EDITIE 2026 · PREMIUM · BE / NL

Cyberveilig Thuis

Het complete doe-pakket voor jouw gezin en zaak.

EDITIE PREMIUM

CyberScore
Versie 2026.1

cyberveiligthuis.eu
10 modules · 1 noodkaart · 1 huishouden

COLOFON & VOORWAARDEN

Colofon

Uitgave

Cyberveilig Thuis — Editie 2026, **Premium** (BE / NL).
Versie 2026.1, eerste druk · mei 2026.

Tekst, redactie en ontwerp: **CyberScore**.

Contact

CyberScore — Cyberscore B.V.
KvK 97451436 · BTW NL868056820B01
cyberscore.nl · hallo@cyberveiligthuis.eu

Auteursrecht

© 2026 **CyberScore** (Cyberscore B.V., ingeschreven bij de Nederlandse Kamer van Koophandel). Alle rechten voorbehouden.

Dit werkboek is bedoeld voor **individueel gebruik per huishouden**. Niets uit deze uitgave mag worden verveelvoudigd, gedeeld, doorverkocht, opgenomen in een geautomatiseerd gegevensbestand of openbaar gemaakt — in welke vorm of op welke wijze dan ook — zonder voorafgaande schriftelijke toestemming van de auteur.

Citaten zijn toegestaan met bronvermelding: "*CyberScore, Cyberveilig Thuis, editie 2026.*"

Privacy & AVG / GDPR

Dit product is AVG/GDPR-conform opgesteld. Bestelgegevens worden verwerkt via [PSP] en uitsluitend gebruikt voor levering, support en updates. Zie het volledige privacybeleid op cyberveiligthuis.eu/privacy.

Disclaimer

> ¡ **Lees dit voor je begint.**
> Cyberveilig Thuis is een **educatief product** en geen vervanging voor persoonlijk advies van een security-consultant, advocaat of accountant. De auteur en uitgever zijn niet aansprakelijk voor schade, verlies of gemiste opbrengsten die voortvloeien uit de uitvoering van — of het nalaten van — handelingen die in dit werkboek worden beschreven.

- Het cyberlandschap evolueert snel. We bevelen een **jaarlijkse update** aan; controleer cyberveiligthuis.eu/updates voor de actuele editie.
- Schermafbeeldingen in dit boek zijn gemarkeerd met de datum van opname. Interfaces van banken, overheden en apps kunnen wijzigen.
- Genoemde merken en diensten dienen ter illustratie. Tenzij expliciet vermeld bestaat er **geen commerciële of affiliate-relatie** met de auteur. Waar wel een relatie bestaat,

VOOR JE BEGINT

Hoe gebruik je dit werkboek?

Cyberveilig Thuis is geen leesboek — het is een **doe-boek**. Je hebt het meeste resultaat als je de modules één voor één doorwerkt, met je laptop of telefoon erbij, en de checklists onderweg afvinkt.

Drie manieren om dit boek te gebruiken

1. ### De snelle triage (30 minuten)
   Geen tijd? Begin met **Module 0 — Quickstart**. In een half uur zet je de belangrijkste hendels om. De rest kun je later doen.

2. ### Eén module per weekend
   Aanrader voor gezinnen. Eén module per zaterdag- of zondagochtend. Na negen weken is je hele huishouden op orde.

3. ### Naslagwerk bij incidenten
   Iets gebeurd? Sla **Module 8 — Incident response** open en volg de stappen. De **Noodkaart achterin** hoort op de koelkast.

Tekens in dit boek

✓ **Tip**
Een handige snelkoppeling of slimme keuze.

⚑ **Gevaar**
Doe dit niet, of stop direct en bel het meldpunt.

! **Let op**
Een veelgemaakte fout of valkuil.

i **Goed om te weten**
Achtergrond die handig is, maar niet verplicht.

Wat je nodig hebt om te starten

- Je **laptop of desktop** en je **smartphone**.
- De inloggegevens van je e-mail, bank en (BE) itsme / (NL) DigiD.
- Een rustig uur per module, ongestoord, met de wifi-naam en het wachtwoord van je router bij de hand.
- Een pen — sommige onderdelen zijn invulbaar.

INHOUD

Inhoudsopgave

VOORWERK

i	Titelpagina	i
ii	Colofon, disclaimer & auteursrecht	ii
iii	Hoe gebruik je dit werkboek	iii
iv	Inhoudsopgave	iv
v	Snelstart-routekaart	v

HOOFDDEEL

0	Quickstart — 30-minuten triage	1
1	Accountbeveiliging & wachtwoorden	5
2	Digitale identiteit: itsme, DigiD, eBox	17
3	Phishing & scams herkennen	29
4	Bankieren, betalen & oplichting	43
5	Apparaten & thuisnetwerk	53
6	Kinderen & tieners online	65
7	Privacy & data-minimalisatie	73
8	Incident response: als het tóch misgaat	79
9	Zelfstandigen-extra (Premium)	85

NASCHRIFT

A	Noodkaart (uitscheurbaar, A5)	95
B	Verklarende woordenlijst	96
C	Bronnen & meldpunten BE / NL	98
D	Update-log	100
E	Achterflap	—

OVERZICHT

Snelstart-routekaart

Tien modules — geen wet, wel een logische volgorde. Pluk eruit wat nu het meest schuurt, of werk er één per weekend door.

0 **Quickstart** — 30 min
De 30-minuten triage: zet de hoofdkraan dicht.

1 **Accounts & wachtwoorden** — 90 min
Wachtwoordkluis + 2FA op alles wat geld of identiteit raakt.

2 **Digitale identiteit** — 75 min
itsme, DigiD, eBox — wie je écht bent online.

3 **Phishing & scams** — 90 min
De zes patronen waar 95% van de oplichting in past.

4 **Bankieren & betalen** — 60 min
Limieten, helpdesk-fraude, en wat je bank wel/niet doet.

5 **Apparaten & netwerk** — 90 min
Telefoon, laptop, router, slimme apparaten — basisinstellingen.

6 **Kinderen & tieners** — 60 min
Afspraken, instellingen en gesprek per leeftijdsfase.

7 **Privacy & data** — 45 min
Minder data weggeven = minder schade als het misgaat.

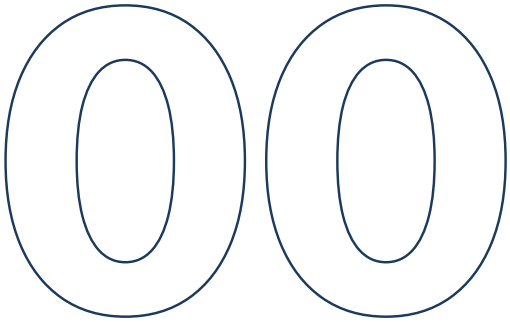
8 **Incident response** — 30 min
Het script voor als er tóch iets gebeurt — wie eerst, wat eerst.

9 **Zelfstandigen-extra** — 120 min
Premium: facturatie, klantgegevens, bedrijfscontinuïteit.

★ **Geen tijd? Doe in deze volgorde.**
Module 0 → 1 → 3 → 8. Dat dekt 80% van het thuisrisico in ongeveer drie uur.

MODULE 00 · QUICKSTART

~ 30 MINUTEN · 4 PAGINA'S



Quickstart: de 30-minuten triage

Geen tijd? Geen plan? Begin hier. Aan het eind van dit half uur staan de drie hendels om die voor 80% van de thuisrisico's zorgen.

WAT GA JE LEREN?

- Wat de drie belangrijkste cyberhendels in een huishouden zijn.
- Hoe je je e-mail in tien minuten een stuk veiliger maakt.
- Hoe je een "noodknop" inricht waar je later op terug kunt vallen.

WAT HEB JE STRAKS?

Een tweestapsverificatie op je hoofd-e-mail, een sterke nieuwe pincode voor je telefoon en een papieren back-up van je herstelcodes.

GESCHATTE TIJD

30 minuten · in één keer doen

WAT HEB JE NODIG?

- Je smartphone (geladen)
- Je laptop of tablet
- Het wachtwoord van je hoofd-e-mail
- Een pen en deze pagina

Sla deze module niet over. Ook als de rest van het boek nooit gelezen wordt: wie deze 30 minuten doet, sluit de meest gebruikte voordeuren.

MODULE 0 · INLEIDING

Waarom precies deze drie dingen?

Het overgrote deel van wat thuis misgaat — gehackte accounts, lege rekeningen, chantage met foto's, kinderen die hun TikTok kwijt zijn — begint op één van drie plekken. In dit half uur sluit je die drie deuren. Niet alles perfect, wel: *de hoofdkraan dicht*.

> ¡ **De drie hendels.**
> (1) je hoofd-e-mail, (2) je telefoon, (3) een papieren noodvoorraad. Doe ze in die volgorde — ze bouwen op elkaar.

Theorie-light: in één blik

1. E-mail is de hoofdsleutel

Bijna iedere knop "wachtwoord vergeten?" stuurt een herstellink naar je e-mail. Wie in je e-mail kan, kan dus ook in je Bol, je Facebook, je Marktplaats, je cloud-foto's. Daarom eerst dáár een tweede slot op.

2. Telefoon is je tweede bewijs

Je bank, je overheid en itsme/DigiD vertrouwen op je telefoon om te bewijzen dat jij het écht bent. Een onbeveiligde telefoon op straat is daarom geen "kwijtgeraakte telefoon" — het is een geopende kluis.

3. Papier is je vangnet

Als je telefoon én e-mail tegelijk vastlopen (gestolen, kapot, gehackt) kun je nergens meer in. Eén papieren A4 met herstelcodes en noodnummers lost dit op — voor altijd, zonder batterij.

> ! **Geen wachtwoordkluis nu.**
> De volledige overstap naar een wachtwoordkluis komt in Module 1. Dat kost een avond. Vandaag alleen de drie hendels.

Casus

Marleen (47), Hasselt. Haar zoon laat zijn telefoon liggen in de bus. Geen schermslot. Binnen twintig minuten staan er overschrijvingen via itsme en is haar Gmail-wachtwoord veranderd. Tegen de tijd dat ze de bank belt, mist er €1.940. — Een schermcode en 2FA op haar Gmail hadden deze hele keten gestopt. Beide kosten samen minder dan dit half uur.

MODULE 0 · AAN DE SLAG

De drie hendels — 30 minuten

1 Tweestapsverificatie (2FA) op je hoofd-e-mail — 10 min

Open op je laptop je e-mail (Gmail, Outlook, Proton of de webmail van je provider). Ga naar `Account → Beveiliging` en zoek naar "*Tweestapsverificatie*" of "*In twee stappen inloggen*". Zet het aan met je telefoonnummer of een authenticator-app.

Tip: zit het ergens diep weggestopt? Google op `[naam provider] tweestapsverificatie aanzetten`.

✓ Klaar als: bij uitloggen + opnieuw inloggen vraagt je e-mail om een code op je telefoon.

2 Sterke schermvergrendeling op je telefoon — 5 min

Op iPhone: `Instellingen → Face ID & Toegangscode`. Op Android: `Instellingen → Beveiliging → Schermvergrendeling`. Zet een **6-cijferige** code in (geen 1234, geen geboortejaar) en activeer Face ID of vingerafdruk. Zet ook "*Wis na 10 mislukte pogingen*" aan als die optie er is.

✓ Klaar als: telefoon na 30 sec automatisch vergrendelt en alleen jouw gezicht/code 'm opent.

3 Schrijf je vangnet op papier — 10 min

Pak het invulblok hieronder. Noteer: (a) je hoofd-e-mailadres, (b) de noodnummers van je bank, (c) je provider voor sim-blokkade, en (d) de 8–10 herstelcodes die je e-mail je heeft gegeven bij stap 1. Vouw het blad en leg het waar je je paspoort bewaart.

✓ Klaar als: je het blad blind kunt vinden zónder telefoon.

Mijn noodvoorraad — invulblok

MIJN HOOFD-E-MAILADRES

_____

NOODNUMMER BANK (BE/NL)

_____

MOBIELE PROVIDER — SIM BLOKKEREN

_____

HERSTELCODES E-MAIL (8–10 STUKS)

MODULE 0 · CONTROLELIJST

Klaar? Loop dit af.

- [ ] Mijn hoofd-e-mail vraagt om een code bij inloggen op een nieuw apparaat.
- [ ] Ik heb mijn 8–10 herstelcodes opgeslagen op een veilige plek, op papier.
- [ ] Mijn telefoon vergrendelt automatisch binnen 30 seconden.
- [ ] Mijn telefoon heeft een 6-cijferige code (geen 1234, geen geboortejaar).
- [ ] Het noodnummer van mijn bank staat op papier — niet alleen in mijn telefoon.
- [ ] Mijn partner of huisgenoot weet waar deze noodvoorraad ligt.

Wat als...

? ...ik mijn e-mailwachtwoord niet meer weet?

Doe eerst "*wachtwoord vergeten*" via de e-mailprovider zelf (Gmail / Outlook / Proton). Lukt dat niet, ga dan naar Module 1 voor het volledige herstelproces vóór je 2FA aanzet.

? ...ik geen sms-codes wil gebruiken?

Beter zelfs: gebruik een authenticator-app (Aegis op Android, Raivo op iOS, of de ingebouwde van je telefoon). Sms werkt ook prima voor nu — perfectie komt in Module 1.

? ...ik per ongeluk word uitgesloten van mijn e-mail?

Daarom de herstelcodes op papier. Heb je die nog niet? Zet 2FA eerst met *twee* methodes aan (telefoonnummer én herstelcodes) en print direct.

⚑ ...iemand belt en zegt dat hij van de bank is en jouw codes nodig heeft?

Ophangen. Altijd. Geen enkele bank, overheid of helpdesk vraagt ooit naar je codes, je wachtwoord of je herstelcodes. Bel zelf terug via het noodnummer dat je net hebt opgeschreven.

✂ Knip uit en hang op

Quickstart-spiekbriefje

- **1.** 2FA aan op mijn hoofd-e-mail.
- **2.** 6-cijferige schermcode + Face ID/vingerafdruk op telefoon.
- **3.** Herstelcodes + noodnummers op papier, bij m'n paspoort.
- **Bij twijfel:** ophangen, zelf terugbellen via opgeschreven nummer.

Samenvatting

Drie hendels om: e-mail, telefoon, papier. Daarmee heb je de meest gebruikte aanvalsroutes thuis

MODULE 01 · ACCOUNTS ~ 90 MINUTEN · 12 PAGINA'S

01

Accountbeveiliging & wachtwoorden

Eén goed wachtwoord per dienst, een kluis die ze voor je onthoudt, en een tweede slot op de deur. Geen Post-its meer onder het toetsenbord.

WAT GA JE LEREN?

- Waarom hergebruik van wachtwoorden het grootste thuisrisico is.
- Hoe je in één middag overstapt op een wachtwoordkluis.
- Welke vorm van tweestapsverificatie wél en niet veilig is.

WAT HEB JE STRAKS?

Een wachtwoordkluis in gebruik, je tien belangrijkste accounts beveiligd met 2FA, en je herstelcodes veilig opgeborgen.

GESCHATTE TIJD

90 minuten · in 2 sessies te doen

WAT HEB JE NODIG?

- Laptop én telefoon
- Lijst van je belangrijkste accounts
- 10 minuten ongestoord voor 2FA-setup

Voorbeelden die we gebruiken: Gmail, Outlook, Apple-ID, je bank (KBC, ING, ABN AMRO, Belfius), Bol/Coolblue, en itsme/DigiD.

MODULE 1 · INLEIDING

Eén wachtwoord per dienst. Geen uitzondering.

De gemiddelde Belg of Nederlander heeft ruim 100 online accounts. Niemand onthoudt 100 verschillende wachtwoorden — dus hergebruiken we ze. En dáár zit het probleem: wordt ergens één wachtwoord gelekt, dan ligt de rest ook open. Vandaag draaien we dat om.

Het domino-effect, eenvoudig

Een hobbywebshop wordt gehackt. Daar stond jouw e-mailadres met het wachtwoord `Zomer2021!`. Twee dagen later probeert een geautomatiseerd script datzelfde combinatie op honderden bekende diensten — Bol, Spotify, Coolblue, Gmail, je bank. Eén match is genoeg.

Dit heet *credential stuffing*. Het kost de aanvaller niets. Jouw verdediging: zorg dat iedere dienst een eigen wachtwoord heeft.

> ¡ **Hoe weet ik of mijn wachtwoord gelekt is?**
> Bezoek `haveibeenpwned.com` en vul je e-mailadres in. Je krijgt een eerlijke lijst van bekende lekken. Schrik niet — bijna iedereen staat er meerdere keren in.

Wat we vandaag doen

1. Je tien belangrijkste accounts in kaart brengen.
2. Een wachtwoordkluis kiezen en installeren.
3. Voor die tien accounts een uniek, sterk wachtwoord genereren.
4. Tweestapsverificatie (2FA) aanzetten waar het kan.
5. Herstelcodes veilig opbergen.

Wat we vandaag *niet* doen

We migreren **niet** alle 100 accounts in één sessie. Dat is geen marathon waard. We pakken de tien die ertoe doen — geld, identiteit, e-mail, opslag — en laten de rest organisch volgen. Je kluis vult vanzelf elke keer dat je ergens inlogt.

Casus

Tom (38), zelfstandig fotograaf in Gent. Gebruikt sinds 2014 overal `Lumix#80mm`. Een lek bij een verouderd forum stelt aanvallers in staat in zijn Gmail te komen, vandaaruit zijn Dropbox over te nemen en al zijn klantleveringen te versleutelen. Schade: drie weken werk en €3.200 om er weer bij te kunnen. — Eén kluis met unieke wachtwoorden had de keten direct gestopt bij dat oude forum.

MODULE 1 · THEORIE-LIGHT · 1 VAN 2

Hoe een wachtwoordkluis werkt

Een wachtwoordkluis is een versleutelde digitale agenda die jouw wachtwoorden onthoudt, ze automatisch invult, en bij elke nieuwe dienst een sterk nieuw wachtwoord voor je verzint. Jij onthoudt alleen nog het **master-wachtwoord** waarmee de kluis opengaat.

Wat zit er in zo'n kluis?

- Inlognamen + wachtwoorden per dienst
- (Optioneel) bankkaart-gegevens
- (Optioneel) veilige notities — rijksregisternummer, BSN, paspoortcopie
- Herstelcodes voor 2FA per dienst

De inhoud staat *versleuteld* opgeslagen — ook bij de aanbieder zelf. Zelfs als hun servers gehackt worden, kan niemand zonder jouw master-wachtwoord erbij.

Een normale dag mét kluis

1. Ochtend: telefoon open met Face ID — kluis ook.
2. Open je e-mail in de browser → kluis vult inlognaam + wachtwoord in.
3. Nieuw account bij webshop → kluis stelt voor: 9k$T#fLm2Qx. Klik *Opslaan*.
4. Bij je bank: kluis vult je wachtwoord in, jij bevestigt via je bank-app of itsme.

Welke kluis kies je?

Drie goede opties — geen affiliate-relatie, kies wat past:

Kluis	Prijs	Voordelen	Nadelen
Bitwarden open source, US	Gratis (gezinsplan €3/mnd)	Werkt overal, gratis is genoeg, broncode openbaar	Iets minder gladde interface
1Password Canada	€3–5/mnd, geen gratis versie	Mooiste interface, makkelijkst voor gezinnen	Verplicht abonnement
Proton Pass Zwitserland (EU/EER)	Gratis (Plus ± €2,50/mnd)	Europese aanbieder, sterke privacy-track record	Jonger product, minder browser-tovenarij

> ★ **In twijfel? Begin met Bitwarden.**
> Gratis, open source, prima voor 95% van de huishoudens. Overstappen naar een ander later is makkelijk — een kluis kun je exporteren.

MODULE 1 · THEORIE-LIGHT · 2 VAN 2

Tweestapsverificatie: drie smaken

"Tweestaps" betekent: naast je wachtwoord vraagt de dienst om een tweede bewijs dat jij het bent. Niet alle tweede bewijzen zijn even sterk. Hier de drie vormen, op volgorde van veilig naar minder veilig.

1. Hardware-sleutel

Een USB-stick (YubiKey, NitroKey) die je in je laptop steekt en even aanraakt. Veiligst dat bestaat. Maar: hardware kopen, twee stuks nodig (back-up), niet alle diensten ondersteunen het.

Wanneer? Voor je e-mail-hoofdaccount of werk-accounts als je vaak reist of gevoelig werk doet.

2. Authenticator-app

Een app op je telefoon die elke 30 seconden een nieuwe 6-cijferige code laat zien. Werkt zonder internet, werkt overal. **Voor iedereen de aanrader.**

Apps: Aegis (Android, open source), Raivo of de ingebouwde "Wachtwoorden"-app (iOS), of Google Authenticator.

3. Sms-code

De code komt per sms binnen. Werkt overal, geen app nodig. Maar: sms is technisch zwak — bij *sim-swap-fraude* zet een aanvaller jouw nummer over naar zijn telefoon en ontvangt jouw codes. Het gebeurt zelden, maar het gebeurt. Beter dan niets, slechter dan een app.

> ! **Sms alleen als het niet anders kan.**
> Veel banken (KBC, Belfius, ABN AMRO) gebruiken hun eigen app of digipass. Dat is praktisch een authenticator-app — prima. Overheidsdiensten via itsme / DigiD app: idem.

Wat is een herstelcode?

Wanneer je 2FA aanzet, krijg je 8–10 eenmalige codes (zoiets als `4f9k-22ma-7vqx`). Eén code = één keer inloggen zónder telefoon. Voor als je telefoon kapot, kwijt of leeg is. **Bewaar deze op papier**, niet op je telefoon. Eventueel ook in je kluis, in een veilige notitie.

> ⚑ **Geef nooit een 2FA-code aan iemand aan de telefoon.**
> Geen enkele bank, helpdesk of overheidsdienst vraagt jou een code voor te lezen. Als iemand dat doet: ophangen.

MODULE 1 · AAN DE SLAG · STAP 1 VAN 5

Stap 1 — Je top-10 accounts

Voor we iets installeren: eerst weten welke accounts ertoe doen. Niet alle 100. De tien die echt schade aanrichten als ze worden overgenomen. Vul hieronder eerlijk in — dit is je werklijst voor vandaag.

De vijf categorieën die altijd op je top-10 horen

1. **E-mail** — Gmail / Outlook / Proton / provider
2. **Bank** — KBC, Belfius, ING (BE/NL), ABN AMRO, Rabobank, bunq, Argenta
3. **Digitale identiteit** — itsme (BE), DigiD (NL)
4. **Cloud-opslag & foto's** — iCloud, Google Drive, Dropbox, OneDrive
5. **Sociale media** — Facebook/Instagram, WhatsApp, LinkedIn

Mijn top-10 voor vandaag

Voeg toe: dienst, e-mail/inlognaam waar je 'm mee opent, en kruis aan of er nu al 2FA op staat.

#	DIENST	INLOGNAAM / E-MAIL	2FA?	KLAAR?
1			☐	☐
2			☐	☐
3			☐	☐
4			☐	☐
5			☐	☐
6			☐	☐
7			☐	☐
8			☐	☐
9			☐	☐
10			☐	☐

MODULE 1 · AAN DE SLAG · STAP 2 VAN 5

Stap 2 — Kluis installeren

Keuze gemaakt op pagina 7? Goed. We doorlopen het pad voor **Bitwarden**; voor 1Password en Proton Pass zijn de stappen vrijwel identiek.

1 Maak een account

Ga op je laptop naar `bitwarden.com` en kies "*Get started*". Gebruik **je hoofd-e-mail** als gebruikersnaam (die heb je in Module 0 al beveiligd).

✓ Klaar als: je een bevestigingsmail hebt ontvangen en bevestigd.

2 Verzin een sterk master-wachtwoord

Dit is het ene wachtwoord dat je nog moet onthouden. Aanrader: drie tot vier willekeurige woorden plus een nummer, bijvoorbeeld `Kabel-Pannenkoek-Schemerlamp-71`.

Sla dit master-wachtwoord **nergens digitaal** op. Schrijf het in dit boek (pagina 13) en op een tweede plek thuis.

✓ Klaar als: je het master-wachtwoord drie keer correct kunt intikken zonder spieken.

3 Browser-extensie en telefoon-app

Installeer Bitwarden in je browser (Chrome / Firefox / Safari / Edge) via de officiële extension store. Installeer de Bitwarden-app op je telefoon vanuit de App Store of Play Store. Log op beide in.

✓ Klaar als: bij elke inlogpagina nu een Bitwarden-icoontje verschijnt.

4 Zet 2FA op je kluis zelf

Ga in Bitwarden naar `Settings → Security → Two-step Login`. Kies bij voorkeur "Authenticator app".

Print of noteer de herstelcodes **direct**. Zonder die codes ben je je kluis kwijt als je telefoon kapotgaat — en daarmee alle nieuwe wachtwoorden.

✓ Klaar als: je 2FA-code wordt gevraagd bij een nieuwe browser.

> ⚑ **Niet skippen: 2FA op de kluis zelf.**
> De kluis is je nieuwe brandkast. Een brandkast zonder slot is een doos.

MODULE 1 · AAN DE SLAG · STAP 3 VAN 5

Stap 3 — Migreer je top-10

Per account herhaal je hetzelfde minirondje. Reken op 3–5 minuten per dienst.

1 **Log in zoals altijd**
Bitwarden vraagt: "*Wil je deze inlog opslaan?*" — klik *Ja*. Vanaf nu staat de huidige (oude) inlog veilig in je kluis.

2 **Ga naar de wachtwoord-instellingen van de dienst**
Bij de meeste diensten heet dit `Account → Beveiliging → Wachtwoord wijzigen`.

3 **Laat Bitwarden een nieuw wachtwoord verzinnen**
Klik in het "nieuw wachtwoord"-veld op het Bitwarden-icoon → *Generate*. Standaard is 14 tekens. Kies "*Use Password*".

4 **Sla op bij de dienst én in de kluis**
Bevestig bij de dienst. Bitwarden vraagt: "*Bijwerken?*" — ja. Vink de regel af op je top-10-lijstje (pagina 9).

Volgorde voor vandaag

Niet alle accounts zijn even kritisch. Hou deze volgorde aan:

1. **E-mail** — eerst. (Je hebt 'm al, alleen wachtwoord verversen.)
2. **Bank** — meestal werkt het bankwachtwoord alleen mét digipass/itsme/app. Gewoon vervangen voor een sterk uniek wachtwoord en doorgaan.
3. **Cloud / foto's** — iCloud, Google, Dropbox.
4. **Sociale media** — Facebook, WhatsApp Web, LinkedIn.
5. **Webshops** — Bol, Coolblue, Amazon, Zalando.

> ! **Bankspecifiek.**
> Veel banken (KBC, Belfius, Argenta, ABN AMRO, Rabobank, bunq) loggen in via hun eigen app of digipass — je "wachtwoord" daar is meestal alleen voor klantenservice. Sla het op in de kluis, maar verwacht dat dagelijks gebruik via de bank-app loopt.

MODULE 1 · AAN DE SLAG · STAP 4 VAN 5

Stap 4 — 2FA op je top-10

Sterke wachtwoorden staan klaar. Nu de tweede deur. Voor elk account met geld of identiteit erin: zet 2FA aan met een authenticator-app.

Eerst: installeer een authenticator-app

- **Android**: `Aegis Authenticator` (open source, ondersteunt back-up).
- **iOS**: ingebouwde "Wachtwoorden"-app (iOS 17+) is uitstekend, of `Raivo`.
- **Beide**: Google Authenticator werkt prima, maar maakt minder makkelijk back-ups.

Per account: het patroon

1 **Open de beveiligingsinstellingen**
Meestal: `Account → Beveiliging → Tweestapsverificatie`.

2 **Scan de QR-code met je authenticator-app**
Je app voegt het account toe en toont meteen een 6-cijferige code die elke 30 seconden vernieuwt. Vul die code in op de website om te bevestigen.

3 **Sla de herstelcodes op**
Print, of plak ze in een veilige notitie in Bitwarden, of schrijf ze op pagina 13 van dit boek. Sluit het venster pas **na** deze stap. Niet skipbaar.

✓ **itsme / DigiD / bank-app tellen al mee.**
De itsme-app en de bank-apps van KBC, Belfius, ABN AMRO, ING, Rabobank en bunq zijn zelf al een sterke tweede stap. Daar hoef je niets extra's aan te zetten — je gebruikt ze al.

ℹ **Wat als een dienst alleen sms biedt?**
Liever sms-2FA dan helemaal geen 2FA. Zet 'm aan en zet 'm later om als de dienst app-2FA toevoegt. Hou je telefoonnummer geheim voor wie het niet hoeft te weten.

MODULE 1 · AAN DE SLAG · STAP 5 VAN 5

Stap 5 — Noodvoorraad op papier

Alles in je kluis, alles met 2FA — maar wat als je telefoon én laptop morgen weg zijn? Je herstelcodes en je master-wachtwoord redden je dan. Vul hieronder met pen in. Vouw deze pagina dubbel en leg 'm op een veilige plek (bijvoorbeeld bij je paspoort, of in een afsluitbare lade).

> ! **Schrijf met pen, niet met potlood. Niet fotograferen.**
> Een foto van dit blad in je telefoon haalt het hele plan onderuit.

Mijn master-wachtwoord — hint

Niet het hele wachtwoord. Een hint die alleen jij begrijpt — voor het geval je het in paniek vergeet.

HINT

Herstelcodes — e-mail (hoofdaccount)

CODE 1

CODE 2

CODE 3

CODE 4

CODE 5

CODE 6

CODE 7

CODE 8

Herstelcodes — Bitwarden (of jouw kluis)

CODE 1

CODE 2

CODE 3

CODE 4

CODE 5

CODE 6

CODE 7

CODE 8

MODULE 1 · CONTROLELIJST

Klaar? Loop dit af.

- [ ] Ik heb een wachtwoordkluis (Bitwarden / 1Password / Proton Pass) geïnstalleerd op laptop én telefoon.
- [ ] Mijn master-wachtwoord is minstens drie willekeurige woorden en sla ik nergens digitaal op.
- [ ] Op mijn kluis zelf staat 2FA aan — met een authenticator-app.
- [ ] Mijn top-10 accounts hebben elk een uniek, sterk wachtwoord uit de kluis.
- [ ] Op mijn e-mail, cloud-opslag en sociale media staat 2FA aan.
- [ ] Mijn bank-app(s) zijn ingelogd en werken — wachtwoord in de kluis als back-up.
- [ ] Mijn herstelcodes staan op papier op pagina 13 — niet in mijn telefoon.
- [ ] Mijn partner of huisgenoot weet wáár het herstelcode-blad ligt (niet wát erop staat).

✂ Knip uit en hang op

Wachtwoord-spiekbriefje

- **Eén kluis**, één master-wachtwoord. Alles erin.
- **Eén wachtwoord per dienst.** Geen hergebruik, ooit.
- **2FA op alles met geld of identiteit.** Liefst via app.
- **Herstelcodes op papier.** Bij je paspoort.
- **Geen 2FA-code aan de telefoon** — ook niet aan "de bank".

MODULE 1 · TROUBLESHOOTING

Wat als...

? **...ik mijn master-wachtwoord vergeet?**

Bij Bitwarden en Proton Pass is herstel niet mogelijk zonder een vooraf gegenereerde herstelcode of een sleutelbestand — bewust, voor jouw veiligheid. Lukt het echt niet meer, dan moet je je kluis legen en opnieuw beginnen. Daarom: schrijf je master-wachtwoord (of een sterke hint) vandaag nog op pagina 13.

? **...ik mijn telefoon verlies, met mijn authenticator-app erop?**

Gebruik je herstelcodes om in te loggen, schakel 2FA tijdelijk uit, en koppel je nieuwe telefoon. Aegis (Android) en de "Wachtwoorden"-app van iOS hebben een back-up-optie — zet die aan voordat je telefoon verdwijnt, niet erna.

? **...een familielid moet erbij kunnen als mij iets overkomt?**

Bitwarden en 1Password hebben een "Emergency Access"-functie. Je geeft een vertrouwd persoon read-only toegang die pas actief wordt na een door jou ingestelde wachttijd (bijv. 7 dagen). Goede aanrader voor partners.

? **...een dienst dwingt me een wachtwoord van max. 12 tekens te gebruiken?**

Helaas bestaat dat nog. Gebruik dan 12 willekeurige tekens uit de kluis-generator. Liever kort en uniek dan lang en hergebruikt.

? **...mijn browser vraagt of hij mijn wachtwoorden mag opslaan?**

Sla af. Eén kluis is genoeg. Twee tegelijk (Bitwarden + Chrome) zorgt voor verwarring en oude, onveilige kopieën.

⚑ **...ik denk dat iemand op dit moment in mijn account zit?**

Sla deze module dicht en ga direct naar Module 8 — Incident response. Eerst: wachtwoord van je e-mail wijzigen, daarna alle actieve sessies uitloggen vanuit de account-instellingen.

MODULE 1 · AFSLUITING

Module 1 — afgerond.

Het zwaarste werk in dit hele boek heb je nu gedaan. Eén kluis, één master, unieke wachtwoorden voor je tien belangrijkste accounts, en een tweede slot op de deur. Vanaf nu vult de kluis zichzelf — elke keer dat je ergens nieuw inlogt, komt er een regel bij.

Samenvatting in drie zinnen

1. Eén wachtwoordkluis, één sterk master-wachtwoord, en een verse generatie unieke wachtwoorden per dienst.
2. 2FA via authenticator-app op alles dat geld of identiteit raakt.
3. Herstelcodes op papier, op een vaste plek thuis.

Huishoudelijke routine vanaf nu

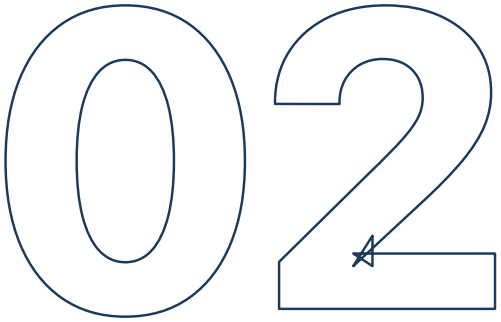
- Elke keer dat je ergens inlogt en de kluis vraagt "opslaan?" → ja. Zo migreer je organisch de overige 90 accounts.
- Elke drie maanden: open de kluis, check of er accounts tussen staan met dubbele wachtwoorden (Bitwarden meldt dit zelf).
- Elke zes maanden: doe een herstel-test. Pak je papieren codes, log in op een nieuw apparaat. Werkt het nog?

Volgende stap → Module 2 — Digitale identiteit: itsme, DigiD & eBox. Daar bouwen we op wat je net hebt opgezet: de officiële sleutels van België en Nederland, hun back-ups, en hoe je ze veilig gebruikt.

Hoeveel tijd heeft Module 1 jou werkelijk gekost? _____ minuten.
Wat ging moeizaam? _____

MODULE 02 · IDENTITEIT

~ 75 MINUTEN · 12 PAGINA'S



Digitale identiteit: itsme, DigiD & eBox

De officiële sleutels van België en Nederland. Wat ze zijn, hoe je ze veilig instelt en wanneer je ze (nooit) overhandigt.

WAT GA JE LEREN?

- Wat het verschil is tussen itsme, DigiD, eID-kaart en eBox.
- Hoe je je app correct instelt en herstelt bij verlies van je telefoon.
- Welke vragen overheid en bank wél en nooit stellen.

WAT HEB JE STRAKS?

Werkende identiteits-app, een back-up-plan bij telefoonverlies, en een ingerichte eBox / MijnOverheid-Berichtenbox.

GESCHATTE TIJD

75 minuten

WAT HEB JE NODIG?

- Je **BE**: eID-kaart + pincode, of bankkaart
- Je **NL**: DigiD-account en herinneringsvraag
- Smartphone met internet

Beide landen aan bod — je doet alleen het stuk dat op jou van toepassing is.

MODULE 2 · INLEIDING

Wie ben je, online?

Voor de meeste websites volstaat een gebruikersnaam en wachtwoord. Maar bij je gemeente, je belastingen, je bank of je zorgverzekeraar wil de andere kant zeker weten dat jij het echt bent. Daarvoor heeft België *itsme* en *de eID-kaart*, en Nederland *DigiD*. Deze module gaat over hoe je ze veilig instelt — en wat te doen als je telefoon morgen weg is.

Twee landen, dezelfde logica

Allebei werken op één principe: er bestaat één digitale jij, gekoppeld aan een fysiek bewijs (je eID-kaart in BE, je paspoort/rijbewijs in NL). Daarboven hangt een app waarmee je honderden diensten kunt openen zonder voor elk daarvan een nieuw wachtwoord te onthouden.

Wat je vandaag doet

- Je officiële app instellen of opfrissen.
- Een back-up regelen voor als je telefoon wegvalt.
- Je officiële berichtenbox (eBox / Berichtenbox) aanzetten.
- Een eerlijke noodprocedure noteren op pagina 25.

> ! **Eén bewijs, twee delen — bewaar ze niet samen.**
> Bewaar je eID-kaart (BE) of paspoort (NL) *niet* in dezelfde tas als je telefoon. Wie beide tegelijk steelt, kan zich op veel plekken voor jou uitgeven. Klein detail, groot verschil.

Casus

Familie Janssen, Eindhoven. Vader gaat met pensioen, weet niet meer hoe zijn DigiD-wachtwoord eruitziet, en heeft de DigiD-app nooit geactiveerd. Bij de eerste keer dat hij belasting wil aanvragen, blijkt herstel zes werkdagen te duren — net te laat voor de aangiftedeadline. — Een avondje DigiD instellen had het hele probleem voorkomen.

> ¡ **Welk deel doe jij?**
> Woon je in **BE**: pagina's 19, 21, 22, dan vanaf 25.
> Woon je in **NL**: pagina's 20, 23, 24, dan vanaf 25.

MODULE 2 · THEORIE · BELGIË

BE — itsme, eID & eBox

In België heb je drie middelen die samen je digitale identiteit vormen. Welk middel waarvoor, en hoe ze samenhangen:

Middel	Waarvoor?	Hoe activeer je het?
eID-kaart je fysieke identiteitskaart met chip	Inloggen op overheidsportalen met een kaartlezer; itsme activeren; ondertekenen van officiële documenten.	Bij ophalen op gemeente. Pincode + pukcode niet kwijtraken.
itsme de privé-app van Belgische banken	Inloggen bij overheid, banken, energie, mutualiteit, telecom; bevestigen van betalingen en documenten.	Activatie via je bankkaart (KBC, Belfius, ING, Argenta, BNP Paribas Fortis, Crelan…) of via je eID-kaart.
eBox officiële digitale brievenbus overheid	Hier komen aanslagbiljetten, brieven van FOD's, gemeente en pensioendienst binnen. Vervangt papieren post.	Via mybox.belgium.be — eenmalig aan-zetten met itsme of eID.

Hoe ze samenhangen

Zie itsme als de *sleutelhanger* waarmee je dagelijks dingen opent. Je eID-kaart is de *moedersleutel*: er is altijd één manier om itsme opnieuw op te starten als je telefoon weg is. eBox is de *brievenbus* die naast die sleutels hangt.

> ★ **Praktijk-aanrader.**
> Activeer itsme op één telefoon, en zorg dat je eID-kaart + pincode op een ándere plek liggen. Verlies van je telefoon ≠ verlies van je identiteit.

Wat itsme níet is

- Het is geen sociale media of betaal-app. Wie zegt dat je via itsme "een bedrag moet bevestigen aan de helpdesk" — dat is fraude.
- Het werkt nooit zonder dat *jij* de actie start. Je krijgt geen legitieme itsme-pop-up uit het niets.

MODULE 2 · THEORIE · NEDERLAND

NL — DigiD, MijnOverheid & betrouwbaarheidsniveau

In Nederland is DigiD de centrale sleutel. Eén account, drie betrouwbaarheidsniveaus en één Berichtenbox die op MijnOverheid hangt.

De drie betrouwbaarheidsniveaus

Niveau	Hoe werkt het?	Waar nodig?
Basis wachtwoord + sms	Inloggen met wachtwoord plus een sms-code.	Studiefinanciering, bibliotheek, sommige zorgverzekeraars.
Midden DigiD-app	Inloggen via de DigiD-app op je telefoon, met een eigen pincode.	Belastingdienst, gemeente, UWV — verreweg de meeste diensten.
Substantieel app + ID-check	Eenmalig je paspoort/rijbewijs scannen via de NFC-chip. Daarna inloggen via de app.	Zorgportalen (huisarts, ziekenhuis), notaris, sommige verzekeraars.

> ★ **Aanrader voor iedereen: minimaal Midden.**
> De DigiD-app is veiliger én sneller dan sms-codes. Substantieel is een extra avondje werk dat je later in dit boek (of bij je eerste zorgportaal) kunt activeren.

Wat is MijnOverheid?

MijnOverheid is je persoonlijke pagina bij de overheid: *Berichtenbox* (officiële post van overheidsdiensten), *Lopende zaken* (lopende aanvragen) en *Persoonlijke gegevens* (wat de overheid van je weet). Je logt in met je DigiD.

Wat DigiD níet is

- Geen betaal-app. De overheid vraagt nooit via DigiD om geld over te maken.
- Geen helpdesk-instrument. Je krijgt geen legitiem DigiD-verzoek zonder dat je zelf eerst hebt geklikt.
- Geen vervanger van je bank. Je bankgegevens zitten *niet* in DigiD.

MODULE 2 · AAN DE SLAG · BE 1/2

BE — itsme correct opzetten

1 Installeer itsme via de officiële store

App Store (iOS) of Play Store (Android). Zoek op `itsme` (uitgever: *Belgian Mobile ID*). Niet vanaf een link uit een mail of sms — alleen via de store zelf.

✓ Klaar als: de app geopend is en een welkomstscherm toont.

2 Kies een activatieweg

Optie A — via je bankkaart (KBC, Belfius, ING, Argenta, BNP Paribas Fortis, Crelan, Beobank): vul je rijksregisternummer en bankkaartgegevens in, bevestig met je kaartlezer of bank-app.

Optie B — via je eID-kaart: nodig is een kaartlezer plus pincode van je identiteitskaart. Werkt via de `eID Viewer` op je laptop.

✓ Klaar als: je in itsme een 5-cijferige itsme-code hebt aangemaakt.

3 Maak je itsme-code, maak 'm sterk

Vermijd `12345`, je geboortejaar of je huisnummer. Onthoud de code; itsme vergeet 'm niet voor je.

4 Test direct met een overheidsdienst

Ga naar `myminfin.be` (FOD Financiën), kies "Aanmelden met itsme". Je krijgt een push op je telefoon, vult je itsme-code in — en je bent binnen.

✓ Klaar als: je MyMinfin-startscherm opent zonder fout.



itsme-app — na succesvolle activatie. Vanaf nu kun je veilig inloggen, gegevens delen en tekenen bij overheid, banken en andere partners.

MODULE 2 · AAN DE SLAG · BE 2/2

BE — eBox aanzetten

Officiële post van FOD's, gemeente, pensioendienst en mutualiteit komt standaard nog op papier — tenzij je de eBox aanzet. Doe het één keer en je hebt voorgoed één plek waar alles binnenkomt, gratis.

1 Ga naar mybox.belgium.be

Typ het adres met de hand in je browser. Klik op "*Aanmelden*" en kies itsme (eenvoudigst).

2 Activeer eBox

Eerste bezoek: doorloop het stappenplan, accepteer de voorwaarden. Vink desgewenst aan dat je papieren post wil *stopzetten*.

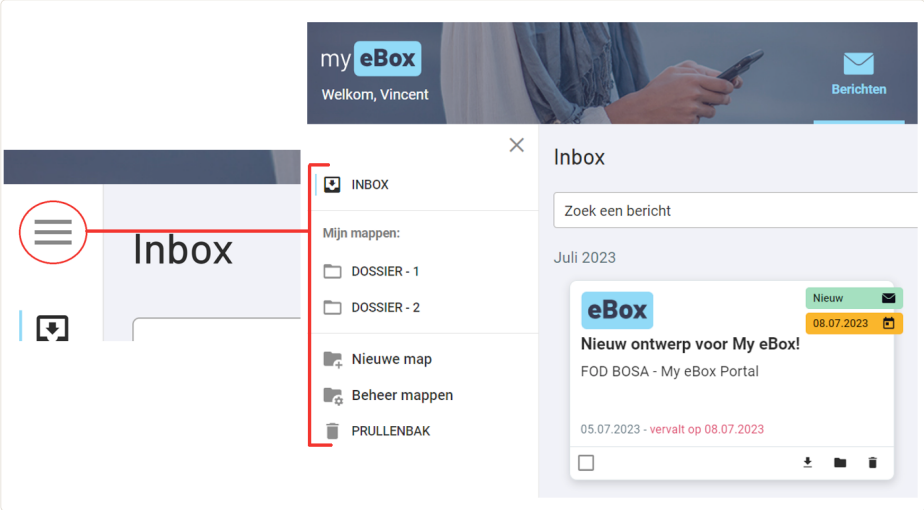
3 Stel notificaties in

Bij "*Mijn voorkeuren*" kies je een e-mailadres voor meldingen. Gebruik je hoofd-e-mail (uit Module 0). Zo mis je geen aanslagbiljet meer.

✓ Klaar als: eBox toont "Notificaties actief" met je e-mailadres.

4 Check een eerste echte brief

Open een van de berichten die er al staan (vaak een welkomstbrief van de FOD). Kijk hoe een echte eBox-melding eruit ziet — dat helpt je in Module 3 om nep van echt te onderscheiden.



mybox.belgium.be — je inbox met officiële post van FOD's en overheid. Het menu links bevat mappen om dossiers te ordenen.

Wat hoort niet in eBox?

- Geen post van privébedrijven (Telenet, Proximus, energie).
- Geen brieven van je bank.
- Geen "betaal nu of we sluiten je account" — dat is altijd fraude.

MODULE 2 · AAN DE SLAG · NL 1/2

NL — DigiD-app activeren

Heb je een DigiD met alleen wachtwoord + sms? Tijd om naar niveau Midden te gaan via de DigiD-app. Sneller, veiliger, en bijna overal vereist.

1 Installeer de DigiD-app via de officiële store

App Store (iOS) of Play Store (Android). Uitgever: *Logius / DUO / Ministerie van Binnenlandse Zaken*. Niet via een link uit een sms of mail.

✓ Klaar als: de app open is en om je DigiD vraagt.

2 Log eenmalig in en koppel

Vul je gebruikersnaam en wachtwoord in, ontvang een sms-code en bevestig. Je app vraagt om een pincode (5 cijfers) of biometrie.

3 Bevestig je app met een activatiecode per brief

DigiD stuurt een fysieke brief naar je geregistreerde adres (3–5 werkdagen). Daarin staat een activatiecode. Voer die in de app in.

✓ Klaar als: de app toont "Activatie gelukt" en je voortaan via de app inlogt.

4 Test op de Belastingdienst

Ga naar `belastingdienst.nl` → "*Inloggen Mijn Belastingdienst*". Kies "DigiD-app", scan de QR-code op je laptop met je telefoon, voer je pincode in.



DigiD-app — bevestigingsscherm na geslaagde activatie. Vanaf nu log je in via de app, met je eigen pincode of biometrie.

Optioneel — naar niveau Substantieel

In de DigiD-app: "*ID-check*". Scan de NFC-chip van je paspoort of rijbewijs. Duurt 5 minuten, geeft je toegang tot zorg- en notarisportalen. Niet verplicht — maar handig om vandaag al te doen als je hier toch zit.[23]

MODULE 2 · AAN DE SLAG · NL 2/2

NL — Berichtenbox en voorkeuren

De Berichtenbox in MijnOverheid is je officiële digitale brievenbus van de overheid. Brieven van de Belastingdienst, UWV, SVB, gemeente en RDW komen daar binnen. Eenmaal aangezet: één plek, één meldingsadres.

1 Log in op mijn.overheid.nl

Typ het adres met de hand in je browser. Kies "Inloggen met DigiD" en gebruik je app.

2 Activeer de Berichtenbox

Eerste bezoek: accepteer de gebruiksvoorwaarden. Klik "*Berichtenbox aanzetten*".

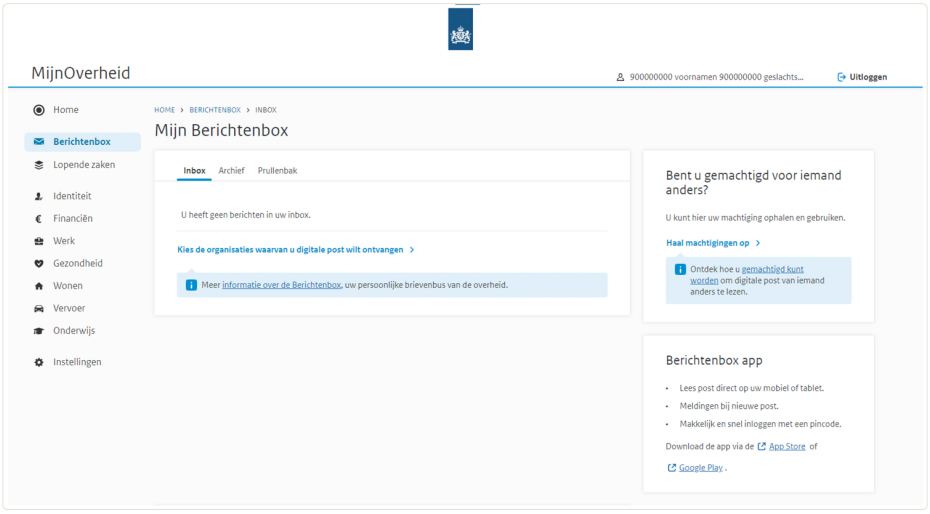
3 Stel notificatie-mail in

Bij "*Instellingen → E-mailadres*" vul je je hoofd-e-mail in. Bevestig via de link die je toegestuurd krijgt. Voortaan krijg je een e-mail als er nieuwe officiële post is.

✓ Klaar als: Berichtenbox toont "Notificaties actief".

4 Selecteer organisaties

Bij "*Organisaties*" kun je per organisatie kiezen of post digitaal of nog op papier komt. Aanrader: zet álles digitaal, behalve waar wettelijk papier nodig blijft.



mijn.overheid.nl — Berichtenbox. Bij eerste gebruik kies je welke organisaties (Belastingdienst, UWV, SVB, gemeente) digitaal post mogen sturen.

Wat hoort niet in MijnOverheid?

- Geen post van banken of energiebedrijven.
- Geen "betaal direct" of "je DigiD verloopt morgen" — dat is altijd fraude.
- Geen Marktplaats- of betaalverzoeken.

MODULE 2 · AAN DE SLAG · BE + NL

Telefoon verloren? Het noodplan.

Eén kwartier nu invullen voorkomt straks een week paniek. Onderstaand noodplan ligt straks dubbelgevouwen bij je paspoort.

BE — itsme & eID

1. **Bel Card Stop:** `078 170 170`. Blokkeer je bankkaart (waarmee itsme is geactiveerd).
2. **Bel je telefoonprovider:** blokkeer je simkaart.
3. **itsme deactiveren:** ga op een ander apparaat naar `my.itsme.be`, log in met eID-kaart + kaartlezer, kies "Deze app uitzetten".
4. **Heractiveer op nieuwe telefoon:** opnieuw via je bankkaart (kan pas na ontvangst nieuwe kaart) of direct via eID-kaart.

NL — DigiD

1. **Bel DigiD-helpdesk:** `088 123 65 55` (werkdagen 08:00–22:00).
2. **Bel je telefoonprovider:** blokkeer je simkaart.
3. **Activeer DigiD opnieuw:** op nieuwe telefoon de app installeren, je DigiD-gebruikersnaam + wachtwoord, daarna activatiecode per post (3–5 werkdagen).
4. **Tussentijds:** sms-niveau blijft werken voor basisdiensten.

Mijn noodgegevens — invullen met pen

MIJN RIJKSREGISTERNUMMER (BE) / BSN (NL)

MOBIELE PROVIDER + KLANTENNUMMER

CARD STOP (BE) — 078 170 170 / BANK (NL)

DIGID-HELPDESK (NL) — 088 123 65 55

PLEK VAN EID-KAART / PASPOORT THUIS

VERTROUWD PERSOON (NAAM + NUMMER)

> ✓ **Plak een kopie in de Noodkaart (pagina 95).**
> Dezelfde nummers, op één A5, op de koelkast. Modulekennis verdwijnt — een gele kaart op de koelkast blijft.

MODULE 2 · CONTROLELIJST

Klaar? Loop dit af.

Algemeen

- [ ] Mijn telefoon heeft een sterke schermcode (uit Module 0).
- [ ] Mijn eID-kaart (BE) of paspoort (NL) ligt niet in dezelfde tas als mijn telefoon.
- [ ] Mijn noodgegevens op pagina 25 zijn ingevuld met pen.

Alleen BE

- [ ] itsme is geactiveerd op precies één telefoon.
- [ ] Mijn itsme-code is geen geboortejaar, geen 12345, geen huisnummer.
- [ ] Ik heb één keer succesvol ingelogd op MyMinfin of een andere overheidsdienst.
- [ ] eBox staat aan, notificaties komen op mijn hoofd-e-mailadres binnen.
- [ ] Mijn pincode + pukcode van de eID-kaart liggen apart bewaard.

Alleen NL

- [ ] DigiD-app is geïnstalleerd en geactiveerd (brief is binnen, code ingevoerd).
- [ ] Ik heb één keer succesvol ingelogd op Mijn Belastingdienst via de app.
- [ ] Berichtenbox in MijnOverheid staat aan, notificatie-mail bevestigd.
- [ ] Mijn DigiD-wachtwoord staat in mijn wachtwoordkluis (Module 1).
- [ ] (Optioneel) ID-check uitgevoerd voor niveau Substantieel.

✂ Knip uit en hang op

Identiteits-spiekbriefje

- Geen onverwachte itsme- of DigiD-push? **Weiger.**
- Geen telefoongesprek met "een ambtenaar" die om codes vraagt. Ophangen.
- Bewaar eID/paspoort en telefoon op verschillende plekken.
- Bij verlies: **BE** 078 170 170 · **NL** 088 123 65 55.

MODULE 2 · TROUBLESHOOTING

Wat als...

? **...ik krijg een onverwachte itsme- of DigiD-push?**

Weiger. Geen enkele dienst stuurt een push zonder dat jij net een actie hebt gestart. Daarna: wijzig je wachtwoord, bel je bank (BE) of DigiD-helpdesk (NL).

? **...ik ben mijn itsme-code of DigiD-wachtwoord vergeten?**

BE

: in itsme zelf onderaan op "Wijzig itsme-code"; je moet opnieuw met je bankkaart of eID bevestigen.

NL: ga naar `digid.nl` en klik "Wachtwoord vergeten". Je krijgt een herstelbrief per post (5 werkdagen).

? **...mijn eID-kaart (BE) is verlopen of beschadigd?**

Vraag een nieuwe aan bij je gemeente. itsme blijft tijdelijk werken via je bankkaart-activatie. Vergeet niet je pincode + pukcode te bewaren.

? **...ik moet inloggen voor een ouder familielid?**

In Nederland: vraag een "machtiging" via `machtigen.digid.nl`. In België: itsme kan niet gedeeld worden, maar je kunt iemand machtigen via `selfservice.bosa.be`. Deel **nooit** de itsme-code of DigiD van een ander, ook niet van je ouder.

⚑ **...ik denk dat iemand zich voor mij heeft uitgegeven?**

Direct naar Module 8.

BE

: bel Card Stop én meld bij safeonweb.be. **NL**: bel DigiD-helpdesk én meld bij fraudehelpdesk.nl. Doe ook aangifte bij de politie — je hebt een proces-verbaal nodig voor de bank.

MODULE 2 · AFSLUITING

Module 2 — afgerond.

Je officiële digitale sleutel werkt, je weet hoe je hem opnieuw aanmaakt bij verlies, en je officiële post komt voortaan op één plek binnen. Bij elke nieuwe overheids- of zorgdienst hoef je vanaf nu geen nieuw account meer aan te maken — je logt in met itsme (BE) of DigiD (NL).

Samenvatting in drie zinnen

1. itsme of DigiD-app is je dagelijkse sleutel; eID of paspoort is je moedersleutel.
2. Geen onverwachte push betekent geen inlog — weiger en bel zelf.
3. eBox (BE) of Berichtenbox (NL) maakt officiële post controleerbaar en nep makkelijk herkenbaar.

Huishoudelijke routine vanaf nu

- Eén keer per maand de eBox / Berichtenbox openen, ook als je geen mail hebt gehad — soms hapert een notificatie.
- Bij elke nieuwe telefoon: itsme of DigiD opnieuw activeren *voordat* je de oude weggooit.
- Loopt je eID-kaart (BE) of paspoort (NL) binnen een jaar af? Zet het in je agenda — verlopen documenten blokkeren herstel.

Volgende stap → Module 3 — Phishing & scams herkennen. Nu je weet hoe een echt overheidsbericht eruit ziet, gaan we leren wat een nep bericht onthult — in zes patronen.

Welke stap kostte de meeste tijd? _____
Nog onduidelijkheden om in Module 3 mee te nemen? _____

MODULE 03 · PHISHING

~ 90 MINUTEN · 14 PAGINA'S

03

Phishing & scams herkennen

Niet alle e-mails zijn echt. Niet alle telefoontjes zijn van je bank. Zes patronen waar bijna alle oplichting in past — en de blik om ze te zien.

WAT GA JE LEREN?

- De zes scampatronen: pakket, betaling, helpdesk, autoriteit, romantiek, urgentie.
- Hoe je in vijf seconden een e-mail of sms checkt.
- Wat te doen als je tóch geklikt hebt.

WAT HEB JE STRAKS?

Een spiekbriefje op je koelkast met de rode vlaggen, en een ingerichte "meld phishing"-route in je e-mailprogramma.

GESCHATTE TIJD

90 minuten

WAT HEB JE NODIG?

- Je e-mailprogramma open
- Je telefoon (sms en WhatsApp)
- 10 minuten met je partner / huisgenoot

Cases uit BE/NL: namaak-Bpost & PostNL, "KBC fraudedesk", Belastingdienst-teruggave, valse Belfius-sms.

MODULE 3 · INLEIDING

Waarom phishing nog steeds werkt

Phishing is geen technische val. Het is een psychologische val. Aanvallers gokken niet op een fout in jouw browser — ze gokken op vermoeidheid, haast en gezag. Wie je vandaag belt of mailt om "iets dringend op te lossen", werkt met dezelfde drie hendels: tijdsdruk, autoriteit en angst.

Wat we vandaag doen

- De zes patronen leren herkennen waarin bijna alle scams passen.
- Een 5-seconden-check oefenen die altijd werkt.
- Bij elke grote dienst leren waar je phishing meldt.
- Een script noteren voor als je tóch geklikt hebt.

De drie hendels van een scam

1. **Tijdsdruk** — "binnen 24 uur", "vandaag nog".
2. **Autoriteit** — "namens de Belastingdienst", "de bank".
3. **Angst** — "anders wordt je account geblokkeerd".

Eén van de drie is genoeg om mensen te laten klikken. Twee tegelijk is al een sterk signaal dat er iets niet klopt.

> ★ **De gouden regel van deze module.**
> Echte instanties laten je *nooit* klikken op een link in een mail of sms om in te loggen. Wil je controleren of een bericht klopt? Sluit het, open je browser, typ het officiële adres met de hand en log via je eigen weg in.

Casus

Anita (62), Mechelen. Krijgt een sms: "*Uw Bpost-pakket kan niet bezorgd worden, betaal €1,82 voor herbezorging*". €1,82 voelt onschuldig. Ze klikt, vult haar bankkaart in op een namaakpagina. Die nacht: drie afschrijvingen van €350 via een nieuwe digitale wallet. — Eén bedrag onderaan een link checken kost vijf seconden. Drie weken bankgeschil voorkomen.

MODULE 3 · THEORIE · 1 VAN 2

De zes scampatronen

Bijna elke scam past in één van deze zes vakjes. Herken het vakje, en het bericht verliest zijn kracht.

Patroon	Wat het belooft / dreigt	Voorbeelden in BE/NL
1. Pakket	Een pakje dat vastzit aan de douane, een herbezorging die "betaald" moet worden, een levering die niet door kan gaan.	Nep-Bpost, nep-PostNL, nep-DHL, nep-Coolblue.
2. Betaling	Een vermoede ongeoorloofde transactie, een geblokkeerde kaart, een verzoek om "te bevestigen".	Nep-Belfius-sms, nep-KBC-fraudedesk, valse Tikkie, valse Payconiq.
3. Helpdesk	Iemand belt of mailt namens Microsoft / Apple / "de bank" / je internetprovider om "een probleem op te lossen".	Microsoft Support, Apple-fraude, "Proximus heeft een storing", "Ziggo systeem".
4. Autoriteit	Een overheid die geld teruggeeft, een boete oplegt, of dreigt met een proces.	Belastingdienst-teruggave, FOD Financiën, politie-mail, CJIB.
5. Romantiek / vertrouwen	Een nieuw "contact" dat na weken vertrouwen geld vraagt, of een familielid dat plots een nieuw nummer heeft en hulp nodig heeft.	"WhatsApp-mama", datingfraude, militair op missie.
6. Urgentie	Een account dat verloopt, een storing, een actie die *nu* moet plaatsvinden.	"Je DigiD verloopt", "iCloud vol — verlies je foto's", Marktplaats-veilig betalen.

> **Combinaties bestaan.**
> Veel berichten combineren patronen — een nep-bank-sms (Betaling) met een tijdslimiet (Urgentie). Twee patronen tegelijk = altijd dubbel controleren.

MODULE 3 · THEORIE · 2 VAN 2

De 5-seconden-check

Vijf vragen, drie tellen elk. Werkt voor mail, sms, WhatsApp en telefoongesprek. Als één antwoord niet klopt: stoppen.

1 **Was ik dit verwachten?**
Heb je écht een pakket besteld? Doe je nu écht een aangifte? Zonder context wachten — fraudeurs werken op timing en geluk.

2 **Klopt de afzender — heel precies?**
Niet alleen de weergavenaam. Het volledige adres of nummer. `bpost.be` is echt; `bpost-be.com` is nep. `+32 478 …` is een gewoon gsm-nummer, niet de bank.

3 **Welk patroon herken ik?**
Pakket, betaling, helpdesk, autoriteit, romantiek, urgentie — of een combinatie. Het herkennen alleen al verlaagt de spanning.

4 **Word ik onder druk gezet?**
"Binnen 24 uur", "klik nu", "anders…". Echte instanties geven je altijd tijd. Druk is bijna altijd een rode vlag.

5 **Wat als ik dit zou negeren?**
Bij echt belangrijke zaken komt er een tweede kanaal — een brief, een telefoontje, een vermelding in je eBox / Berichtenbox. Bij een scam is dat ene kanaal alles.

✂ Knip uit en hang op

Spiekbriefje: 5-seconden-check

- **Verwacht?** Klopt de aanleiding?
- **Afzender precies?** Volledige adres / nummer.
- **Welk patroon?** Pakket / betaling / helpdesk / autoriteit / romantiek / urgentie.
- **Druk?** Tijdslimiet of dreiging?
- **Negeren?** Kom je elders hetzelfde tegen?

★ **Twijfel? Wacht een uur.**
Geen enkel echt verzoek wordt slechter binnen een uur. Een scam loopt meestal binnen een uur dood — de aanvaller is alweer verder.

MODULE 3 · PATROON 1 VAN 6 · PAKKET

"Uw pakket kan niet worden bezorgd"

Veruit het meest voorkomende type sms-scam in BE en NL. Werkt omdat iedereéén weleens iets verwacht — Bol, Coolblue, AliExpress, Bpost, PostNL.

ECHT VOORBEELD · SMS BE / NL

```
Van: +33 6 24 88 17 92
Aan: jij — 14:07

Bpost: uw pakje is geblokkeerd in
het sorteercentrum wegens onvoldoende
adresgegevens. Bevestig hier:
hxxps://bpost-tracking-be[.]com/r/8f2

— Reageer binnen 24u om vertraging
te vermijden.
```

Drie rode vlaggen.

1. **Afzender klopt niet.** Bpost stuurt geen sms vanaf een Frans mobielnummer. Officieel: alleen `bpost.be`-mailing of de eigen Bpost-app.
2. **Linkdomein wijkt af.** Het echte domein is `bpost.be`, niet `bpost-tracking-be.com`. Een streepje of extra woord = altijd verdacht.
3. **Tijdsdruk.** "Binnen 24u" is patroon "urgentie" — opgeplakt om je te laten klikken voor je nadenkt.

Hoe controleer je een pakket veilig?

1. Open de app of website van de verzender (Bol, Coolblue, AliExpress) zelf.
2. Klik daar door naar "track and trace". Daar staat de échte status.
3. Bpost (BE): `bpost.be/track`. PostNL (NL): `postnl.nl/tracktrace`. Met de hand intypen.

> ¡ **Echte Bpost / PostNL vraagt niet om je bankgegevens.**
> Voor een kleine herbezorging of douanetax bestaat dat — maar betalingen lopen altijd via de officiële app, niet via een sms-link.

MODULE 3 · PATROON 2 VAN 6 · BETALING

"Verdachte transactie — bevestig"

Het meest schadelijke patroon. Speelt direct op angst voor verlies van geld. Vaak gevolgd door een telefoontje van "de fraude-afdeling".

ECHT VOORBEELD · SMS BE

```
Van: BELFIUS
Aan: jij — 22:41

Belfius — Wij detecteerden een
ongeoorloofde overschrijving van
EUR 749,00 op uw rekening. Indien u
deze niet erkende: hxxps://belfius-
secure[.]eu/blokkeer

Onze fraudedienst belt u op 0800-…
```

Drie rode vlaggen.

1. **Afzender "BELFIUS" als sms-naam zegt niets.** Iedereen kan een sms versturen met een willekeurige naam (sms-spoofing). Het beschermt je niet.
2. **Linkdomein.** Echt: `belfius.be`. Hier: `belfius-secure.eu` — nep.
3. **"Onze fraudedienst belt u op".** Hier wordt fase 2 aangekondigd: een vervolggesprek waarin om codes of overschrijvingen wordt gevraagd. **Geen enkele bank doet dat zo.**

Wat doet je bank wél?

- Een melding *in de eigen bank-app* ("Bevestig deze betaling met je app").
- Een blokkade van de kaart, met instructie om **zelf** Card Stop (BE, 078 170 170) of het bekende noodnummer (NL) te bellen.
- **Nooit** een link in een sms naar een loginpagina.
- **Nooit** "lees uw 2FA-code voor".

> ⚑ **Bel zelf het noodnummer terug.**
> Twijfel je over een belletje "van de bank"? Hang op. Bel het nummer van de achterkant van je bankkaart of het nummer dat je in Module 0 hebt opgeschreven — niet het nummer dat door de beller wordt genoemd.

MODULE 3 · PATROON 3 VAN 6 · HELPDESK

"Wij hebben een probleem op uw computer ontdekt"

Speelt vaak per telefoon, soms in Engels met accent, soms in vlot Nederlands. De beller wil "samen even meekijken" via een afstandbedienings-programma.

ECHT VOORBEELD · TELEFOONTJE BE / NL

```
Beller: "Microsoft Support" — onbekend nummer

"Goedemiddag, u spreekt met Mark
van Microsoft. Onze systemen
detecteren al drie dagen een
virusinfectie op uw computer.
Heeft u even tijd? Dan los ik het
voor u op.

Kunt u op uw toetsenbord op de
Windows-toets + R drukken? En dan
intypen: anydesk.com..."
```

Drie rode vlaggen.

1. **Microsoft / Apple bellen je niet.** Onmogelijk. Ze hebben je nummer niet, en zelfs als ze het hadden: het is hun businessmodel niet.
2. **"Op afstand meekijken"** via AnyDesk, TeamViewer of Quick Assist. Hierdoor geef je iemand volledige controle over je computer.
3. **Druk.** "Drie dagen", "nu meteen", "anders volledige crash". Klassiek patroon urgentie + autoriteit.

Standaardantwoord — hardop oefenen

"*Dank u, ik bel u terug via het officiële nummer.*" En ophangen. Geen enkele echte helpdesk neemt je dat kwalijk.

Andere variant: "uw internet ligt zo plat"

Belt iemand namens Proximus, Telenet, Orange, KPN, Ziggo of Odido en zegt dat er "een storing aankomt"? Vraag een dossiernummer, hang op, bel je eigen provider terug via het nummer op je factuur.

> ! **Familieoverleg-tip.**
> Spreek met je ouders, schoonouders en partner af: "*als iemand ons belt en zegt dat hij van Microsoft, Apple of de bank is, hangen we altijd op.*" Eén afspraak, hele jaar veiliger.

MODULE 3 · PATROON 4 VAN 6 · AUTORITEIT

"U krijgt €428 terug. Bevestig uw rekening."

Een teruggave die om jouw bankgegevens vraagt. Speelt op het gunstige gevoel van geld terugkrijgen — verlaagt je waakzaamheid.

ECHT VOORBEELD · E-MAIL NL

```
Van: Belastingdienst <return@mijn-belasting-dienst[.]nl>
Onderwerp: Uitbetaling teruggave 2024 – actie vereist

Geachte heer/mevrouw,

Wij hebben uw aangifte verwerkt en
constateerden een teruggave van
EUR 428,17. Om deze uit te keren
verzoeken wij u uw bankrekening te
bevestigen via onderstaande beveiligde
omgeving:

[ Bevestig rekening – IDIN ]

Reageer voor 31 mei, anders vervalt
de teruggave.
```

Drie rode vlaggen.

1. **Domein.** Echt: `belastingdienst.nl`. Nep: `mijn-belasting-dienst.nl`. Streepjes en woordvolgorde altijd nakijken.
2. **De Belastingdienst kent je rekeningnummer al.** Anders kan het de aangifte niet hebben verwerkt. Een verzoek om "bevestiging" via mail is onnodig en dus altijd verdacht.
3. **Officiële post komt in je Berichtenbox** op mijn.overheid.nl (NL) of eBox (BE). Nooit per mail met een knop.

Hoe je een teruggave écht ziet

- **NL:** log met DigiD-app in op `mijn.belastingdienst.nl`. Daar staat eventueel een teruggave.
- **BE:** via itsme op `myminfin.be` onder "Mijn fiscale dossier".
- Wijzigen van rekeningnummer voor uitbetaling kan alleen via diezelfde eigen omgeving — niet via een link uit een mail.

> ¡ **Politie en CJIB bellen je niet vooraf.**
> Een boete is altijd schriftelijk, met een dossiernummer dat je op `cjib.nl` (NL) of via je gemeente (BE) zelf kunt opzoeken. Wie aan de telefoon "een aanhouding" aankondigt en "een borgsom" vraagt: scam.

MODULE 3 · PATROON 5 VAN 6 · ROMANTIEK & VERTROUWEN

"Mam, dit is mijn nieuwe nummer."

Werkt op familieliefde en lange-termijn-vertrouwen. Soms in een paar uur gespeeld (WhatsApp-mama), soms over maanden opgebouwd (datingfraude).

ECHT VOORBEELD · WHATSAPP BE / NL

```
Onbekend nummer +31 6 …
19:08

Hoi mama, mijn telefoon is gevallen
en mijn simkaart werkt niet meer.
Dit is mijn tijdelijke nummer.
Sla je dit op?

(20:14) Mam, ik moet vandaag nog
een rekening betalen anders krijg ik
een boete. Kan jij dit even voor me
voorschieten? IBAN: NL12 RABO ...

Ik betaal je morgen terug 💞
```

Drie rode vlaggen.

1. **Nieuw nummer + dringend.** Je zoon/dochter zou normaal eerst bellen. Tekstjes zijn makkelijk uit naam van iemand anders te sturen.
2. **Vraag om geld voor te schieten.** De typische tweede stap. Zonder die stap is er geen scam.
3. **Onbekende IBAN.** De rekening die om geld vraagt is bijna nooit een Belgische of bekende Nederlandse rekening van je kind. Vaak een doorvoerrekening uit Litouwen, Bulgarije, Roemenië.

Het tegengif

1. **Bel het oude nummer.** Werkt 'm? Mooi — dan is de appende persoon niet je kind.
2. **Stel een vraag die alleen je kind kan beantwoorden.** "Waar gingen we vorig jaar Pasen heen?" Geen "wat is mijn naam".
3. **Maak vooraf een familie-codewoord.** Eén ongebruikelijk woord dat alleen jullie kennen. Zonder dat woord: geen geld.

Datingvariant

Iemand op een datingsite die nooit kan videobellen, op missie zit met het leger, of in het buitenland vastzit en geld nodig heeft om "thuis te komen": scam. Eén vraag stopt 't: "*Kunnen we elkaar morgen ontmoeten?*" Het antwoord is altijd nee.

> ! **Schaam je niet — meld het.**
> Datingfraude treft duizenden mensen per jaar in BE en NL, ook hoogopgeleiden. Een melding bij safeonweb.be of fraudehelpdesk.nl helpt anderen.

MODULE 3 · PATROON 6 VAN 6 · URGENTIE

"Uw account verloopt binnen 24 uur"

Het mengsmeer dat overal doorheen loopt — vaak het laatste duwtje bij een van de andere patronen. Maar bestaat ook op zichzelf.

ECHT VOORBEELD · E-MAIL BE / NL

```
Van: Apple Support <noreply@apple-id-security[.]com>
Onderwerp: Laatste waarschuwing – uw Apple-ID

Beste gebruiker,

Wij hebben verdachte aanmelding
gedetecteerd vanuit Lagos, Nigeria.
Uw Apple-ID wordt binnen 24 uur
gedeactiveerd. Bevestig uw account
om deactivatie te voorkomen:

[ Bevestig Apple-ID ]
```

Drie rode vlaggen.

1. **Domein.** Apple-mails komen alleen van `@apple.com` of subdomeinen daarvan. Nooit van `apple-id-security.com`.
2. **"Bevestig uw account"-knop.** Apple, Google, Facebook en je bank vragen je *nooit* via een mailknop in te loggen. Wel: "ga zelf naar onze website / app".
3. **Algemene aanhef.** "Beste gebruiker", "Geachte klant". Echte aanbieders schrijven je naam.

Variant: Marktplaats / Vinted / 2dehands "veilig betalen"

Je verkoopt iets, de koper stuurt een link voor "veilig betalen" via een payment service provider. Op die nepsite vul je je bankgegevens in om "de betaling te ontvangen". In werkelijkheid is dat een betalingsopdracht áf van jouw rekening.

- Marktplaats, Vinted en 2dehands sturen **nooit** links in privéchats om te betalen of te ontvangen.
- Verdacht? Houd communicatie binnen het platform en gebruik alleen de officieel ondersteunde betaalmethodes.

> ★ **De algemene anti-urgentie-regel.**
> Als de tijdsdruk wegvalt, blijft er meestal geen reden over om in te gaan op het verzoek.
> *Hou een uur de telefoon weg en kijk wat er overblijft.*

MODULE 3 · ALS JE GEKLIKT HEBT

Wel geklikt. Wat nu?

Iedereen klikt weleens. Geen schaamte — wel snelheid. Hoe sneller je reageert, hoe meer schade je voorkomt. Loop dit script af in deze volgorde.

1 **Heb je alleen geklikt? Dat is meestal nog oké.**
Geen wachtwoord ingevuld, geen bestand geopend, geen code gegeven? Sluit het tabblad, verwijder de mail. Eventueel een virusscan op je laptop draaien — maar paniek is niet nodig.

2 **Heb je een wachtwoord ingevuld? Direct wijzigen.**
Ga naar de echte website van die dienst — typ het adres met de hand — en wijzig het wachtwoord. Heb je hetzelfde wachtwoord ook ergens anders gebruikt? Daar ook wijzigen. (Met je kluis uit Module 1 gaat dat snel.)

3 **Heb je je bankgegevens ingevuld? Bel je bank — nu.**
BE: Card Stop — 078 170 170 — blokkeert direct. Bel daarna je eigen bank-noodnummer voor terugboekingen.

NL: bel het noodnummer van je bank dat je in Module 0 hebt opgeschreven. ABN AMRO, ING, Rabobank en bunq hebben allemaal 24/7-bereik.

4 **Heb je een 2FA-code voorgelezen? Stop alles.**
Direct naar Module 8 (Incident response). Iemand probeert nu in jouw account in te loggen. Wijzig wachtwoord, log alle sessies uit, bel je bank.

5 **Meld het — voor jezelf en voor anderen.**
BE: stuur de mail of sms door naar `verdacht@safeonweb.be`. Niet beantwoorden — alleen doorsturen.

NL: meld bij `fraudehelpdesk.nl`. Voor sms: stuur door naar `7726` (gratis).

MODULE 3 · INRICHTEN

"Phishing melden" in je e-mail

Met één klik laten weten dat een mail nep is — je e-mailprogramma leert ervan, en je beschermt anderen. Het zit overal, maar nooit op dezelfde plek.

1 **Gmail (web of app)**
Open het bericht → menuknop (⋮) rechtsboven → "*Phishing melden*". Niet alleen "Spam" — phishing is een aparte categorie.

2 **Outlook / Hotmail (web)**
Open bericht → menuknop → "*Junk → Phishing melden*". Outlook stuurt het rapport door naar Microsofts veiligheidsteam.

3 **Apple Mail (iPhone of Mac)**
Apple Mail heeft geen ingebouwde "phishing"-knop. Stuur de mail door naar `reportphishing@apwg.org` (anti-phishing working group) of naar het officiële meldpunt van je land.

4 **Sms (Android & iPhone)**
Druk lang op het bericht → "*Doorsturen*". Stuur naar 7726 (NL, gratis) of naar `verdacht@safeonweb.be` (BE, via mail). Daarna: bericht verwijderen.

Mijn meldpunten — invullen

BE — MELDPUNT E-MAIL

NL — MELDPUNT SMS

BE — MELDPUNT WEBSITE

NL — MELDPUNT WEBSITE

★ **Eén keer in de week even kijken.**
Zet een wekelijkse herinnering op zondagmorgen: "spamfolder en phishingmap legen". Voorkomt dat een echte mail per ongeluk verdwijnt tussen de troep.

MODULE 3 · CONTROLELIJST

Klaar? Loop dit af.

- [ ] Ik kan de zes scampatronen uit mijn hoofd noemen.
- [ ] De 5-seconden-check ken ik (of hangt aan de koelkast).
- [ ] Ik heb één keer een verdachte mail of sms gemeld bij safeonweb.be (BE) of 7726 / fraudehelpdesk.nl (NL).
- [ ] "Phishing melden" werkt in mijn e-mailprogramma (Gmail / Outlook / Apple Mail).
- [ ] Mijn meldpunten staan op pagina 40 ingevuld.
- [ ] Ik heb met mijn partner of huisgenoot afgesproken: bij twijfel — ophangen en samen kijken.
- [ ] Met mijn ouders / familie heb ik het familie-codewoord afgesproken (als toepasselijk).

✂ Knip uit en hang op

Phishing-spiekbriefje · 5-seconden-check

- **Verwacht?** — heb ik hier om gevraagd?
- **Afzender exact?** — heel domein/nummer.
- **Welk patroon?** — pakket / betaling / helpdesk / autoriteit / romantiek / urgentie.
- **Druk?** — tijdslimiet of dreiging.
- **Negeren?** — wat als ik dit links laat liggen?

Geklikt? Bel direct je bank · Wijzig je wachtwoord · Meld bij safeonweb.be (BE) of fraudehelpdesk.nl (NL).

MODULE 3 · TROUBLESHOOTING & AFSLUITING

Wat als...& afsluiting

? ...ik twijfel of een mail nep is?
Open een nieuw browser-tabblad, typ zelf het officiële adres in, log in via je eigen weg. Staat het bericht óók daar? Echt. Niet? Nep.

? ...ik denk dat een ouder familielid gepakt is?
Bel ze, ga langs. Loop samen het script van pagina 39 af. Schaamte blokkeert vaker dan de scam zelf — toon begrip, niet boosheid.

? ...de scam komt via WhatsApp van een echt contact?
Vermoedelijk is het account van die contact gehackt. Bel ze (geen WhatsApp) en waarschuw ze. Vraag ze hun WhatsApp-tweestapsverificatie aan te zetten (Module 1, principe).

Samenvatting in drie zinnen

1. Bijna elke scam past in zes patronen — kennen verkort je reactietijd.
2. De 5-seconden-check (verwacht? afzender? patroon? druk? negeerbaar?) werkt overal.
3. Echte instanties laten je nooit via een mailknop inloggen. Punt.

Huishoudelijke routine vanaf nu

- Bij elke nieuwe scam-trend in het nieuws: 5 minuten met je gezin bespreken aan tafel.
- Eén keer per maand spam- en phishingmap legen.
- Bij twijfel: ophangen, een uur wachten, dan terugbellen via een nummer dat je *zelf* hebt opgezocht.

Volgende stap → Module 4 — Bankieren, betalen & oplichting. Nu je nep-bankberichten herkent, gaan we ervoor zorgen dat je bank zelf klaarstaat als er wel iets misgaat.

MODULE 04 · BANKIEREN

~ 60 MINUTEN · 10 PAGINA'S



Bankieren, betalen & oplichting

Beperk de schade van een fout. Limieten omlaag, meldingen aan, en een vast antwoord paraat als "de bank" belt.

WAT GA JE LEREN?

- Welke limieten verstandig zijn voor een gezinsrekening.
- Hoe je betaalmeldingen en kaartmeldingen aanzet.
- Wat je bank wél en níet doet — en welke zin altijd verdacht is.

WAT HEB JE STRAKS?

Aangepaste daglimieten, ingestelde meldingen voor uitgaande betalingen, en de juiste noodnummers van je bank op de Noodkaart.

GESCHATTE TIJD

60 minuten

WAT HEB JE NODIG?

- Je bankapp (BE: KBC, Belfius, ING België, Argenta — NL: ABN AMRO, ING, Rabobank, bunq)
- Bankkaart bij de hand

We laten zien hoe limieten en meldingen heten bij de meest gebruikte banken in BE en NL.

MODULE 4 · INLEIDING

Beperk de schade vóór er iets gebeurt

De voorgaande modules gingen over de deuren dicht houden. Deze module gaat over wat er kan gebeuren als iemand er tóch doorheen komt. Drie kleine handelingen in je bankapp zorgen ervoor dat een fout van een uur niet een schade van een maand wordt.

Wat we vandaag doen

- Je daglimieten verlagen naar wat je in een normale week écht uitgeeft.
- Meldingen aanzetten zodat je elke uitgaande betaling ziet.
- Een witte lijst van vertrouwde rekeningen instellen waar dat kan.
- Een vast antwoord oefenen voor als "de bank" belt.

Waarom werkt dit?

Fraude is in 90% van de gevallen één van twee dingen: een onomkeerbare overschrijving naar een buitenlandse rekening, of een reeks online aankopen met je kaart. Limieten en meldingen pakken precies die twee aan.

De bank vergoedt veel — maar lang niet alles. Eigen schuld door "grove nalatigheid" (codes gedeeld, niet snel gemeld) is vaak een reden tot weigeren.

> ¡ **Een limiet is niet alleen tegen fraude.**
> Het is ook een stop op een paniek-overschrijving die jij zelf doet onder druk van een telefoontje. Lagere limieten = meer tijd om na te denken.

Casus

Joris (54), Antwerpen. Krijgt een telefoontje van "de KBC fraudedienst" die zegt dat zijn rekening "geblokkeerd moet worden via een overboeking naar een veilige rekening". Joris werkt mee, twee overschrijvingen van €4.500 vertrekken. Probleem: zijn daglimiet stond op €10.000 — standaard bij veel banken. Met een limiet van €1.500 was de schade beperkt geweest. — Limieten zetten kost 4 minuten.

MODULE 4 · THEORIE-LIGHT

Wat je bank wél en niet doet

Drie zinnen die de helft van alle bankfraude voorkomen — leer ze uit je hoofd.

Wat je bank wél doet.
(1) Een melding sturen *in de eigen app* ("Bevestig deze transactie"). (2) Je kaart blokkeren bij vermoede fraude, en jou per brief of in-app vragen zelf contact op te nemen. (3) Vragen om identificatie via de eigen bank-app, niet via een sms-link.

Wat je bank nooit doet.
(1) Bellen en vragen om een 2FA-code, app-pincode of digipass-code voor te lezen. (2) Vragen om "voor de zekerheid" geld over te maken naar een "veilige rekening". (3) Toegang vragen tot je computer via AnyDesk, TeamViewer of Quick Assist.

Wat je bank misschien doet — afhankelijk van bank en situatie.
Bellen om te verifiëren of jij een bepaalde betaling hebt gedaan ("Heeft u net €230 overgemaakt aan…?"). Antwoord altijd: "Ik bel u zelf terug via het nummer op mijn kaart." Geen echte fraude-medewerker neemt dat kwalijk.

Sterke klantauthenticatie (SCA)

Sinds 2019 is "Strong Customer Authentication" verplicht in de EU. Concreet betekent dat: bij elke betaling boven een drempelbedrag (meestal €30) moet je actief bevestigen via je bank-app, itsme, of digipass. Dat is een goede ontwikkeling — maar het maakt jouw bevestigingsactie cruciaal. Wat jij bevestigt, gaat door.

Lees vóór bevestigen.
Bij elke bevestiging in je bank-app of itsme zie je het *bedrag* en de *begunstigde*. Lees ze. Klopt het niet? Weigeren. Dat ene moment is de hele bescherming.

MODULE 4 · AAN DE SLAG · STAP 1 VAN 4

Stap 1 — Daglimieten verlagen

Hoeveel geef je in een normale week écht uit? Honderd euro? Driehonderd? Zet je daglimiet daar net boven. Doe je af en toe een grote aankoop, dan verhoog je 'm tijdelijk voor één dag.

Drie limieten om aan te kijken

1. **Overschrijvingen per dag** — vaak standaard €5.000–€10.000. Aanrader: €1.000–€2.000.
2. **Kaartbetalingen / online aankopen per dag** — vaak standaard €2.500. Aanrader: €500–€1.000.
3. **Geldopname aan automaat per dag** — vaak standaard €1.250. Aanrader: €250–€500.

Waar vind je het — per bank

Bank	Pad in app (juni 2026)
KBC (BE)	`Mijn KBC → Beveiliging → Limieten`
Belfius (BE)	`Profiel → Veiligheid → Limieten beheren`
ING België	`Instellingen → Mijn kaarten → Limieten`
Argenta (BE)	`Meer → Veiligheid → Limieten`
ABN AMRO (NL)	`Profiel → Veiligheid → Daglimieten`
ING (NL)	`Mijn instellingen → Pas → Limieten`
Rabobank (NL)	`Service → Pas en pinnen → Pasinstellingen`
bunq (NL)	`Kaart → tik op kaart → Limieten`

Mijn limieten — invulblok

MIJN BANK(EN)

DAGLIMIET KAART / ONLINE (NIEUW)

DAGLIMIET OVERSCHRIJVINGEN (NIEUW)

DAGLIMIET AUTOMAAT (NIEUW)

> ! **Wachttijd na verhoging.**
> Bij veel banken duurt een verhoging 24–48 uur voor hij actief wordt — een goede beveiliging. Dus plan je grote aankoop een dag vooruit.

MODULE 4 · AAN DE SLAG · STAP 2 VAN 4

Stap 2 — Meldingen aanzetten

Een push of e-mail bij elke uitgaande betaling. Klinkt opdringerig — went binnen een week. Als er iets vreemds gebeurt, weet je het binnen seconden, niet bij het volgende rekeningoverzicht.

1 **Push-meldingen voor uitgaande betalingen**
Zet in je bank-app de meldingen aan voor: (a) elke afschrijving boven een drempelbedrag (bv. €25), (b) elke betaling buiten je land, (c) elke nieuw aangemaakte begunstigde.

2 **Kaartmeldingen (debet- en kredietkaart)**
Idem voor je bankkaart en eventuele kredietkaart. Zet er een melding op voor elke online aankoop, niet alleen offline.

3 **Een (klein) bedrag op spaarrekening apart zetten**
Zet je spaarrekening op een aparte rekening die *niet* standaard zichtbaar is in je app, of die alleen via een extra bevestiging benaderbaar is. Bij KBC, Belfius en ABN AMRO kan dat met één klik. Geld dat moeilijker bereikbaar is, is moeilijker te stelen.

4 **Contactloos uit als je 'm bijna nooit gebruikt**
Contactloos betalen is veilig — maar als je 'm zelden gebruikt, schakel 'm uit in de app. Eén knop, hele functie weg, weer aan wanneer je hem nodig hebt.

Mijn meldingen — checklist

- [ ] Push aan voor uitgaande betalingen boven €25.
- [ ] Push aan voor buitenlandse betalingen.
- [ ] Push aan voor nieuwe begunstigde.
- [ ] Kaartmeldingen aan voor online aankopen.
- [ ] Spaarrekening minder zichtbaar / met extra bevestiging.

MODULE 4 · AAN DE SLAG · STAP 3 VAN 4

Stap 3 — Vertrouwde begunstigden

Veel banken laten je rekeningen als *vertrouwd* markeren. Naar die rekeningen mag je vrijuit overschrijven; naar nieuwe rekeningen geldt automatisch een extra bevestiging of een wachttijd van enkele uren.

Wat zet je op de witte lijst?

- Je eigen andere rekeningen (spaar, beleggingen, partner).
- Je vaste rekening voor huur of hypotheek.
- Je vaste leveranciers (kinderopvang, energie, telecom).
- Familieleden waar je regelmatig naar overschrijft.

Wat zet je er *niet* op?

- Webshops en eenmalige aankopen.
- Tikkies en betaalverzoeken — die werken al via een andere route.
- Zakelijke klanten (voor zelfstandigen — zie Module 9).

> ★ **Praktijk: een avond vrijmaken.**
> Loop één keer je laatste drie bankafschriften door. Iedere terugkerende ontvanger met dezelfde IBAN gaat op de witte lijst. Voortaan vraagt je bank alleen extra bevestiging bij nieuwe namen — precies waar het ertoe doet.

Voor wie het kan: een vaste cooldown op nieuwe begunstigden

Sommige banken (bunq, ABN AMRO, KBC) laten je een vaste wachttijd instellen voor overschrijvingen naar nieuwe rekeningen (bv. 4 of 24 uur). Voor een huishouden is 4 uur al gouden — fraude wordt vaak in <30 minuten uitgevoerd; je hebt na 4 uur al gemerkt dat er iets niet klopt.

Mijn witte lijst — top-5 om in te stellen

1. _____
2. _____
3. _____
4. _____
5. _____

MODULE 4 · AAN DE SLAG · STAP 4 VAN 4

Stap 4 — Het telefoonscript

Het meest schadelijke type bankfraude in BE en NL is "bankhelpdesk-fraude": iemand belt en doet zich voor als medewerker van de fraude-afdeling. Eén standaardantwoord pareert ze allemaal. Oefen 't hardop.

ECHT VOORBEELD · TELEFOONGESPREK BE / NL

```
Beller (kalme, vriendelijke stem):

"Goedemiddag mevrouw, u spreekt met
Tim van de fraude-afdeling van uw
bank. Wij detecteren op dit moment
een verdachte transactie van EUR
1.470 vanuit Roemenië. Om uw geld
te beschermen moet ik u helpen het
over te boeken naar een veilige
rekening op uw eigen naam..."
```

Vier rode vlaggen.

1. De bank belt nooit met de vraag om geld over te boeken.
2. "Veilige rekening op uw eigen naam" bestaat niet.
3. Druk en tijd ("op dit moment", "nu").
4. Vraag om je 2FA-code of digipass-code voor te lezen.

Jouw vaste antwoord — leer 't uit je hoofd

"*Dank u, ik bel u zelf terug via het nummer op de achterkant van mijn bankkaart.*"

Daarna: ophangen. Pak je kaart. Bel het nummer dat erop staat. Vraag of er inderdaad fraude is gemeld. Het echte antwoord is in 99% van de gevallen: "Nee mevrouw, niet aan onze kant."

Voor familieleden — oefen het samen

1. Spreek af: **nooit** codes voorlezen aan iemand aan de telefoon.
2. Spreek af: **nooit** overschrijven onder telefoondruk.
3. Spreek af: **altijd** eerst even bellen met partner / kind voor je iets bevestigt.

> ⚑ **"De agent staat al voor uw deur."**
> Variant waarin "de politie" of "een koerier" naar je toe komt om je kaart op te halen "voor onderzoek".
> **Geef nooit je kaart af aan iemand die aan de deur staat.**
> Geen enkele bank, politie of koeriersdienst werkt zo.

MODULE 4 · NOODNUMMERS

Wie bel je als het misgaat?

Vul deze pagina nu in met pen. Niet op je telefoon — als die het probleem is, kun je je telefoon niet gebruiken om de nummers op te zoeken.

Algemene nummers

Dienst	Nummer (2026)
BE · Card Stop — bankkaart, kredietkaart, betaalapps blokkeren	`078 170 170` (24/7)
BE · Safeonweb — verdachte mails doorsturen	`verdacht@safeonweb.be`
NL · Spam-/phishing-sms doorsturen	`7726` (gratis)
NL · Fraudehelpdesk	`088 786 73 72` · fraudehelpdesk.nl
NL · Politie (geen spoed)	`0900-8844`
BE · Politie (geen spoed, fraude)	`101` · meld bij lokale politie

Mijn bank-noodnummers — invullen met pen

MIJN HOOFDBANK

NOODNUMMER HOOFDBANK

MIJN TWEEDE BANK (INDIEN)

NOODNUMMER TWEEDE BANK

KREDIETKAART-UITGEVER (VISA / MASTERCARD / AMEX)

NOODNUMMER KREDIETKAART

MOBIELE PROVIDER

KLANTENNUMMER / CONTRACTNR.

★ **Plak dezelfde gegevens op je Noodkaart (pagina 95).**
Twee plekken thuis: één in dit boek, één op de koelkast. Eén bij je paspoort als reserve.

MODULE 4 · CONTROLELIJST

Klaar? Loop dit af.

- ☐ Mijn daglimiet voor overschrijvingen staat op een bedrag dat past bij wat ik werkelijk gebruik.
- ☐ Mijn daglimiet voor kaartbetalingen / online aankopen staat redelijk laag.
- ☐ Push-meldingen voor uitgaande betalingen staan aan.
- ☐ Mijn spaarrekening is minder zichtbaar / vraagt extra bevestiging.
- ☐ Mijn vaste ontvangers staan op de witte lijst van vertrouwde begunstigden.
- ☐ Mijn bank-noodnummer staat op pagina 50 én op de Noodkaart (pagina 95).
- ☐ Ik ken het standaardantwoord uit mijn hoofd: *"Ik bel u zelf terug via het nummer op mijn bankkaart."*
- ☐ Mijn partner en eventueel oudere familieleden hebben dit gesprek óók gehad.

✂ Knip uit en hang op

Bank-spiekbriefje

- **Limieten laag.** Tijdelijk verhogen voor grote aankoop.
- **Meldingen aan.** Voor elke betaling, vooral buitenland en nieuwe begunstigden.
- **Witte lijst.** Bekende rekeningen vrij, nieuwe met extra bevestiging.
- **Telefoon van "de bank":** ophangen, zelf terugbellen via nummer op de kaart.
- **Code voorlezen?** Nooit.
- **Misgegaan:** Card Stop 078 170 170 (BE) · eigen noodnummer (NL).

MODULE 4 · TROUBLESHOOTING & AFSLUITING

Wat als…& afsluiting

? …ik heb tóch onder druk overgeschreven?

Direct bellen — Card Stop (BE) of je bank (NL) — en vragen om *terugroeping van betaling*. Binnen 1–2 uur is er soms nog wat te redden; later wordt het moeilijker. Doe diezelfde dag aangifte bij de politie — je hebt een proces-verbaal nodig voor het bankgeschil.

? …mijn bank weigert te vergoeden ("grove nalatigheid")?

Vraag schriftelijk om uitleg.
BE
: klacht bij Ombudsman in financiële geschillen (`ombudsfin.be`). **NL**: Kifid (`kifid.nl`). Beide gratis en onafhankelijk.

? …ik wil mijn kind een eigen pas geven?

Doe dat met een aparte rekening (KBC Bizz Junior, ING U-pas, ABN AMRO Pas op Maat). Lage limieten, geen rood staan, eigen app. Goede oefenomgeving.

? …ik beleg via een app (DEGIRO, Bolero, BUX)?

Dezelfde regels: lange unieke wachtwoord uit je kluis, 2FA aan, uitkeringsrekening alléén jouw bekende eigen rekening. Een namaak- "broker-supportgesprek" werkt nét zo als bank-helpdesk-fraude.

Samenvatting in drie zinnen

1. Lage limieten en meldingen zorgen dat een fout van een uur geen schade van een maand wordt.
2. De bank vraagt nooit codes, nooit "veilige rekeningen", nooit afstandbediening.
3. Eén vaste zin pareert elk verdacht telefoontje: "*Ik bel u zelf terug via het nummer op mijn bankkaart.*"

Volgende stap → Module 5 — Apparaten & thuisnetwerk. De infrastructuur waarop al het bovenstaande draait, op orde brengen.

MODULE 05 · APPARATEN & NETWERK ~ 90 MINUTEN · 12 PAGINA'S

05

Apparaten & thuisnetwerk

Telefoon, laptop, router en slimme apparaten. Niet alles tegelijk perfect, wel: updates aan, basisinstellingen goed, gast-wifi voor de rest.

WAT GA JE LEREN?

- Welke instellingen op je telefoon en laptop écht uitmaken.
- Hoe je je router checkt, bijwerkt en een gastnetwerk opzet.
- Wat een "smart device" veilig of onveilig maakt.

WAT HEB JE STRAKS?

Automatische updates aan op alle apparaten, een gastnetwerk voor bezoek en slimme apparaten, en een korte inventaris van wat er thuis aan het internet hangt.

GESCHATTE TIJD

90 minuten

WAT HEB JE NODIG?

- Toegang tot je router (sticker met inloggegevens)
- Je telefoon en laptop
- Lijstje slimme apparaten in huis

We werken met routers van Proximus, Telenet, Orange (BE) en KPN, Ziggo, Odido (NL) als voorbeeld.

MODULE 5 · INLEIDING

De infrastructuur van een veilig huis

De vorige modules gingen over accounts en mensen. Deze module gaat over de apparaten waar alles op draait. Doel: niet alles tegelijk perfect, wel de basisinstellingen op orde, met een gastnetwerk voor de rest.

Drie principes voor de hele module

1. **Updates aan.** Verreweg de meest onderschatte beveiliging. Een telefoon van 2022 met de nieuwste software is veiliger dan een telefoon van 2024 die nog op de fabrieksversie staat.
2. **Scheid wat je vertrouwt van wat je niet kent.** Je belangrijke apparaten op je hoofdnetwerk; de slimme stekkers, thermostaat, robotstofzuiger en bezoek op het gastnetwerk.
3. **Minimaliseer.** Een slim apparaat dat je niet écht nodig hebt, is een aanvalsoppervlak dat je niet nodig hebt.

Wat we vandaag doen

- Updates op alle apparaten automatisch maken.
- De router controleren, bijwerken en een gastnetwerk inrichten.
- Een korte inventaris maken van alles wat thuis aan het net hangt.
- Eén eenvoudig back-upschema in gang zetten.

> ℹ **Geen IT-afdeling nodig.**
> Alles in deze module kan een geduldige doorsnee-gebruiker zelf, met de router-sticker op de zijkant van het kastje. Vermijd betaalde "security check-ups" door derden tenzij je echt vastloopt.

Casus

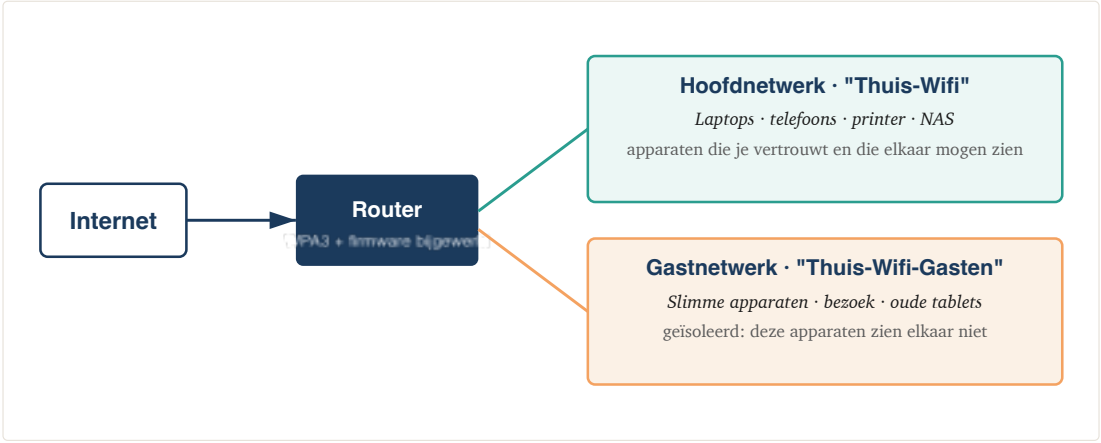
Sara & Mohamed (41 / 39), Rotterdam. Krijgen een slimme deurbel cadeau. Ze koppelen 'm aan hun hoofd-wifi met een standaardwachtwoord. De fabrikant gaat een jaar later failliet — updates stoppen. Twee jaar later toont een onderzoeker dat duizenden van die deurbellen een gat hebben. Het apparaat zit op hetzelfde netwerk als hun laptops en NAS. — Een gastnetwerk had dat gat geïsoleerd.

MODULE 5 · THEORIE · 1 VAN 2

Twee netwerken, geen ingewikkelde server

Een veilig thuisnetwerk hoeft niet duur of complex te zijn. Met twee wifi-netwerken op één router heb je 80% van wat een professionele omgeving biedt.

Hoe ziet het schema eruit?



Waarom twee?

- **Een slim apparaat dat een gat krijgt** kan niet bij je laptop, telefoon of NAS — die zitten op een ander netwerk.
- **Bezoek** krijgt jouw wifi-wachtwoord nooit te zien. Je laat ze gewoon op het gastnetwerk.
- **Wachtwoord van het gastnetwerk veranderen** kan met één klik, zonder al je apparaten opnieuw te koppelen.

> ★ **Werkende vuistregel.**
> Apparaten die jij actief inlogt (telefoon, laptop, tablet) → hoofdnetwerk. Apparaten die alleen "op de wifi staan" (slimme stekker, lamp, thermostaat, printer, TV) → gastnetwerk.

MODULE 5 · THEORIE · 2 VAN 2

Wat hangt er thuis aan het internet?

Schrik niet — bij een doorsnee Belgisch of Nederlands gezin staan al snel 20–30 apparaten op de wifi. Vul de tabel hieronder in. Wat je niet kent, kun je niet beveiligen.

Tip: bijna elke router-app toont een lijst van actieve apparaten. Daar krijg je een snelle inventaris.

#	APPARAAT	TYPE (LAPTOP / IOT / ETC.)	NETWERK?	UPDATES AAN?
1			□ H □ G	□
2			□ H □ G	□
3			□ H □ G	□
4			□ H □ G	□
5			□ H □ G	□
6			□ H □ G	□
7			□ H □ G	□
8			□ H □ G	□
9			□ H □ G	□
10			□ H □ G	□
11			□ H □ G	□
12			□ H □ G	□

H = hoofdnetwerk · G = gastnetwerk

MODULE 5 · AAN DE SLAG · STAP 1 VAN 6

Stap 1 — Je telefoon op orde

Twee paden — kies de jouwe.

iPhone (iOS)

1 **Updates automatisch**
`Instellingen → Algemeen → Software-update → Automatische updates`. Zet "Download iOS-updates" en "Installeer iOS-updates" beide aan.

2 **Zoek mijn iPhone**
`Instellingen → [je naam] → Zoek mijn`. "Zoek mijn iPhone" + "Zoek netwerk" + "Stuur laatste locatie" alle drie aan.

3 **Lockdown-modus? Meestal niet.**
Extreme beveiligingsmodus. Aanrader alleen voor journalisten, advocaten of mensen met bekende dreigingen. Voor een gewoon gezin overkill.

Android

1 **Updates automatisch**
`Instellingen → Beveiliging & privacy → Updates` (of `Systeem → Software-update`). Zet "Automatisch downloaden" en "Automatisch installeren" aan.

2 **Vind mijn apparaat**
`Instellingen → Beveiliging → Vind mijn apparaat`. Aan. Test eenmaal via `android.com/find`.

3 **Hoe lang krijgt jouw toestel nog updates?**
Bij Samsung, Google en Pixel-toestellen: meestal 5–7 jaar. Bij oudere of goedkopere merken: vaak 2–3 jaar. Geen updates meer? Tijd om te overwegen het toestel niet meer voor bankzaken te gebruiken.

> ! **Apps alleen uit de officiële store.**
> App Store (iOS) of Play Store (Android). Geen APK's uit forums, geen "alternatieve stores", geen QR-codes uit reclame. Op iOS is sideloading mogelijk in de EU sinds 2024 — verstandig om uit te laten voor wie het niet nodig heeft.

MODULE 5 · AAN DE SLAG · STAP 2 VAN 6

Stap 2 — Je laptop op orde

macOS

1. **Updates automatisch**
   `Systeeminstellingen → Algemeen → Software-update →` ⓘ bij "Automatische updates". Alles aan, inclusief "Snelle beveiligingsupdates".

2. **FileVault aan**
   `Systeeminstellingen → Privacy & beveiliging → FileVault` → Aan. Dit versleutelt je harde schijf zodat een gevonden of gestolen Mac geen open boek is. Schrijf de herstelsleutel ergens veilig op.

3. **Firewall aan, automatisch inloggen uit**
   Firewall: `Privacy & beveiliging → Firewall → Aan`. Inloggen: zet "Automatisch inloggen" uit (`Gebruikers & groepen → Inlog-opties`).

Windows

1. **Updates automatisch**
   `Instellingen → Windows Update → Geavanceerde opties`. Zet "Onder gemeten verbindingen" en "Updates ontvangen voor andere Microsoft-producten" aan.

2. **BitLocker aan (Pro / 11)**
   `Instellingen → Privacy & beveiliging → Apparaatversleuteling` (Windows 11 Home) of `BitLocker` (Pro). Sla de herstelsleutel op in je Microsoft-account of op papier.

3. **Windows Security checken**
   Open `Windows-beveiliging`. Loop alle zes onderdelen langs (Virus-/dreigingsbescherming, Account, Firewall, App-/browserbescherming, Apparaat, Familie). Geen uitroeptekens? Klaar.

> ¡ **Antivirus: meestal genoeg wat ingebouwd is.**
> macOS heeft XProtect / Gatekeeper ingebouwd. Windows heeft Defender — tegenwoordig prima. Aparte betaalde antivirus is voor de meeste mensen overbodig en soms zelfs riskanter (extra software, extra fouten). Wel: een browser met goede phishing-bescherming (Chrome, Firefox, Edge, Safari — moderne versie).

MODULE 5 · AAN DE SLAG · STAP 3 VAN 6

Stap 3 — Je router fatsoenlijk instellen

De router is het kastje van je internetprovider. Bij Proximus / Telenet Box / Orange Box (BE) en KPN ExperiaBox / Ziggo Connectbox / Odido (NL) werk je meestal via een app — sneller dan vroeger via het webadres.

1 Open de officiële app of het webadres

De router-sticker op het kastje vermeldt vaak het webadres (`192.168.1.1` of vergelijkbaar) plus beheernaam en -wachtwoord. Of: installeer de officiële provider-app uit de App / Play Store.

2 Verander het beheerwachtwoord

Het standaardwachtwoord van een nieuwe router staat op de sticker — leesbaar voor iedereen die fysiek toegang heeft. Wijzig 'm naar iets uit je kluis (Module 1).

3 Controleer firmware-updates

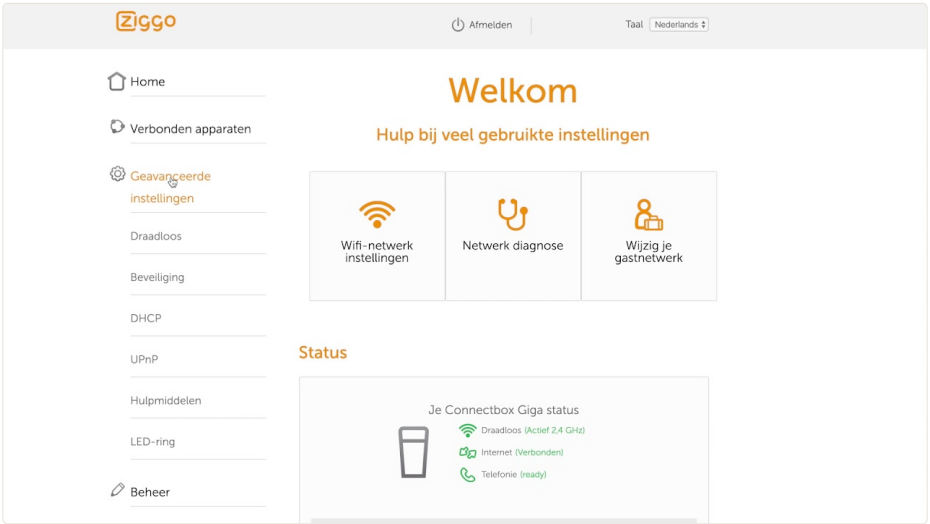
Bij de meeste BE/NL-providers: *automatisch* aan. Check één keer of dat klopt (vaak onder `Systeem → Firmware` of `Onderhoud`).

4 Versleuteling: WPA3 of WPA2 (geen WEP, geen open)

Onder `Wifi-instellingen → Beveiliging`. Moderne routers staan standaard goed; check dat het niet op "WEP" of "Open" staat. WPA3 is mooi maar oudere apparaten ondersteunen het niet — WPA2 is prima.

5 UPnP en WPS uit (waar dat kan)

UPnP opent automatisch poorten — handig voor spelconsoles, ongewenst voor de rest. Soms uitzetten kan een gameconsole hinderen; pas dan eventueel terug aan.
WPS (de drukknop-koppeling) heeft een bekende zwakte. Liever uit.



Voorbeeld — Ziggo Connectbox-beheer. Links: *Geavanceerde instellingen → Draadloos / Beveiliging / UPnP*. Rechts: snelkoppelingen naar wifi-instellingen en gastnetwerk. Bij andere providers (KPN, Odido, Proximus, Telenet) verschillen de menu-namen, niet de logica.

MODULE 5 · AAN DE SLAG · STAP 4 VAN 6

Stap 4 — Het gastnetwerk inrichten

Bijna elke moderne router kan dit. Eén keer instellen, voorgoed van profijt.

1 **Zoek "gastnetwerk" of "Guest Wi-Fi"**
In de provider-app of router-interface. Soms onder `Wifi → Extra netwerken`. Schakel het in.

2 **Naam (SSID) en wachtwoord**
Geef het een herkenbare naam — bijvoorbeeld `[Jouwnaam]-Gasten`. Kies een fatsoenlijk wachtwoord (geen `welkom123`); vier willekeurige woorden volstaat.

3 **Isolatie aanzetten**
Cruciaal: vink "Client isolation" of "Gasten kunnen elkaar niet zien" aan, plus "Geen toegang tot lokaal netwerk". Sommige routers noemen het anders; de bedoeling is altijd dat apparaten op het gastnetwerk elkaar én jouw hoofdapparaten niet kunnen bereiken.

4 **Verhuis de slimme apparaten**
Een avond werk. Per apparaat: in de bijbehorende app loskoppelen van je hoofd-wifi en opnieuw aanmelden op het gastnetwerk. Begin met de minst kritische (verlichting, thermostaat) en bewaar bewust ingewikkelde (printer, smart-TV) voor het einde.

Mijn netwerken — invulblok

NAAM HOOFDNETWERK (SSID)

WACHTWOORD GASTNETWERK (IN JE KLUIS)

NAAM GASTNETWERK (SSID)

PROVIDER-NOODNUMMER

★ **Print een kaartje "Onze gast-wifi" voor op de keukenkast.**
SSID + wachtwoord erop. Iedere bezoeker kan zichzelf aanmelden zonder dat jij je hoofdwachtwoord ooit hardop hoeft te zeggen.

MODULE 5 · AAN DE SLAG · STAP 5 VAN 6

Stap 5 — Slimme apparaten (IoT)

Een lijst van vijf vragen voor elk slim apparaat in huis. Antwoord twee of meer keer "nee" en je hebt een goed argument om dat apparaat *niet* op je hoofdnetwerk te zetten — of het helemaal niet aan te schaffen.

De 5-vragen-test

1. Heeft het apparaat een fabrikant die over 3 jaar nog bestaat?
2. Krijgt het automatische beveiligingsupdates?
3. Werkt het ook nog als de fabrikant zijn dienst stopt? (Lokale werking, geen verplichte cloud.)
4. Heeft de bijbehorende app een privacybeleid dat je kan vinden en begrijpen?
5. Is het apparaat genoeg waardevol om de extra onderhoudslast waard te zijn?

Wat te doen met wat je al hebt

Type apparaat	Advies
Slimme TV / streaming-stick	Gastnetwerk. Microfoon en camera (indien aanwezig) uit. Geen account-koppelingen met betaalgegevens als het niet hoeft.
Slimme thermostaat / stekker / lamp	Gastnetwerk. Updates aan, anders niet houden.
Slimme deurbel / beveiligingscamera	Strenger: alleen kopen van fabrikanten met goede updategeschiedenis (Reolink, UniFi, Logitech, Apple HomeKit). Sterke 2FA op de bijbehorende account. Gastnetwerk.
Robotstofzuiger	Gastnetwerk. Camera-functies (indien aanwezig) goed nakijken — sommige sturen foto's naar de fabrikant.
Spelconsole (PlayStation, Xbox, Switch)	Hoofdnetwerk akkoord (krijgt actieve updates). 2FA aan op de account. Kinderaccounts apart (zie Module 6).
Slim speelgoed / smartwatch voor kinderen	Wees streng: lees de reviews. Veel goedkope merken sturen ongerichte data naar het buitenland. In twijfel: niet kopen.

> ! **Wegdoen kost ook gegevens.**
> Voor je een slim apparaat verkoopt of weggeeft: reset naar fabrieksinstellingen, ontkoppel het uit de bijbehorende app, en wis je account-koppeling. Anders staat de volgende eigenaar in je smarthome.

MODULE 5 · AAN DE SLAG · STAP 6 VAN 6

Stap 6 — Eén simpele back-up

Niet voor cyberaanvallers, wel voor de hond die je laptop omver gooit, de val van een trap, of de plotseling overleden harde schijf. Eén routine, eens per week, klaar.

De 3-2-1-regel — voor wie 't precies wil weten

- **3 kopieën** van je belangrijke bestanden.
- **2 verschillende media** (bv. laptop + externe schijf).
- **1 kopie buitenshuis** (cloud, of bij familie).

De minimumversie voor een gezin

1. ### Cloud-synchronisatie aan voor wat ertoe doet
   iCloud (Mac) of OneDrive (Windows) of Google Drive: in elk geval je documenten en foto's. Eén keer instellen, het regelt zichzelf.

2. ### Eén keer per maand een lokale back-up
   Externe SSD aansluiten. macOS: `Time Machine` aan. Windows: `Instellingen → Back-up → Bestandengeschiedenis`. Een uur draaien, schijf los, in een la.

3. ### Foto's van je telefoon
   iCloud-foto's (iPhone) of Google Foto's / Microsoft Photos (Android): aan. Of: één keer per maand handmatig kopiëren naar je laptop. Kies wat je doet, doe het consequent.

> ! **Een back-up die je nooit hebt getest, is geen back-up.**
> Eén keer per jaar: open een willekeurig bestand uit je back-up. Lukt dat? Mooi. Lukt dat niet? Nu fixen, niet in een crisis.

MODULE 5 · CONTROLELIJST

Klaar? Loop dit af.

Telefoon

- [ ] Automatische updates aan (iOS / Android).
- [ ] "Zoek mijn iPhone" / "Vind mijn apparaat" aan en getest.
- [ ] Apps alleen uit App Store / Play Store.

Laptop

- [ ] Automatische updates aan (macOS / Windows).
- [ ] FileVault (macOS) of BitLocker (Windows) aan, herstelsleutel bewaard.
- [ ] Firewall aan, automatisch inloggen uit.

Router & netwerk

- [ ] Beheerwachtwoord van router aangepast en in mijn kluis.
- [ ] Firmware-updates automatisch aan.
- [ ] WPA2 of WPA3 actief; geen WEP, geen open netwerk.
- [ ] UPnP en WPS uit (tenzij echt nodig).
- [ ] Gastnetwerk ingericht, met client-isolatie.
- [ ] Slimme apparaten staan op gastnetwerk.

Back-up

- [ ] Cloud-synchronisatie aan voor documenten en foto's.
- [ ] Lokale back-up gedraaid in de laatste maand.
- [ ] Eén keer een willekeurig bestand teruggehaald om te testen.

✂ Knip uit en hang op

Apparaten-spiekbriefje

- **Updates aan.** Op alles. Echt alles.
- **Twee netwerken.** Hoofd voor jou, gast voor de rest.
- **Geen apps buiten de officiële store.**
- **Eén back-uproutine.** Cloud + maandschijf, test jaarlijks.
- **Slim ≠ noodzakelijk.** In twijfel: niet kopen.

MODULE 5 · TROUBLESHOOTING & AFSLUITING

Wat als...& afsluiting

? ...ik ben mijn router-beheerwachtwoord vergeten?

De meeste providers laten je via hun app of klantenservice resetten, of er zit een kleine resetknop op de router (10 seconden indrukken). Daarna: alles opnieuw instellen — inclusief gastnetwerk.

? ...een slim apparaat past niet op het gastnetwerk?

Sommige apparaten (printers, oudere Hue-bridges) "willen" op hetzelfde netwerk staan als je telefoon om gevonden te worden. Twee opties: tijdelijk je telefoon op gastnetwerk om te koppelen, of — bij twijfel — bij de apparaten in de bijbehorende app de "lokale ontdekking" via cloud doen. Lees de handleiding.

? ...mijn telefoon krijgt geen updates meer?

Tijd om te overwegen 'm niet meer voor bank- en identiteits-apps te gebruiken. Een verouderd toestel als tweede toestel voor wifi-radio of muziek is prima; voor itsme, DigiD en bankieren liefst niet.

⚑ ...ik denk dat er ongewenste apparaten op mijn netwerk staan?

In de router-app: lijst van actieve apparaten. Naam onbekend? Eerst proberen te herkennen (slimme stekker met cryptische naam komt voor). Echt onbekend → blokkeer in de app, wijzig wifi-wachtwoord. Daarna alle eigen apparaten opnieuw koppelen.

Samenvatting in drie zinnen

1. Updates aan op alles wat aan internet hangt.
2. Twee netwerken: vertrouwde apparaten op hoofd, alles wat "alleen op de wifi staat" op gast.
3. Eén back-uproutine, met jaarlijkse test.

Volgende stap → Module 6 — Kinderen & tieners online. Nu de infrastructuur staat, gaan we kijken hoe je met je kinderen tot werkbare afspraken komt.

MODULE 06 · KINDEREN & TIENERS

~ 60 MINUTEN · 8 PAGINA'S

06

Kinderen & tieners online

Geen filters die alles oplossen, maar afspraken die meegroeien. Per leeftijdsfase: gesprek, instellingen, en wanneer je je er níet mee bemoeit.

WAT GA JE LEREN?

- Welk gesprek hoort bij welke leeftijd (6–9, 10–12, 13–15, 16+).
- Welke instellingen op iPhone, Android en console het meest opleveren.
- Hoe je sextortion, online pesten en grooming herkent en wat je doet.

WAT HEB JE STRAKS?

Een gezinsovereenkomst over schermtijd en apps, ingerichte ouder-toezichtsinstellingen, en een eerlijk gesprek achter de rug.

GESCHATTE TIJD

60 minuten (+ gesprek)

WAT HEB JE NODIG?

- De telefoon van je kind, in overleg
- Tijd en geduld — niet doen wanneer je gehaast bent

Met praktijkvoorbeelden van Snapchat, TikTok, WhatsApp en gaming-platformen.

MODULE 6 · INLEIDING

Geen filter lost dit op. Afspraken wel.

Filters, content-blockers en schermtijdlimieten zijn nuttig, maar ze vervangen het gesprek niet. Kinderen vinden manieren om dingen werkbaar te maken; jij wilt vooral dat ze naar je toe komen als er iets schuurt. Deze module helpt je dat gesprek voeren — en daarnaast de instellingen scherp te zetten.

Drie principes voor de hele module

1. **Meegroeien.** Wat goed werkt voor een 9-jarige werkt averechts voor een 14-jarige. Hou ruimte voor herijking.
2. **Eerlijk uitleggen wat je doet en waarom.** Heimelijk toezicht gaat een keer uitkomen — en dan is het vertrouwen weg.
3. **Geen schaamte als straf.** Een kind dat bang is voor jouw reactie meldt straks niets meer. Reageer kalm, ook als het schrikt.

Wat we vandaag doen

- Per leeftijdsfase weten wat ertoe doet.
- Eén keer een echt gesprek voeren met een script om op terug te vallen.
- iPhone- of Android-instellingen passend bij de leeftijd zetten.
- Per veelgebruikte app de drie belangrijkste instellingen weten.
- Herkennen wanneer iets meer is dan "iets vervelends online".

> ¡ **Niet doen wanneer je gehaast bent.**
> Reserveer een avond. Eén goed gesprek werkt jaren door; tien snelle verbieden-uitwisselingen werken een week.

Casus

Familie De Smedt, Leuven. Hun zoon (13) krijgt op Snapchat een verzoek van een "leeftijdsgenoot uit Amerika" en deelt na een paar dagen een naaktfoto. Een uur later komt de chantage. Hij durft het niet thuis te vertellen tot een leerkracht het merkt. — Niet de instellingen waren het probleem (Snapchat was correct ingesteld), maar dat hij dacht dat zijn ouders boos zouden zijn. Eerlijke reactie van zijn ouders had hem 24 uur eerder kunnen helpen.

MODULE 6 · THEORIE

Vier leeftijdsfasen, vier gesprekken

Leeftijd	Het kerngesprek	De kerninstelling	Wat je wilt herkennen
6–9 basisschool, eerste apparaat	"Het internet is een grote stad — we gaan samen. Vreemden krijgen niets van jou (foto, naam, leeftijd, school)." Geen eigen telefoon, alleen gezamenlijke tablet of console.	Schermtijd / Family Link in kindermodus. Inkopenbevestiging verplicht. YouTube Kids in plaats van YouTube.	Plotse boosheid of teruggetrokken gedrag na schermtijd. In-game-chats met onbekenden.
10–12 overgang, eerste eigen toestel	"Wat je online deelt blijft soms voor altijd. Niet alles waar mama-papa naar vragen is straf — soms is het bescherming." Begin het familie-codewoord-gesprek (Module 3).	Apple Schermtijd / Google Family Link met app-limieten. Geen sociale media tenzij echt nodig (WhatsApp uitzondering); dan ouder als beheerder.	Geheimzinnigheid over apps, schermen die snel kantelen als je binnenkomt.
13–15 middelbare school, sociaal leven	"Als er iets pijnlijks gebeurt — een foto, een chantage, een gesprek dat eng werd — kom je naar mij. Ik word niet boos. Eerst lossen we het op." Zeg dit hardop, meerdere keren.	Geleidelijk minder strikte limieten, behoud van: 's nachts geen telefoon op de slaapkamer, locatiedeling binnen het gezin, 2FA op alle accounts.	Pijnlijke berichten op school, plotselinge geld-vragen ("ik moet een Steam-kaart kopen"), gewichtsverlies door gameverslaving.
16+ jongvolwassen, eigen verantwoordelijkheid	"Vanaf nu is dit jouw zaak. Ik blijf beschikbaar voor de moeilijke gesprekken." Werk mee aan eigen bankrekening, eigen DigiD / itsme.	Familie-account-overzicht (Apple ID Family, Google Family) blijft maar zonder dwingende limieten. 2FA blijft.	Datingfraude, beleggingsscams, "snel rijk worden"-trends.

★ **Mijlpaal: eigen telefoon.**
Een goede gelegenheid om er één gezinsovereenkomst aan te koppelen (zie pagina 68). Niet vooraf alle regels uitspugen; samen invullen.

MODULE 6 · AAN DE SLAG · STAP 1 VAN 4

Stap 1 — Het gezinsgesprek

Eén avond, geen telefoons aan tafel, niet na een ruzie. Het script hieronder is een aanzet — schrap wat niet past, voeg toe wat ontbreekt.

Vijf vragen — voor jullie samen

1 **Waar gebruiken we onze schermen voor?**
Inventariseer eerlijk: school, vrienden, ontspanning, social, gamen. Geen oordeel — alleen kijken.

2 **Welke afspraken hebben we al, zonder ze opgeschreven te hebben?**
Niet eten met telefoon? Niet 's nachts op de slaapkamer? Maak ze expliciet.

3 **Wat doen we als er iets vervelends gebeurt?**
Vooraf afspreken is goud. "Eerst stoppen, daarna komen we naar mama of papa. Geen boosheid, eerst oplossen."

4 **Wat gebeurt er als een afspraak niet werkt?**
Een afspraak die in maand drie kromtrekt is geen drama; het is informatie. Plan een herijking — bijvoorbeeld elke drie maanden.

5 **Wat verwachten we van elkáár als ouder?**
Geen telefoon op de bank tijdens een gesprek. Niet door blijven scrollen als de ander iets vertelt. Voorbeeldgedrag is alles.

Onze gezinsovereenkomst — schrijf 'm hier op

ONZE DRIE AFSPRAKEN

PLEK WAAR DE TELEFOONS 'S NACHTS LIGGEN

VOLGENDE HERIJKING — DATUM

MODULE 6 · AAN DE SLAG · STAP 2 VAN 4

Stap 2 — Ouder-toezichtsinstellingen

Eén keer instellen, daarna meegroeien met de leeftijd. Doe het sámen met je kind — niet stiekem. Leg uit wat je instelt en waarom.

iPhone — Schermtijd

1. **Familiekoppeling**
   `Instellingen → [je naam] → Familie`. Voeg het kind toe (eigen Apple-ID onder 13 jaar maak je daar).

2. **Schermtijd inrichten**
   Op het toestel van het kind: `Instellingen → Schermtijd`. Stel een ouder-toegangscode in. *Niet hetzelfde* als de telefoon-pin.

3. **Belangrijkste drie schakelaars**
   - `Communicatiebeperkingen` — wie mag bellen / FaceTimen.
   - `Inhouds- en privacy-beperkingen` — leeftijdsindicatie media + apps.
   - `Aankopen in iTunes & App Store` — vraagtoestemming aan.

Android — Family Link

1. **Family Link installeren**
   Op jouw toestel én op dat van het kind. Een Google-account voor kinderen onder 13 maak je via Family Link.

2. **Apparaat koppelen**
   De app stuurt je door alle stappen: tijdslimieten, slaaptijd, app-toegangen. Stel een ouder-pin in.

3. **Belangrijkste drie schakelaars**
   - App-installatie: *vraagtoestemming aan*.
   - Aankopen in Play Store: *vraag-toestemming aan*.
   - SafeSearch: *aan*.

> ! **Tieners zonder ouder-toezicht.**
> Vanaf ongeveer 14 jaar is strikt toezicht vaak averechts. Liever: ouder-account als *vertrouwde tweede ogen* (locatiedeling binnen het gezin, gedeeld inzicht in aankopen), zónder dwingende blokkades.

MODULE 6 · AAN DE SLAG · STAP 3 VAN 4

Stap 3 — Per app: de drie schakelaars

App	Min. leeftijd	Drie schakelaars die ertoe doen
Snapchat	13 (officieel)	Snap Map → *Ghost Mode*. Wie kan contact opnemen → *Alleen vrienden*. Family Center koppelen aan ouder-account (vanaf 13).
TikTok	13 (officieel)	Account → *Privé*. Reacties & duet → *Alleen vrienden*. Family Pairing koppelen.
Instagram	13 (officieel)	Account → *Privé*. Berichten van onbekenden → *Uit*. Tieneraccount (sinds 2024) met ouderkoppeling.
WhatsApp	13 (officieel)	Tweestapsverificatie aan. "Wie kan me toevoegen aan groepen" → *Mijn contacten*. Profielfoto → *Mijn contacten*.
Discord	13 (officieel)	Privacy → *DM-filter altijd op "Strikt"*. Vriendverzoeken → *Alleen wederzijdse vrienden*. 2FA aan.
Roblox	geen minimum (kindgericht)	Account-PIN aan. Chat → *Alleen vrienden*. Maandlimiet Robux. Ouder-account koppelen.
Minecraft (Bedrock)	geen minimum	Microsoft-familie-koppeling. Multiplayer met vreemden → *Uit* (jonger dan 12). Aankopen → vraag toestemming.
YouTube	13 (volwaardig)	Onder 13: YouTube Kids gebruiken. Tieners: *Beperkte modus*. Aanbevelingsgeschiedenis af en toe wissen.

> **"Maar al mijn vriendinnen hebben het al."**
> Vaak waar. Niet altijd reden om mee te gaan, maar wel reden om het eerlijk te bespreken. Een app onder voorwaarden installeren is meestal werkbaarder dan een totaalverbod.

MODULE 6 · AAN DE SLAG · STAP 4 VAN 4

Stap 4 — Als het écht ergens om gaat

Drie ernstige patronen die specifiek bij kinderen en tieners voorkomen. Voor elk: hoe het eruit ziet, en wat je doet als het bij jouw kind speelt.

1. Sextortion (afdreiging met een naaktfoto)

Patroon: een "leeftijdsgenoot" maakt snel contact, vraagt om een foto, chanteert daarna met publicatie tenzij geld of meer foto's worden gestuurd. Werkt op schaamte en tijdsdruk — vooral bij jongens 12–16 jaar.

- **Niet betalen.** Ooit. Het stopt niet bij één betaling.
- **Niet meer reageren.** Blokkeer het account in de app.
- **Bewaar bewijs.** Screenshots van het account, niet van de foto.
- **Meld bij de app** én bij het meldpunt in jouw land (zie pagina 98). **NL**: `helpwanted.nl`. **BE**: Child Focus 116 000.
- **Doe aangifte** bij de politie. Sextortion is een misdrijf — jouw kind is slachtoffer, niet dader.

2. Online pesten

Niet altijd zichtbaar voor ouders. Tekenen: stil worden na school, telefoon wegleggen, niet meer naar bepaalde plekken willen. Wat te doen:

- Luister eerst. Verbieden van de app is zelden de oplossing — voor het kind is dat een tweede straf.
- Bewaar bewijs (screenshots).
- Betrek school: in BE/NL hebben scholen meldplicht en protocollen.
- Blokkeer en rapporteer in de app.
- Niet-anonieme pestberichten op school: aangifte mogelijk.

3. Grooming (volwassene bouwt vertrouwen op met minderjarige)

Patroon: complimenten, geheimzinnigheid ("dit is tussen ons"), vragen om foto's, voorstel om af te spreken. Kan maanden duren.

- Praat eerlijk: "*Een volwassene die je vraagt iets geheim te houden voor papa-mama, is geen vriend.*"
- Bewaar bewijs, blokkeer, meld bij de app.
- BE: `childfocus.be` — Child Focus, 116 000.
  NL: `veiligthuis.nl` — 0800-2000 (24/7).
- Aangifte bij de politie: grooming is strafbaar in BE en NL.

> ⚑ **Reageer kalm, ook als je schrikt.**
> Kinderen melden eerder bij ouders die niet ontploffen. Je eerste reactie bepaalt of ze het volgende incident wél of niet vertellen. Jouw verdriet en boosheid mogen er zijn — maar later, niet in dat eerste gesprek.

MODULE 6 · CONTROLELIJST & AFSLUITING

Klaar? Loop dit af.

- [ ] We hebben één gesprek gevoerd over schermen en afspraken — zonder telefoons aan tafel.
- [ ] De drie gezinsafspraken staan op pagina 68 opgeschreven.
- [ ] Een herijkingsdatum (3–6 maanden) staat in de agenda.
- [ ] Op de telefoon van mijn kind staan Schermtijd (iOS) of Family Link (Android) ingericht.
- [ ] Voor elk van de gebruikte apps zijn de drie schakelaars (pagina 70) goed gezet.
- [ ] Ik heb hardop tegen mijn kind gezegd: *"Als er iets gebeurt, kom je naar mij. Ik word niet boos."*
- [ ] De meldpunten Child Focus 116 000 (BE) en Veilig Thuis 0800-2000 (NL) staan in mijn contacten.
- [ ] 's Nachts liggen de telefoons niet op de slaapkamer.

✂ Knip uit en hang op

Kinder-spiekbriefje

- **Afspraken > filters.** Plus filters.
- **Reageer kalm.** Eerst oplossen, dan voelen.
- **"Komt naar mij." Hardop. Vaak.**
- **Bij chantage:** niet betalen, bewijs bewaren, melden, aangifte.
- **Bij twijfel:** BE Child Focus 116 000 · NL Veilig Thuis 0800-2000.

Samenvatting in drie zinnen

1. Eén gezinsovereenkomst die meegroeit slaat tien losse instellingen.
2. Schermtijd / Family Link zet je sámen op — niet stiekem.
3. Bij sextortion, pesten of grooming: niet betalen, bewijs bewaren, melden, en kalm reageren.

Volgende stap → Module 7 — Privacy & data-minimalisatie. Wat je niet weggeeft, kan ook niet lekken.

MODULE 07 · PRIVACY

~ 45 MINUTEN · 6 PAGINA'S

07

Privacy & data-minimalisatie

Wat je niet weggeeft, kan ook niet lekken. Drie kleine gewoontes die je digitale voetafdruk merkbaar verkleinen.

WAT GA JE LEREN?

- Wat "strikt noodzakelijk" écht betekent in een cookiebanner.
- Hoe je tien minuten per maand besteedt aan opschoning.
- Welke rechten je hebt onder AVG/GDPR, en hoe je ze inzet.

WAT HEB JE STRAKS?

Een opgeschoond e-mailadres voor nieuwsbrieven, een lijstje afgemelde diensten en een ingerichte e-mail-alias voor anonieme aanmeldingen.

GESCHATTE TIJD

45 minuten

WAT HEB JE NODIG?

- Je e-mail-inbox
- Een rustig kwartier per week voor opvolging

Inclusief een sjabloon-mail voor een AVG-verwijderverzoek.

MODULE 7 · INLEIDING

Wat je niet weggeeft, kan ook niet lekken

Privacy is geen alles-of-niets-keuze. Het is een dagelijkse rekensom: levert het delen van deze data me genoeg op om het risico waard te zijn? Drie kleine gewoontes verkleinen je digitale voetafdruk merkbaar — en daarmee de schade als ergens iets misgaat.

De drie gewoontes

1. **Bewuster klikken.** Cookies, e-mails, accounts — niet alles aanvinken, niet voor alles aanmelden.
2. **Maandelijks opruimen.** Tien minuten op zondagochtend — nieuwsbrieven, accounts en oude apps.
3. **AVG-rechten gebruiken.** Niet alleen kennen, ook inzetten. Eén sjabloon-mail per maand.

Wat we vandaag doen

- Cookie- en trackerbanners leren afhandelen in vijf seconden.
- Een browserkeuze en -instelling maken die past bij jouw gebruik.
- Een opschoonroutine voor je inbox en accounts opzetten.
- Een sjabloonmail voor een AVG-verzoek (BE: GBA · NL: AP) klaarzetten.

Theorie-light: drie soorten data

Niet alle data is even gevoelig. Een eenvoudige rangschikking:

Type	Voorbeeld	Houding
Publiek	Naam, beroep op LinkedIn, dorp waar je woont.	Mag bekend zijn.
Persoonlijk	E-mailadres, telefoonnummer, geboortedatum, exact adres.	Alleen geven aan diensten die het echt nodig hebben.
Gevoelig	Rijksregisternummer / BSN, paspoortcopie, gezondheidsgegevens, religie, seksualiteit, bankgegevens.	Alleen geven als wettelijk verplicht. Twee keer nadenken.

> ¡ **Een webshop heeft je geboortedatum niet nodig.**
> Net zomin als een nieuwsbrief je telefoonnummer. Vraagt een dienst om data die niet bij de transactie hoort? Lege velden, of verzin een datum (bijvoorbeeld 1 januari, het jaar waarin je hen voor het eerst zag).

MODULE 7 · AAN DE SLAG · STAP 1 VAN 3

Stap 1 — Cookies en browser

De 5-seconden-cookiebanner-routine

1. Zoek de knop "*Alles weigeren*" of "*Alleen noodzakelijke*" — vaak verstopt onder "Instellingen" of als kleine grijze tekst.
2. Geen weigeren-knop? Klik op "*Voorkeuren beheren*", schakel alles uit behalve "Strikt noodzakelijk", en bevestig.
3. Veel websites in de EU moeten weigeren even makkelijk maken als accepteren. Doen ze dat niet? Sluit het tabblad, gebruik een andere bron.

> ★ **Tracker-blocker als ruggensteun.**
> Een extensie als `uBlock Origin` (Firefox / Chrome / Edge) of de ingebouwde tracker-bescherming van Safari, Brave en Firefox vangt veel weg vóór de banner überhaupt verschijnt. Eén keer installeren, jaren plezier.

Welke browser past bij jou?

Browser	Voor wie?
Firefox	Solide privacy uit de doos, niet van een advertentiebedrijf, goede extensie-keuze. Aanrader voor de meeste mensen.
Safari (iOS / Mac)	Sterk geïntegreerd, blokkeert trackers standaard, weinig in te stellen — fijn als je weinig wilt regelen.
Brave	Tracker- en reclame-blocker ingebouwd. Sneller op rommelige sites. Negeer de eigen reclame- en crypto-onderdelen.
Chrome / Edge	Werken prima, vereisen meer instelwerk en een tracker-blocker. Edge heeft betere privacy-defaults dan Chrome.

Eén keer instellen — drie schakelaars in elke browser

- `Browser-instellingen → Privacy → "Strict" tracking-bescherming.`
- `Cookies van derden → Blokkeren.`
- `Do Not Track / Global Privacy Control → Aan.`

MODULE 7 · AAN DE SLAG · STAP 2 VAN 3

Stap 2 — De zondagmorgen-routine

Tien minuten per maand. Niet langer. Zo houd je 'm vol.

1 **Eén nieuwsbrief afmelden**
Open de oudste nieuwsbrief in je inbox. Scroll naar onder. Klik "*Afmelden*" / "*Unsubscribe*". Klaar. Eén per week maakt 50 per jaar.

2 **Eén oud account opzeggen**
Een dienst die je een jaar niet hebt gebruikt? Log in, ga naar "*Account verwijderen*". Lukt het niet via de website? Mail ze met de sjabloon op pagina 77.

3 **Eén app van je telefoon halen**
Apps die je twee maanden niet hebt geopend mogen weg. Verwijderen stopt ook hun toegang tot locatie, contacten en achtergrondactiviteit.

E-mail-aliassen — één e-mail, veel kanalen

In plaats van bij elke webshop hetzelfde e-mailadres in te vullen: gebruik aliassen. Eén echte inbox, maar elke dienst krijgt een uniek alias dat je kunt uitschakelen als de spam te erg wordt.

- **iCloud (iPhone / Apple-account)**: "*Verberg mijn e-mailadres*" bij Apple ID → Privacy → Verberg mijn e-mailadres. Onbeperkt aliassen.
- **Proton Pass / SimpleLogin**: gratis aliasdienst, werkt overal. Goede aanvulling op een wachtwoordkluis.
- **Gmail-truc**: zet `+webshop` achter je naam: `jij+coolblue@gmail.com` komt in dezelfde inbox, maar je kunt sorteren en filteren.

> ★ **Tweede e-mailadres voor "ja-maar-ik-moet-ergens-een-mail-geven".**
> Geen alias-dienst nodig? Maak één wegwerp-Gmail of -ProtonMail aan die je gebruikt voor accounts die je echt niet vertrouwt. Eens per jaar legen.

MODULE 7 · AAN DE SLAG · STAP 3 VAN 3

Stap 3 — Je AVG-rechten gebruiken

Onder de AVG (BE/NL) heb je vijf bruikbare rechten. Bedrijven moeten binnen één maand reageren. Niet doen? Dan kun je een klacht indienen bij de toezichthouder.

Recht	Wat het inhoudt
Inzage	Een kopie van alle data die de dienst over jou heeft.
Correctie	Foutieve gegevens laten aanpassen.
Verwijdering ("recht om vergeten te worden")	Je gegevens (geheel) laten wissen. Geldt niet absoluut — wettelijke bewaarplicht gaat soms voor.
Bezwaar / opt-out	Stop gebruik van jouw data voor reclame, profilering, doorverkoop.
Dataportabiliteit	Je gegevens in machineleesbare vorm meekrijgen (om over te stappen).

Sjabloonmail — verwijderverzoek

SJABLOON · VERWIJDERVERZOEK BE / NL

```
Aan: privacy@[bedrijf].be / .nl
Onderwerp: AVG-verzoek tot verwijdering

Geachte heer/mevrouw,

Op grond van artikel 17 AVG (recht op
wissing van persoonsgegevens) verzoek
ik u alle persoonsgegevens te
verwijderen die u over mij verwerkt.

Mijn account is geregistreerd onder:
  - e-mailadres: [JOUW E-MAIL]
  - klantnummer: [INDIEN BEKEND]

Conform artikel 12 lid 3 AVG verwacht
ik binnen één maand een bevestiging
dat aan dit verzoek is voldaan, of een
gemotiveerde reactie.

Met vriendelijke groet,
[JOUW NAAM]
```

Werkt niet? Klacht indienen.

- **BE — Gegevensbeschermingsautoriteit (GBA)**: `gegevensbeschermingsautoriteit.be`. Online klachtenformulier, gratis.
- **NL — Autoriteit Persoonsgegevens (AP)**: `autoriteitpersoonsgegevens.nl`. Online klachtenformulier, gratis.

MODULE 7 · CONTROLELIJST & AFSLUITING

Klaar? Loop dit af.

- [ ] Ik weet welke knop in cookiebanners "Alles weigeren" doet (of "Alleen noodzakelijke").
- [ ] Mijn browser heeft strikte tracking-bescherming aan + tracker-blocker geïnstalleerd.
- [ ] Ik heb één keer een nieuwsbrief afgemeld in de laatste maand.
- [ ] Ik heb één oude dienst opgezegd of verwijderd.
- [ ] Ik gebruik een alias of "+"-truc voor nieuwe webshops.
- [ ] De sjabloon op pagina 77 staat ergens dat ik 'm zo terugvind.
- [ ] Ik weet waar ik klacht indien (BE: GBA · NL: AP).

Wat als...

> ? **...een dienst weigert mijn account te verwijderen?**
> Vraag schriftelijk om de juridische grond. Krijg je geen of een onzin antwoord, klacht indienen bij GBA (BE) of AP (NL). Vermeld bij de indiening: bedrijfsnaam, datum verzoek, kopie van hun antwoord.

> ? **...ik krijg ineens veel spam?**
> Vermoedelijk is er ergens een lek. Check `haveibeenpwned.com` met je e-mailadres. Verander wachtwoorden van de getroffen diensten. Bij twijfel: alias creëren en vanaf nu daarmee verder.

> ? **...een familielid heeft mij overal getagd op social media?**
> Vraag het ze. Stel tag-bevestiging in (Facebook / Instagram → privacy → "Berichten waarin ik word getagd controleren"). Familielid kan het verwijderen — politieker dan AVG, maar werkt sneller.

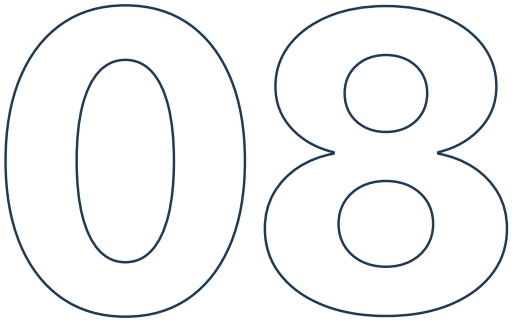
Samenvatting in drie zinnen

1. Bewuster delen + tracker-blocker = grootste privacywinst.
2. Tien minuten per maand opruimen verslaat één keer per jaar grote schoonmaak.
3. AVG-rechten werken — als je ze daadwerkelijk gebruikt.

Volgende stap → Module 8 — Incident response. Want zelfs met alles goed ingericht: soms gebeurt het toch.

MODULE 08 · INCIDENT RESPONSE

~ 30 MINUTEN · 6 PAGINA'S



Incident response: als het tóch misgaat

Geen paniek. Een vast volgordeplan: wie eerst, wat eerst, en welke meldpunten in BE en NL je dezelfde dag belt.

WAT GA JE LEREN?

- Het 60-minuten-protocol voor een vermoedelijke hack of fraude.
- Wat je doet bij gestolen telefoon, gestolen kaart, of gehackt e-mailaccount.
- Hoe je netjes aangifte doet — wat je nodig hebt om gehoord te worden.

WAT HEB JE STRAKS?

Een geprinte Noodkaart op de koelkast, en een ingevuld "in geval van nood"-blad in je administratie.

GESCHATTE TIJD

30 minuten

WAT HEB JE NODIG?

- De Noodkaart achterin (pagina 95)
- Telefoonnummers van je bank en mobiele provider

Met meldpunten: safeonweb.be / verdacht@safeonweb.be (BE) en fraudehelpdesk.nl / 1701 (NL).

MODULE 8 · HET PROTOCOL

Het eerste uur — wat te doen, in welke volgorde

Adem in. Pak deze pagina. Loop het schema af. Niet alles is van toepassing — sla over wat niet past. Maar wat wél van toepassing is: in deze volgorde, direct.



Welk scenario heb je?

- **Scenario A — Gehackte e-mail of account** → pagina 81
- **Scenario B — Gestolen of verloren telefoon** → pagina 82
- **Scenario C — Frauduleuze betaling of gestolen bankkaart** → pagina 83

> ! **Bel niet eerst je IT-vriend.**
> Geld terugkrijgen heeft een tijdslot van uren, niet dagen. Pas ná de bank- en sim-blokkade is er tijd voor verdere zorg.

MODULE 8 · SCENARIO A

Gehackte e-mail of account

Tekenen: je kunt niet meer inloggen, er staan verzonden berichten die niet van jou zijn, of vrienden krijgen vreemde mails uit jouw naam.

1 Op een ánder apparaat — wijzig wachtwoord

Ga via een schoon apparaat (geen mogelijk besmette laptop) naar je e-mailprovider. Gebruik "*wachtwoord vergeten*". Lukt het niet via je telefoonnummer of herstelmail? Gebruik je herstelcodes (Module 1, pagina 13).

2 Log alle sessies uit

In de account-instellingen: `Beveiliging → Apparaten / Actieve sessies → "Uitloggen op alle apparaten"`. De aanvaller raakt zijn toegang kwijt.

3 Zet 2FA aan (of opnieuw)

Authenticator-app of sms — wat dan ook. Print direct nieuwe herstelcodes en schrijf ze op pagina 13.

4 Check doorstuurregels en herstel-e-mail

Aanvallers zetten vaak een *doorstuurregel* op (al jouw post stuurt door naar hun adres) of voegen een herstel-e-mail toe. Check `Instellingen → Filters / Doorsturen / Beveiliging → Herstelopties`. Onbekende regels: verwijder.

5 Wijzig wachtwoorden van gekoppelde accounts

E-mail geeft toegang tot bijna alles. Wijzig minstens: bank, cloud-opslag, sociale media, marktplaatsen — met unieke wachtwoorden uit je kluis (Module 1).

6 Waarschuw je contacten

Een korte bericht: "*Mijn account is gehackt geweest. Negeer vreemde berichten van mij van gisteren.*" Voorkomt dat vrienden door de oplichting heen vallen.

> **!** **Sociale media-account gehackt?**
> Vraag bij "*Account-herstel*" een nieuwe code aan via een tweede e-mail of telefoonnummer. Facebook / Instagram: ondersteund via `facebook.com/hacked`. Bij Google: `accounts.google.com/signin/recovery`.

MODULE 8 · SCENARIO B

Telefoon gestolen of verloren

1 Lokaliseer en vergrendel — op afstand

iPhone: ga op een ander apparaat naar `iCloud.com/find`, log in met je Apple-ID, kies "Modus Verloren". Het toestel toont een bericht en blokkeert.

Android: `android.com/find`. Vergrendel, laat een bericht zien, of wis.

2 Blokkeer je simkaart

Bel je mobiele provider. De simkaart wordt onbruikbaar — geen sms-codes meer voor de dief.

3 Deactiveer itsme / DigiD

BE — itsme: log op een ander apparaat in op `my.itsme.be` met je eID-kaart + kaartlezer, kies "Deze app uitzetten".

NL — DigiD: bel de DigiD-helpdesk `088 123 65 55`.

4 Bel Card Stop (BE) of je bank (NL)

Banken kunnen je bank-app op het verloren toestel deactiveren — ook al heeft de dief je pincode niet, dit voorkomt aanvaller-pogingen.

5 Wijzig je belangrijkste wachtwoorden

Vooral als je 2FA-codes op het toestel kreeg via sms. E-mail eerst, daarna keten.

6 Wis als je het toestel niet terug verwacht

Na 24–48 uur zonder vinden: kies in Find My / Vind mijn apparaat voor "*Wis dit apparaat*". Onomkeerbaar — maar dat is precies wat je wil als het toestel echt weg is.

★ **Goed nieuws.**

Een telefoon met een sterke schermcode + Face ID/vingerafdruk + Wis na 10 pogingen is voor een dief vrijwel waardeloos. De moderne smartphone is goed beveiligd — mits je Module 5 hebt gedaan.

MODULE 8 · SCENARIO C

Frauduleuze betaling of gestolen kaart

1 Card Stop (BE) — `078 170 170`

24/7 bereikbaar. Geeft direct een blokkade op alle Belgische bankkaarten gekoppeld aan jouw rijksregisternummer. Ook voor digitale wallets (Payconiq, Apple Pay, Google Pay).

2 NL — bel je bank op het nummer op de kaart

ABN AMRO, ING, Rabobank, bunq — alle 24/7. Vraag om "*terugroeping van betaling*" (recall) als de overschrijving recent is.

3 Verzamel bewijs

Screenshots van de frauduleuze transactie. Eventuele sms/mail die de fraude voorafging. Datum, tijd, bedrag, ontvangende IBAN — alles wat je nodig hebt voor aangifte.

4 Doe aangifte bij de politie

BE: lokaal politiekantoor, of online via `police-on-web.be`.
NL: `0900-8844` of online via `politie.nl` → "Aangifte doen".

Vraag om een proces-verbaal-nummer. Geef dat door aan je bank binnen 48 uur.

5 Meld bij het centrale meldpunt

BE: `verdacht@safeonweb.be` (mail) of `safeonweb.be` (web).
NL: `fraudehelpdesk.nl` of `088 786 73 72`.

Bewijslijst — vul nu in

DATUM + TIJD VAN INCIDENT

CARD STOP-REFERENTIE (BE)

BEDRAG

BANKDOSSIERNUMMER

ONTVANGENDE IBAN (INDIEN BEKEND)

PV-NUMMER POLITIE

MODULE 8 · AANGIFTE & AFSLUITING

Hoe je netjes aangifte doet

Wie netjes aangifte doet, wordt serieuzer genomen. Bereid dit voor:

- Wat is er precies gebeurd? Schrijf in 5–10 zinnen het verloop op.
- Wanneer? Datum, tijd, in welke volgorde.
- Bedragen / accounts / IBANs.
- Schermafbeeldingen (mail, sms, app, bankafschrift).
- Wat heb je zelf al gedaan? (Bank gebeld, codes gewijzigd, gemeld.)

Wanneer is het écht spoed (112)?

- Iemand bedreigt jou of je familie nu, persoonlijk.
- Iemand staat letterlijk voor de deur die zegt "namens de bank" of "politie" jouw kaart of geld op te halen.
- Sextortion van een minderjarige waarbij chantage binnen uren wordt uitgevoerd.

Voor alle andere zaken: het niet-spoednummer of online aangifte.

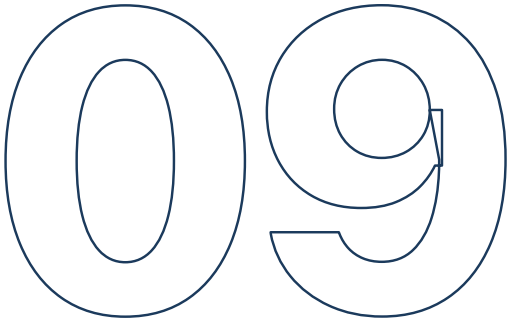
Controlelijst

- [ ] Bank is gebeld (Card Stop BE of bank NL) — referentie genoteerd.
- [ ] Simkaart geblokkeerd bij provider.
- [ ] Hoofd-e-mail-wachtwoord gewijzigd, sessies uitgelogd, 2FA aan.
- [ ] itsme of DigiD gedeactiveerd (indien telefoon weg).
- [ ] Schermafbeeldingen / bewijs verzameld.
- [ ] Aangifte gedaan — PV-nummer doorgegeven aan bank.
- [ ] Gemeld bij safeonweb.be (BE) of fraudehelpdesk.nl (NL).
- [ ] Familie / partner ingelicht.

Tot slot. Het gebeurt iedereen weleens. Geen schaamte — wel snelheid. Hoe sneller en methodischer je handelt, hoe minder schade blijft hangen. En als het achter de rug is: pauze van een avond, daarna kijken wat je in modules 1–7 nóg een tandje strakker kunt zetten.

Volgende stap → Module 9 — Zelfstandigen-extra (Premium) als je een eenmanszaak hebt. Anders: gefeliciteerd — je hebt het hoofddeel afgerond.

MODULE 09 · ZELFSTANDIGEN (PREMIUM) ~ 120 MINUTEN · 10 PAGINA'S



Zelfstandigen-extra

Voor wie thuis werkt of een eenmanszaak heeft. Klantgegevens, facturatie en bedrijfscontinuïteit — zonder een hele IT-afdeling op te tuigen.

WAT GA JE LEREN?

- Wat AVG-conforme klantadministratie thuis minimaal vraagt.
- Hoe je factuurfraude en CEO-fraude voorkomt.
- Een eenvoudig back-up- en herstelplan voor één persoon.

WAT HEB JE STRAKS?

Een ingevuld verwerkingsregister, een back-upschema (3-2-1), en een continuïteitsblad voor het geval je laptop morgen verdwijnt.

GESCHATTE TIJD

2 uur · in 2–3 sessies

WAT HEB JE NODIG?

- Je facturatieprogramma en/of boekhouder-toegang
- Een externe schijf of cloud-opslag
- Een rustig uur zonder klanten aan de lijn

Alleen relevant voor eenmanszaken / freelancers. Gezinslezers slaan deze module gerust over.

MODULE 9 · INLEIDING

Eén persoon. Eén laptop. Heel veel verantwoordelijkheid.

Voor een eenmanszaak gelden grotendeels dezelfde regels als voor een multinational — minus de IT-afdeling. Deze module behandelt drie zaken die een gezinsmodule niet raakt: AVG-conforme klantadministratie, factuur- en CEO-fraude, en een back-up-plus-continuïteitsblad dat je werk redt als jij of je laptop morgen weg is.

Drie principes voor deze module

1. **Documenteer minimaal, maar wel.** Eén bladzijde verwerkingsregister, één bladzijde continuïteit. Geen 40-pagina-handboek.
2. **Aanvallers volgen het geld.** Hoe groter je facturen, hoe gerichter de poging. Wees extra paraat rond loonweek of grote contractmomenten.
3. **Plan voor je afwezigheid.** Ziekte, verhuizing, vakantie — niet alles mag stilvallen omdat het op één telefoon staat.

Wat we vandaag doen

- Een verwerkingsregister invullen (één pagina).
- Beslissen waar klantgegevens leven en hoe lang.
- Een IBAN-wijzigingsprocedure invoeren om factuurfraude te stoppen.
- Een 3-2-1 back-up draaien én testen.
- Een continuïteitsblad invullen voor vertrouwd persoon / partner.

> ¡ **Reken op 2 uur — in 2 of 3 sessies.**
> Niet alles tegelijk; dat houdt geen freelancer vol. Eén weekend voor AVG-pagina's, één avond voor back-up, één lunchpauze voor continuïteitsblad.

Casus

Sofie (39), grafisch ontwerper, Mechelen. Stuurt een factuur via e-mail aan een grote klant. Aanvaller had eerder via een gehackte mailtoegang het bericht onderschept en stuurt een dag later een "correctie": "Excuses, betaal aub op deze rekening: BE… (nieuw)." De klant betaalt €4.870 op die andere rekening. — Eén IBAN-wijzigingsprocedure (pagina 90) had het voorkomen.

MODULE 9 · THEORIE-LIGHT

AVG voor de eenmanszaak — in één bladzijde

De AVG is niet voor multinationals geschreven; ze geldt ook voor jou. De belangrijkste verplichtingen voor een freelancer of eenmanszaak in BE/NL:

Verplichting	Wat het concreet betekent
Doel-binding	Klantgegevens alleen gebruiken waarvoor ze gegeven zijn. Geen nieuwsbrief sturen aan klanten die daar niet expliciet toestemming voor gaven.
Dataminimalisatie	Vraag alleen wat je nodig hebt. Geen geboortedatum als je 'm niet nodig hebt voor een rolverdeling of contract.
Beveiliging	Wachtwoordkluis, 2FA, versleutelde schijf, back-up. (Modules 1, 5.) Voor papier: afsluitbare kast.
Verwerkingsregister	Eén document waarin je opschrijft welke data je waarvoor verwerkt. Verplicht boven 250 medewerkers, sterk aanbevolen voor élke onderneming.
Verwerkersovereenkomst	Met elke externe partij die klantdata voor jou verwerkt (boekhouder, factuurtool, e-mailmarketing): een korte overeenkomst (DPA).
Datalekmeldplicht	Lek? Binnen 72 uur melden bij GBA (BE) of AP (NL) als er risico voor de betrokkenen is.
Rechten van betrokkenen	Klanten mogen inzage / correctie / verwijdering vragen. Reageer binnen één maand.

★ **De boete die mensen vrezen, valt mee — maar het reputatieverlies niet.**
De GBA / AP geeft eerst meestal een waarschuwing en een termijn om het op te lossen. Echte boetes komen vooral als je traineert. Maar een datalek dat in de pers komt: dat is voor een eenmanszaak vaak veel duurder dan welke boete dan ook.

MODULE 9 · AAN DE SLAG · STAP 1 VAN 6

Stap 1 — Verwerkingsregister

Eén pagina, eens per jaar bijwerken. Vul de tabel hieronder in met jouw situatie.

VERWERKING	DOEL	CATEGORIE GEGEVENS	BEWAARTERMIJN	WAAR OPGESLAGEN	VERWERKERS
Facturatie	Boekhouding (wettelijk verplicht)	Naam, adres, btw-nr., bedrag	7 jaar (BE/NL fiscaal)		
Klantcontact	Uitvoering opdracht	Naam, e-mail, tel.	2 jaar na laatste opdracht		
Nieuwsbrief	Marketing (met toestemming)	Naam, e-mail	Tot uitschrijving		
CV's / sollicitatie	Werving	CV, brief, contact	4 weken na afwijzing		

Mijn typische verwerkers — invullen

BOEKHOUDER

FACTURATIE-TOOL

E-MAIL / AGENDA

CLOUD-OPSLAG (DRIVE / ICLOUD / ONEDRIVE)

NIEUWSBRIEF-PLATFORM

BETALING (PSP / BANKKOPPELING)

> **DPA's verzamelen kost één avond.**
> Elke aanbieder (Google, Microsoft, Apple, Stripe, Mollie, Mailchimp, Teamleader…) heeft een verwerkersovereenkomst op zijn site. Download, sla op in je administratie. Klaar.

MODULE 9 · AAN DE SLAG · STAP 2 VAN 6

Stap 2 — Waar leven je klantgegevens?

Voor een freelancer is dat zelden één plek. Doel: een eerlijke kaart maken, dubbele kopieën opruimen, en bewaartermijnen instellen.

Veelvoorkomende plekken

- E-mail-inbox — vooral oude mails met bijlagen.
- Facturatie-tool (Teamleader, Yuki, MoneyMonk, Bonsai, e-Boekhouden).
- CRM of spreadsheet met klanten.
- Cloud-mappen met projecten (Drive / iCloud / Dropbox).
- Lokale mappen op je laptop ("Bureaublad/Klanten 2023").
- WhatsApp Business of gewone WhatsApp — chats met klanten.

De opruim-routine — één keer per kwartaal

1 **Centraliseer**
Eén officiële plek voor klantcontracten en facturen (bij voorkeur je facturatie-tool of een vaste cloud-map). Geen dubbele kopieën in 4 plekken.

2 **Verwijder oude bijlagen**
E-mails met grote bijlagen ouder dan 3 jaar: archiveer of verwijder. Buiten de wettelijke bewaartermijnen (7 jaar fiscaal) geen reden om ze in je inbox te laten rondhangen.

3 **Versleutel waar mogelijk**
Cloud-mappen: gebruik clients die end-to-end versleutelen (Proton Drive, Tresorit) voor gevoelige projecten. Anders: in elk geval een versleutelde schijf op je laptop (Module 5).

4 **Audit-spoor bijhouden**
Bij grotere klanten: noteer kort wanneer je hun gegevens hebt ontvangen, waarvoor, en wanneer je ze hebt verwijderd. Eén regel per klant — niet meer.

> ! **WhatsApp Business is niet AVG-vriendelijk by default.**
> Praktisch is het soms onvermijdelijk. Houd dan: zo min mogelijk gevoelige info in chats, en haal exports / back-ups regelmatig op om WhatsApp niet je enige bron te laten zijn.

MODULE 9 · AAN DE SLAG · STAP 3 VAN 6

Stap 3 — Factuurfraude voorkomen

Eén van de meest schadelijke vormen voor zelfstandigen: een aanvaller onderschept jouw factuur, verandert de IBAN, en je klant betaalt aan een ander. Of omgekeerd: jij betaalt aan een factuur die niet van je leverancier blijkt te zijn.

De IBAN-wijzigingsprocedure

Spreek met alle klanten en leveranciers af:

1. Een gewijzigd rekeningnummer wordt **nooit** per e-mail bevestigd.
2. Bij elke wijziging: één telefoongesprek via een eerder bekend nummer (niet uit de mailhandtekening) ter bevestiging.
3. Schriftelijk vastleggen — bv. PDF op briefpapier met handtekening.

ECHT VOORBEELD · FACTUURFRAUDE-MAIL BE / NL

```
Van: factuur@sofie-design[.]be (vermoedelijk vervalst)
Onderwerp: Re: Factuur 2026-104 – correctie

Beste klant,

Met excuses – ons rekeningnummer
is recent gewijzigd. Wilt u de
betaling op deze rekening uitvoeren:

  BE.. .... .... ....
  t.n.v. Sofie Design

Vriendelijke groet,
Sofie
```

Drie rode vlaggen.

1. Wijziging van IBAN per e-mail, zonder telefoongesprek.
2. Afzender lijkt op die van Sofie, maar is subtiel anders (streepje, ander TLD, extra letter).
3. Urgentie ("snel betaling uitvoeren") — patroon 6 uit Module 3.

In je factuur expliciet vermelden

Zet onderaan je factuur, in dezelfde regel als je IBAN:

> ℹ *"Onze betaalgegevens wijzigen niet zonder schriftelijke aankondiging op papier. Twijfel? Bel ons op [nummer]."*

Voor jouzelf: leveranciersfacturen

- Eerste keer aan een nieuwe leverancier betalen → bel ze voor bevestiging.
- Bestaande leverancier met "nieuw rekeningnummer" → bellen, niet mailen.
- Betaal grote bedragen niet 's avonds onder druk; slaap er een nacht over.

MODULE 9 · AAN DE SLAG · STAP 4 VAN 6

Stap 4 — Spear-phishing & CEO-fraude

"CEO-fraude" is klassiek voor grote bedrijven, maar de variant bestaat ook voor freelancers — een gerichte phishing met inhoudelijke kennis over jouw werk en klanten. Aanvallers volgen je LinkedIn, je portfolio, je nieuwsbrieven.

Typische zinnen — herken ze

ECHT VOORBEELD · SPEAR-PHISHING NL / BE

```
Van: "Jeroen van [klantbedrijf]" <jeroen.va.[bedrijf]@gmail.com>
Onderwerp: Snelle vraag – tussen vergaderingen door

Hoi [JOUW VOORNAAM],

Zit nu in vergaderingen met onze
juridische team. Kun jij voor mij
even snel een Bol-voucher van EUR
500 kopen en de codes doorsturen?
Hou je in de gaten – ik betaal je
vandaag terug.

Sorry voor de haast, dit moet snel.
Verstuurd vanaf mijn telefoon.
```

Vier rode vlaggen.

1. Afzender lijkt een klant maar gebruikt een Gmail / extern adres in plaats van het bedrijfsdomein.
2. Vraag om cadeaubonnen — wereldwijd de #1 indicator van fraude.
3. Druk ("snel", "tussen vergaderingen", "vandaag terug").
4. Verzoek dat *buiten* de normale werkrelatie valt.

De drie verdedigingsregels

- **Cadeaubonnen kopen voor anderen — nooit.** Geen enkele legitieme klant of werkgever vraagt dit.
- **Buitengewone verzoeken — buitengewone verificatie.** Bel terug via een eerder bekend nummer voor je iets doet.
- **Slaap erover.** Buiten brand of bloed is er bijna nooit een verzoek dat niet 24 uur kan wachten.

> ★ **Beperk je publiek zichtbare informatie.**
> LinkedIn-bio met "freelance copywriter voor [klant]" of een nieuwsbrief die exacte project-details deelt — dat is precies de informatie waar een spear-phisher mee werkt. Houd het vager.

MODULE 9 · AAN DE SLAG · STAP 5 VAN 6

Stap 5 — 3-2-1 back-up, getest

De gezinsversie (Module 5) was een mooi begin. Voor een onderneming wil je de strenge versie: drie kopieën, twee media, één buitenshuis. Want als jouw laptop morgen verdwijnt, verdwijnt je bedrijf niet.

1 **Kopie 1 — live op je werkapparaat**
Je dagelijkse werkbestanden, op een laptop met versleutelde schijf (FileVault / BitLocker). Niets bijzonders — je hebt 'm al.

2 **Kopie 2 — wekelijks op een externe schijf**
Externe SSD, ook versleuteld. Eén keer per week aansluiten, back-up (Time Machine / File History) laten draaien, schijf uitwerpen, in een kast leggen. Liefst niet altijd in de werkkamer.

3 **Kopie 3 — continu in een veilige cloud**
Een aanbieder met "versies" en "papierwand"-functie tegen ransomware (iCloud Drive, OneDrive Business, Google Drive Business, Proton Drive). Synchronisatie aan voor je werkbestanden.

4 **Test — twee keer per jaar**
Pak een willekeurig bestand uit elke kopie. Open het. Bewerk een regel. Sla op. Lukt het? Mooi. Zet een herinnering op 1 januari en 1 juli.

> ! **Ransomware: de back-up moet "los" zijn.**
> Ransomware versleutelt alles wat je laptop kan zien — inclusief gekoppelde externe schijven. Daarom: schijf altijd loskoppelen na back-up. En cloud-opslag met "versies" — niet alleen synchronisatie.

Mijn back-up — schema

EXTERNE SCHIJF — WAAR / WANNEER

EERSTVOLGENDE TEST-DATUM

CLOUD-AANBIEDER

TWEEDE TEST-DATUM

MODULE 9 · AAN DE SLAG · STAP 6 VAN 6

Stap 6 — Continuïteitsblad

Eén bladzijde die je partner, vertrouwd persoon of boekhouder in staat stelt jouw onderneming voor één tot vier weken voort te zetten — of netjes op pauze te zetten — als er jou iets overkomt.

Belangrijke contacten

MIJN VERTROUWD PERSOON (VOLLEDIGE NAAM + TEL.)

BELANGRIJKSTE 1–3 KLANTEN + CONTACTPERSOON

MIJN BOEKHOUDER

MIJN BANK — RELATIEBEHEERDER

MIJN VERZEKERAAR (BA, RECHTSBIJSTAND)

DOMEIN / HOSTING — BIJ WIE?

Toegang tot de essentie

Schrijf hieronder *geen wachtwoorden*. Wel: waar de wachtwoordkluis-master ligt, welke kluis-aanbieder, en welke "*Emergency Access*" is ingesteld voor wie. (Module 1, pagina 15.)

WACHTWOORDKLUIS (AANBIEDER + E-MAIL)

EMERGENCY ACCESS INGESTELD VOOR

MASTER-HINT / -PLEK

WACHTTIJD INGESTELD OP

Wat te doen — eerste 48 uur

1. Vertrouwd persoon belt boekhouder + bank.
2. Out-of-office instellen op zakelijk e-mailadres met verwijzing naar boekhouder.
3. Lopende opdrachten: contact opnemen met de 1–3 klanten hierboven.
4. Eventueel: site-update — "Tijdelijk niet beschikbaar".
5. Geen overhaaste opzeggingen of grote betalingen.

> ★ **Bespreek dit blad met je vertrouwd persoon.**
> Vooraf, in rustige tijd. Eén koffie. Met dit blad. Dat ene gesprek is meer waard dan elk handboek.

MODULE 9 · CONTROLELIJST & AFSLUITING

Klaar? Loop dit af.

- [ ] Mijn verwerkingsregister (pagina 88) is ingevuld en in mijn administratie opgeslagen.
- [ ] Verwerkersovereenkomsten (DPA's) van mijn belangrijkste tools zijn gedownload.
- [ ] Eén officiële plek voor klantcontracten en facturen — geen dubbelen.
- [ ] Mijn factuur vermeldt de IBAN-wijzigingsprocedure.
- [ ] Bij elke leverancier die zijn IBAN wijzigt: bellen, niet mailen.
- [ ] 3-2-1 back-up draait — laptop, externe schijf, cloud — en is getest.
- [ ] Mijn continuïteitsblad (pagina 93) is ingevuld en met mijn vertrouwd persoon doorgenomen.
- [ ] Emergency Access in wachtwoordkluis is ingesteld voor mijn vertrouwd persoon.
- [ ] Ik weet bij welk meldpunt ik een datalek meld (BE: GBA · NL: AP) en binnen welke termijn (72 uur).

Wat als...

? ...ik per ongeluk klantdata kwijt ben (verloren USB, gehackte e-mail)?
Direct: inventariseer wat is gelekt en wie het betreft. Risico voor betrokkenen? Melden bij GBA / AP binnen 72 uur. Vorm: korte mail met feiten, zelfs als nog niet alles duidelijk is. Beter te vroeg en onvolledig, dan te laat.

? ...een klant betaalt mijn factuur niet, maar wel een vervalste?
Geen makkelijke. De juridische realiteit: meestal moet de klant alsnog jou betalen, maar dat kan een rechtszaak betekenen. Direct: aangifte doen voor beide partijen, banken contacteren voor recall, en een advocaat raadplegen (rechtsbijstandsverzekering — Module 4 callout einde).

? ...ik wil een verwerkersovereenkomst weigeren voor mijn klant?
Als klant van jou kan een grote organisatie vragen om een DPA waar jij als verwerker tekent. Lees 'm. Te zware verplichtingen (24/7-rapportageplicht, onbeperkte audits)? Onderhandel, of wijs af. Een rechtsbijstandsverzekering en een DPA-sjabloon van je boekhouder/organisatie helpen hier.

Samenvatting in drie zinnen

1. Eén bladzijde register en één bladzijde continuïteit — meer is voor een eenmanszaak zelden nodig.
2. IBAN-wijziging gaat nooit per e-mail, en cadeaubonnen kopen voor "een klant" is altijd fraude.
3. 3-2-1 back-up met halfjaarlijkse test redt je bedrijf van zowel ransomware als domme pech.

NOODKAART · A5 · UITSCHEUREN OF FOTOKOPIËREN

Eerst dit. Daarna pas paniek.

Hang op de koelkast. Bewaar een tweede in je portefeuille.

1. **Stop alle betalingen.** Bel **Card Stop (BE) 078 170 170** of jouw bank-noodnummer (NL).
2. **Wijzig je e-mailwachtwoord** op een ander apparaat. Log alle sessies uit.
3. **Blokkeer je simkaart** bij je mobiele provider (nummer hieronder).
4. **Deactiveer itsme (BE)** op my.itsme.be of **DigiD (NL)** via 088 123 65 55.
5. **Meld het.** BE: verdacht@safeonweb.be · NL: fraudehelpdesk.nl of 088 786 73 72.
6. **Aangifte bij de politie** — BE: lokaal of police-on-web.be · NL: 0900-8844. Vraag PV-nummer.

Mijn nummers — invullen met pen

Bank noodnummer	Tweede bank
Mobiele provider	Kredietkaart-uitgever
Vertrouwd persoon	Boekhouder (zelfstandigen)

Drie gouden regels — bij twijfel

- De bank, Microsoft en de politie **bellen je nooit** voor codes of overschrijvingen.
- Geef **nooit** een 2FA-, app- of itsme-/DigiD-code aan iemand aan de telefoon.
- Bij druk: **ophangen, een uur wachten, zelf terugbellen** via een nummer dat je kent.

Volledige uitleg: Module 8 (pagina 79).

© CyberScore 2026 · v2026.1

NASCHRIFT · B · 1 VAN 2

Verklarende woordenlijst

In dit werkboek gebruikte termen, B1-niveau uitgelegd. Modules tussen haakjes verwijzen naar de eerste keer dat de term valt.

2FA · tweestapsverificatie
Naast je wachtwoord een tweede bewijs (code, app, hardware-sleutel) voor je kunt inloggen. (Module 0, 1)

Aegis
Open-source authenticator-app voor Android, met back-up-functie. (Module 1)

Authenticator-app
Telefoonapp die elke 30 seconden een nieuwe code laat zien, als tweede stap bij inloggen. (Module 1)

AVG / GDPR
Europese privacywet (Algemene Verordening Gegevensbescherming). Geldt voor BE en NL. (Module 7, 9)

BitLocker
Windows-versleuteling van je harde schijf. Zonder wachtwoord/herstelsleutel onleesbaar. (Module 5)

Bitwarden
Gratis, open-source wachtwoordkluis. Aanrader voor de meeste mensen. (Module 1)

BSN
Burgerservicenummer — Nederlandse identificatie. Behandel als gevoelige data. (Module 2)

Card Stop
Belgische 24/7-dienst om bankkaarten en betaalapps te blokkeren. 078 170 170. (Module 4, 8)

CCB
Centre for Cybersecurity Belgium — federale cyberautoriteit. Beheert safeonweb.be. (Module 3)

CEO-fraude
Aanvaller doet zich voor als jouw klant of leidinggevende om je een snelle betaling of cadeaubon te laten doen. (Module 9)

Credential stuffing
Geautomatiseerde aanvaller-techniek waarbij gelekte e-mail/wachtwoord-combinaties op honderden diensten worden geprobeerd. (Module 1)

Datalek
Onbedoelde toegang tot, verlies van of openbaarmaking van persoonsgegevens. Meldplicht binnen 72 uur (zelfstandigen). (Module 9)

DigiD
Nederlandse digitale identiteit voor inloggen bij overheid en zorg. Drie betrouwbaarheidsniveaus. (Module 2)

DPA · verwerkersovereenkomst
Contract tussen jou en een dienst die voor jou klantdata verwerkt (boekhouder, e-mailtool). (Module 9)

eBox
Officiële digitale brievenbus van de Belgische overheid. mybox.belgium.be. (Module 2)

eID-kaart
Belgische identiteitskaart met chip. Vereist soms een kaartlezer en pincode. (Module 2)

Emergency Access
Functie in 1Password/Bitwarden waarmee een vertrouwd persoon na een wachttijd toegang krijgt tot je kluis. (Module 1, 9)

Family Link
Google-app voor oudertoezicht op Android-toestellen van kinderen. (Module 6)

FileVault
macOS-versleuteling van de harde schijf — de Apple-tegenhanger van BitLocker. (Module 5)

NASCHRIFT · B · 2 VAN 2

Verklarende woordenlijst (vervolg)

FOD Financiën / Belastingdienst
Belgische resp. Nederlandse fiscus. Bereikbaar via myminfin.be / belastingdienst.nl. (Module 3)

Fraudehelpdesk
Nederlandse landelijke meldlijn voor scams en oplichting. fraudehelpdesk.nl · 088 786 73 72. (Module 3, 4, 8)

GBA
Belgische Gegevensbeschermingsautoriteit. Houdt toezicht op AVG-naleving. gegevensbeschermingsautoriteit.be. (Module 7, 9)

Grooming
Volwassene die online vertrouwen opbouwt met een minderjarige, vaak voor seksuele uitbuiting. Strafbaar. (Module 6)

Have I Been Pwned
Site waar je controleert of je e-mailadres in bekende lekken voorkomt. haveibeenpwned.com. (Module 1)

Herstelcode
Eenmalige code (8–10 stuks) die je krijgt bij het inschakelen van 2FA. Voor als je telefoon weg is. (Module 0, 1)

IoT · slim apparaat
Internet-of-Things: apparaat dat zonder klassieke computer aan het internet hangt (deurbel, thermostaat). (Module 5)

itsme
Belgische digitale identiteits- en bevestigings-app, beheerd door Belgian Mobile ID. (Module 2)

Kifid
Klachteninstituut Financiële Dienstverlening — Nederlandse ombudsman voor bankgeschillen. kifid.nl. (Module 4)

MijnOverheid
Nederlandse portaal voor overheidscontact, met de Berichtenbox. mijn.overheid.nl. (Module 2)

Ombudsfin
Belgische ombudsman voor financiële geschillen. ombudsfin.be. (Module 4)

Phishing
Oplichting via mail, sms of telefoon waarin men jou laat klikken of inloggen op een nepsite. (Module 3)

Proton Pass / Proton Drive
Europese (Zwitserse) wachtwoordkluis en versleutelde cloud-opslag. Privacy-vriendelijk. (Module 1, 9)

Ransomware
Schadelijke software die je bestanden versleutelt en losgeld vraagt om ze vrij te geven. (Module 9)

Rijksregisternummer
Belgisch persoonsnummer (op de eID). Gevoelige data — niet zomaar weggeven. (Module 2)

Safeonweb
Belgische meldsite voor verdachte berichten. verdacht@safeonweb.be. (Module 3, 8)

SCA · sterke klantauthenticatie
EU-eis dat banken bij grotere betalingen een tweede bevestiging vragen (via app of digipass). (Module 4)

Sextortion
Chantage met (vermeende) intieme beelden. Komt veel voor bij tieners. (Module 6)

Sim-swap-fraude
Aanvaller zet jouw telefoonnummer over op zijn telefoon om sms-codes te onderscheppen. (Module 1)

Spear-phishing
Gerichte phishing waarbij de aanvaller persoonlijke informatie over jou gebruikt. (Module 9)

Verwerkingsregister
Document waarin je opschrijft welke persoonsdata je waarvoor verwerkt. (Module 9)

WPA2 / WPA3
Versleutelingsstandaarden voor wifi-netwerken. WPA3 is nieuwste; WPA2 is acceptabel. (Module 5)

NASCHRIFT · C · 1 VAN 2

Bronnen & meldpunten — België

Stand: mei 2026. Telefoonnummers en URL's wijzigen soms; check cyberveiligthuis.eu/updates voor de laatste lijst.

Cyberveiligheid & phishing

Safeonweb (CCB)	`safeonweb.be` · meld phishingmail: `verdacht@safeonweb.be`
CCB — Centre for Cybersecurity Belgium	`ccb.belgium.be` — federaal cyberbureau

Bank- en betaalfraude

Card Stop (kaart blokkeren, 24/7)	`078 170 170`
Ombudsfin — geschil met bank	`ombudsfin.be` · gratis
Febelfin — bankensector	`febelfin.be/nl/consumenten`

Identiteit & overheid

itsme	`itsme-id.com` · zelfbediening `my.itsme.be`
eBox — officiële digitale brievenbus	`mybox.belgium.be`
MyMinfin — FOD Financiën	`financien.belgium.be`
BOSA Self-Service — machtigingen	`selfservice.bosa.be`

Privacy & data

Gegevensbeschermings-autoriteit (GBA)	`gegevensbeschermingsautoriteit.be`

Kinderen & tieners

Child Focus (24/7, gratis)	`116 000` · `childfocus.be`
Awel — luisterlijn jongeren	`102` · `awel.be`
Mediawijs — gezinsadvies	`mediawijs.be`

Spoed

Politie (geen spoed, fraude)	`101` · online: `police-on-web.be`
Politie / hulpdiensten (spoed)	`112`

NASCHRIFT · C · 2 VAN 2

Bronnen & meldpunten — Nederland

Stand: mei 2026.

Cyberveiligheid & phishing

Fraudehelpdesk	`fraudehelpdesk.nl` · `088 786 73 72`
Spam- of phishing-sms doorsturen	`7726` (gratis)
NCSC — Nationaal Cyber Security Centrum	`ncsc.nl`
Veiliginternetten — algemene info	`veiliginternetten.nl`

Bank- en betaalfraude

Kifid — geschil met bank/verzekeraar	`kifid.nl` · gratis
Betaalvereniging Nederland	`betaalvereniging.nl/veiligbetalen`

Identiteit & overheid

DigiD-helpdesk (werkdagen 08–22)	`088 123 65 55` · `digid.nl`
MijnOverheid — Berichtenbox	`mijn.overheid.nl`
Machtigen via DigiD	`machtigen.digid.nl`
Belastingdienst	`belastingdienst.nl`

Privacy & data

Autoriteit Persoonsgegevens (AP)	`autoriteitpersoonsgegevens.nl`

Kinderen & tieners

Veilig Thuis (24/7, gratis)	`0800-2000` · `veiligthuis.nl`
Helpwanted — online seksueel misbruik	`helpwanted.nl`
Kindertelefoon	`0800-0432` · `kindertelefoon.nl`
Pestweb / Stichting Stop Pesten Nu	`stoppestennu.nl`

Spoed

NASCHRIFT · D

Update-log

Het cyberlandschap evolueert snel. Hieronder zie je per versie wat wijzigde. Actuele versie altijd op `cyberveiligthuis.eu/updates`.

v2026.1 mei 2026	**Eerste editie.** Volledig werkboek met 10 modules (0–9), noodkaart, woordenlijst en bronnenlijst voor BE en NL. Verifieerbare nummers: Card Stop 078 170 170 · DigiD 088 123 65 55 · Fraudehelpdesk 088 786 73 72 · Child Focus 116 000 · Veilig Thuis 0800-2000.
v2026.2 najaar 2026 (geplande update)	Halfjaarlijkse herziening: gecontroleerde URL's en nummers, nieuwe scampatronen uit BE/NL-meldingen, eventuele wijzigingen in bank-app-paden (Module 4).
v2027.1 mei 2027 (geplande update)	Jaarlijkse hoofdupdate.

Iets gemerkt dat klopt niet meer?

Help mee de volgende editie scherp te krijgen. Mail je opmerking, foto van een achterhaalde URL of nieuwe scam-trend naar `updates@cyberveiligthuis.eu`. Met naamsvermelding (als je dat wil) in de volgende editie.

Een rustig, doe-gericht werkboek voor wie thuis wil weten dat het klopt — zonder cybersecurity-jargon en zonder bangmakerij.

10 modules · 1 noodkaart · 100 pagina's · BE & NL