

Digitaalgids

● **Nephelpdesks**

De nieuwste trucs

● **Kantoorsoftware**

Kijk verder dan Microsoft

● **Slimmer appen**

WhatsApp en Signal



Digitale erfenis

Regel tijdig toegang voor je nabestaanden

Inhoud

Van de redactie

Adressenboekje

Mijn schoonmoeder had het slim bedacht: ze had de inlognamen en wachtwoorden van haar accounts genoteerd in zo'n adressenboekje dat vroeger bij veel mensen naast de telefoon lag. Bij de G stond het mailadres en wachtwoord voor Google, bij de M die van Microsoft, enzovoort. Maar toen ik haar hielp met het installeren van haar nieuwe laptop en die wachtwoorden moest invullen, bleek dat systeem toch niet helemaal waterdicht. Sommige wachtwoorden waren inmiddels alweer veranderd, een paar waren onleesbaar, sommige ontbraken helemaal. Toen ik vroeg of ze verder iets voor nabestaanden had geregeld, zei ze dat ze een bestandje had gemaakt op de computer. Alleen wist ze niet meer waar dat stond.

Dat wordt voor de nabestaanden (ons) te zijner tijd nog een puzzeltocht als we accounts willen opzeggen of toegang nodig hebben tot bepaalde bestanden. Wettelijk is er niks geregeld omtrent digitale nalatenschap. Elk bedrijf hanteert een eigen beleid, en bedrijven als Microsoft geven alleen toegang als ze door een rechter worden gedwongen. Gelukkig zijn er oplossingen om alles ordentlich achter te laten – lees ons dossier op pagina 29. Mijn favoriet: zet alle inloggegevens in een wachtwoordmanager met speciale noodtoegang voor het geval dat. Ik zal snel weer eens langsgaan.

Vincent van Amerongen

Hoofdredacteur



vvanamerongen@
consumentenbond.nl



10 Nieuwe nephelpdesks



QR-codes
► pag. 18



MacOS Spotlight
► pag. 38

Rubrieken

4 Enter

Digitale nieuwtjes en producten

8 Back-up

Updates over onze acties

22 Helpdesk

Digitale problemen opgelost

44 Tips & trucs

De beste tips en gratis software

Service

50 Jaarindex

Alle artikelen van 2025

50 Contact en colofon

Het team achter de Digitaalguides

51 Extra's

Online extra's voor abonnees



► Lees de DigitaalGids ook online via consumentenbond.nl/onlinelezen

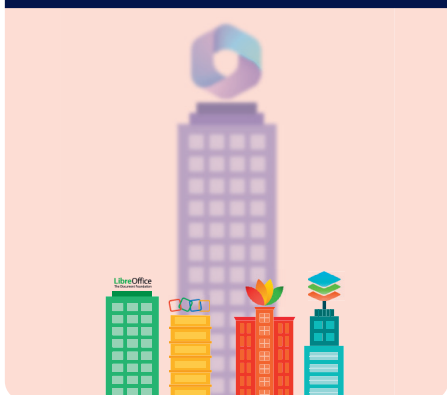
14 WhatsApp & Signal



26 Gehackt of niet?

Is mijn PC gehackt?

40 Kies een andere Office



Artikelen

10 Nieuwe nephelpdesks

Nu bankhelpdeskfraude beter wordt bestreden, bellen criminelen namens andere bedrijven. Doorzie hun trucs.

14 Tips voor chatapps

WhatsApp en Signal worden steeds verder uitgebreid met handige functies die de moeite waard zijn. Een overzicht.

18 Vragen over QR-codes

Op allerlei plekken open je websites met een QR-code. Hoe werkt dat precies? En wat zijn de risico's van zo'n gecamoufleerde weblink?

20 Hou je pc up-to-date

Helaas werkt niet alle Windows-software zichzelf automatisch bij. Gelukkig is er een tool om je apps bij de tijd te houden.

26 Laptop gehackt?

Veel mensen zijn bang voor een hack. Dat is lang niet altijd terecht. Herken de écht gevaarlijke signalen.

28 Een datalek, wat nu?

Steeds vaker komen datalekken aan het licht. Wat kun je doen als je gegevens zijn gelekt?

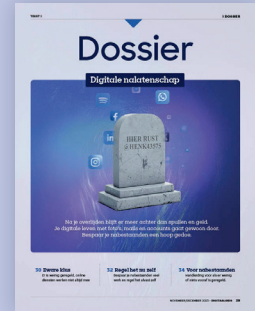
38 MacOS Spotlight

In het nieuwe macOS 26 is de Spotlight-zoekfunctie uitgebreid. Ontdek de nieuwe mogelijkheden.

40 Office-alternatieven

Microsoft Office is dé standaard als het gaat om kantoorsoftware. Maar er zijn goede gratis en privacyvriendelijke alternatieven.

29 Dossier



Digitale nalatenschap

Na je overlijden laat je ook veel digitale informatie achter: mails, foto's, bestanden. Bedenk tijdig wie waar toegang toe moet krijgen.

- 30 Inleiding
- 32 Wat je zelf kunt regelen
- 34 Gids voor nabestaanden

Eerlijk is eerlijk

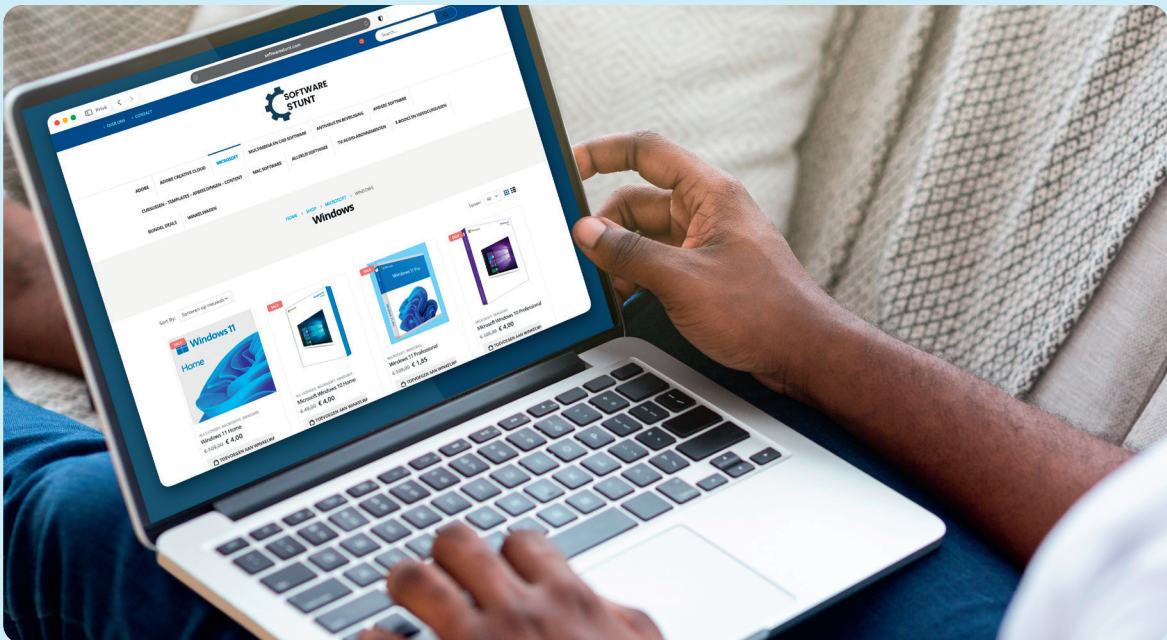
De Consumentenbond is er voor iedereen. Wij beschermen je tegen bedrijven die misleiden of misbruik maken van hun macht. Zo maken we de wereld een beetje eerlijker.

Wij maken geen winst, al onze inkomsten zetten we in voor ons werk voor consumenten. Zodat je de beste keuze kunt maken en krijgt waar je recht op hebt.

**Consumenten
bond**

Enter

Nieuwe producten en ontwikkelingen



Spotprijzen

Pas op voor foute softwaresites

Vrijwel dagelijks ontdekt de politie nieuwe online nepwinkels. Meestal zijn dat sites met kleding, maar onlangs zat daar een foute softwaresite tussen: softwarestunt.com. Je zou daar peperdure softwarepakketten van onder meer Microsoft en Adobe kunnen bestellen voor spotprijzen. Ook worden er laptops, telefoons en andere hardware aangeboden. De politie signaleert een handvol van dit soort softwaresites, allemaal van dezelfde persoon. Twee

andere sites van hem zijn licentiedeals.com en softwarebestellen.be. Op het moment van schrijven, half oktober, zijn deze drie sites nog in de lucht. Maar ook als ze verdwijnen moet je blijven opletten: er kunnen zo weer nieuwe opduiken. Ons advies is dan ook: pas extra op bij online software bestellen, zeker als de prijzen te mooi lijken om waar te zijn. Zoek altijd vooraf op internet naar reviews en ga op de site op zoek naar de contactgegevens.

Schild

Plan voor 'opgeschoond' internet

Het ministerie van Justitie en Veiligheid laat volgend jaar een advies uitbrengen over de landelijke invoering van een Anti Phishing Shield (APS). Dit internetfilter zou werken op elk apparaat in ieders thuisnetwerk en malafide sites automatisch kunnen blokkeren. Het werkt op basis van DNS, de standaardmethode om webadressen te koppelen aan IP-adressen. Bijna elke internetgebruiker surft via de DNS-server van zijn provider.



Door een kleine toevoeging kan dit knooppunt bij de internetgebruiker een waarschuwing tonen als de site die men wil bezoeken wordt ingezet voor phishing. KPN doet momenteel een test onder de noemer 'Veilig browsen'. Volgend jaar besluit het ministerie of een landelijke uitrol wenselijk is. Het doel is een structurele aanpak van phishing in Nederland. In België is al een vergelijkbaar internetfilter in gebruik.

Thundermail

Thunderbird breidt uit met webmail

Heel wat consumenten mailen met het gratis Thunderbird. De ontwikkelaars komen nu met een 'Pro'-versie. Met een agenda en een alternatief voor WeTransfer, maar ook met webmail met de naam 'Thundermail'. Hierbij wordt je adres jouwnaam@thundermail.com of jouwnaam@tb.pro, of je gebruikt een eigen domeinnaam. Het voordeel van webmail is dat je geen software hoeft te



installeren en dat je niet langer vast zit aan een mailadres van een provider. Dit vergemakkelijkt overstappen naar een andere provider. Het is nog even wachten op informatie over prijzen en beschikbaarheid. Je kunt bij Google en Microsoft al jaren een gratis webmailadres krijgen, maar daarbij betaal je met je gegevens. Meer informatie op blog.thunderbird.net.

Einde ondersteuning

Vervang Office 2016 en 2019

Op 14 oktober is Microsoft gestopt met het ondersteunen van Office 2016 en 2019. Deze programma's krijgen geen veiligheidsupdates meer. Je kunt ze blijven gebruiken, maar dat is onverstandig: ontdekte kwetsbaarheden worden niet meer

gerepareerd. Vervang de kantoorsoftware door Microsoft 365 (abonnement voor €99 per jaar) of Office 2024 (eenmalig €149). Of kies een goed gratis alternatief. Lees de Keuzehulp Office-software op pagina 40.

KORT

Word-docs gaan naar de cloud

Nieuwe Word-documenten worden voortaan automatisch in de cloud opgeslagen. Dat is standaard OneDrive. Zo zou je minder snel je werk verliezen. Maar het betekent ook meer afhankelijkheid van Microsofts diensten. Excel en PowerPoint volgen later dit jaar.

Nieuw: tab Aankopen in Gmail

Gmail krijgt er een tabblad bij: Aankopen. Hier komen alle berichten binnen over aankomende pakketten. Handig om je mail gescheiden te houden. De nieuwe tab staat in de telefoon- en de computer-app. Klik op de tab en schakel de functie in.

Betrouwbare telefoons

Gemiddeld gaat 8% van de telefoons binnen 3 jaar stuk. Toestellen van Apple, Google en Samsung zitten op dat gemiddelde. Betrouwbarder zijn die van OnePlus en Realme (3 à 4%). Het slechtst scoren Nokia, Huawei en Sony (12 à 13%). Dat blijkt uit een enquête van onze Britse collega's van Which?.

KORT

Firefox krijgt gratis VPN

Mozilla, de maker van Firefox, test het toevoegen van VPN aan de browser. Via een VPN-verbinding kun je vrijwel anoniem en veiliger internetten. Het is nog niet bekend wanneer de functie in Nederland verschijnt.

Stap af van Big Tech met Bitsoffreedom

Wil je weg bij de grote Amerikaanse techbedrijven als Meta, Google en Microsoft? De burgerrechtenorganisatie Bits of Freedom helpt je daar stap-voor-stap bij met de campagne 'Stap af van Big Tech'. Kijk op bitsoffreedom.nl/campaigns/stap-af-van-big-tech

Airbnb past instructies aan

Na onze publicatie in het vorige nummer over ID-verificaties (zie pagina 10) heeft Airbnb zijn instructies verbeterd. De site vraagt nog steeds om een ID-kopie, maar er staat nu bij dat je er 'Kopie bedoeld voor Airbnb' op moet schrijven.

Test

Hoe privé is je browser?

Websites en apps verzamelen gegevens van je, maar hoe ver gaat dat precies? De Amerikaanse Electronic Frontier Foundation (EFF) ontwikkelde daarom een gratis test op coveryourtracks.eff.org. Deze vertelt hoeveel informatie je browser prijsgeeft. Elke keer dat je een website bezoekt, laat je digitale kruimels achter: van schermresolutie tot lettertypen. Samen vormen die gegevens een unieke vingerafdruk waarmee adverteerders en andere partijen je kunnen volgen. Volgens de EFF kan dat leiden tot misbruik, zoals identiteitsdiefstal. Uit recente tests blijkt dat browsers als Chrome en Edge gemiddeld meer data verzamelen en sneller unieke profielen opleveren. Safari en Vivaldi doen het beter. Een waterdichte oplossing bestaat niet, maar gebruikers kunnen zich beter beschermen met privacyvriendelijke browsers, extensies als Privacy Badger en het gebruik van VPN of de incognito-modus.

Privacy

Deurbel moet buurvriendelijker

De Autoriteit Persoonsgegevens (AP) wil dat deurbelcamera's standaard privacyvriendelijk zijn ingesteld. Het is ondoenlijk om alle deurbellen te controleren en daarom wil de AP een preventieve aanpak. Fabrikanten moeten camera's zo instellen dat ze geen onnodige beelden van burens of de openbare ruimte maken. Verder wil de AP meer voorlichting geven over de regels. De groei van



het aantal deurbellen met camera verloopt explosief. De teller staat nu op circa 1,5 miljoen en het aantal klachten erover groeit navenant. Vorig jaar ontving de AP 370 klachten, halverwege 2025 stond de teller al boven de 300. Veel meldingen gaan over camera's die tuinen of voordeuren van burens

filmen. Zie consumentenbond.nl/privacydeurbellen.

WhatsApp

Criminelen kapen accounts

WhatsApp-gebruikers opgelet. Criminelen hebben een nieuwe truc om accounts over te nemen. Ze sturen een link naar een website waar je zogenaamd kunt stemmen op bijvoorbeeld je favoriete sporter. Als je klikt, word je doorgestuurd naar de website van de criminelen. Daar vragen ze om je telefoonnummer. Onschuldig? Nee. Met dat nummer vragen ze bij WhatsApp een verificatiecode aan om hun eigen compu-

ter aan jouw account te kunnen koppelen. De criminelen sturen de code naar jou en vragen je die in te voeren op je telefoon. Als je dit doet, kunnen ze bijvoorbeeld namens jou geld vragen aan je contacten. Zorg ervoor dat je wordt gewaarschuwd als er een vreemd apparaat wordt gekoppeld. Zet voor WhatsApp de meldingen aan. Ga in WhatsApp naar **Instellingen** en tik op **Apps > WhatsApp > Meldingen**.



Prijzen Digitaalguids 2026

Een jaarabonnement op de Digitaalguids stijgt in 2026 met €1 naar €41,50 voor leden en naar €45,50 voor niet-leden. Lees je de Digitaalguids online? Dan krijg je 20% korting. Je ontvangt de gids 6 keer per jaar.



AI

Nieuwe Meta-bril privacyrisico

Meta heeft een nieuwe AI-bril uitgebracht, de eerste die ook in Nederland te koop is. Voor €419 koop je een bril met ingebouwde camera en speakers waarmee je foto's en video's kunt maken, muziek kunt luisteren en telefoongesprekken kunt voeren. Je kunt ook vragen stellen over wat je ziet ('Meta, wat zie ik?'). Als je foto's of video's maakt, gaat een wit led-lampje aan om omstanders te waarschuwen. Dat lampje kun je eenvoudig afplakken. Vanwege stiekem filmen zijn er al concertzalen die bezoekers met een AI-bril weigeren. Wij vinden dat Meta met deze bril opnieuw de grenzen van de privacy opzoekt, en vinden dat de Autoriteit Persoonsgegevens moet onderzoeken of deze technologie voldoet aan de AVG.



Gemini

Zoeken met AI in Google

De zoekmachine van Google is opnieuw flink veranderd. In oktober is er een tabblad toegevoegd met de naam 'AI-modus'. Klik erop en je kunt in plaats van een gewone zoekopdracht intikken, complexe vragen stellen aan Googles AI-chatdienst Gemini. Zo kun je vragen welke tv de beste voor jou is en het antwoord in een tabel laten zetten. Je kunt ook afbeeldingen laten maken. AI-modus gaat hiermee veel verder dan de 'AI-overzichten' die eerder naast de zoekresultaten verschenen. Uit ons onderzoek bleek dat de kant-en-klaar antwoorden van AI-overzichten regelmatig rammelen. En net als bij de andere AI-chatbots moet je kritisch kijken naar de antwoorden van AI-modus. Zie het stukje op pagina 9.

macOS 26

Apple wordt 'vloeibaar'

Ook afgelopen september heeft Apple weer nieuwe versies uitgebracht van zijn besturingssystemen. Het bedrijf heeft de nummering gelijkgetrokken, waardoor iOS, iPadOS, watchOS, tvOS en macOS allemaal versienummer 26 hebben gekregen. Alle systemen krijgen een zogeheten vloeibaar glas-ontwerp: de knoppen en menu's worden half transparant met de laag eronder nog gedeeltelijk zichtbaar. Daar is al kritiek op gekomen: volgens sommige tests verbruikt 'liquid glass' 10% meer rekenkracht. Ook klagen sommige gebruikers over duizeligheid. In macOS 26 (Tahoe) is Spotlight flink uitgebreid, zie pagina 38. In iOS zitten verder geen grote aanpassingen. Handig is wel dat je een waarschuwing kunt krijgen als je telefonisch in een wachtrij staat en de klantenservicemedewerker gaat praten. En er zit nu een live vertaalfunctie in onder meer Berichten, Facetime en Telefoon – binnenkort ook in het Nederlands, volgens Apple.



6,9

is het gemiddelde cijfer dat de Nederlander zichzelf
geeft voor de omgang met online risico's

IPSOS I&O

Back-up

De Consumentenbond strijdt voor je rechten als consument.
Het laatste nieuws en lopende acties van onze belangenbehartigers.

Toch extra jaar gratis Windows 10-updates

Onder druk van consumentenorganisaties krijgen Europese consumenten met een Microsoft-account nog een jaar lang gratis Windows 10-updates. Dat is winst, maar blijft te kort.

Microsoft wilde op 14 oktober 2025 stoppen met de ondersteuning van Windows 10-computers, waardoor deze kwetsbaar zouden worden voor hackers. Computers gaan steeds langer mee en er zijn nog zeker 2 miljoen Nederlandse consumenten met goed werkende Windows 10-computers. Deze apparaten kunnen niet over op Windows 11 vanwege strengere hardware-eisen.

Tegen betaling van \$30 zouden consumenten nog een jaar extra veiligheidsupdates kunnen ontvangen. Na maatschappelijke druk konden consumenten die updates gratis krijgen, maar alleen in ruil voor het gebruik van bepaalde Microsoft-diensten.

Eind juli riep de Consumentenbond Microsoft op om Windows 10 gratis te ondersteunen zonder voorwaarden, en de harde grens van één jaar te laten vallen (zie de DigitaalGids van september).

Mog steeds te kort

Microsoft versoepelt nu de voorwaarde voor een jaar gratis updates: alleen een

Microsoft-account is nog nodig. Consumentenbond-directeur Sandra Molenaar: 'We zijn blij met deze stap, maar vinden een jaar nog steeds te kort. Daarna zijn er waarschijnlijk nog steeds veel goed werkende Windows 10-computers. Ook een Microsoft-account zou niet nodig moeten zijn'.

Bovendien kunnen zakelijke Windows 10-gebruikers tot 2028 updates ontvangen.

Dat is dus technisch gewoon mogelijk.

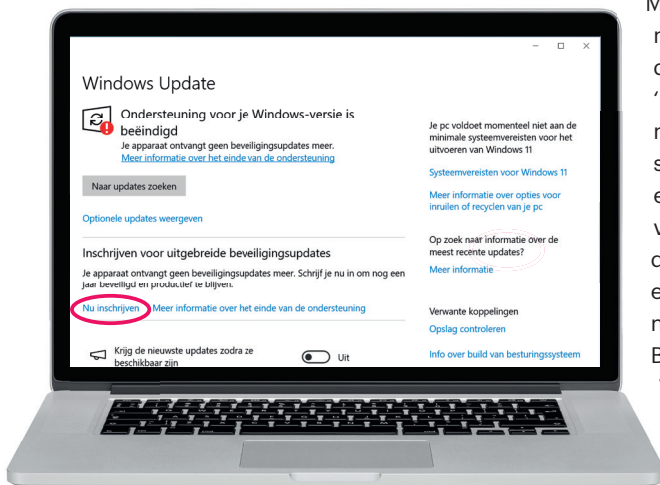
2.000.000

computers in Nederland met Windows 10 zijn ongeschikt voor Windows 11

Hoe krijg ik die extra updates?

Heb je een Windows 10-pc die ongeschikt is voor Windows 11? Dan moet je het extra jaar updates zelf aanzetten:

- 1 Ga naar **Start > Instellingen > Bijwerken en beveiliging > Windows Update**.
- 2 Klik onder de kop 'Ondersteuning voor Windows 10 eindigt in oktober 2025' op de link **Nu inschrijven**. Als je bij Windows bent aangemeld met een lokaal account, word je gevraagd je aan te melden bij je Microsoft-account.
- 3 Klik op **Volgende**.
- 4 Klik op **Registreren**.
- 5 Je ziet een bevestiging dat de inschrijving gelukt is. Klik op **Gereed**.



► Het scherm om je in te schrijven voor een jaar extra updates

Meta moet tijdlijn aanpassen

De rechtbank in Amsterdam heeft geoordeeld dat Meta, het moederbedrijf van Facebook en Instagram, gebruikers zelf moet kunnen laten bepalen welke inhoud hen wordt voorgeschoteld op hun tijdlijn. Volgens de Europese wet DSA moeten gebruikers op sociale media een tijdlijn kunnen kiezen die algoritmevrij is. Dat kan al wel, maar Meta heeft de optie verstopt en zet hem weer uit als je naar een ander deel van de app

gaat of de app herstart. Door de uitspraak van de rechter moet Meta hier nu mee stoppen.

De Consumentenbond steunde de rechtszaak die is aangespannen door Bits of Freedom, en is dan ook blij met de uitspraak. Het is ook een belangrijk signaal naar andere big tech-bedrijven dat ze Europese wetgeving moeten respecteren. Meta heeft laten weten in beroep te zullen gaan tegen de uitspraak.

Europese marktwet moet beter

Onze Europese koepelorganisatie BEUC vindt allereerst dat de Europese Commissie meer werk moet maken van een betere naleving van de Europese Digitale Market Act (DMA). Deze wet trad in 2023 in werking en is bedoeld om marktmacht en machtsmisbruik door 'poortwachters' tegen te gaan. Dat zijn de grote (vaak Amerikaanse) techbedrijven. De Europese consumentenorganisatie heeft verder een aantal aanbevelingen. Eén ervan

is dat ook clouddiensten en generatieve AI-diensten als ChatGPT onder de wet moeten gaan vallen. Die markten worden vaak door dezelfde bedrijven gedomineerd. Verder moeten gebruikers op hun apparaat kunnen kiezen voor een eigen clouddienst. Ook moet het verboden worden dat poortwachters hun eigen producten, zoals AI-diensten, bundelen met hun dominante platforms (zoals Meta doet met AI in WhatsApp).

Google's AI gaat vaak de mist in

Sinds dit jaar toont Google standaard AI-antwoorden boven de zoekresultaten. Deze 'AI-overzichten' blijken geregeld de plank mis te slaan. In onze test verschenen bij 70 van de 100 complexe zoekvragen AI-antwoorden. Daarvan waren er 20 onjuist of misleidend, vaak gebaseerd op commerciële bronnen. Ook zijn de antwoorden te stellig, ongenueanceerd of achterhaald. De AI-functie is niet uit te zetten. Dat vinden wij kwalijk, zeker

omdat veel antwoorden niet kloppen en het veel energie kost. We hebben Google gevraagd de AI-functie te kunnen laten uitzetten. Door de AI-resultaten vaak bovenaan te zetten, bevoordeelt Google zijn AI-overzicht boven andere zoekresultaten. Dit kan tot oneerlijke concurrentie leiden en dat is in strijd met de Digital Markets Act. We hebben dit aangekaart bij onze Europese koepelorganisatie. consumentenbond.nl/google-ai

Stop met ons AI opdringen

Sinds een paar maanden geeft de zoekmachine van Google AI-antwoorden. Ik vind het opmerkelijk dat je ze helemaal niet kunt uitschakelen, als je ze niet wilt. Er staan daarnaast ook nog aardig wat fouten in (zie het bericht onderaan deze pagina) en de AI-reacties kosten extra energie, water en zorgen voor meer CO₂-uitstoot.

Ook Facebook en Instagram gebruiken AI volop, al doen ze dit meer op de achtergrond bij het rangschikken van je tijdlijn. Die tijdlijn wordt al jaren persoonlijk (en verslavend) gemaakt met algoritmes en AI. Sinds 2023 zijn de onlineplatforms verplicht ons ook een algoritmevrije tijdlijn te bieden. Maar deze optie hebben Facebook en Instagram zo goed verstopt dat bijna niemand hem gebruikt of zelfs weet van het bestaan. Moederbedrijf Meta heeft ondertussen WhatsApp van een heel zichtbare AI-chatbot voorzien. Ook weer niet uit te schakelen.

Het opdringerige AI-aanbod is vooral in het belang van de platforms zelf. Nog meer opdringerigheid: veel platforms zijn bezig hun AI-modellen te verbeteren en melden botweg dat ze je persoonlijke klantgegevens gaan gebruiken voor het trainen van de AI. Je kunt je er wel voor uitschrijven, maar dat vergt dus een actie van jouw kant. Dat is niet netjes en gaat niet uit van eigen kracht: als hun AI zo geweldig is zouden we er zelf graag voor kiezen en hoef je het ons ook niet zo op te dringen.

Peter Kulche
Redacteur-
onderzoeker
Digitaal



Fraude

Nieuwe nephelpdesks



Nu banken helpdeskfraude beter bestrijden, bellen fraudeurs namens andere bedrijven, zoals webshops en telecomaanhouders. Het aantal meldingen stijgt snel. Bestrijding is lastig omdat de fraudeurs hun tactiek steeds aanpassen.

● Robert de Wit* werd begin dit jaar telefonisch opgelicht door iemand die zich voordeed als een medewerker van Vodafone. ‘De man vertelde dat ik mijn telefoonnummer en enkele andere gegevens opnieuw moest bevestigen via een speciale verificatieapp.’ De Wit was niet direct wantrouwend omdat hij klant is bij Vodafone. ‘Het gesprek verplaatste zich al snel naar WhatsApp. Daar gaf de man mij instructies terwijl ik die app installeerde. Om de verificatie af te ronden, moest ik inloggen bij mijn bank. Enige tijd later zag ik dat er in totaal €170 van mijn rekening was afgeboekt door meerdere betalingen aan webwinkels.’

De directe financiële schade was relatief gering, maar daarna volgde voor het slachtoffer nog veel gedoe. Op advies van de Fraudehelpdesk blokkeerde hij zijn bankrekening, vroeg een nieuwe bankpas en pincode aan en deed aangifte bij de politie. De Fraudehelpdesk verwees hem ook naar de klantenservice van Samsung om de telefoon te laten nakijken. Het slachtoffer had onder druk van de fraudeur allerlei handelingen op zijn toestel uitgevoerd, maar hij wist niet meer welke.

Meer fraudetelefoontjes

De Fraudehelpdesk krijgt steeds vaker meldingen over nephelpdesks. Het aantal gemelde fraudetelefoontjes steeg van ruim

5000 in de eerste helft van 2024 naar bijna 18.000 in dezelfde periode dit jaar. Ruim 3,5 keer zoveel. Ruim de helft (55%) van de fraudetelefoontjes komt van ‘helpdeskbellers’. De steeds actievare helpdeskfraudeurs maken steeds meer slachtoffers.

De aard van de helpdeskfraude verandert wel. Jarenlang deden fraudeurs of ze namens de bank belden. Die methode bestaat nog altijd, maar de schade erdoor loopt terug. De eerste 6 maanden van dit jaar meldden 92 slachtoffers in totaal €1,5 miljoen schade. In het voorjaar van 2024 verloren 177 personen nog €4,4 miljoen. Let wel: niet elke gedupeerde Nederlander meldt zich bij de Fraudehelpdesk, dus de schade moet flink hoger zijn. Maar de dalende trend is onmiskenbaar. De kans is groot dat het een positief effect is van de antifraudemaatregelen die de banken doorvoerden (en waar wij ons hard voor hebben gemaakt).

Daar staat tegenover dat het aantal registraties van niet-bancaire helpdeskfraude explodeert. Hierbij doen de criminelen zich bijvoorbeeld voor als een medewerker van Microsoft, een telecombedrijf, webwinkel Amazon of een handelsplatform voor cryptovaluta. Hierbij kan de schade per persoon meevallen maar ook bijzonder hoog zijn, bijvoorbeeld als cryptovaluta worden gestolen. De teller bij de Fraude-

helpdesk stond vorig jaar op €80.000 schade in de eerste zes maanden. In dezelfde periode dit jaar gaat het al om €2,2 miljoen. Ruim 27 keer zoveel.

Robot aan de lijn

Ook Tim van Boekelo* werd in juni slachtoffer van een bellende fraudeur. ‘Ik stond net te koken toen een telefoontje ►

Loop niet in de fuik

- Word je gebeld door een helpdesk, of op een andere manier benaderd, terwijl je daar zelf niet om hebt gevraagd? Hang dan direct op of negeer het bericht.
- Klik niet op een pop-up die waarschuwt dat contact met een helpdesk nodig is.
- Als je zelf contact wilt met een helpdesk, controleer dan of het telefoonnummer of e-mailadres klopt. Oplichters gebruiken valse websites, waarop ze zich voordoen als de helpdesk van een bekend bedrijf.

Signalen van fraude

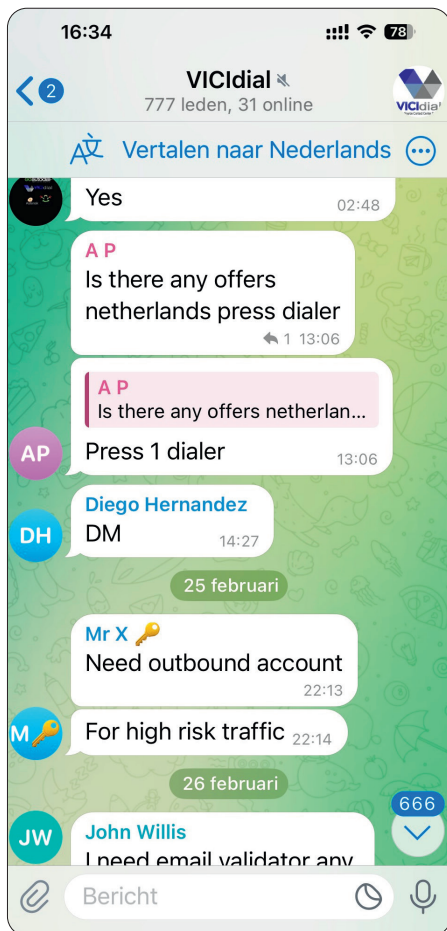
- Je wordt gebeld terwijl je daar zelf niet om hebt gevraagd. Medewerkers van een helpdesk bellen bijna nooit uit zichzelf. Als de bank dit wel doet: bel deze dan terug op het nummer dat de banksite of -app weergeeft.
- Een onbekende (helpdesk) vraagt je toegang te geven tot de computer.
- Je moet geld overmaken of persoonlijke gegevens geven.

Bron: fraudehelpdesk.nl

Helpdeskfraude

	2024 tot 1 juli	2025 tot 1 juli
Bancair (incl. PayPal)		
Aantal meldingen	1.381	4.570
Financieel gedupeerden	177	92
Schade totaal	€4.355.911	€1.504.192
Schade gemiddeld per persoon	€24.610	€16.350
Niet-bancair (incl. Bitvavo)		
Aantal meldingen	372	5.954
Financieel gedupeerden	16	117
Schade totaal	€80.159	€2.221.604
Schade gemiddeld per persoon	€5.010	€18.988

Bron: fraudehelpdesk.nl



Hulp nodig bij het telefonisch oplichten?
Op Telegram zitten experts voor je klaar

binnenkwam op mijn mobiel. Ik nam op en een Engelstalige robotstem zei dat er een bedrag was afgeschreven voor een aankoop bij Amazon. Als dit onterecht was moest hij een toets indrukken om een medewerker te spreken. Ik kreeg een man aan de lijn. Hij sprak keurig Engels maar wel met een Indiaas accent. De man bood aan mijn geld terug te boeken. Tijdens het gesprek moest ik allerlei acties uitvoeren op mijn telefoon, ik weet niet meer precies welke. Hij belde verschillende keren en zou de volgende ochtend terugbellen. Ik werd die ochtend echter gebeld door de échte fraudehelpdesk van ING. Ze hadden mijn creditcard geblokkeerd. Uiteindelijk waren er twee creditcardbetalingen gedaan en een bankoverschrijving naar een webshop waar je tegoedbonnen kunt kopen. Boeklo's schade bedroeg in totaal €1500.

Helpdeskfraude door de jaren heen

2011 – nu: techsupport-scam

Criminelen bellen consumenten zogenaamd namens Microsoft (of een ander tech-bedrijf) om te waarschuwen voor niet-bestaande computerproblemen. Ze halen slachtoffers over software te installeren of persoonlijke gegevens te geven, waardoor zij toegang krijgen tot de computer en bankgegevens. De fraude maakt vele honderden slachtoffers per jaar. De schade loopt in de miljoenen euro's.

2019 – nu: bankhelpdeskfraude

Oplichters bellen mensen namens hun bank. Bij deze fraude passen zij ook 'spoofing' toe: het telefoonnummer wordt vervalst, zodat het lijkt alsof de bank belt. Consumenten krijgen te horen dat hun rekening in gevaar is en dat geld 'veiliggesteld' moet worden. De schade schoot in coronajaar 2020 omhoog naar €26,7 miljoen. Vanaf 2022 sturen de bankhelpdeskbellers een 'collega' of zelfs een nepagent langs om de bankpas op te halen.

2024 – nu: fraude uit naam van meer partijen

Door diverse maatregelen van de banken is frauderen lastiger geworden. Opnieuw reageerden de fraudeurs. Zij bellen of sms'en namens andere autoriteiten, zelfs namens de Fraudehelpdesk. Ze wekken vertrouwen, bijvoorbeeld met een verhaal over een ongebruikelijke overboeking. Vervolgens proberen ze het slachtoffer over te halen een programma te installeren of ergens in te loggen. Als dat lukt kan de fraudeur meekijken en toegang krijgen tot de rekening van het slachtoffer. Fraudeurs bellen ook namens webwinkels en telecombedrijven. Veel mensen krijgen berichten over problemen met hun cryptorekening, met soms enkele tonnen aan schade tot gevolg.

Wie zitten achter de diverse vormen van helpdeskfraude? Het gaat bijna altijd om groepen criminelen in binnen- en buitenland die in wisselende samenstelling ope-

regelen (zoals ophalen van bankpassen of apparatuur) en de criminelen die het geld wegsluizen. Bij bankhelpdeskfraude gaat het regelmatig om Nederlandse verdachten. In een zaak in Noord-Holland speelden twee jonge mannen (21 en 22 jaar) een centrale rol als 'casher' (degene die geld opneemt) en tussenpersoon. Op rechtspraak.nl staan ruim 200 vergelijkbare zaken met Nederlandse verdachten.

De Engelssprekende helpdesks die uit naam van technologiebedrijven 'hulp' verlenen zitten vooral in het buitenland. In juli werd nog een groot crimineel callcenter opgerold in India. Dat had voor miljoenen schade veroorzaakt bij Europeanen door zich als een Microsoft-helpdesk voor te doen. Dit kordate optreden is een uitzondering. Het kost vaak veel tijd en moeite om lokale autoriteiten buiten Europa in

In juli werd nog een groot crimineel callcenter opgerold in India

regelen. De betrokkenen hebben uiteenlopende rollen: helpdeskmedewerkers die bellen, de mensen die fysieke onderdelen

beweging te krijgen. Dat merken de Europese politiediensten die tegen de groeiende stapel aangiften over helpdeskfraude zitten aan te kijken.

Voorkennis door datalekken

De bellende criminelen blijken steeds vaker voorkennis te hebben over persoonlijke gegevens, namen, bankrekeningen en recente transacties. Zij gebruiken die om vertrouwen te winnen. Vaak komt deze informatie uit phishing, datalekken of andere cyberinbreuken. Ouderen, mensen die minder digitaal vaardig zijn of sociaal geïsoleerd zijn worden vaker benaderd. Beide slachtoffers in dit artikel zijn 65-plussers en dat is geen toeval. De fraude is

vaak zo opgezet dat urgentie of angst wordt gebruikt om mensen snel beslissingen te laten nemen.

De fraudeurs gebruiken onder andere software om geautomatiseerd mensen te bellen of berichten te sturen, zoals ViciDial. Met dit programma op de computer kun je tientallen robottelefoontjes tegelijk uit laten gaan, inclusief de optie bij de ontvanger om op 1 te drukken om met een medewerker te spreken. Zo werken ze in een paar uur een lijst van duizenden telefoonnummers af. 'Helpdeskmedewerkers' van vlees en bloed zitten klaar om mensen op te lichten.

Het inrichten van een compleet telefoonsysteem met ViciDial vergt de nodige technische kennis. Maar we zagen dat er wereldwijd 'freelancers' zijn die je daar graag bij helpen. In de chat-app Telegram bieden zij hun diensten aan. Het is niet zeker dat alle opdrachtgevers criminele intenties hebben (niemand die dat hardop zegt) maar de openbare gesprekken wekken sterk die indruk. Alle personen communiceren onder pseudoniem.

We zagen een Telegram-oproep van iemand die specifiek met Nederlandse nummers wilde gaan bellen (zie afbeelding op pagina 12). Die kreeg dezelfde dag een reactie: 'DM mij' (stuur een direct bericht). Een andere Telegramgebruiker vroeg om telefoonlijsten met alleen oudere telefoonabonnees. Sommigen vragen specifiek een 'gespoofd' uitgaand telefoonnummer. Dan zien consumenten een aangepast telefoonnummer in hun telefoondisplay als ze worden gebeld. Bijvoorbeeld het nummer van hun bank of telecomprovider.

Wat is er tegen te doen?

Hoe de helpdeskfraude te bestrijden? Sinds enkele jaren is er een breed consortium van overheden en bedrijven dat werkt aan een integrale aanpak van fraude. De Consumentenbond neemt daar ook aan deel. We zijn voor een minder vrijblijvende deelname van de partners (zoals betaal- en telecombedrijven) en een betere informatie-uitwisseling. We willen dat financiële dienstverleners, telecombedrijven en advertentieplatforms de malafide partijen

Kwaadaardige pop-ups

Sommige gedupeerden leggen zelf per ongeluk contact met een helpdeskfraudeur. Ze zoeken op internet naar de klantenservice van Google, Microsoft of Windows en belanden op de webpagina van een valse helpdesk met een telefoonnummer. Malafide helpdesks kunnen ook spontaan, vanuit het niets, op het computerscherm komen. Zo'n kwaadaardige pop-up kan verschijnen als de pc besmet is met malware of als je een website bezoekt met een malafide advertentie.

beter tegenhouden en sneller van hun systemen weren. En we spreken de bedrijven aan die daarin achterblijven.

Blijf ondertussen ook zelf waakzaam. Vuistregel: bellen of sms'en organisaties spontaan over een probleem? Negeer dit. Het is bijna altijd een scam. Ben je toch onzeker geworden door het belletje of berichtje, bel dan zelf met het nummer van de genoemde organisatie dat je kunt vinden op de officiële website en doe navraag. Lees meer tips in het kader 'Zo loop je niet in de fuik'.

*) Omwille van hun privacy publiceren we niet de echte namen van de verschillende fraudeslachtoffers. De quotes in dit artikel komen uit door Fraudehelpdesk geregistreerde gesprekken met gedupeerden.

Meer lezen

Lees over (telefonische) oplichting en hoe je soms je geld kunt terugvorderen: consumentenbond.nl/veilig-internetten



Het tweede sms'je over een inlog in Spanje kwam niet van ING, het telefoonnummer is van een criminele helpdesk. Extra gevaarlijk: het bericht erboven kwam wél van ING!

Digitaal blijblijven?

In de Digitaalgids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding

