

BEWAAR
GIDS

BEWUST ONLINE

Van chatten met een robot tot veilig online gaan en je digitale erfenis op orde hebben. Deze bewaargids staat boordevol informatie over een bewust leven online. Om te lezen, leren én te bewaren.



**GELUKSPSYCHOLOOG
JOSJE SMEETS**

'Zeg niet: jeetje, wat dom!
Online fraude kan iedereen overkomen'



3 GENERATIES

'Zowel met mijn moeder als mijn dochter heb ik gesprekken over online veiligheid en digitale fraude'



JANNY VAN DER HEIJDEN

'Mijn foto's zijn gewoon van internet geplukt. Je zou denken dat je daartegen kunt optreden, maar nee'

Wat jullie van de digitale wereld vinden



“Ik heb wel duizenden foto’s in mijn telefoon staan. Geen idee wat daarmee gebeurt als ik er niet meer ben”

Mildred (64)

“Mijn kleinkinderen spelen bijna nooit meer buiten. Maar ze leren wel sneller Engels”

Yvonne (58)

“Laatst kreeg ik een raar mailtje van mijn bank. Ik vertrouwde het niet en heb de bank gebeld. Bleek het phishing te zijn”

Ingrid (48)

“Ik klik nergens op maar bel meteen mijn dochter!”

Tineke (67)

“We zouden worden afgeluisterd via smart apparaten in huis of via je telefoon. Ik neem het maar met een korreltje zout, je doet er toch niks tegen”

Fatima (45)

“Eigenlijk gebruik ik AI alleen maar als veredelde zoekmachine. Ik zou best willen weten wat je er nog meer mee kunt”

Chantal (54)

“Alle nieuwe communicatiemiddelen gaan mijn pet te boven. Maar appen en beeldbellen vind ik wel heel fijn”

Astrid (72)



Tech-expert

VIVIANNE BENDERMACHER

EEN GORILLA MET EEN BASEBALLJASJE

*Love it or hate it, maar de digitale revolutie is niet te stoppen.
Tech-expert Vivianne Bendermacher over de voor- en nadelen ervan.*

“Wat wil je voor plaatje op je verjaardagsuitnodiging, Merle?” vroeg ik mijn dochter vlak voordat ze zeven werd. Ze dacht even na en zei toen stellig: “Een gorilla met een baseballjasje en een unicorn met een bikini en een tutu op een springkussen!” Welja. Ik dacht dat dat wel te veel gevraagd zou zijn voor de door een slim computerprogramma aangedreven plaatjesgenerator. Maar niets was minder waar... Ik tikte de omschrijving van mijn dochter in en na een paar seconden had ik een plaatje dat exact vertolkte wat mijn dochter in haar hoofd had. Ik was verbijsterd. Merle haalde haar schouders op.

Terwijl mijn generatie nog wikt en weegt over wat we wel en vooral niet moeten willen met zoiets als artificiële intelligentie (AI), groeit de generatie van mijn dochter er in vanzelfsprekendheid mee op. De mogelijkheden zijn eindeloos! De risico's ook. Want: wat vreselijk dat criminelen de stem van ons (klein)kind kunnen namaken om ons ermee te bellen met een of ander paniekverhaal. Het wordt knap lastig nep van echt te onderscheiden. En wat een uitdaging voor docenten dat leerlingen hun verslagen stiekem kunnen laten schrijven door AI-chatprogramma's.



‘Na een paar seconden had ik een plaatje dat exact vertolkte wat mijn dochter in haar hoofd had’

accepteren dat AI er is en niet meer weggaat. Stap 2 ligt voor je. Dat is deze bewaargids waarin je alles leest over nieuwe digitale technologie. Onder meer dat we zelf AI gebruiken zonder dat we het merken, hoe je online oplichters herkent en wat termen als tweestapsverificatie en algoritme betekenen. En dan is er nog stap 3. Een verjaardagsuitnodiging voor mijn jongste dochter. Een parse dinosaurus met een unicormpakje aan, likkend aan een ijsje... Gelukt!

Veel leesplezier met deze bewaargids. Pak hem er vooral nog eens bij als alle digitale ontwikkelingen je blijven verrassen.

Vivianne Bendermacher is tech-expert en spreker en voormalig hoofdredacteur van het wetenschaps- en technologieblad Kijk. Ook was ze oprichter van het platform Techionista, dat vrouwen inspireerde en opleidde in technologie en digitale vaardigheden, met als doel de genderkloof in de tech-industrie te verkleinen.



Artificiële intelligentie is een vloek én een zegen. Het is aan ons hoe we ermee om willen gaan'

DIGITAAL BEWUST DOOR DE GENERATIES HEEN

‘IK DENK DAT IK
ZELF
heel
gezond
OMGA MET
ALLES’

*Anita Vlaar (50) heeft alle digitale ontwikkelingen vanaf haar achttiende bewust meegemaakt. Moeder **Janny** (75) is nog van de zittend-bellen-generatie, terwijl dochter **Liva** (16) tot de eerste lichting peuters behoort die opgroeide met filmpjes kijken op de tablet.*

Anita: “Ongelofelijk hoe snel de digitalisering is gegaan. De werkstukken voor het behalen van mijn havodiploma heb ik nog uitgetikt op een typemachine. Mijn ouders stonden altijd open voor nieuwe ontwikkelingen, dus toen de eerste computers kwamen, hadden we er vrij snel een. Een IBM MS-DOS, zo’n enorm grote bak met een zwart scherm en groene letters. Alleen was er toen nog geen internet, dus je kon er alleen spelletjes op spelen of op tekstverwerken. Dat vond ik nog niet zo interessant.”

VAN BELLEN TOT MAILEN

Anita: “Bellen met vriendinnen deed ik in mijn tienerjaren nog met een ‘ouderwetse’ telefoon, op de trap. Later had ik een buzzer, waarmee je elkaar korte berichtjes kon sturen. Dat vond ik al heel cool. Toen ik studeerde, kocht ik mijn eerste mobieltje; dat vond ik direct leuk, want het maakte mijn wereld zoveel groter. Na mijn studie ging ik werken in de media, waardoor ik bijna automatisch met alle digitale ontwikkelingen meega. Van mailen en bestanden versturen via WeTransfer tot met z’n allen werken aan een project in Google Drive en het sinds corona ingeburgerde vergaderen via Teams. Ik houd van mooi beeld, daarom ben ik zowel voor werk als privé fan van socialemediaplatforms als Pinterest en Instagram. Liva kent niet anders dan deze digiwereld. Ik weet nog dat ik van haar aan het

Van links naar rechts: Anita, Janny en Liva.



bevallen was en haar vader voor het eerst zo’n grote dikke iPhone uit Amerika had. ‘Kijk, ik kan ermee mailen’, zei hij enthousiast. Ik dacht: zullen we eerst dit kind even op de wereld zetten, haha. Tijdens Liva’s geboorte is het eerste mailtje met die telefoon verstuurd. Zij is van de eerste generatie peuters die een filmpje op de iPad mocht kijken. Door haar en mijn tweeling van elf jaar, Jacob en Josephine, krijg ik mee waar de jongere generatie zich mee bezighoudt. TikTok en Snapchat zijn het helemaal, maar daar heb ik zelf niet zo veel mee. Wat betreft ChatGPT ben ik sceptisch. Liva laat geschreven teksten door dit AI-programma nakijken op spelfouten. Best slim. Het is natuurlijk wel een eerste stap naar een heel werkstuk

ANITA

‘Mijn eerste mobieltje vond ik direct leuk, want het maakte mijn wereld zoveel groter’



door AI laten maken. Ik ben benieuwd hoe dit zich ontwikkelt de komende jaren. Zelf zie ik het altijd als een artikel door ChatGPT is geschreven. Ik schrijf het ook sneller zelf dan dat ik vijf keer een opdracht daarvoor moet invoeren in een computerprogramma. Laatst had Liva een debat en dan haalt ze daarvoor de basis uit ChatGPT. Dat vind ik dan weer heel slim. Het gaat erom hoe je ermee omgaat, natuurlijk. Al vind ik het lastig bepalen waar de grens ligt.”

NIEUWE COMMUNICATIE

Liva: “Wij hadden altijd de nieuwste apparaten in huis, omdat mijn vader daar erg van houdt. Dat mijn moeder Instagram gebruikt, vinden mijn vriendinnen maar raar. Hun moeders gebruiken Facebook of niets. Mijn moeder stuurt me soms twintig video’s per week via Instagram: van wijze lessen en hoe je handig huiswerk maakt tot grappige filmpjes. Bellen en appen doen mijn vrienden en ik trouwens nooit, we chatten via Snapchat.”

Janny: “Die nieuwe manier van communiceren, daar snap ik niets van. Ik kreeg van Anita mijn eerste mobieltje op mijn 51ste. Ik heb het lang afgehouden. Iedereen die je overal kan bereiken, dat ik niet even rustig met mijn hondje kon wandelen zonder dat ze me ‘lastigvielen’... Maar ik moet zeggen: het is toch erg handig!”



JANNY

‘Eerst vond ik het maar niets om altijd bereikbaar te zijn. Nu vind ik zo’n mobieltje toch erg handig’

ANITA

‘Tijdens het eten wil ik niet dat er een telefoon op tafel ligt, dan gaan ze allemaal in een grote schaal’

Anita: “Mijn moeder heeft elke dag een belronde, dat vind ik zo schattig. Dan gaat ze echt zitten om te bellen. Nu heeft ze van die ‘oortjes’ van mij gekregen, dus dan zou ze ook nog iets anders ernaast kunnen doen.”

Janny: “Nee, ik blijf aan tafel zitten.”

Anita: “Voor mijn moeder is bellen echt een activiteit. Voor mij is het iets wat ik erbij doe, als ik in de auto zit of opruim. Wel ben ik een echte beller. Soms schrikken mensen daarvan, vooral stagiairs op het werk of mijn kinderen. Die jongere generatie heeft echt belangst, zelf vind ik het juist heerlijk. Even bellen en dan is het binnen vijf minuten opgelost, in plaats van dat er drie mailtjes of appjes overheen gaan. Daar is de mobiele telefoon ook oorspronkelijk voor bedoeld. Ik wil sowieso niet afhankelijk worden van mijn telefoon. Om te betalen gebruik ik mijn pinpas en ik heb altijd contant geld bij me. En als ik naar een concert ga, wil ik ervan genieten. Dan ben ik liever in het moment, dan dat ik de hele tijd sta te filmen.”

MINDER VERBINDING

Anita: “Soms mis ik de zaterdagavonden uit mijn jeugd, samen voor de televisie. Dat was supergezellig en verbindend. Nu zit iedereen op zijn eigen apparaat in een andere ruimte. De een kijkt een serie of zit op YouTube, de ander chat met vrienden of luistert naar Spotify. Er is minder verbinding dan vroeger en door al die apparaten is er ook minder rust. Tijdens het eten wil ik niet dat er een

'We zullen samen moeten blijven leren'

"De verhalen van Anita, Liva en Janny illustreren heel mooi hoe we enerzijds op onze hoede zijn voor financiële onveiligheid en anderzijds genieten van het gemak dat online administratie ons brengt. Hoe we ervaren dat sociale verbinding zoals vroeger lastiger wordt, maar ook zien dat digitale technologieën nieuwe manieren van verbinding met zich meebrengen – zoals het sturen van filmpjes via sociale media. We voelen dat een versplinterde aandacht op de loer ligt en genieten ook van het kunnen multitasken. Deze ervaringen bestaan allemaal naast elkaar. Het is voor elke generatie belangrijk stil te

staan bij de 'digitale balans' en op welke manieren technologieën bijdragen of afbreuk doen aan onze mentale, sociale en fysieke gezondheid. Essentieel hiervoor zijn reflectie en open gesprekken, waarin we zonder schaamte obstakels of onzekerheden bespreekbaar moeten kunnen maken. De digitale wereld ontwikkelt zich zo snel dat we allemaal – zelfs *generation Alpha*, die ermee is opgegroeid – samen zullen moeten blijven leren hoe we met digitale technologie om willen gaan. Dat is dan meteen weer een mooie kans voor meer verbondenheid en wederzijds begrip."

Tips

- Zet niet overal een AI-tool voor in, zoals voor het schrijven van teksten. Dan ontnem je jezelf de kans vaardigheden te ontwikkelen en sterk te houden.
- Schermtijd zegt niet alles, het gaat vooral om wat je kind online ziet en doet, met wie, en waarom. Ga het gesprek daarover aan. Zo kun je inschatten op welke vlakken je kind misschien gevoelig is en meer ondersteuning nodig heeft.



Nastasia Griffioen is onderzoeker en coördinator van het Expertisecentrum Digitalisering en Welzijn bij het Trimbos-instituut. Als gedragswetenschapper promoveerde ze in 2022 aan de Radboud Universiteit op socialemediagebruik en jongerenwelzijn.

telefoon op tafel ligt, dan gaan ze allemaal in een grote schaal. Zo kunnen we even gezellig met elkaar de dag doornemen. Kinderen lezen bijna niet meer. Eigenlijk vind ik dat ze dat elke dag moeten doen voor hun ontwikkeling. Daarom heb ik vorig jaar verplicht een halfuurtje lezen na het eten ingesteld. We hebben dat een halfjaar volgehouden. Door de zomervakantie en ieders verschillende sporttijden kwam de klad erin. Jammer, want ik vond het heel gezellig dat we allemaal met een boek zaten. Qua schermtijd ben ik nooit zo streng geweest. De kinderen hebben voor de avond wel schermtijd met een code op hun telefoon. Om acht uur gaat-ie uit en dan kunnen ze niet meer appen tot zeven uur 's ochtends, behalve met mij. Voor Liva is de code er sinds een halfjaar af. Daar hebben we af en toe nog weleens discussie over, als ik

merk dat ze daardoor te laat naar bed gaat. Lastig, want hoeveel vrijheid en verantwoordelijkheid geef je en tot welke leeftijd? Ik ga maar een beetje op mijn gevoel af in combinatie met de cijfers op school en hoe ze uit hun ogen kijken, haha."

VERPLICHTE KOST

Liva: "Dat verplichte lezen vond ik niet zo heel tof. Mijn zusje wel, zij is een echte boekenwurm. Ik kan mijn mobiel steeds makkelijker wegleggen en dan gaan slapen, ik weet dat ik me dan de volgende dag beter voel. Als ik eerlijk ben: met huiswerk maken leidt mijn mobiel me soms wel erg af. Als ik voor een toets moet leren, vind ik het makkelijker om 'm weg te leggen dan als ik gewoon huiswerk te doen heb."

Anita: "Die verantwoordelijkheid over telefoongebruik tijdens het huiswerk maken laat ik bij haar, ook

LIVA

'Mijn moeder stuurt me soms twintig video's per week: van hoe je handig huiswerk maakt tot grappige filmpjes'



ANITA
 ‘Tegen mijn moeder heb ik gezegd: ik vraag nooit geld aan jou via de telefoon of de app’

omdat ze soms juist dingen op haar mobiel moet opzoeken. Wel check ik haar cijfers. Als ik daar een dip in zie, praten we erover en desnoods gaat er weer een slot op haar mobiel. Mijn eigen schermtijd houd ik niet echt bij, maar ik heb niet het idee dat ik daar heel erg van zou schrikken. Wel kan ik me soms een beetje verliezen in scrollen op Instagram voor het slapengaan. Tegenwoordig zet ik daarom de timer op een kwartiertje, dat helpt. Ook speel ik spelletjes op mijn telefoon. Ik heb sinds een paar maanden last van tinnitus. Door een potje Two Dots te spelen, een soort sudoku met kleurtjes en stipjes, ben ik geconcentreerd bezig en hoor ik die piep in mijn hoofd even niet.”

ONLINE VEILIGHEID

Anita: “Zowel met mijn kinderen als met mijn moeder heb ik gesprekken over online veiligheid en digitale fraude. Het profiel van mijn kinderen staat op privé en ik heb ze uitgelegd

dat online niet iedereen je vriend is. En dat je alleen online vrienden moet worden met mensen die je ook kent in het echte leven. Ook stuur ik geregeld artikelen die ik lees door aan Liva, zoals dat het chanteren via Snapchat vaak start met vragen of je foto’s van je voeten op wilt sturen. Wat dat betreft is het een lastige tijd.

Met zo’n telefoon voelt het alsof je ‘alleen op straat’ loopt, als het ware. Ook al lig je thuis veilig in je bed of op de bank. Er loert gewoon constant gevaar om de hoek. Op je telefoon kun je altijd opgelicht of aangevallen worden. Dat vind ik er wel lastig aan.”

Liva: “In het verleden heb ik weleens jongens toegevoegd op social media die ik niet kende, maar dat doe ik niet meer. Je weet gewoon niet met wie je praat, het kan ook een oudere man zijn. Ook krijg je foto’s die je niet wilt hebben, dat gebeurt heel veel, dus je moet ermee oppassen.”

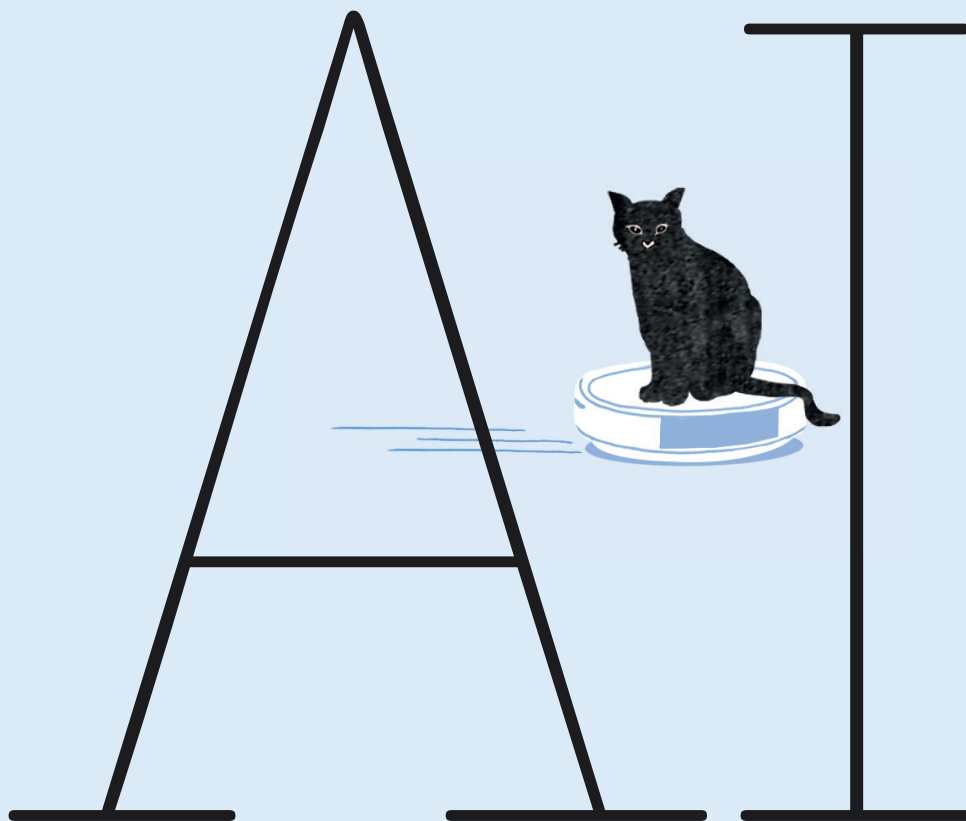
Anita: “Tegen mijn moeder heb ik gezegd: ‘Mam, ik vraag nooit geld aan jou via de telefoon of de app. Als ik geld nodig zou hebben, vraag ik het je persoonlijk.’ Ik heb haar ook gewaarschuwd voor phishing mails van onder andere banken en pakketbezorgers. Die zien er zo echt uit, dat ik zelf ook weleens twijfel. Maar jij bent daar heel scherp op, mam.”

Janny: “Ja, je hoort zo veel dat ouderen in die fraudepraktijken tuinen. Ik heb me voorgenomen dat dat mij niet gaat overkomen. Als ik twijfel aan mails of berichten, check ik het bij Anita. Dat heb ik ook als er mensen aan de deur staan aan wie ik twijfel. Dan zeg ik: ‘Ik bespreek het eerst even met mijn dochter’. Een tijd geleden kreeg ik een appje met: ‘Ik ben je dochter en ik heb geld nodig.’ Weet je wat ik terug-appte? ‘Dikke neus!’”

Anita: “Toen heb ik wel gezegd: ‘Mám, je moet niet reageren, maar zo iemand direct blokkeren!’ Je wilt fraudeurs zo min mogelijk input geven. Zo zie je maar: digitaal raken we nooit uitgeleerd.”

Verrassende plekken

WAAR JE



TEGENKOMT



Artificiële intelligentie (AI) klinkt misschien sciencefiction-achtig, maar stiekem speelt het al een heel grote rol in ons dagelijks leven. Loop maar eens een dag mee in het leven van de fictieve Liesbeth (53).



AI is superslim, maar heeft wel onze hulp nodig om te kunnen leren

START

Van de
dag van
Liesbeth

8:00

WAKKER WORDEN

Liesbeth wordt gewekt door een zacht muziekje. Ze vraagt haar wekker wat voor weer het vandaag wordt en hoort dat het de hele dag gaat regenen. Balen, want dat betekent files.



8:15

SLOW YOGA

Liesbeth is een beetje stijf wakker geworden. Ze tikt op haar tablet de zoektermen 'slow yoga' en '15 minuten' in. Ze kiest voor de bovenste yogales die ze als zoekresultaat voorgeschoteld krijgt om haar spieren los te maken. Daarna poetst ze tijdens een snelle douche haar tanden. Haar elektrische tandenborstel geeft aan dat ze haar achterste kiezen nog wat beter moet poetsen.

Wat is AI?

Artificiële intelligentie (AI) is overal en komt in veel verschillende vormen voor. Zelfs de wekker van Liesbeth maakt gebruik van AI. Dat zit hem in de stemherkenning én dat het systeem weet waar zij zich bevindt. Omdat het systeem ook weet wat voor weer het bij Liesbeth in de buurt is, kan het haar een actuele weersvoorspelling geven. Wat AI eigenlijk is? Simpel gezegd is artificial intelligence – ofwel kunstmatige intelligentie – een technologische ontwikkeling waarbij machines het menselijk leren nabootsen.



Hoe werkt AI?

Liesbeth maakt drie keer gebruik van artificiële intelligentie: de gezichtsherkenning op haar tablet, de zoekactie op internet én haar elektronische tandenborstel. AI is superslim, maar heeft wel hulp nodig om te leren. Van ons. AI leert namelijk doordat het 'gevoed' wordt met heel veel teksten, afbeeldingen, geluiden en andere soorten informatie. Neem Liesbeths elektrische tandenborstel. Nieuwe elektrische tandenborstels zijn vaak uitgerust met verschillende sensoren, zoals bewegings-, druk- en tijdsensoren. Als je daarvoor toestemming geeft als gebruiker van de tandenborstel, worden de data van die sensoren verzameld en geanalyseerd, net als die van miljoenen andere gebruikers over de hele wereld. AI kan in deze data vervolgens patronen ontdekken. Zoals hoe vaak iemand gemiddeld poetst en welke tanden daarbij vaak worden overgeslagen. Op basis van de analyse van al die gegevens herkent de tandenborstel ook het poetsgedrag van elke individuele gebruiker en geeft-ie diegene gerichte tips. In het geval van Liesbeth dat ze haar achterste tanden beter moet poetsen, omdat ze die vaak overslaat. Door te trainen en fouten te maken, wordt het systeem steeds nauwkeuriger. AI kan zichzelf namelijk aanpassen en verbeteren. Dat wordt het zelflerend vermogen van AI genoemd.



9:00

FILES ONTWIJKEN

Na Liesbeths dagelijkse koffieshot en ontbijt stapt ze in de auto. Omdat er door het slechte weer veel files staan, gebruikt ze haar navigatiesysteem om de snelste route naar het werk te vinden en files te omzeilen.



Persoonlijke assistent

AI kan je op vele manieren helpen. Liesbeth gebruikt een AI-programma bijvoorbeeld ter inspiratie en voor tekstsuggesties. Maar je kunt er ook compleet nieuwe teksten, afbeeldingen, muziek en video's mee maken. Of je kunt het gebruiken als je persoonlijke assistent. Bijvoorbeeld om bepaalde informatie voor je op te zoeken en overzichtelijk op een rijtje te zetten. Het is wel belangrijk om het nog handmatig aan te passen én te controleren. Want de door AI verkregen informatie is niet waterdicht, het kan nog fouten maken. Daarom is het dus goed dat Liesbeth altijd kritisch blijft.

Algoritmen

Ook navigatiesystemen gebruiken AI. Om Liesbeth zo snel mogelijk van haar huis naar haar werk te brengen, maakt het onder andere gebruik van wiskundige formules en regels. Die noemen we algoritmen. Zo heeft een navigatieapp een 'kortste-weg-algoritme' om je snel van A naar B te brengen. Algoritme klinkt misschien ingewikkeld, maar je gebruikt de hele dag door algoritmen om iets voor elkaar te krijgen. In feite is het gewoon een stappenplan. Wil je bijvoorbeeld een appeltaart bakken, dan ga je eerst naar de winkel om de ingrediënten te kopen. Daarna maak je thuis het deeg, je schilt de appels, verwarmt de oven voor, bereidt de appeltaart verder, zet hem in de oven, haalt hem er weer uit, laat hem afkoelen en smult er daarna lekker van. Dit is een algoritme: een patroon dat je volgt. Laat je één stap uit het patroon weg, dan klopt de uitkomst niet meer.

9:30

BRAINSTORMEN MET AI

Het is druk op het werk en Liesbeth heeft even niet zo veel inspiratie. Ze zoekt naar een creatieve titel voor het stuk dat ze aan het schrijven is en vraagt de AI-chatbot om tien verschillende titels ervoor te genereren.

Voorbeelden van zulke AI-programma's zijn Dall-E, ChatGPT en Midjourney. Ze kiest een van de voorgestelde titels uit en bewerkt die nog een beetje. Het artikel zelf haalt ze absoluut niet door de chatbot. Vanwege de persoonsgegevens en bedrijfsgevoelige informatie die zo wellicht op straat kunnen komen te liggen.

AI-programma's kunnen de ingevoerde informatie namelijk (her)gebruiken voor leerdoeleinden.



***Een algoritme is niets
meer dan gewoon
een stappenplan***



12:30

PAUZE

Pauze! Liesbeth eet haar lunch op achter haar laptop. Haar collega vraagt of ze zin heeft om in het weekend naar de tentoonstelling van een Turkse AI-kunstenaar in Rotterdam te gaan. Liesbeth zoekt zijn werk snel online op en is erg enthousiast.



AI-kunst

Steeds meer digitale kunstenaars gebruiken AI om nieuwe werken te creëren. Maar zijn deze werken wel zo nieuw? AI wordt immers getraind met data van onder meer kunstenaars, schrijvers en zangers. Momenteel is er een wereldwijde discussie over bij wie de rechten liggen van door AI gegenereerde kunstwerken.



Big Brother

Bekruipt je soms het gevoel dat je wordt afgeluisterd, omdat je opens overal online dat item ziet verschijnen waarop je eerder op internet hebt gezocht? Dit heet advertentie-targeting. Dit is mogelijk doordat bedrijven gebruikmaken van tracking-technologieën, die bijvoorbeeld cookies en pixels heten. Deze trackingtechnologie volgt jouw online gedrag en gebruikt gegevens zoals je zoekgeschiedenis, klikgedrag en locatie om je gerichte advertenties te laten zien die voor jou interessant (kunnen) zijn. Als je eerder hebt gezocht naar bepaalde reizen of vakanties, kan het algoritme dus advertenties laten zien die aansluiten bij jouw interesses. Ditzelfde geldt voor de film- en serie-suggesties die je streamingdienst je voorschotelt, omdat je vaak films of series in een bepaald genre (bijvoorbeeld comedy) kijkt.

12:45

VERZEKERING OMZETTEN

Liesbeth is gek op reizen en gaat het liefst zo vaak mogelijk weg. Ze denkt erover haar tijdelijke reisverzekering om te zetten naar een doorlopende. Kan dit tussentijds? Ze checkt de app van haar zorgverzekeraar waar ze ook haar reisverzekering bij heeft afgesloten, maar vindt de informatie niet zo snel terug. Dus stelt ze haar vraag via de chatfunctie in de app.



Chatbots

Steeds meer zorgverzekeraars, maar bijvoorbeeld ook internetproviders, banken en webwinkels, maken voor de chatfunctie op hun website of in hun app gebruik van AI. Dit gebeurt met zogeheten chatbots, een samentrekking van de woorden 'chat' en 'robot'. Als je bijvoorbeeld naar de

website van je zorgverzekeraar gaat, verschijnt er onderaan het scherm een pop-up met: "Hallo, ik ben XXX. Kan ik je ergens mee helpen?" Dit is geen echt persoon, maar vaak een AI-computer die 'getraind' is om vragen te beantwoorden en waarmee je 24 uur per dag kunt chatten. Zo kun je ook buiten kantooruren bij je verzekeraar terecht met vragen. De robot kan vrij snel simpele standaardvragen beantwoorden. Kom je er met de chatbot niet uit, dan word je – tijdens kantooruren – verbonden met een medewerker.

Chatten met je zorgverzekeraar? Grote kans dat dit met een chatbot is

15:30

TOE AAN VAKANTIE

Liesbeth zit in haar vierde vergadering van die dag. Ze is moe en begint weg te dromen... Ze is toe aan vakantie. Stiekem zoekt ze op internet naar een citytrip. Eerder deze week heeft ze als eens op Rome gezocht en nu krijgt ze stedentrips naar deze stad als advertenties bovenaan de pagina aangeboden.



**Spaar- en bonuskaarten
maken ook gebruik
van AI. Handig, maar ook
privacygevoelig**



18:45

SPAARKAART

Liesbeth stopt onderweg naar huis bij de supermarkt om geraspte kaas te halen voor de spaghetti die haar partner heeft gemaakt voor het avondeten. Ze haalt haar spaarkaart langs de kassa voor extra korting.

Korting op maat

Spaarkaarten van bedrijven waar je winkelt maken ook gebruik van AI. Winkels zetten het in om je gepersonaliseerde kortingen en promoties aan te bieden, te zien op welke momenten je winkelt en hoe vaak je de winkel bezoekt. In de hoop dat je daardoor natuurlijk meer winkelt bij deze specifieke winkel(s). Dat kan handig zijn voor je, omdat je zo echt kortingen en aanbiedingen op maat ontvangt. Alleen moet je je wel realiseren dat je hiervoor een deel van je privacy inlevert.



19:30

SLIMME APPARATEN

Liesbeth is eindelijk thuis na een vermoeiende dag. Haar robotstofzuiger heeft zijn werk in de woonkamer gedaan. Ze belt met haar moeder om te kijken hoe het met haar gaat. Haar moeder heeft last van ouderdomskwalen, maar wil nog niet naar een verzorgingshuis. Er komt gelukkig regelmatig een thuiszorgmedewerker langs. Liesbeth bedenkt manieren om het huishouden zo makkelijk mogelijk te maken voor de thuiszorgmedewerker, zodat die meer tijd heeft voor haar moeder. Zal ze haar moeder zo'n handige robotstofzuiger cadeau geven? Daar heeft de thuiszorgmedewerker dan ook profijt van.



**Robots in ons
dagelijks leven**

In 2002 kwam de eerste robotstofzuiger op de markt. Er komen steeds meer handige zogeheten robotica bij: AI-aangestuurde huishoudapparaten om ons leven makkelijker te maken. Zo is er zelfs een dweilrobot. Verwacht wordt dat er in zorginstellingen in de toekomst steeds meer gebruikgemaakt zal worden van zorgrobots. Zo kunnen servicebots deuren openen, opruimen, afstoffen, koffie- of thee-zetten en helpen met medicijngebruik. Ook zijn er sociale robots die worden ingezet bij zieke kinderen, mensen met dementie of eenzame ouderen. Op kleine schaal gebeurt dit nu al. Zo worden in Japan robotdieren ingezet om de eenzaamheid onder ouderen te bestrijden.

Zelf blijven nadenken!

AI kan razendsnel patronen ontdekken. Doordat artsen door AI worden ondersteund, kan bijvoorbeeld twee keer zo snel borstkanker geconstateerd worden. Dat is natuurlijk heel mooi. Maar het risico bestaat dat we te veel vertrouwen gaan hebben in computersystemen en de uitkomst ervan automatisch

overnemen zonder zelf kritisch na te blijven denken. AI voedt zich met data die wij erin stoppen, speurt het internet af, vergelijkt gegevens en komt op basis daarvan met de meest logische oplossingen. Maar die zijn niet waterdicht, AI-systemen kunnen ook fouten maken. Dat is niet zo erg als je daardoor een keer een

film krijgt voorgeschoteld waar je niet op zit te wachten, maar wel als de uitkomst een grote impact heeft op je leven. Denk aan een verkeerde aanbeveling bij een sollicitatie van je zoon of dochter. Geniet en leer daarom van alle mogelijkheden die AI biedt, maar blijf ook altijd zelf kritisch nadenken.

Poeh, Liesbeth is echt toe aan vakantie, dat weet zelfs haar streamingdienst!

20:00

STREAMINGDIENST

Met het bord op schoot zet Liesbeth een streamingdienst op de tv aan, waar ze een documentaire over Italië krijgt aangeraden. Poeh, ze is echt toe aan vakantie, dat weet zelfs haar streamingdienst! Ondertussen checkt Liesbeth nog even haar socialmedia-account.

Na een halfuur verdwaald te zijn in kattenfilmpjes en de beslommeringen van haar vrienden en kennissen, merkt ze dat ze amper wat heeft meegekregen van de documentaire.



Schermtijd

Het gevaar van social media schuilt hem in het feit dat je net als Liesbeth verdwaald kunt raken in een bubbel van kattenfilmpjes. Je kijkt een keer naar zo'n filmpje, het systeem denkt dat je dit leuk vindt en dus krijg je er meer, en meer, en meer. Dankzij deze gepersonaliseerde algoritmes weten sociale media namelijk precies hoe ze je aandacht vast kunnen houden en ben je zo weer een halfuur aan het scrollen. Wees je hiervan bewust en laat je niet te veel meeslepen in de fuik. Stel een max aan je schermtijd, eventueel met behulp van een timerfunctie op je tablet of smartphone, en leg daarna je telefoon weg.

22:30

BEDTIJD

Om haar schermtijd voor het slapengaan te beperken, leest Liesbeth sinds kort elke avond even wat in een boek in bed. Zo valt ze rustiger in slaap. Deze nacht droomt ze over een nieuwe carrière. Liesbeth is uitgekeken op haar baan, ze overweegt een carrièreswitch. Ze denkt erover om voor zichzelf te beginnen. Hoe zou de wereld met AI er straks uitzien? En hoe ziet de arbeidsmarkt er straks uit met AI? Misschien komen er wel heel nieuwe banen bij! Met deze vragen in haar hoofd droomt Liesbeth verder.

EINDE

Van de dag van Liesbeth

MEER WETEN?

Volg de gratis Nationale AI-Cursus via ai-cursus.nl



Tv-presentatrice

JANNY VAN DER HEIJDEN

HELP, MIJN GEZICHT EN IDENTITEIT ZIJN GESTOLEN

Wat als je gezicht én goede naam worden gebruikt voor illegale advertenties? Janny van der Heijden kan er helaas over meepraten.



“Janny, ben jij zo afgefallen?” “Maak jij reclame voor afslankpillen?” Ineens ontving ik allemaal berichtjes. Van bekenden, maar ook van mensen die me volgen op social media. Pas een dag later drong tot me door dat er iets goed mis was. Ik vroeg om screenshots en links, want zelf zag ik die advertenties nergens; kennelijk was ik geblokkeerd. Talloze advertenties kreeg ik binnen. Met zogenaamde vóór- en ná-foto’s van mij. Ik zou tien kilo in enkele weken zijn afgefallen. De ene keer met pillen, de andere keer met gummies.

“Neeee, dat ben ik niet. Zeker niet bestellen”, antwoordde ik als mensen me vroegen of die middelen echt zo goed werkten. Vrienden en kennissen rapporteerden de advertenties, maar ze bleven verschijnen. Het werden er zelfs meer. Maandenlang. En ineens was het voorbij. Wat de advertenties betreft. De schade was al aangericht. Honderden, misschien wel duizenden mensen hebben die rommel gekocht. “Ik dacht echt dat jij iets met die pillen te maken had, dat ze zouden werken”, zeiden ze. Dat doet pijn.

Mijn goede naam is aangetast, maar dat kwetsbare mensen hierin trapt en maakt me nog het meest boos en verdrietig. Ze vertrouwden mij en werden in de maling genomen.

FOTO'S VAN INTERNET

Mijn foto's zijn gewoon van internet geplukt. Je zou denken dat je daartegen kunt optreden, maar nee. Je kunt aantonen dat er illegaal reclame wordt gemaakt met jouw foto's en identiteit en dat er in jouw naam wordt geantwoord, maar je blijkt geen verhaal te kunnen halen bij platforms die zulke advertenties plaatsen. Die zijn compleet onbereikbaar en blijven zo lekker buiten schot. En de politie weet niet wat ze met

‘Mensen vertrouwden me en werden in de maling genomen. Dat doet me nog het meest verdriet’

dit soort criminaliteit aanmoet. Opstandig werd ik ervan. Ik hoorde verhalen van mensen wier foto's werden gebruikt om anderen mee op te lichten. Niet alleen maar BN'ers, maar gewone mensen die ineens via fake-accounts hun foto's en verkoopadvertenties op social media voorbij zagen komen. Ik kan oprecht zeggen dat het iets met me heeft gedaan, me wantrouwig heeft gemaakt. Mede door de podcastserie die ik erover maakte, heb ik gezien hoe makkelijk het is om iemand op te lichten. En om opgelicht te worden. Hoe stemmen kunnen worden nagebootst, hoe je aan de telefoon wordt gepusht direct te handelen. Als je je telefoonnummer achterlaat op een op het oog legale website, kan het worden gebruikt voor identiteitsfraude. Ik zou het wel van de daken willen schreeuwen: check, check en dubbelcheck al die (te) mooie aanbiedingen op social media en websites. Trap niet in mooie woorden en te 'snelle' bestelsites, maar zoek eerst online op of het wel klopt.

Janny (70) is culinair auteur, tv-maker en columnist voor Margriet. Ze heeft twee zonen, drie kleinkinderen en een teckel, Nhaan. In 2023 kreeg Janny te maken met identiteitsfraude. Samen met Jeroen Bos van Omroep MAX maakte ze er de vijfdeelige podcastserie Gestolen Gezicht over, te beluisteren in je favoriete podcast-app.



Te mooie aanbieding of smeeke-appje om geld?

TRAP ER NIET IN

Online criminelen verzinnen steeds weer nieuwe manieren om te frauderen. Dit zijn hun meest voorkomende trucs. Plus een plan van aanpak ertegen.

'Bij het nieuwe telefoonnummer stond gewoon de profielfoto van mijn dochter'

WHATSAPPFRAUDE

Caroline (70): "Hoi ma, door problemen met de provider heb ik een nieuw nummer.' Zo begon het appje dat ik twee jaar geleden dacht te ontvangen van mijn dochter. Ze had voor de volgende dag geld nodig om de btw aan de Belastingdienst te betalen, appte ze. En dat ze krap bij kas zat, het bijna niet durfde te vragen, maar dat ze het heel snel zou terugbetalen. Dit verbaasde me niets, want mijn dochter maakt nog weleens een potje van haar financiële zaken. Bij het nieuwe telefoonnummer stond gewoon haar profielfoto. We kletsten wat, ik maakte grapjes over dat ze echt eens minder moest winkelen en uitgaan. Ze zei dat ik de allerliefste moeder was, met veel hartjes-emoji's erbij. Natuurlijk wilde ik mijn dochter helpen, dus maakte ik bijna drieduizend euro over via een betaalverzoek.

De volgende dag kwam ik erachter dat ik in de maling was genomen. Ik voelde me zo stom. Hoe heb ik hier nou in kunnen trappen? Maar het zag er zó echt uit." WhatsAppfraude kan iedereen overkomen. Het is een van de meest voorkomende vormen van online oplichting. Online criminelen doen zich voor als een bekende – vaak een zoon of dochter. Meestal hebben ze geen andere manier van communiceren dan via WhatsApp.

..... Wat te doen

1

Maak géén geld over totdat je telefonisch contact hebt gehad. Bel ze op het nummer dat je van henzelf hebt. Zorg ervoor dat je zeker weet dat hij of zij de afzender van het appje is. Het best spreek je een codewoord of antwoord op een bepaalde vraag af met je kinderen en bekenden.

2

Heb je wel geld overgemaakt? Neem contact op met je bank en meld het op [fraudehulpdesk.nl](https://www.fraudehulpdesk.nl).

3

Doe aangifte bij de politie. Dat kan telefonisch en vaak ook online.

WEBWINKELFRAUDE

Maud (48): "Het is alweer een aantal jaar geleden, maar ik kan er nog steeds kwaad om worden. Ik wilde kaartjes voor een uitverkocht concert van U2 regelen voor mij en mijn partner. Op een online verkoopsite vond ik er twee. Wel wat duurder dan de originele prijs, maar niet schrikbarend. Ik was zo gebrand op die kaartjes dat ik de verkoper niet checkte. Ik had dus niet gezien dat hij helemaal geen account had dat al lang actief was op die verkoopsite. Via de app had ik contact met de verkoper, ik maakte het geld over en weg was-ie. De advertentie ging offline, het telefoonnummer werkte niet meer. En mijn kaartjes? Die heb ik nooit ontvangen." Webwinkel fraude komt ontzettend veel voor. De politie krijgt zelfs elke tien minuten een melding binnen van deze specifieke vorm van fraude. Om de websites zo echt mogelijk te laten lijken, gebruiken criminelen trucs en

'Via de app had ik contact met de verkoper. Ik maakte het geld over en weg was-ie'

valse zekerheden. Zoals logo's en namen van bekende partijen, nepkeurmerken en de mogelijkheid om te betalen via iDeal. Lijkt de aanbieding te mooi om waar te zijn – 'Alleen vandaag 60% korting!' – dan is-ie dat meestal ook.

**NU OF
NOOIT!**



..... Wat te doen

1

Kijk of de websitenaam klopt. Soms staat er bijvoorbeeld maar één lettertje anders dan bij een bekend of vertrouwd merk.

2

Lees de online reviews. Zoek echt naar gebruikerservaringen en filter de louter positieve (en soms nep-)reviews eruit.

3

Wil je iets kopen of verkopen op een online verkoopsite? Maak gebruik van kopersbescherming. De verkoper krijgt pas zijn geld nadat jij hebt aangegeven dat je het product daadwerkelijk hebt ontvangen, in goede staat.

4

Geld overgemaakt en nooit iets ontvangen? Meld het bij de Fraudehulpdesk en doe aangifte bij de politie.

'De mail zag er echt uit, helemaal in de huisstijl van mijn provider'

PHISHING

Farida (63): "Ik kreeg een mail van mijn internetprovider, dat er een dubbele betaling was gedaan. De mail was helemaal in de huisstijl. Natuurlijk wilde ik mijn geld terug, dus ik klikte op de button 'Terugbetaling aanvragen'. Op de volgende pagina vulde ik mijn e-mailadres, inloggegevens en geboortedatum in. Toen er twee dagen later geen geld op mijn rekening was bijgeschreven, belde ik mijn provider. De helpdesk-medewerker vertelde me dat ik te maken had met phishing. Internet-criminelen hadden mijn mailadres in handen gekregen. Door me vervolgens via de mail persoonlijke gegevens te ontfutselen, konden ze proberen in te loggen bij mijn andere online accounts, zoals mijn socialmedia-accounts. Mij werd aangeraden direct mijn inloggegevens en wachtwoord bij al mijn online accounts te veranderen. Ik schrok er ontzettend van en snapte het ook niet helemaal, dus heb ik mijn zoon gevraagd me te helpen. Hij draaide een antivirus-



programma op mijn computer en ik heb voor al mijn online accounts nieuwe, unieke wachtwoorden ingesteld. Gelukkig was ik er op tijd bij en is er bijvoorbeeld geen geld van mijn bankrekening gehaald. Ik ben nu superalert op gekke mails en appjes. En als ik het niet vertrouw, bel ik mijn zoon." Bij phishing word je via de mail of een bericht op je telefoon benaderd door iemand die zich voordoeft als een persoon, bedrijf of instantie. Uit de Veiligheidsmonitor van het CBS blijkt dat maar liefst twee op de drie Nederlanders in 2023 ten minste één keer een telefoontje, e-mail of ander bericht hebben ontvangen dat (waarschijnlijk) van een oplichter was.

..... Wat te doen

1

Kijk goed naar het taalgebruik, de aanhef en of het bericht in je spambox staat.

2

Je bank, internetprovider, creditcardmaatschappij of andere organisatie vraagt nóóit om je inlogcodes of wachtwoorden. Wordt daar wel om gevraagd, klik dan niet op een link in de e-mail, maar bel de betreffende instantie om te verifiëren of die jou deze mail heeft gestuurd.

3

Doet iemand zich aan de telefoon voor als medewerker van jouw bank die bijvoorbeeld zegt dat je rekening is geblokkeerd of je instellingen voor internetbankieren niet goed staan? Verbreek de verbinding en bel direct je bank. Geef nóóit toegang tot je persoonlijke gegevens en computer.

De cyberexpert

DIGITAAL BEZOEK?

WEES GOED VOORBEREID

Hoe wapen je je nu het best tegen online fraude én de gevolgen ervan? **Cyberexpert Rutger Leukfeldt** deelt drie belangrijke lessen over cybercrime met ons.



1 Iedereen kan slachtoffer worden
“Uit alle onderzoeken blijkt dat iedereen het risico loopt om slachtoffer te worden van cybercriminaliteit. Dat komt doordat digitale delicten veel en vaak gepleegd kunnen worden. Daardoor is het heel moeilijk je ertegen te wapenen. Er staat niet één keer een oplichter in levenden lijve bij je aan de voordeur. Maar er staan heel vaak, heel veel online criminelen aan je digitale deur te rammelen. De eerste paar keren herken je ze misschien. Maar heb je het druk of ben je gespannen, dan kun je zomaar slachtoffer worden omdat je even niet alert was. Je hoeft je echt niet schuldig te voelen als je erin bent getrap. Die oplichters zijn zó geraffineerd en slinks, ze verzinnen telkens weer wat nieuws om mensen geld afhandig te maken.”

‘Geef jezelf een time-out. Dat kan een hoop ellende voorkomen’

2 De impact van digitale fraude is heel groot
“Heel lang werd gedacht dat de impact van digitale delicten niet zo groot was, want ‘het gebeurt achter een beeldscherm’. Maar uit onderzoek blijkt dat het niet alleen financieel, maar ook emotioneel heel veel met mensen doet. De impact van een delict waarbij online en offline door elkaar lopen is nog groter. Stel, iemand krijgt je wachtwoord in handen en kan bij al je opgeslagen foto’s. Diegene gaat je vervolgens afpersen met foto’s van jou. Zelfs al wordt de dader gepakt, dan blijft dat beeldmateriaal voor altijd rondzwerfen op internet. Als je gaat daten of solliciteren, weet je dus nooit of die beelden weer opduiken. Daar is gelukkig steeds meer aandacht voor bij instanties zoals de overheid, de politie en Slachtofferhulp. Al gaat het nog niet altijd goed. Onderzoek ernaar staat nog in kinderschoenen en dat maakt het lastig er beleid op te maken.”

‘Voel je zeker niet schuldig als je er toch bent ingetrapt’

3 Wees gezond argwanend
“Veel slachtoffers zeggen: ergens voelde ik dat het niet helemaal pluis was. Vertrouw op dat gevoel en wees gezond argwanend. Zeker als mensen druk op je gaan uitoefenen of zeggen dat je nú direct moet beslissen. Dat is wat de criminelen willen: dat je hun verhaal wordt ingezogen en geen tijd meer hebt om na te denken. Als je bij de bank je limiet wilt verhogen om geld over te maken, duurt het vier uur voordat die nieuwe limiet ingaat. Geef jezelf ook zo’n time-out. Stop, luister naar je niet-pluis-gevoel. Geef jezelf de tijd om iets uit te zoeken. Dat kan een hoop ellende voorkomen.”



Rutger Leukfeldt is criminoloog en bijzonder hoogleraar cybercrime en victimologie.

Al sinds 2007 doet hij onderzoek naar cybercriminaliteit.

7X

ZO DOORZIE JE HET

Internetcriminelen gebruiken een aantal standaardmethoden om jou in de val te lokken. Bij deze situaties moeten alle alarmbellen afgaan. Vaak is er een oplichter aan het werk, dus check grondig of alles klopt.

1 Bekende in nood

Stuurt een bekende je een whatsappje of sms, maar met een vreemd telefoonnummer?

2 Inspelen op emoties

Wordt er een beroep gedaan op je vertrouwen, hulpvaardigheid, medelijden of onwetendheid?

3 Haast

Word je onder druk gezet om nú die gegevens te geven?

4 Noodgeval

Gaat het echt he-le-maal mis als je nú niet doet wat er wordt gezegd?

Wordt bijvoorbeeld je bankrekening geblokkeerd?

5 Nu of nooit

Geldt die superkorting echt alleen maar vandaag, toevallig?

6 Persoonlijk

Weet iemand iets heel persoonlijks van je? Weet je zeker dat diegene het niet gewoon op internet heeft gevonden?

7 Overdreven

Probeert iemand je vertrouwen te winnen door overdreven vriendelijk, netjes en behulpzaam te zijn?

Tips

Check de afzender

Twijfel je of een e-mail of appje wel echt van je bank of een goede vriend is? Controleer dan de afzender. Is dit wel het juiste e-mailadres of telefoonnummer van die persoon of dat bedrijf? Laat je niet opjagen. Twijfel je of een mailtje of appje nep of echt is? Neem dan gerust gratis contact op met de **Digihulplijn** via tel. **0800-1508** of via **digihulp.nl**. Zij kunnen je helpen bij het beoordelen of het oplichting betreft.

'Veel slachtoffers zeggen: ergens voelde ik dat het niet helemaal pluis was. Vertrouw daarop'

Opgelicht?

Ben je opgelicht of denk je dat je bent opgelicht? Meld dit dan bij Fraudehulpdesk, via **fraudehulpdesk.nl** of via tel. **088-7867372**. Doe ook altijd aangifte van online oplichting bij de politie via **0900-8844**. Van phishing en betaalverzoekfraude kun je ook online aangifte doen.

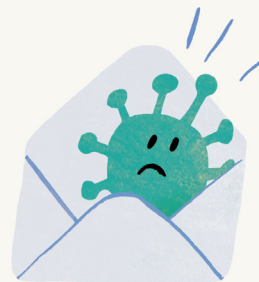
Digitaal je mannetje staan?

We doen steeds meer dingen online, maar hoe zorg je dat dit veilig en verantwoord gebeurt? Volg de **gratis** online cursus op **digitale-weerbaarheid.nl**.

Bescherm je privacy online

Wees voorzichtig met de persoonlijke gegevens die je online zet. En let op je instellingen op sociale media. Zo heb je de mogelijkheid om berichten en content af te schermen zodat alleen je vrienden die kunnen zien. Zet geen persoonlijke gegevens zoals je geboortedatum of adres openbaar online. Deel ze dus niet publiekelijk in een

bericht online dat iedereen kan lezen. Criminelen kunnen deze gegevens gebruiken als ze contact opnemen met een helpdesk. De controlevragen van helpdesks zijn namelijk vaak je geboortedatum, geboorteplaats en adres. Met deze gegevens kunnen criminelen bij helpdesks van bedrijven dingen laten aanpassen of veranderen.

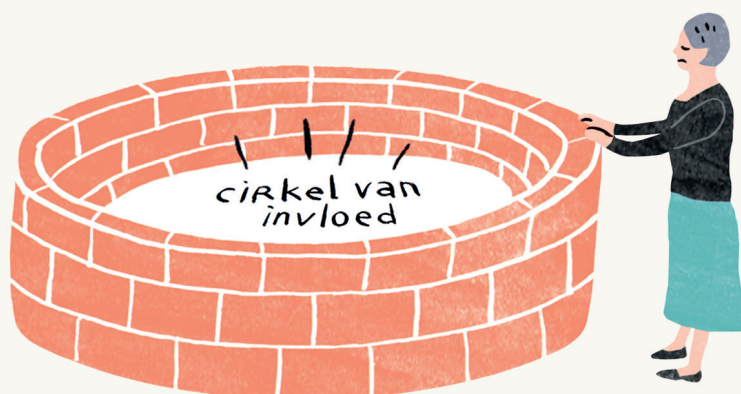


➔ *Meer weten over online veiligheid?*
veiliginternetten.nl

De geluksexpert

HOE NU VERDER?

PAK DE CONTROLE TERUG



Ben je online opgelicht? Dan kan het zijn dat je je daarna onzeker, boos of verdrietig voelt of je schaamt. **Gelukpsycholoog**

Josje Smeets vertelt hoe je daar het best mee om kunt gaan.

“Als je wordt opgelicht, is er niets meer wat je eraan kunt doen. Het kwaad is al geschied. Wat je wél kunt doen, is preventief aan de slag gaan voor de toekomst. Doe aangifte. Neem contact op met je bank en vraag hoe je dit had kunnen voorkomen. Beveilig je computer extra goed. Volg een cursus over online veiligheid. Heel belangrijke stappen om alles een plekje te geven en beter om te kunnen gaan met je emoties. Je pakt de controle terug. Daardoor voel je je fijner en is het makkelijker om het gebeurde los te laten. Wees daarnaast compassievol naar jezelf. Dit kan iedereen overkomen. Verwen jezelf met fijne dingen, mediteer of ga naar

yoga. Praat er ook over met mensen. Het liefst met mensen die er geen oordeel over hebben.”

Heeft iemand in je omgeving te maken gehad met online fraude?

“Het helpt niet als je tegen diegene zegt: ‘Jeetje, wat dom! Dit zou mij nooit overkomen.’ Houd je oordeel voor je als je het slachtoffer wilt helpen. Kom ook niet direct met

‘Zeg niet: ‘jeetje, wat dom! Dit zou mij nooit overkomen’

rationele oplossingen. Het is belangrijk dat je luistert naar de emotie. Dat je die herkent en bevestigt. Zeg iets als: ‘Ik kan me voorstellen dat je enorm schaamt en boos bent. Dat zou ik ook hebben.’ Een aantal weken later kun je vragen: ‘Wat zou je helpen om hier overheen te komen?’ Laat mensen altijd zelf denken over hun cirkel van invloed en welke stappen ze daarin kunnen nemen. Als ze zeggen dat ze geen idee hebben, kun je altijd voorzettes geven. Duw ze bijvoorbeeld voorzichtig in de richting van een cursus online veiligheid. Of wijs ze erop dat er bij veel bibliotheken digicafés zijn, waar ze met hun vragen over de digitale wereld terecht kunnen.”



Josje Smeets is gelukpsycholoog. Haar kennis over psychologie, geluk en het brein is volledig gebaseerd op wetenschappelijk onderzoek.

IS DIE ONLINE INFORMATIE WEL BETROUWBAAR?

ZO CHECK JE DAT IN 6 STAPPEN!

isdatechtzo.nl

1 Check je emotie

Wees extra kritisch als een bericht, foto of video een bepaalde emotie bij je oproept, bijvoorbeeld boosheid, verdriet of angst. Vooral in dit tijdperk van polarisatie ('wij tegen zij') komt het online veel voor dat anderen willen inspelen op je emotie. Zodat je bijvoorbeeld bang wordt voor of boos wordt op een bepaalde bevolkingsgroep. Check je onderbuikgevoelens én je eigen vooroordelen. Kijk ook wat andere onderzoeken of onafhankelijke mediabronnen erover zeggen. Bijvoorbeeld door in een zoekmachine de titel van het bericht, foto of video in te tikken met het woord 'factcheckers' erbij.

2 Check de bron

Wie is de afzender? Welk belang heeft diegene? Via de 'over ons'-pagina op een website kom je veel te weten over de bron van het nieuws. Of check het socialmedia-account waarvan het bericht afkomstig is. Deelt dit account vaker ongeloofwaardig nieuws uit een bepaalde (politieke) hoek? Bestaat de persoon wel echt of is het misschien een nepaccount?

Heb je een
hevige emotie bij een
bepaald bericht?
Wees dan extra
kritisch

3 Check de cijfers

Cijfers zijn we sneller geneigd te geloven. Alleen zitten ook achter cijfers mensen, die kiezen hoe ze iets meten. Let daarom op of de cijfers de werkelijkheid goed weergeven. Zo zegt een gemiddelde niet zoveel als de verschillen tussen de getallen erg groot zijn. En klinkt een toename van '10x zoveel' als heel veel, terwijl dit helemaal niet zoveel is als de kans bijvoorbeeld 0,03 was.

Desinformatie versus misinformatie

Bij desinformatie wordt doelbewust misleidende informatie verspreid omdat de afzender een eigen agenda heeft.

Bij misinformatie wordt valse of misleidende informatie verspreid zonder dat de afzender schadelijke bedoelingen heeft; diegene denkt dan dat de informatie waar is.

4 Check oorzaak en gevolg

Soms worden onderwerpen die niets met elkaar te maken hebben, aan elkaar verbonden. Bijvoorbeeld dat je je kind laat vaccineren tegen de mazelen en dat het daardoor autisme zou ontwikkelen. Stel jezelf dan deze vragen: kan het toeval zijn of zijn er misschien andere zaken die meespelen?

Controleer de
'over ons'-pagina om
te zien wie er achter
een website zit

5 Check dat beeld

Hoort die foto wel bij dat nieuwsbericht of komt-ie misschien ergens anders vandaan, een compleet andere oorlog misschien? Ook tricky: tegenwoordig worden veel beelden automatisch gegenereerd met artificiële intelligentie (AI). Alleen heeft AI nog moeite met details. Dus heeft iemand zes vingers of geen oorlel, dan kun je ervan uitgaan dat het geen echte foto is. Maar omdat AI zichzelf constant verbetert, komen dit soort fouten 'helaas' steeds minder voor. Het is dus heel belangrijk om zelf goed op te blijven letten. Zo is er sinds kort nieuwe Europese AI-wetgeving. Daarbij wordt het verplicht om AI-gegenereerde video's en foto's te watermerken. Ook aan de reacties van anderen onder een bericht op social media kun je soms al aflezen of een beeld (of bericht) AI of nep is.

6 Check je eigen rol

Ben je niet zeker of een bepaald bericht, of een bepaalde foto of video echt of nep is? Deel het dan niet zelf op social media. Zo voorkom jij in elk geval dat onjuiste informatie anderen misleidt of een groter bereik krijgt.

DIGITALE ERFENIS BLIJKT NOG VAAK EEN VER-VAN-MIJN-BEDSHOW

WAT LAAT JIJ ONLINE ALLEMAAL NA?

Testament geregeld? Check! Je digitale nalatenschap ook? Ehm... Tegenwoordig heb je ook een online erfenis: alles wat digitaal en/of online van jou is opgeslagen. Wat gebeurt daarmee als jij er niet meer bent?

'Er is leven na de dood', zong Freek de Jonge al in 1997. Een vooruitziende blik, want anno nu leven we in elk geval online oneindig voort. Hoewel we ons testament over het algemeen goed regelen, blijkt de digitale erfenis voor velen van ons een ver-van-mijn-bedshow. Uit onderzoek van Kantar* blijkt dat slechts drie op de tien Nederlanders bekend is met het begrip digitale nalatenschap. Oftewel: alles wat je digitaal of online achterlaat, van je socialmedia-accounts tot

alle bestanden en foto's op je laptop of mobiele telefoon. En dat zes op de tien Nederlanders er zelfs nog nooit over heeft nagedacht. Nu denk je misschien: ik doe helemaal niet zo veel online, dus ik hoef me nergens zorgen om te maken (en mijn nabestaanden ook niet). Maar je online leven is wellicht groter dan je denkt.

DIT IS JOUW DIGITALE LEVEN

In de loop der jaren verzamelen we een enorme hoeveelheid aan accounts en digitale data, vaak zonder dat we het doorhebben. Ga het maar eens voor jezelf na. Bestel je weleens iets via een webshop en heb je daar een account? Heb je een account bij (officiële) instanties, zoals je zorgverzekeraar of Mijn Overheid? En bij je internet- en telefonieprovider? Gebruik je internetbankieren? Kijk je films en series of luister je weleens naar muziek via een streamingdienst? Ook daarvoor heb je een account nodig. Misschien heb je wel een eigen website. En wat dacht je van de eindeloze lijst aan wachtwoorden om bij apps, websites, organisaties en

instanties in te loggen? Die behoren allemaal tot je digitale nalatenschap. Net zoals die mailbox(en) vol mappen, e-mails en bijlagen. Of die duizenden foto's en filmpjes die je op je mobiele telefoon hebt staan. Tel daar nog de back-ups online en eventueel op een externe schijf bij op. En ga zo maar door...

WAAR TE BEGINNEN?

Je digitale voetafdruk is dus immens groot. Wat wil jij zelf dat er met al je persoonlijke digitale data gebeurt als je er straks niet meer bent? Wat mogen mensen níét vinden na jouw dood? In de wet staat dat overledenen geen recht hebben op privacy. Dus wil je die behouden na je dood, dan is het verstandig om je wensen en grenzen wat betreft je online nalatenschap nu al vast te leggen. Ook om lastige en verdrietige situaties en ethische dilemma's voor je nabestaanden te voorkomen.

Wat wil je dat je nabestaanden wél vinden na je dood? Zorg dat ze toegang hebben tot bepaalde of al je accounts. Dat kun je regelen met een wachtwoordenkluis. In die digitale 'kluis' kun je met één wachtwoord, een zogeheten moederwachtwoord, terecht bij allerlei verschillende wachtwoorden voor verschillende accounts. Soms kun je hier een noodpersoon voor aanwijzen. Die nabestaande krijgt dan, als je lang niet hebt ingelogd, na een tijdje de

46%
van de Nederlanders zou de afwikkeling van de digitale nalatenschap overlaten aan zijn of haar partner

3 OP DE 10

Nederlanders zijn bekend met het begrip digitale nalatenschap, 6 op de 10 heeft er nog nooit over nagedacht

mogelijkheid om in te loggen in je wachtwoordkluis, en kan daarna bij al je online accounts. Als dit niet kan of als je dit niet wilt, dan kun je het wachtwoord van de online kluis delen met (een van) je nabestaanden door het bijvoorbeeld op te schrijven in een boekje en dat te bewaren op een veilige plek in huis. Ook kun je ervoor kiezen je wachtwoorden in een schriftje op te schrijven en dat veilig ergens op te bergen. Voor de veiligheid is het wel belangrijk dat je niet voor alle of meerdere accounts hetzelfde wachtwoord gebruikt.

STAPPENPLANNEN

Als je je inschrijft voor de nieuwsbrief van oneindigonline.nl, ontvang je een handig achtstappenplan in je mailbox voor het regelen van je digitale nalatenschap. Je vindt de link om je in te schrijven voor dit stappenplan ook op digitaalsamenleven.nl.

Er bestaat niet zoiets als het recht op privacy na de dood. Regel dit dus goed vooraf



‘Op het bureaublad van mijn zoons laptop vond ik een afscheidsbrief’

Als de negentienjarige zoon van Margo Hendriks (50) drie jaar geleden plotseling overlijdt, krijgt ze meteen al te maken met digi-nalatenschapsstress.

“We hadden een code, vingerafdruk of gezichtsherkenning nodig om toegang te krijgen tot zijn mobiel. We twijfelden zelfs of we in de kist met zijn vingerafdruk zijn telefoon moesten ontgrendelen, zoveel druk gaf dat digitale gebeuren. Ook vroeg ik me af: wil ik wel alles zien? Zou Max willen dat ik zijn appjes lees? Pas een jaar later was ik er klaar voor om zijn mobiel en laptop te ontgrendelen.

‘Ik vroeg me af: wil ik wel alles zien? Zou Max willen dat ik zijn appjes lees?’

Dat is technisch ingewikkeld als je niet alle wachtwoorden hebt. Hiervoor kun je hulp vragen bij Digital Life Legacy (kennis- en expertisecentrum voor digitale nalatenschap, red.). Op het bureaublad van Max’ laptop vond ik een afscheidsbrief. Dit voelde voor mij als een toestemming. Hij wist dat wij toegang zouden krijgen tot zijn laptop. Naast die afscheidsbrief trof ik tientallen foto’s aan van de katten, websites met de games die hij speelde, voice-memo’s. Heel herkenbaar allemaal. Wanneer je toegang krijgt tot de digitale nalatenschap van een dierbare, moet je beseffen dat je alles te zien krijgt. Het is zo intiem en privé. Je dierbare is er niet meer om eventueel de context ervan uit te leggen.”

5x

BEWUST ONLINE

is een uitgave van Libelle en Margriet en wordt aangeboden door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

VEILIG IN DE BASIS

Geef intercriminelen geen of in elk geval een stuk minder kans.

Deze tips helpen je om je online veiligheid op orde te hebben.

1 Voer altijd alle updates uit

Zorg dat alle apparaten die met internet zijn verbonden – zoals je computer, mobiel, tablet of smart-tv – altijd up-to-date zijn. Zie je een update of vraagt een van je apparaten of je een bepaalde update wilt uitvoeren? Voer die dan meteen uit. Of stel 'automatische updates' in zodat je er niet meer aan hoeft te denken. Zorg ook dat je virusscanner altijd helemaal up-to-date is.

2 Zorg voor veilige wachtwoorden

Op de site haveibeenpwned.com kun je checken of je e-mail bekend is bij criminelen. Is dit het geval, verander dan het wachtwoord van je e-mailadres. Kies altijd een lang wachtwoord, bijvoorbeeld een zin met hoofdletters, kleine letters, leestekens en cijfers. Gebruik voor elk account een uniek wachtwoord, zo blijven je andere accounts beschermd als een wachtwoord uitlekt. Sla wachtwoorden het liefst op met een wachtwoordmanager, een online programma om wachtwoorden veilig op te slaan.

3 Eerst checken dan klikken

Cybercriminelen gebruiken links om virussen te installeren of je naar nepsites te leiden om je inloggegevens te stelen. Krijg je een bericht met een link of bijlage? Controleer de afzender en de link goed. Het e-mailadres hoeft namelijk niet te matchen met de naam van de afzender. En de link kan naar een andere website leiden dan het lijkt. Ga met je muis over de link heen zonder erop te klikken. We noemen dat 'hoveren'. Zo zie je waar je echt naartoe gaat als je erop zou klikken.

4 Tweestapsverificatie als extra beveiligingslaag

Met tweestapsverificatie (inloggen in twee stappen) voeg je een extra beveiligingslaag toe. Naast een wachtwoord gebruik je ook een code om in te loggen. Die ontvang je bijvoorbeeld via je e-mail, sms of een app op je telefoon.

• Ga voor meer adviezen, tips en handige stappenplannen naar veilig-internetten.nl

5 Maak regelmatig een back-up van je bestanden

Zo loop je de minste kans alles kwijt te zijn. Bijvoorbeeld na een hack (als er online bij je is ingebroken en je account misschien zelfs is overgenomen) of als je apparaat kapotgaat. Je kunt een back-up maken via een externe harde schijf of usb-stick of online 'in the cloud', oftewel een opslagaccount op een online server. Met cloudopslag heb je alleen internet nodig om je bestanden terug te halen. Beveilig die online opslagplaats wel goed met een wachtwoord dat je nergens anders voor gebruikt.

COLOFON

• **Projectmanager** Annerieke Bijeman **Algemene artdirection** Cilla Tibbe, Bret Hartman **Coördinatie** Esther Monsanto **Artdirection** Monique Zevenhuizen **Beeldcoördinatie** Afra Veerman **Teksten** Jessica van Zanten **Tekstredactie** Claudia Coenen **Technische eindredactie** Aleida Bos **Fotografie** Marloes Bosch (drie-generatie-interview), Walter Kallenbach (portret Vivianne Bendermacher), Femke Kamps (portret Margo Hendriks), Iris Planting (portret cover Janny van der Heijden). **Styling** Ora Bollegraaf **Visagie** Astrid Timmer **Locatie** Loes op Locatie (drie-generatie-interview) **Illustraties** Deborah van der Schaaf **Beeldbewerking** Frans Rappange **Commerciële samenwerkingen** Jony Gruijters, Corine Schumacher © 2024

