SNEAK PREVIEW

Digitale Veiligheidsgids
voor Particulieren

52 concrete tips uit 20 jaar cybersecurity-praktijk

52	8	20
praktische tips	thema's	jaar ervaring

Wanneer heeft u voor het laatst gecontroleerd wat er over u te vinden is?

Uw adres, telefoonnummer, uw huis op straatniveau, welke apps meelezen met uw gezondheid, welke bedrijven uw gegevens doorverkopen. Voor de meeste mensen is dat véél meer dan zij vermoeden.

Het goede nieuws: het merendeel daarvan kunt u zelf terugdraaien. Meestal in een middag, vrijwel altijd gratis. Deze gids laat u precies zien hoe.

Wat zit er in de volledige gids?

De gids is opgebouwd uit acht thema's. Elk onderdeel bestaat uit concrete stappen — geen theorie, maar exact welke knop u waar indrukt, op zowel iPhone, Android, Windows als Mac.

	THEMA	WAT U LEERT
1	**Basisbeheer & updates**	Ook firmware en BIOS bijwerken
2	**Wachtwoorden & accounts**	2FA, datalekken, herstelcodes
3	**Netwerk & apparaten**	SIM-swapping, DNS, gratis Ziggo-modem
4	**Virusbeveiliging & software**	Browser, extensies, Windows-privacy
5	**Phishing & oplichting**	Tikkie-fraude, QR-codes, deepfakes
6	**Privacy & digitale voetafdruk**	Locatiegeschiedenis, foto-metadata, reclamepost
7	**Extra & geavanceerd**	E-mailmaskers, back-ups, nalatenschap
8	**Identiteit, gezin & fysiek**	DigiD, BKR-fraude, kinderen online

Vier tips krijgt u nu alvast — gratis

Om te laten zien wat u kunt verwachten, deel ik hieronder vier complete tips uit de gids. Direct toepasbaar, vanavond nog.

GRATIS VOORPROEFJE

Tip 28. Uw foto's verraden uw thuisadres

Elke foto die u met uw telefoon maakt bevat verborgen EXIF-gegevens: exacte GPS-coördinaten, datum, tijdstip en het gebruikte toestel. Zet u zo'n foto op Marktplaats, dan deelt u onbedoeld uw thuisadres met iedere kijker.

➡ Zet locatie in de camera-app uit. iPhone: Instellingen → Privacy → Locatievoorzieningen → Camera → Nooit. Android: Camera openen → Instellingen → Locatietags uit.

➡ Wilt u de locatie wél bewaren maar niet meesturen? iPhone: selecteer de foto → Deel → Opties bovenaan → zet 'Locatie' uit vóór verzenden. Android: open de foto in Google Foto's → drie puntjes → Locatie verwijderen.

💡 Facebook en Instagram wissen EXIF automatisch. Marktplaats, WhatsApp-documenten, e-mailbijlagen en clouddiensten vaak níét.

⚠ Fotografeer producten die u verkoopt nooit vóór uw eigen huis. Een straatnaam of huisnummer op de achtergrond is genoeg om u te vinden.

GRATIS VOORPROEFJE

Tip 22. De regel die u honderden euro's kan besparen

Betaalverzoekfraude en oplichting op Marktplaats en Vinted behoren tot de meest voorkomende vormen van digitale criminaliteit in Nederland.

⚠ Onthoud deze ene regel bij verkopen: een échte koper hoeft NOOIT geld over te maken om úw geld te ontvangen. Krijgt u een betaalverzoek van 1 cent 'ter verificatie'? Dat is altijd oplichting — u logt dan in op een nepsite van uw bank.

➡ Krijgt u een WhatsApp-bericht van 'familie met een nieuw nummer'? Verifieer via een videobelletje of het oude nummer. Vraag iets dat alleen die persoon kan weten.

➡ Klik nooit op betaallinks uit WhatsApp, sms of e-mail. Open in plaats daarvan zelf uw bankapp.

➡ Handel op Marktplaats en Vinted uitsluitend binnen het platform af. Wijkt iemand uit naar WhatsApp of een andere betaalmethode? Stop de transactie.

GRATIS VOORPROEFJE

Tip 9. Uw wifi-netwerk staat waarschijnlijk op een openbare kaart

Op wigle.net worden wereldwijd wifi-netwerken verzameld en op een kaart gezet, compleet met netwerknaam, beveiligingstype en locatie. Die gegevens worden opgepikt door apps en auto's die langsrijden. Iedereen kan de site doorzoeken — op naam, op gebied, op adres.

⚠ Het gevolg: staat uw netwerk daar met een herkenbare naam (bijvoorbeeld 'Familie Jansen', 'Achterstraat12' of uw bedrijfsnaam), dan is uw woning eenvoudig te lokaliseren en gericht te benaderen.

➡ Wijzig daarom elke 6 maanden uw netwerknaam (SSID) en wachtwoord. Zo raakt de koppeling tussen naam en adres steeds weer verouderd.

➡ Kies een neutrale naam die niets zegt over u, uw gezin, uw adres of uw apparatuur. Dus niet uw achternaam, huisnummer, bedrijfsnaam of routermerk — en zeker niet de naam van uw provider (bijvoorbeeld 'Ziggo62846'), want dat verraadt precies welke apparatuur u gebruikt.

💡 Zet achter uw SSID de toevoeging '_nomap'. Google en enkele andere partijen sluiten netwerken met die toevoeging uit van hun locatiedatabases. Het werkt niet bij alle verzamelaars, maar het kost u niets.

💡 Bent u Ziggo-klant? Vraag dan meteen om inwisseling van uw modem voor het nieuwe SmartWifi-modem (het zwarte toestel). Vermeld dat uw wifi erg traag is — u krijgt er dan kosteloos een. Let op: men probeert u waarschijnlijk ook 'wifi boosters' aan te smeren. Die heeft u niet nodig.

➡ Log daarna in op uw modem (inloggegevens staan op de onderkant), wijzig het standaardwachtwoord en zet UPnP en WPS uit. Dit is een van de meest effectieve maatregelen die u thuis kunt nemen.

GRATIS VOORPROEFJE

Tip 19. Windows 11? Uw pc deelt meer dan u denkt

Windows 10 en 11 sturen standaard veel gegevens naar Microsoft: telemetrie, diagnostische gegevens, een advertentie-ID, locatiegegevens en een gesynchroniseerde activiteitengeschiedenis. Die instellingen staan verspreid over tientallen schermen, waardoor vrijwel niemand ze allemaal terugvindt.

Het gratis programma O&O ShutUp10++ brengt bijna 300 privacy-instellingen samen op één scherm, met per instelling een kleurcode: groen is veilig uit te zetten, oranje vraagt om aandacht, rood kan functionaliteit beïnvloeden. Te downloaden via oo-software.com/en/shutup10

Geen installatie nodig: u downloadt één bestand, dubbelklikt erop en het draait direct. Er wordt niets meegeïnstalleerd.

Zo pakt u het aan: start het programma → kies bovenin 'Acties' → 'Alleen aanbevolen instellingen toepassen'. Dat is de veilige middenweg waarbij Windows gewoon blijft werken. Herstart daarna uw computer.

Maak vooraf een herstelpunt. Het programma biedt dit zelf aan bij de eerste start — accepteer dat. Alle wijzigingen zijn met één klik terug te draaien.

Draai het opnieuw na elke grote Windows-functie-update (twee keer per jaar). Microsoft zet bij zulke updates regelmatig instellingen terug naar de standaardwaarden.

En dit zit er nog meer in

De overige 48 tips vindt u in de volledige gids. Een greep uit wat er nog meer aan bod komt:

- Beveilig uw DigiD — de sleutel tot vrijwel elke overheidsinstantie
- Bescherm uzelf tegen SIM-swapping (en waarom sms-codes onveilig zijn)
- Denk na over wat een app verzamelt vóór u hem installeert
- Zet uw locatiegeschiedenis uit — en wis wat er al jarenlang is opgeslagen

- Verberg uw echte e-mailadres met een e-mailmasker
- Vraag geheimhouding van uw persoonsgegevens aan bij uw gemeente
- Stop reclamepost en telemarketing — Postfilter, ACM en Kadaster
- Controleer gratis uw BKR-rapport op identiteitsfraude

- Nieuw of refurbished apparaat kopen? Check éérst de softwareondersteuning
- Bescherm kinderen online — ouderlijk toezicht, in-game chat en 'sharenting'
- Stappenplan: wat te doen ná een hack of datalek
- Regel uw digitale nalatenschap (inclusief cryptovaluta)
- … en 36 andere tips

Voor wie is deze gids bedoeld?

Voor iedereen die zijn digitale leven serieus neemt, maar geen technische achtergrond heeft. U hoeft niets te installeren en niets te programmeren — elke tip bestaat uit stappen die u letterlijk kunt volgen.

Bijzonder waardevol als u:

- te maken heeft (gehad) met stalking, intimidatie of een moeizame scheiding
- thuiswerkt of uw thuisadres als vestigingsadres gebruikt
- kinderen heeft die online actief zijn
- een beroep uitoefent waarbij zichtbaarheid een risico vormt
- ouders of grootouders wilt helpen die kwetsbaar zijn voor oplichting

Wat kost het als het misgaat?

Een eerlijke afweging hoort erbij. Onderstaande cijfers komen van het Centraal Bureau voor de Statistiek en gaan uitsluitend over particulieren — niet over bedrijven.

1 op de 7	Nederlanders van 15 jaar en ouder werd in één jaar tijd slachtoffer van online criminaliteit — ruim 2,2 miljoen mensen.
€ 2.000+	Bij een kwart van alle spoofingzaken in 2023 lag de schade boven de tweeduizend euro. Bij bankspoofing lag de helft van de schades zelfs boven de vierduizend euro.
± 1 op 3	Slechts ongeveer een derde van de totale schade werd vergoed door banken of verzekeraars. De rest bleef voor rekening van het slachtoffer.

Daar komt bij wat zich niet in euro's laat uitdrukken: de tijd die het kost om alles terug te draaien, het gedoe met banken en instanties, en het ongemakkelijke gevoel dat uw gegevens ergens rondzwerven. Een gestolen identiteit herstelt u niet in een middag.

Voorkomen is geen garantie — maar het scheelt in vrijwel alle gevallen een veelvoud aan tijd, geld en ergernis.

Klaar om uw digitale leven op orde te brengen?

De volledige gids telt 52 tips verdeeld over 8 thema's, met directe links, stap-voor-stap instructies per besturingssysteem en verwijzingen naar de juiste Nederlandse instanties.

Prijs op aanvraag

U ontvangt de gids per e-mail. Aanvragen via **www.inventix.nl**

Liever persoonlijk advies op maat? Ik adviseer particulieren, ZZP'ers en MKB over het opschonen van hun digitale voetafdruk en het beveiligen van hun apparaten, website of webwinkel.

⚠ Goed om te weten: veiligheid is een doorlopend proces

Digitale veiligheid is nooit voor 100% te garanderen. Deze gids biedt de belangrijkste fundamenten en praktische stappen om het risico op een digitale inbraak drastisch te verlagen — maar absolute garanties bestaan niet. Alert blijven is en blijft, naast het up-to-date houden van al uw software, de allerbeste beveiliging.