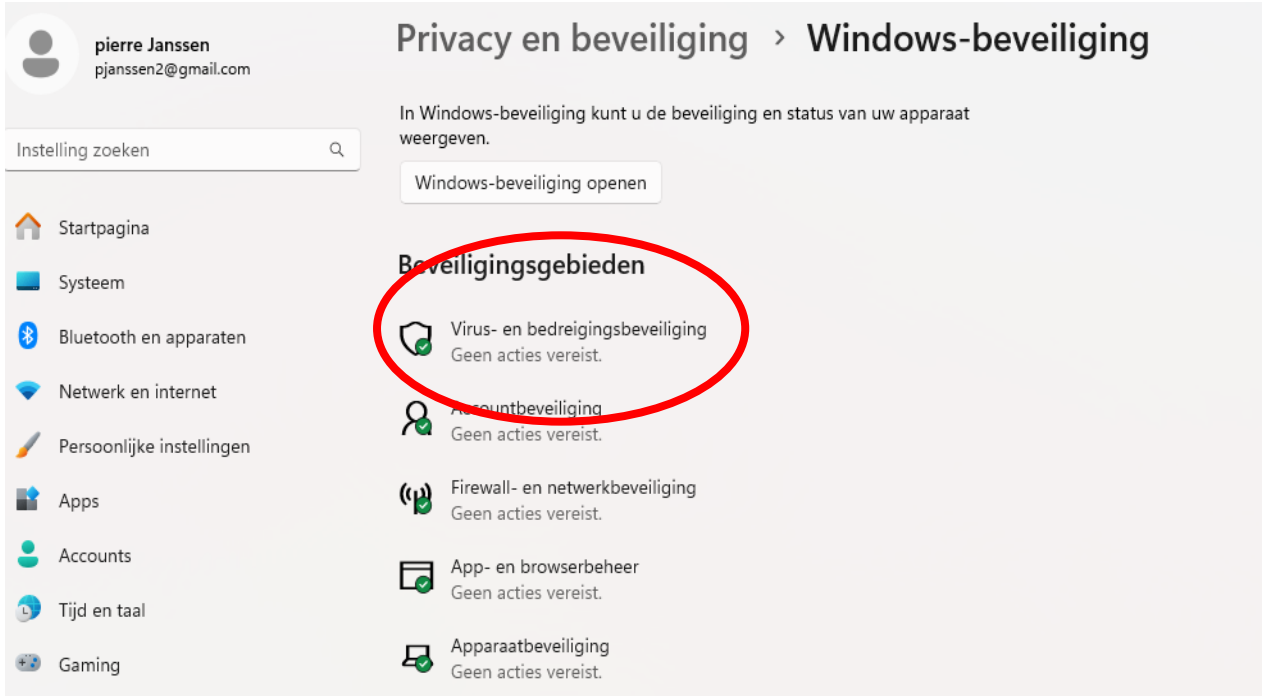
Gratis of betaald

Weeg de voor- en nadelen van gratis en betaalde virusscanners goed tegen elkaar af. Er zijn tegenwoordig veel gratis virusscanners die kwalitatief even goed zijn als betaalde producten. Wees je er wel van bewust dat gratis of goedkope scanners soms minder functies hebben of een lagere kwaliteit hebben.
Kies je voor een betaalde virusscanner, let dan op de kosten om verrassingen te voorkomen. Soms moet je namelijk niet alleen de aanschafprijs betalen, maar ook nog af en toe betalingen doen voor het ontvangen van updates of ondersteuning.

Maak gebruik van de ingebouwde virus scanner in Windows 11

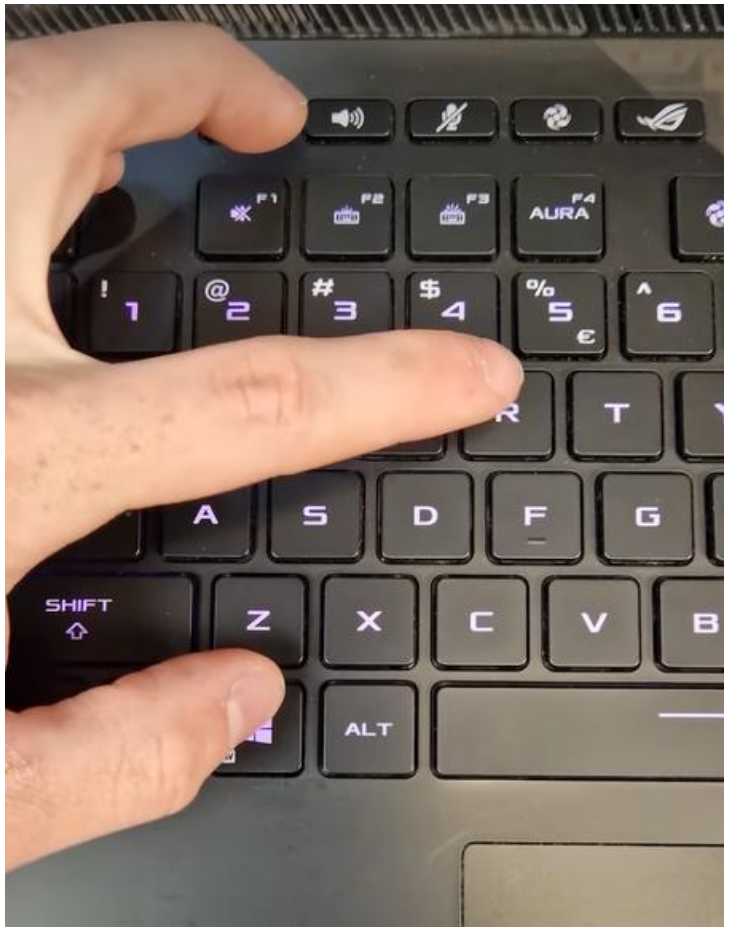
Ga naar instellingen en dan naar Privacy en beveiliging





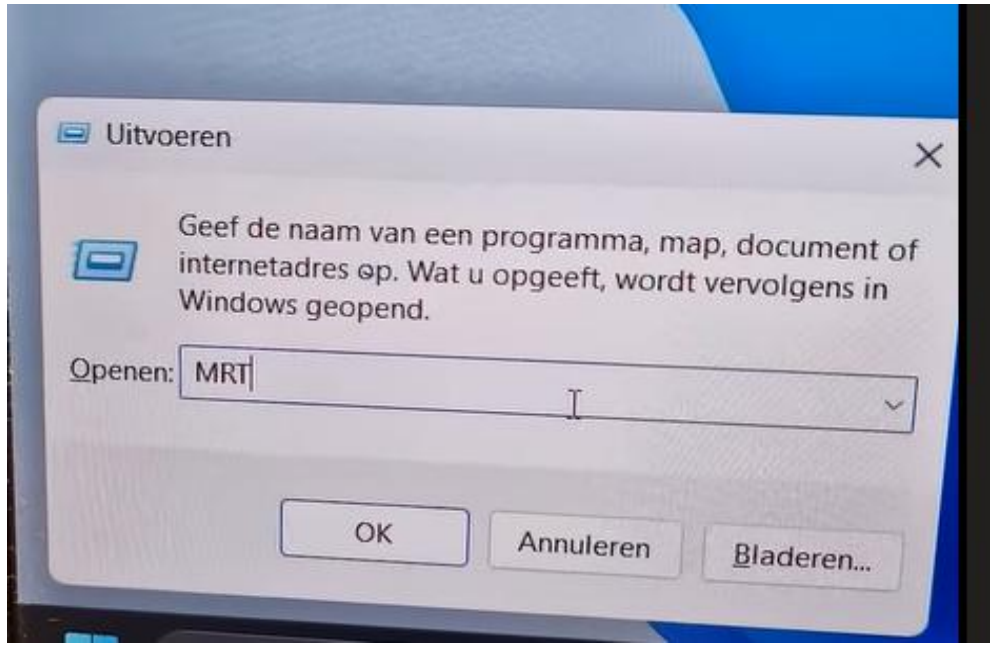
4 Controleer of schadelijke software op Uw PC staat

Window 11 heeft een extra functie in combinatie met de window toets



Window plus toets “R” opent nieuw venster

En kijk of en MRT in de balk staat en druk OK

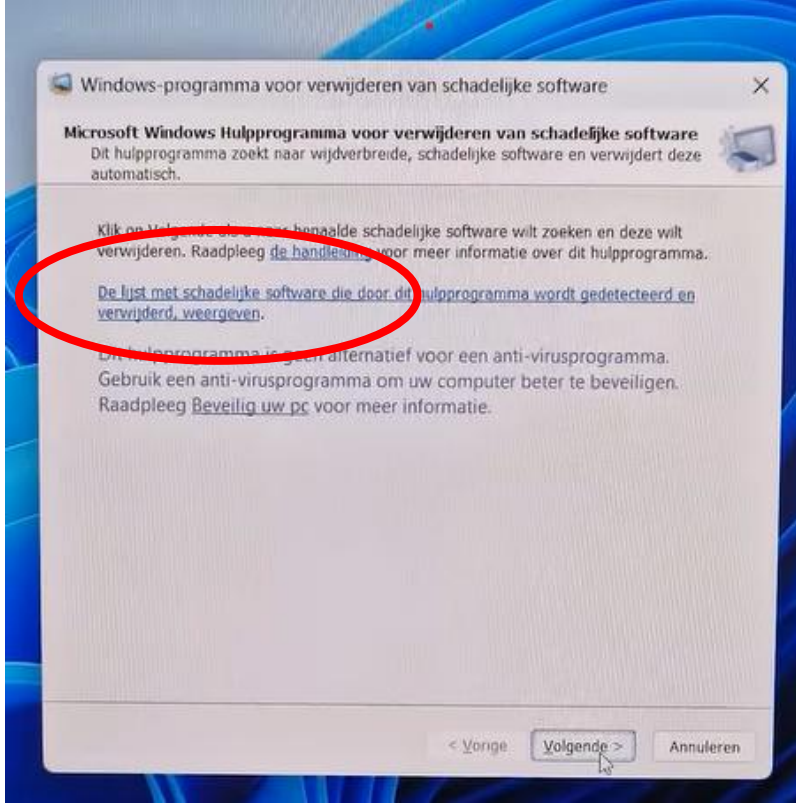


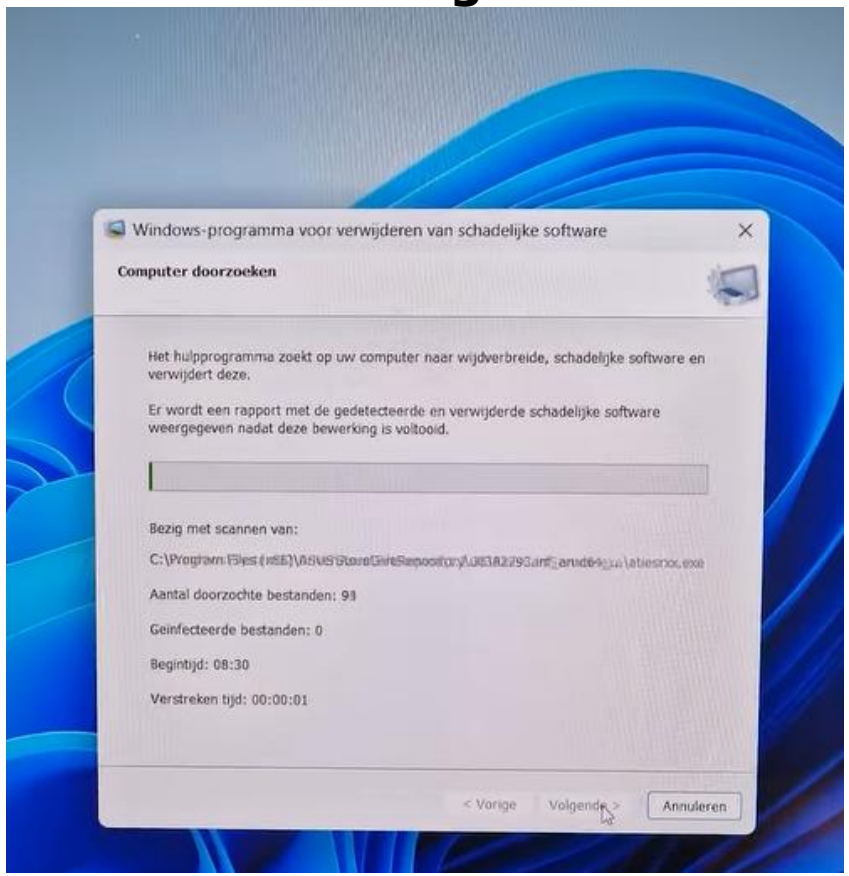
Vervolg op controle

Het volgend scherm opent in Windows en

klik op “volgende”

In volgende scherm selecteert u de scantype





Windows start nu met zoeken naar schadelijke software en zal hiervan een melding geven en verwijderen

Groene balk geeft proces weer:

Bluetooth-apparaat met Windows verbinden

- **Bluetooth** is een draadloze technologie die communicatie op korte afstand mogelijk maakt.

- Wanneer Bluetooth is ingeschakeld, maken het Bluetooth-apparaat en het Windows-apparaat automatisch verbinding wanneer de twee apparaten zich biWanneer Bluetooth is ingeschakeld, maken het Bluetooth-apparaat en het Windows-apparaat automatisch verbinding wanneer de twee apparaten zich binnen het bereik van elkaar bevinden. binnen het bereik van elkaar bevinden.

- Altijd bluetooth uitzetten na gebruik of alleen maar bij gebruik App’s

5 Gebruik van een VPN (virtual private network)

Een openbaar wifi-netwerk gebruiken van bijvoorbeeld een café, hotel, vliegveld of trein is nooit veilig, of je nu een wachtwoord gebruikt of niet. Zodra je inlogt op een openbaar wifi-netwerk, kan een criminele hacker toegang krijgen tot je apparaat en daardoor tot je persoonlijke en belangrijke gegevens.

Een VPN werkt als een soort beveiligde tunnel. Als je per ongeluk verbinding maakt met een netwerk van een criminele hacker (omdat je denkt dat je gebruikmaakt van openbare wifi in een hotel of restaurant), dan zorgt de VPN ervoor dat de hacker geen gegevens op jouw computer kan inzien of veranderen.

Door het gebruik van een VPN:

- **Ben je veiliger op het internet**

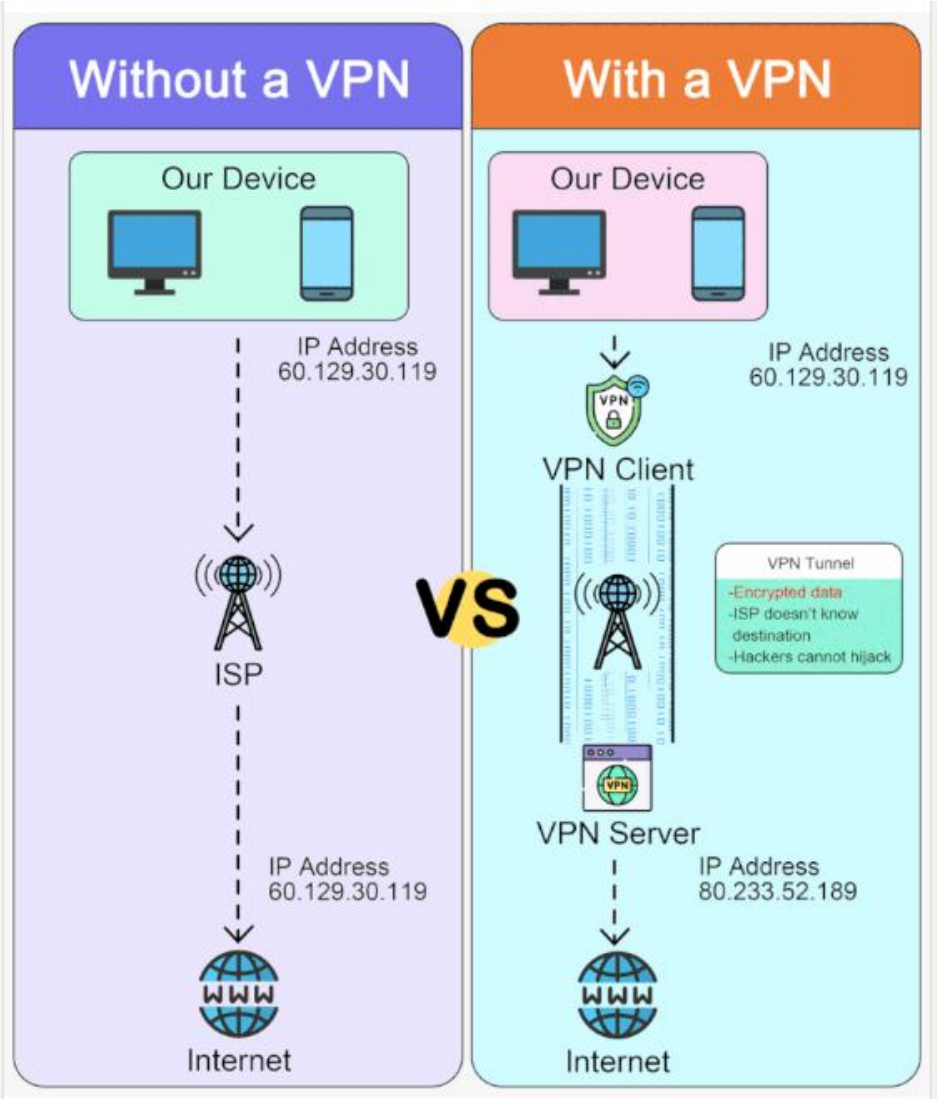
Een VPN versleutelt alle gegevens die jij verzendt of invult. Bijvoorbeeld je creditcardgegevens bij een aankoop, je BSN bij een inschrijving en je inloggegevens voor een bepaald account. Deze zijn dan onleesbaar voor internetcriminelen.

Ben je anoniemer op internet

Een VPN verbergt je IP-adres en je locatie. Je IP-adres is een uniek adres dat terug te leiden is tot jouw computer (net zoals een mobiel nummer of je woonadres). Als je gebruikmaakt van een VPN neem je het IP-adres en locatie van de VPN-server aan

Waarom zou je een VPN gebruiken?

- Privacy: Je beschermt je persoonlijke gegevens tegen hackers, overheden en nieuwsgierige bedrijven.
- Veiligheid op openbare wifi: Op plekken zoals cafés en luchthavens is je verbinding beter beveiligd.
- Toegang tot geblokkeerde content: Je kunt websites en streamingdiensten bereiken die normaal gesproken in jouw land niet beschikbaar zijn.
- Anonimiteit: Je online gedrag is minder eenvoudig te herleiden tot jouw persoon of locatie.



Elke vorm van cybercrime is strafbaar. Denk aan hacking, DDos-aanvallen, ransomware, virussen, malware, internetoplichting, afpersing via e-mail, phishing.

Altijd aangifte doen

Ben je slachtoffer van cybercrime, zet je computer of ander apparaat niet uit en bewaar zoveel mogelijk informatie, want het kan bewijsmateriaal zijn en kan de politie helpen om de criminelen op te sporen. Maak bijvoorbeeld screenshots van berichten of meldingen van de cybercrime als dat mogelijk is.

Doe vervolgens direct aangifte en verwijder pas na de aangifte malware van je apparaat. Aangifte doen kan via 0900-8844 of op een politiebureau. Van een aantal vormen van cybercriminaliteit kunt u ook online aangifte doen.

Hoe vind ik de juiste Hulp voor mij ?

En waar

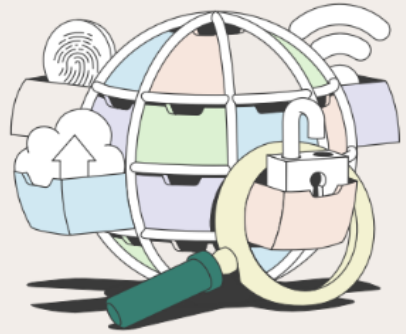
veiliginternetten.nl

alertonline.nl

Met Checkjelinkje® ga je veiliger online.

veiliginternetten.nl

Menu



Veilig internetten begint hier

Waar ben je naar op zoek? Wat is cryptojacking?

Aangifte | Accountdiefstal | AI | Alert online | Apps | Back-up | meer

Nieuws Nieuws

Cybercrime meldingen in juni #1

6 juni 2025

Nieuws Nieuws

Politie Noord-Nederland nu digitaal ter plaatse

6 juni 2025

Nieuws Nieuws

Politie haalt wereldwijd illegale netwerken offline om cybercriminaliteit te bestrijden

23 mei 2025

Nieuws Nieuws

Thuiswerkvacatures: nieuwe vorm van vacaturefraude

20 mei 2025

Nieuws Nieuws

Jongeren steeds vaker online geronseld voor criminele activiteiten

15 mei 2025

Nieuws Nieuws

Wat is een AI-hiring scam?

14 mei 2025

Nieuws Nieuws

Themamaand Online Seksueel Geweld

13 mei 2025

Nieuws Nieuws

EchtNietVandaag regio Rotterdam

13 mei 2025

Nieuws Nieuws

Oplichting met de aanvraag van je visum of ETA

30 april 2025

Nieuws Nieuws

Cyberbeeld april

30 april 2025

Nieuws Nieuws

Als je niet wilt dat Meta AI traint met jouw data, kan je bezwaar maken

Nieuws Nieuws

TikTok introduceert dashboard voor extra beveiliging

24 april 2025

Dagelijks gebruik Nieuws

Nieuws Nieuws

April is de maand van senioren en veiligheid

1 april 2025

Phishing Nieuws

Let op! Valse brief van DigiD

15 maart 2025

Social media Nieuws

Kogelvis emoji bij misleidende influencer-reclames

24 februari 2025

Digitaal opgroeien Nieuws

Kinderen aangehouden vanwege choking challenge

31 januari 2025

Nieuws Nieuws

Onderwijs- en onder-zoeksinstellingen doelwit van cyberaanvallen

17 januari 2025

Cyberbeeld maart 2025

8 april 2025

Digitaal opgroeien Nieuws

VodafoneZiggo lanceert platform om kinderen online veilig op te voeden

25 maart 2025

Cybercrime Nieuws

DDoS-aanval op DigiD

3 maart 2025

AI Nieuws

Sextortion door AI gegeneerde naaktfoto's

3 februari 2025

Malware Nieuws

Infostealer zorgde voor criminele hack bij TU Eindhoven

27 januari 2025

Nieuws Nieuws

Cyberbeeld december

15 januari 2025

Nieuws Nieuws

1 op de 5 jongeren wordt slachtoffer van valse webshops

27 maart 2025

Cybercrime Nieuws

Cyberbeeld februari 2025

12 maart 2025

Digitaal opgroeien Nieuws

11 februari is het Safer Internet Day

10 februari 2025

Accountdiefstal Nieuws

Politie haalt internationale criminele webshop offline

30 januari 2025

Nieuws Nieuws

Jongeren krijgen te maken met afpersing via Snapchat

22 januari 2025

Opgelicht?! waarschuwt met alerts op tv voor online oplichting

3 april 2025

Digitale veiligheid Nieuws

Vanaf vandaag heeft veiliginternetten.nl een nieuwe website

18 maart 2025

Cybercrime Nieuws

Cyberbeeld januari 2025

11 februari 2025

Cyberpesten Nieuws

(Online) pesten neemt toe op scholen

3 februari 2025

Social media Nieuws

Let op: klik niet op accounts die 'sexy' gifjes plaatsen in comments op Instagram

27 januari 2025

Nieuws Nieuws

Security technologie

Consultancy

Technical writer

Zijn er nog vragen ?