

 [LUISTER DIT VERSLAG](#)

-10%

1,0x

+10%

+25%

1,0x

↓ [Download naar telefoon](#)

►  [Lees mee met de podcast](#)

Waar dit vandaan komt

Je stuurde vanochtend een Spotify-afl levering: "What's your data worth on the dark web?" Dat is de podcast van Malwarebytes, het beveiligingsbedrijf. 24 minuten, Engels.

Ik heb de hele afl levering getranscribeerd en gelezen. Dit is wat erin zit, en wat jij ermee moet.

Het schokkende antwoord: 95 cent

Een complete gestolen identiteit kost op het dark web **95 dollarcent**.

Zo'n pakket heet een "fullz": volledige naam, burgerservicenummer, geboortedatum, adres. Genoeg om op jouw naam een lening te openen, een belastingteruggave te claimen, of zorg af te nemen.

De maker zegt het zo: voor minder dan een kop koffie koopt een crimineel genoeg om iemands financiële leven te slopen.

De schaal: alleen al in de eerste helft van 2026 vond Malwarebytes **8,4 miljard gestolen records** op het dark web, verdeeld over 7.500 datasets.

De kern van de afl levering

Adverteerders en cybercriminelen doen hetzelfde: allebei kopen ze jouw data om je gedrag te sturen.

- De adverteerder gebruikt je zoekgedrag om je een bank te verkopen.
- De crimineel gebruikt precies dezelfde soort data om een nepmail geloofwaardig te maken.

Het verschil is alleen wat legaal is.

De makkelijkste aanval: jouw herhaalde wachtwoord

Dit is het belangrijkste stuk voor jou.

De nummer 1 aanval heet credential stuffing. Die werkt zo:

- Een site waar jij ooit een account had wordt gehackt
- Jouw wachtwoord belandt op het dark web
- Automatische tools proberen dat wachtwoord op AL je andere accounts
- Gebruik je hetzelfde wachtwoord voor je mail, je bank en Netflix, dan is één lek genoeg voor alles

Je mailbox is daarbij de hoofdprijs. Wie in je mail zit, kan zich als jou voordoen bij iedereen die je kent.

De "hello pervert"-truc — goed om te herkennen

Er gaat een afpersmail rond die begint met "hello pervert". De afzender beweert dat hij je camera heeft overgenomen en een gênante video van je heeft. Betaal 1.200 dollar in bitcoin, anders stuurt hij hem naar al je contacten.

Het is leeg. Er is geen video. Er is geen hack.

Wat het eng maakt: de mail bevat soms een ECHT oud wachtwoord van je, of zelfs een Google Maps-foto van je huis. Die zijn los gekocht op het dark web en erin geplakt als nepbewijs.

Krijg jij of iemand van het team zo'n mail: niet betalen, niet antwoorden, weggooien.

De nieuwe dreiging: deepfakes

Uit hun onderzoek van vorige maand: **1 op de 10 mensen** is al eens afgeperst met een AI-gemaakte nepfoto (naakt).

Daar is geen dark web voor nodig. Eén foto van Instagram of Facebook is genoeg.

De maker noemt het treffend: we gaan van identiteitsdiefstal naar identiteitsmisbruik.

Wat dit voor jou en Haarvisie betekent

Vier acties, in volgorde van belang:

1. **De zes wachtwoorden die al op je lijst staan vervangen.** Dit verslag is precies de reden waarom dat punt bestaat. Uniek wachtwoord per dienst, uit een wachtwoordmanager.
 2. **Tweestapsverificatie op alles wat ertoe doet:** mail, bank, Meta, Telegram. De Meta-hack van 2.649 euro was een account-overname — dit is het slot dat die deur dichthoudt.
 3. **Het team één ding leren:** een dreigmail met een echt wachtwoord of een foto van je huis erin is GEEN bewijs van een hack. Het is knip- en plakwerk van gekochte data.
 4. **Klantendata is ook data.** De salon bewaart namen, nummers en afspraken. Alles wat wij lekken, wordt handel. Dat is geen paniek, dat is een reden om het netjes te houden.
-

De zin om te onthouden

"Voor een crimineel ben jij een rekensom: wat kost het om bij jouw geld te komen. Maak die som zo duur mogelijk."

Bron: Lock and Code (Malwarebytes), aflevering van 26 juli 2026, volledig getranscribeerd op 11 augustus.