

Team VDM

VEILIG INTERNETTEN VOOR SENIOREN

Met vertrouwen en gemak veilig aan de slag met internet

inclusief
gratis webversie
van het boek



VANDUUREN
MEDIA

VEILIG INTERNETTEN VOOR SENIOREN

Team VDM

VAN DUUREN
MEDIA

INHOUDSOPGAVE

	Inleiding	8
Hoofdstuk 1:	De digitale wereld – kansen en risico's	12
	Het nut van internet: gemak en nieuwe mogelijkheden	13
	De schaduwkant: online gevaren en veelvoorkomende bedreigingen	15
	Veiligheidsbewustzijn: alert blijven zonder angst	20
	Checklist: hoofdregels voor veilig internetgebruik	22
Hoofdstuk 2:	Sterke wachtwoorden en accountbeveiliging	24
	Uniek en veilig: hoe stelt u een sterk wachtwoord op?	25
	Hulp bij wachtwoorden: wachtwoordmanager in het kort	29
	Tweestapsverificatie als extra slot op de deur	33
	Checklist: veilige wachtwoorden in de praktijk	38
Hoofdstuk 3:	Apparaten en thuisnetwerk beveiligen	40
	Houd software up-to-date en gebruik antivirus	41
	Veilig thuisnetwerk: wifi en router instellen	45
	Oppassen met openbare wifinetwerken	50
	Checklist: apparaten en thuisnetwerk beveiligen	55
Hoofdstuk 4:	Veilig surfen en bestanden downloaden	58
	Vertrouwde websites herkennen	59
	Klik met beleid: voorkom foute links en malware	63
	Bestanden downloaden zonder risico's	67
	Cloud: foto's en documenten veilig online opslaan	72
	Checklist: veilig surfen en downloaden	78
Hoofdstuk 5:	Oplichting via e-mail, berichten en telefoon	80
	Phishing via e-mail: valse berichten herkennen	81
	Iedereen kan erin trappen: de CEO-fraude bij Pathé	86

	WhatsApp-fraude en valse hulpvragen van ‘bekenden’	88
	Telefonische oplichters en nephelpdesks	92
	Checklist: zo herkent u oplichting via e-mail, berichten en telefoon	96
Hoofdstuk 6:	Veilig internetbankieren en winkelen	98
	Internetbankieren zonder zorgen	99
	Online aankopen doen: veilig en bewust shoppen	100
	Betaalmethoden en valkuilen	106
	Checklist: veilig bankieren en online kopen	111
Hoofdstuk 7:	Privacy en sociale media	112
	Bewust omgaan met persoonlijke informatie	113
	Instellingen en veiligheid van uw socialemedia-accounts	119
	Nepprofielen en valse vriendverzoeken herkennen	124
	Checklist: bescherm uw online privacy	129
Hoofdstuk 8:	Omgaan met AI: AI-geletterdheid	130
	Wat is AI en waar merkt u er iets van?	131
	Deepfakes, nepvideo’s en slimme chatbots:	
	nieuwe trucs van oplichters	135
	Kritisch blijven: omgaan met desinformatie en nepnieuws	138
	Checklist: kritisch blijven bij nieuws en berichten	143
Hoofdstuk 9:	Hulp, melding maken en digitaal verder leren	144
	Als u slachtoffer wordt: eerste hulp bij cybercrime	145
	Meldpunten en professionele hulp inschakelen	149
	Blijf digitaal vaardig: leren en oefenen met steun	154
	Checklist: blijf digitaal vaardig met vertrouwen	159
Bijlage A:	Bitwarden	160
	Bitwarden kiezen en uw hoofdwachtwoord maken	161
	Bitwarden installeren op uw apparaten	165
	Bitwarden in het dagelijks gebruik	170
	Extra mogelijkheden en veilige gewoonten	176
	Index	181

INLEIDING

INLEIDING

Internet is voor veel mensen een praktisch onderdeel van het dagelijks leven geworden. Even het nieuws lezen, een afspraak maken bij de huisarts, bankzaken regelen of foto's delen met familie: het gaat vaak sneller en makkelijker dan vroeger. Ook voor vijftigplussers kan internet veel vrijheid geven. U kunt dingen zelf doen, op uw eigen moment, zonder afhankelijk te zijn van openingstijden of een bezoek aan een loket.

Tegelijk is internet geen 'neutrale' omgeving. Er zijn partijen die vooral geïnteresseerd zijn in uw aandacht, uw gegevens of uw geld. Dat klinkt ongemakkelijk, maar het is wel de realiteit. En het belangrijke punt is: u hoeft geen technisch expert te zijn om uzelf daartegen te beschermen. De meeste problemen ontstaan niet door ingewikkelde hacks, maar doordat iemand wordt verleid om net iets te snel te klikken, een code door te geven of een verzoek te geloven dat eigenlijk niet klopt. Daarom draait veilig internetten minder om techniek en meer om gedrag: rustig blijven, controleren en pas daarna handelen.

In dit boek komt u daarom regelmatig korte cases tegen: herkenbare situaties die laten zien hoe iets mis kan gaan. Sommige zijn hypothetisch, maar ze zijn gebaseerd op patronen die in de praktijk vaak voorkomen. Het doel van die cases is niet om u bang te maken. Integendeel: ze helpen u om misleiding sneller te herkennen. Oplichters spelen namelijk graag met gevoelens zoals urgentie ("dit moet nu"), autoriteit ("ik bel namens de bank") of schaamte ("u hebt iets verkeerd gedaan"). Wie die trucjes eenmaal doorziet, krijgt rust. U weet beter welke vragen u uzelf kunt stellen en wanneer u juist even moet stoppen. Bovendien: dit soort fraude is niet enkel iets voor senio-

ren. Zelfs grote organisaties en ervaren professionals kunnen misleid worden als een bericht overtuigend genoeg is en precies op het verkeerde moment binnenkomt.

U kunt dit boek van voor naar achter lezen, maar u kunt het ook gebruiken als naslagwerk. Elk hoofdstuk behandelt een herkenbaar onderdeel van het online leven. We beginnen met de kansen en risico's van internet en met de basis: een gezonde houding online. Daarna gaan we in op sterke wachtwoorden en accountbeveiliging, omdat uw e-mail en andere accounts vaak de sleutel vormen tot de rest. Vervolgens kijken we naar uw apparaten en thuisnetwerk: updates, antivirus, wifi en veilig omgaan met openbare netwerken. Ook veilig surfen en downloaden krijgt veel aandacht, omdat daar veel misleiding plaatsvindt: nepwebsites, misleidende knoppen en bijlagen die niet zijn wat ze lijken.

Daarna volgt een belangrijk blok over oplichting: phishing-mails, WhatsApp-fraude, telefonische nephelpdesks en andere vormen van sociale manipulatie. Ook veilig online bankieren en winkelen komt aan bod, inclusief betaalmethoden en bekende valkuilen. In het hoofdstuk over privacy en sociale media leert u bewuster delen, instellingen aanscherpen en nepaccounts herkennen. We sluiten af met een hoofdstuk over AI-geletterdheid, omdat kunstmatige intelligentie internet verandert: deepfakes en nepnieuws kunnen overtuigender worden, en chatbots kunnen heel overtuigend klinken. U hoeft AI niet te begrijpen als technologie, maar u moet wel weten waar de grenzen liggen en wanneer u informatie extra moet controleren.

Aan het eind van elk hoofdstuk staat een checklist. Zie die checklists als uw kompas. U hoeft niet alles in één keer perfect te doen. Als u na elk hoofdstuk één of twee verbeteringen doorvoert, boekt u al snel veel winst. Veiligheid is

zelden één grote handeling. Het is vaker een paar kleine gewoonten, steeds opnieuw.

Tot slot: als het ooit misgaat, onthoud dan dat schaamte u niet helpt. Oplichters zijn hier goed in. Achterin vindt u een lijst met relevante webadressen en telefoonnummers van instanties en organisaties in zowel Nederland als België. Het belangrijkste is immers dat u weet wat u kunt doen, waar u terechtkunt en dat u hulp durft te vragen.

Dit boek is geschreven om u daarbij te ondersteunen: met duidelijke uitleg, praktische handvatten en vooral met het vertrouwen dat u prima online kunt zijn, zolang u het op uw eigen tempo doet.

Wij wensen u fijn en veilig internetplezier!

Team VDM
Januari 2026

DE DIGITALE WERELD – KANSEN EN RISICO'S

DE DIGITALE WERELD – KANSEN EN RISICO'S

HET NUT VAN INTERNET: GEMAK EN NIEUWE MOGELIJKHEDEN

Internet is al lang niet meer weg te denken uit het dagelijks leven. Steeds meer zaken verlopen digitaal: van het regelen van bankzaken tot het maken van afspraken met de huisarts of gemeente. Ook voor de wat oudere burger biedt internet grote voordelen, mits goed begrepen en verstandig gebruikt. In dit hoofdstuk verkennen we op toegankelijke wijze de belangrijkste mogelijkheden en het gemak dat internetgebruik met zich meebrengt.

CONTACT ONDERHOUDEN MET FAMILIE EN VRIENDEN

E-mail, WhatsApp, videobellen en sociale media zoals Facebook en Instagram maken het eenvoudiger dan ooit om contact te houden met dierbaren, ook als zij ver weg wonen. Voor veel senioren is het een uitkomst om via beeldbellen (bijvoorbeeld met WhatsApp, Zoom, Teams of Facetime) kleinkinderen te zien opgroeien of in contact te blijven met vrienden van vroeger. Het geschreven woord wordt aangevuld met foto's, video's en gesproken berichten, waardoor communicatie persoonlijker en directer wordt.

BANKZAKEN EN OVERHEIDSDIENSTEN REGELEN VANUIT HUIS

Internetbankieren is inmiddels de standaard geworden. Met een veilige app op de smartphone of tablet kan men betalingen doen, saldo controleren, automatische incasso's beheren of geld overmaken. Ook contact met de overheid verloopt steeds vaker digitaal: via DigiD kunnen burgers inloggen bij instanties zoals de Belastingdienst, het UWV, de ziektekostenverzekeraar of de gemeente. Veel aanvragen en afspraken kunnen daardoor gemakkelijk

vanuit huis worden geregeld, zonder papieren formulieren of wachtrijen.

ONLINE WINKELN: GEMAK AAN HUIS

Online shoppen biedt uitkomst voor wie niet altijd makkelijk naar de winkel kan. Via betrouwbare webwinkels kunnen producten worden besteld, thuisbezorgd of zelfs retour gestuurd. Denk aan kleding, boeken, elektronica of zelfs boodschappen. Voor wie minder mobiel is of in een rustige omgeving woont biedt dit veel comfort. Belangrijk is wel om bewust en veilig te winkelen – dat komt later in het boek uitgebreid aan bod.

INFORMATIE ZOEKEN EN OP DE HOOGTE BLIJVEN

Internet biedt een schat aan informatie. Of het nu gaat om het laatste nieuws, de weersverwachting, medische informatie of recepten: met een paar klikken is veel kennis binnen handbereik. Zoekmachines zoals Google en apps zoals NU.nl of Buienradar maken het mogelijk snel betrouwbare informatie op te zoeken. Tegelijkertijd is het belangrijk te leren onderscheid te maken tussen betrouwbare en misleidende informatie – ook dat komt in latere hoofdstukken aan bod.

HOBBY'S EN INTERESSES VERDIEPEN

Van tuinieren tot genealogie, van muziek luisteren tot fotografie: op internet zijn talloze websites, fora, blogs en video's te vinden die aansluiten bij uiteenlopende hobby's. Platforms zoals YouTube bieden instructievideo's voor knutselprojecten, cursussen of het instellen van apparatuur. Wie van puzzelen of spelletjes houdt, vindt online ook een breed aanbod aan digitale kruiswoordraadsels, bridgeclubs of schaaksites.

CURSUSSEN EN ONLINE LEREN

Internet biedt laagdrempelige manieren om nieuwe kennis op te doen. Online cursussen, webinars en instructievideo's maken het mogelijk om in eigen tempo iets nieuws te leren: een taal, computervaardigheden of creatieve technieken. Websites als SeniorWeb, de bibliotheek of Oefenen.nl bieden speciaal op senioren afgestemde leermaterialen. Voor wie nieuwsgierig blijft is internet een uitstekende leeromgeving.

ZORG EN GEZONDHEID

Steeds meer huisartsenpraktijken en ziekenhuizen bieden patiëntenportalen aan waarop men zelf afspraken kan maken, uitslagen kan bekijken of herhaalrecepten kan aanvragen. Ook beeldbellen met een arts of apotheker is mogelijk. Gezondheidsapps helpen bij het bijhouden van medicatie, stappen tellen of bloeddruk monitoren. Hoewel deze digitale zorgontwikkeling soms wennen is, kan het ook zelfstandigheid en regie versterken.

TOT SLOT

Internet is dus meer dan alleen 'iets voor jongeren'. Het is een veelzijdig hulpmiddel dat – mits veilig en met vertrouwen gebruikt – veel comfort, verbinding en zelfredzaamheid kan bieden. In de volgende paragrafen gaan we dieper in op de risico's en aandachtspunten, zodat u optimaal profiteert van al het goede dat internet te bieden heeft.

DE SCHADUWKANT: ONLINE GEVAREN EN VEELVOORKOMENDE BEDREIGINGEN

Internet biedt veel gemak, maar helaas schuilen er ook risico's achter de schermen. Iedereen die online actief is – jong of oud – kan te maken krijgen met digitale bedreigingen. Gelukkig hoeft u geen technische expert te zijn om uzelf te beschermen: een beetje kennis en gezond wantrouwen brengen u al een heel eind. In deze paragraaf

geven we een overzicht van de meest voorkomende online gevaren, in begrijpelijke taal uitgelegd.

COMPUTERVIRUSSEN EN MALWARE

Een computervirus is een kwaadaardig programma dat zich onzichtbaar op uw apparaat nestelt en daar schade kan aanrichten. Het kan bestanden wissen, uw computer traag maken of zelfs gegevens doorspelen aan anderen. Onder de verzamelnaam *malware* vallen ook andere kwaadaardige programma's, zoals:

- **Spyware** Deze software volgt wat u doet en verzamelt ongemerkt gegevens over u, zoals wachtwoorden of bankgegevens.
- **Ransomware** Gijzelt uw bestanden door ze te versleutelen. U krijgt pas weer toegang als u 'losgeld' betaalt, meestal in de vorm van cryptogeld (zoals bitcoin).
- **Adware** Toont ongewenste reclame en kan uw browser overnemen.

Vaak komt malware ongemerkt binnen via onbetrouwbare websites of door op een besmette bijlage in een e-mail te klikken. Daarom is het belangrijk om nooit zomaar op links of bestanden te klikken die u niet vertrouwt.

PHISHING: VALSE BERICHTEN DIE OP ECHT LIJKEN

Phishing is een vorm van oplichting waarbij criminelen u proberen te misleiden met nepberichten, zogenaamd van uw bank, de overheid of een bekende organisatie. In zo'n bericht staat vaak dat u dringend iets moet doen: inloggen, betalen of uw gegevens bevestigen. Maar als u op de link klikt, komt u op een valse website terecht die uw gegevens probeert te stelen.

Phishingberichten worden steeds moeilijker te onderscheiden van echte e-mails of sms'jes. Let daarom goed op:

- Komt het bericht onverwacht?
- Zit er een taalfout in?
- Wordt u onder druk gezet ("binnen 24 uur actie vereist")?
- Klopt het webadres wel?

Bij twijfel: klik niet. Neem liever zelf contact op met de instantie via het officiële telefoonnummer of de website die u zelf intypt.

DATALEKKEN EN MISBRUIK VAN GEGEVENS

Bij een datalek raken persoonsgegevens – zoals naam, e-mailadres, wachtwoord of bankrekening – onbedoeld op straat. Dit kan gebeuren door een hack bij een webshop, zorgverlener of andere organisatie waar u klant bent. Criminelen kunnen deze gegevens vervolgens gebruiken om in te breken in accounts of identiteitsfraude te plegen.

U kunt niet voorkomen dat anderen een datalek hebben, maar u kunt wél de schade beperken:

- gebruik voor elk account een ander wachtwoord;
- controleer of uw gegevens zijn gelekt via websites zoals **haveibeenpwned.com**;
- verander wachtwoorden als u een melding krijgt van een lek.

IDENTITEITSFRAUDE

Bij identiteitsfraude gebruikt iemand anders uw persoonlijke gegevens om zich als u voor te doen. Bijvoorbeeld om op uw naam spullen te bestellen, een lening af te sluiten of toegang te krijgen tot uw accounts. Hoe komen criminelen aan die gegevens?

- via datalekken;
- door phishing;
- door informatie die u zelf online deelt (adres, geboortedatum, foto's van ID).

Let dus op met welke gegevens u openbaar deelt en wees terughoudend met kopieën van identiteitsbewijzen.

OPLICHTING VIA TELEFOON OF WHATSAPP

Niet alle digitale oplichting verloopt via de computer. Ook via de telefoon of berichtenapps proberen criminelen mensen geld afhandig te maken. Enkele veelvoorkomende vormen:

- **De nep-bankmedewerker** Iemand belt zogenaamd namens uw bank met een smoes ("er is verdachte activiteit op uw rekening"). U wordt onder druk gezet om geld over te maken of gegevens door te geven. Trap daar niet in: uw bank belt nooit met zo'n verzoek.
- **Hulpvraagfraude via WhatsApp** U krijgt een bericht van een onbekend nummer, zogenaamd van uw zoon of dochter, die zegt een nieuw nummer te hebben en dringend geld nodig heeft. Vaak heel geloofwaardig – maar het is oplichterij. Bel het vertrouwde nummer van uw familielid om te checken.
- **Technische helpdeskfraude** U wordt gebeld door iemand die beweert dat uw computer is geïnfecteerd. Ze vragen om toegang tot uw computer om het op te lossen – maar ze willen juist schade aanrichten of geld eisen.

De regel is simpel: geef nooit gegevens of toegang op basis van een telefoontje of bericht, hoe geloofwaardig het ook klinkt. Beter een keer te veel wantrouwen dan één keer te goedgelovig.

CASE

Een herkenbaar voorbeeld

U krijgt een e-mail die op het eerste gezicht van een bezorgdienst lijkt. Er staat dat er een pakketje klaarstaat, maar dat u nog “een kleine vergoeding” moet betalen om de bezorging af te ronden. Het bedrag is laag, de toon is dringend en de knop om te betalen is opvallend groot. U klikt, vult uw gegevens in en denkt: klaar.

Een dag later belt ‘uw bank’. De medewerker zegt dat er verdachte betalingen zijn gedaan en dat u snel moet handelen om schade te voorkomen. U wordt gerustgesteld: de bank ‘helpt’ u stap voor stap. Daarna wordt u gevraagd om een code door te geven die u op uw telefoon ontvangt. Het klinkt logisch en u wilt het probleem oplossen, dus u geeft de code door.

Wat er in werkelijkheid gebeurt: de eerste e-mail was phishing en de betaling was een manier om gegevens te verzamelen. Het telefoontje was een tweede stap om u onder druk te zetten en u zelf de deur te laten openen. Het is een combinatie die veel voorkomt: eerst een klein haakje, daarna een groter verzoek. Dit voorbeeld laat ook zien waarom oplichters zo succesvol zijn: zij mikken niet op technische kennis, maar op ons gevoel voor urgentie en onze wens om het snel goed te regelen.

In de volgende hoofdstukken duiken we dieper in deze vormen van digitale oplichting. U leert hoe u verdachte signalen herkent, welke maatregelen u kunt nemen en wat u kunt doen als u tóch slachtoffer wordt. Zo blijft u een stap voor op de oplichters.

VEILIGHEIDSBEWUSTZIJN: ALERT BLIJVEN ZONDER ANGST

Internetveiligheid gaat niet over wantrouwen naar alles en iedereen. Het gaat vooral over een paar verstandige gewoonten, net zoals u in het verkeer oplet zonder voortdurend bang te zijn. Met een gezonde houding wordt internet een stuk veiliger, zonder dat het ten koste gaat van plezier en gemak.

VEILIG GEDRAG IS VAAK EENVOUDIGER DAN HET LIJKT

U hoeft geen technische kennis te hebben om veel ellende te voorkomen. De meeste online problemen ontstaan niet doordat iemand een ingewikkelde hack uitvoert, maar doordat iemand wordt verleid om iets te doen wat achteraf niet verstandig was: klikken op een link, een code doorgeven, een app installeren of geld overmaken. Een klein moment van twijfel en een korte controle kunnen al genoeg zijn om een oplichter te stoppen.

GEZOND WANTROUWEN IS GEEN PARANOIA

Een nuttige vuistregel is: *als iets te mooi lijkt om waar te zijn, is dat het meestal ook*. Dat geldt voor prijzen, winacties, “korting alleen vandaag”, maar ook voor mensen die ineens heel vriendelijk zijn en snel uw vertrouwen proberen te winnen.

Daarnaast geldt: *urgentie is vaak een truc*. Berichten waarin u direct moet handelen of waarin wordt gedreigd met afsluiting, boetes of verlies van toegang zijn vaak bedoeld om u te laten schrikken. Oplichters rekenen erop dat u in paniek klikt of betaalt. Neem juist dan de tijd: lees rustig, controleer en beslis pas daarna.

NEEM TIJD, VERTRAAG EN CONTROLEER

De beste bescherming is vaak een simpele gewoonte: even vertragen. Maak het uzelf standaard makkelijk door altijd dezelfde controlevragen in uw hoofd te hebben:

- Verwachtte ik dit bericht, telefoontje of verzoek?
- Klopt het webadres en de afzender echt?
- Word ik onder druk gezet om meteen te handelen?
- Kan ik dit via een ander kanaal controleren (bijvoorbeeld zelf bellen met een officieel nummer)?

Wie even pauze neemt, wint bijna altijd.

WEES NIET BANG OM “NEE” TE ZEGGEN

Oplichters zijn vaak overtuigend. Ze klinken professioneel, vriendelijk, behulpzaam of juist dringend. Dat kan iedereen overkomen. Het helpt om één zin paraat te hebben die u altijd kunt gebruiken, bijvoorbeeld:

- “Ik hang nu op en bel zelf terug via het nummer dat ik al heb.”
- “Ik wil dit eerst controleren, ik doe nu niets.”
- “Ik geef geen codes of persoonsgegevens door.”

U hoeft zich niet te verantwoorden. Echt betrouwbare organisaties begrijpen dat u voorzichtig bent.

SCHAAMTE IS EEN WAPEN VAN OPLICHTERS

Veel slachtoffers schamen zich achteraf. Dat is begrijpelijk, maar het helpt oplichters juist. Zij zijn erop uit u te laten twijfelen, te laten schrikken of u te laten denken dat u iets doms hebt gedaan. In werkelijkheid zijn dit goed getrainde trucs die ook slimme en ervaren mensen kunnen misleiden. Als u ooit twijfelt of u ergens in bent getrapt, is snel handelen belangrijker dan schaamte.

KENNIS EN ROUTINE GEVEN RUST

Zodra u de meest voorkomende trucs kent, ziet u ze sneller aankomen. Dat geeft rust. U leert herkennen hoe oplichters druk op u zetten, hoe phishing eruitziet en welke gegevens u nooit moet delen. U hoeft dan niet meer alles te wantrouwen, maar u krijgt een helder kompas: wat veilig is, wat verdacht is en wat u het beste kunt doen bij twijfel.

TOT SLOT

Veilig internetten is vooral: rustig blijven, kritisch kijken en uzelf de tijd gunnen om te controleren. Met die houding kunt u met vertrouwen online zijn, zonder angst voor elke klik. In de checklist aan het eind van elk hoofdstuk zetten we de belangrijkste basisregels en/of bevindingen op een rij.

CHECKLIST: HOOFDREGELS VOOR VEILIG INTERNETGEBRUIK

- **Klik niet zomaar op links of bijlagen** Twijfelt u? Klik niet. Open geen bijlagen van onbekenden en typ bij voorkeur een webadres zelf in.
- **Controleer wie iets van u vraagt** Een bank, overheid of bezorgdienst vraagt nooit om wachtwoorden, pin-codes of het overnemen van je scherm. Bij twijfel: zelf terugbellen via een officieel nummer.
- **Laat u niet opjagen** “Direct actie vereist” is vaak een truc. Neem de tijd, lees rustig en controleer eerst.
- **Houd uw apparaten en apps up-to-date** Updates lossen beveiligingslekken op. Stel automatische updates in waar dat kan.
- **Gebruik sterke, unieke wachtwoorden** Voor elk account een ander wachtwoord. Deel wachtwoorden nooit, ook niet met ‘de helpdesk’.

- **Zet tweestapsverificatie aan waar het kan** Vooral voor e-mail, sociale media en bankzaken. Het is een extra slot op de deur.
- **Deel minder persoonlijke informatie dan u denkt nodig te hebben** Denk na vóór u iets plaatst: adres, telefoonnummer, geboortedatum, reisplannen en foto's van documenten zijn gevoeliger dan ze lijken.
- **Gebruik openbare wifi met beleid** Geen bankzaken of belangrijke aankopen op open netwerken. Gebruik liever mobiele data of een vertrouwd netwerk.
- **Luister naar uw onderbuikgevoel** Voelt iets vreemd, te mooi of te dringend? Stop en controleer.
- **Weet waar u hulp kunt krijgen** Bewaar een paar betrouwbare adressen of telefoonnummers (bank, Fraudehelpdesk, SeniorWeb, bibliotheek, Informatiepunt Digitale Overheid). Bij twijfel: vraag hulp voordat u handelt.