# Naslagwerk Cybersecurity

fox & fish cyberdefense

## Tips, Referenties & Nuttige Links

# Top 10 Tips

1. **Hergebruik geen wachtwoorden**, maar bewaar ze in je browser of in een password manager. Heb je al op 200 plaatsen hetzelfde wachtwoord? Neem dan gewoon je 10 meest gebruikte accounts (bedrijfsaccounts, privé email, Facebook, …) en verander daar je wachtwoord naar iets uniek.

2. **Kies je wachtwoorden niet zelf**, maar gebruik steeds een écht willekeurig wachtwoord. Zo kom je later niet bedrogen uit. Dankzij je browser of password manager hoef je in principe slechts een paar wachtwoorden zelf te kunnen onthouden. In dit document staan enkele password generators voor het genereren van veilige én onthoudbare wachtwoorden.

3. **MFA (multi-factor authenticatie) is een grote stap vooruit, maar enkel als je er voorzichtig mee omspringt.** Geef je MFA codes daarom nooit door via de telefoon of op een onbetrouwbare website/toestel, en omgekeerd, neem nooit MFA codes aan van een onvertrouwde bron.

4. **Bij vermoeden van een geïnfecteerd toestel, schakel het onmiddellijk uit** door de aan/uit-knop te blijven inhouden, en contacteer nadien meteen een IT deskundige. Zie ook de eerste hulp pagina van Safeonweb.

5. **Bij het lezen van je emails, wees alert, maar ook niet paranoïde**. Bij twijfel, aarzel dan niet om de afzender even te bellen ter verificatie. Handel proportioneel: hoe riskanter de email, hoe nuttiger om de inhoud onafhankelijk te verifiëren.

6. **Mobiele toestellen (Android en iOS) zijn over het algemeen veiliger dan desktops (Windows en macOS)**. Wil je jezelf of anderen eenvoudig beter online beschermen? Overweeg dan om zo veel mogelijk gebruik te maken van een Android tablet, een iPad, een Chromebook, of dergelijke.

7. **Zorg dat alle software op je toestellen up-to-date blijft.** Op Android en iOS hoef je hier weinig tot niets voor te doen; de Play Store of App Store installeert updates automatisch. Wees conservatief met het downloaden van software van willekeurige websites, het installeren van spelletjes, enzovoort. Als je software niet langer gebruikt, verwijder deze dan weer. Windows en macOS moeten ten allen tijde een up-to-date antivirus hebben. Op Windows kies je best Microsoft Defender, op macOS kan je een populaire antivirus naar keuze nemen.

8. **Hackers verzinnen de meest creatieve scenario's om je onder druk te zetten, in de war te brengen, op je emoties in te spelen, te chanteren, enzovoort.** Als een bepaalde situatie je overvalt, wees dan assertief, neem tijd om na te denken, of overleg met iemand anders. Even wachten met reageren leidt meestal niet tot problemen, overhaaste beslissingen vaak wel.

9. **Zie je iets verdachts op kantoor (een onbekende persoon die zich vreemd gedraagt, USB sticks op ongebruikelijke plaatsen, etc.)?** Spreek onbekende personen aan en meld mogelijke risico's.

10. **Hackers zijn geen tovenaars**. Iedere demo die we zagen, vertrouwde op een zwakke plek: lang geen updates installeren, traag of verkeerd op een incident reageren, voorspelbare of hergebruikte wachtwoorden, … Met een beetje goede gewoontes en een gezonde kritische ingesteldheid kom je bijzonder ver.

# Veilig Online

## Safeonweb

De overheidssite Safeonweb biedt uitstekende middelen om te helpen met je online veiligheid:

- Een **app** om je WiFi netwerk te monitoren op verdachte activiteit, en om op de hoogte te blijven van de nieuwste phishing aanvallen die de ronde doen: https://safeonweb.be/safeonweb-app.
- Een **browser plugin** om te helpen de betrouwbaarheid van websites in te schatten: https://safeonweb.be/nl/safeonweb-browser-extension.
- **Lesmateriaal** om spelenderwijs over cybersecurity te leren: https://safeonweb.be/lesmateriaal.
- Tal van **nuttige links**, bijvoorbeeld naar overheidssites om melding te maken van incidenten, of gewoon naar websites om meer te leren over cybersecurity: https://safeonweb.be/nuttige-links.

In het bijzonder de volgende drie pagina's zijn waardevol:

Eerste hulp!

Heb je een probleem?

Hoe veilig ben jij?

Doe onze testen!

Veilig internetten

Tips om veilig te surfen

# Datalekken

Hieronder staan enkele websites waarmee je kan controleren welke data er ooit over jou is gelekt op het internet. Er staan ook betalende sites bij waarmee je vrij datalekken kan doorzoeken. Je mag dergelijke sites gerust gebruiken om jezelf op te zoeken, maar je mag niet zomaar de persoonlijke gegevens van anderen opvragen zonder hun toestemming.

*Dit document is geen juridisch advies. Wij aanvaarden geen enkele verantwoordelijkheid of aansprakelijkheid voor de in dit document verstrekte informatie.*

## Have I Been Pwned

Op deze gratis site kan je een emailadres of telefoonnummer ingeven om na te gaan welke informatie over jou is gelekt, en via welke websites. De gelekte gegevens zelf krijg je daarbij niet te zien. Je kan ook vragen om op de hoogte gehouden te worden over nieuwe datalekken via dit formulier: https://haveibeenpwned.com/notifyme. Het waarschuwen over gelekte wachtwoorden, zoals Have I Been Pwned onder meer kan doen, is overigens ingebouwd in alle moderne password managers. Dat is dus een reden te meer om een password manager te gebruiken.

- https://haveibeenpwned.com

## DeHashed

Op deze **betalende site** kan je gelekte gegevens doorzoeken uit tal van verschillende datalekken.

- https://dehashed.com

## Snusbase

Op deze **betalende site** kan je gelekte gegevens doorzoeken uit tal van verschillende datalekken.

- https://snusbase.com

## Hardware Tokens


Hardware tokens zijn USB sticks die fungeren als fysieke sleutels om je online accounts te beveiligen. Net zoals je een autosleutel nodig hebt om je auto te starten, kan je ook een fysieke sleutel vereisen om bijvoorbeeld op je Google, Microsoft of Facebook account in te loggen. Hoewel geen enkele login methode je onhackbaar maakt, kan een hacker niet langer je login gegevens stelen via phishing wanneer je login methode bestaat uit een fysiek object.

Als je deze login methode zou gaan gebruiken, denk dan ook aan mogelijk verlies van je sleutel. Je kan ofwel 2-3 sleutels aankopen die je op verschillende plaatsen bewaart, ofwel accountherstel methoden instellen die geen sleutel vereisen. Onder Accountbeveiliging vind je de juiste pagina's terug om dit in te stellen.

Populaire hardware tokens zijn:

- De **YubiKeys** van Yubico: https://yubico.com/store. Je kiest hier best voor de YubiKey 5 Series, of, als je de sleutels wilt beveiligen met je vingerafdruk, voor de YubiKey Bio Series.
- De **Titan Security Key** van Google: https://store.google.com/product/titan_security_key.

In tegenstelling tot wachtwoorden, kan je hardware tokens veilig voor verschillende accounts tegelijk gebruiken. Mocht je hardware tokens van je werkgever krijgen, dan kan je deze ook veilig voor je privé accounts gebruiken, maar hou er rekening mee dat je niet meer over deze sleutels beschikt als je van werkgever verandert. De bovenvermelde hardware tokens werken ook allemaal op smartphones en tablets via NFC (houd de sleutel simpelweg tegen de rug van het toestel om aan te melden).

## Privacy

- Awesome Privacy: deze pagina bevat een lange lijst van websites en software die je privacy niet respecteren, en alternatieven die dat wel doen. Of je nu op zoek bent naar een media player, een chat app, een password manager, een email provider, een fitness app of een VPN, dankzij deze pagina kan je privacy-vriendelijke opties terugvinden.
- *Privacy Not Included: privacy scores voor tal van producten, gaande van internet of things (smartwatches, smart speakers, smart camera's, slimme weegschalen, ...), tot dating apps, tot zelfs automerken. Alvorens een product te kopen of een abonnement te nemen, kan je op deze site nakijken in hoeverre je privacy gerespecteerd zal worden.
- Privacy Matters: een gecureerde lijst van Firefox add-ons die je helpen om van Firefox een nog meer privacy-vriendelijke browser te maken.
- Proton: een privacy-vriendelijk online ecosysteem. Bedrijven als Google, Microsoft en Apple bieden allemaal een ecosysteem bestaande uit email, kalenders, cloud opslag, enzovoort. Proton biedt hiervoor zowel gratis als betalende alternatieven die je privacy respecteren.

# Password Generators

Hieronder een selectie aan password generators om onthoudbare wachtwoorden te genereren in verschillende stijlen. Het idee is dat je deze generators slechts gebruikt voor de 2-3 wachtwoorden die je uit je hoofd moet kennen. Al je overige wachtwoorden zitten best in een password manager, en hoeven dan ook niet onthoudbaar te zijn.

## Willekeurige Nederlandse Woorden

Een reeks van willekeurige Nederlandse woorden. Je kiest zelf of je spaties tussen de woorden zet; dit heeft geen invloed op de sterkte van het wachtwoord.


https://password.utwente.io/nl/#nl/diceware/8k;4

Aanbevolen instellingen:

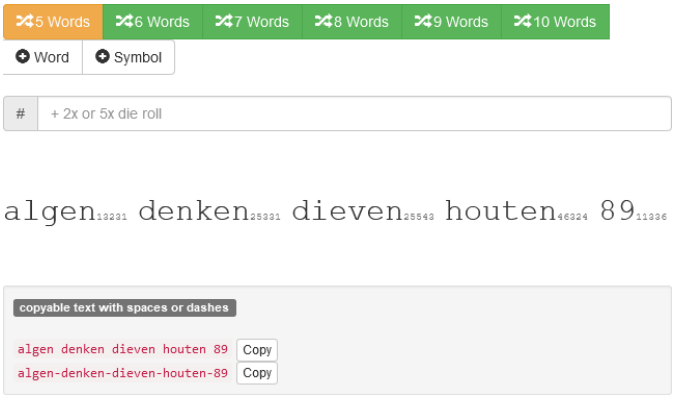
- **Lijst:** Diceware (zonder samenstellingen)
- **Woorden:** 4

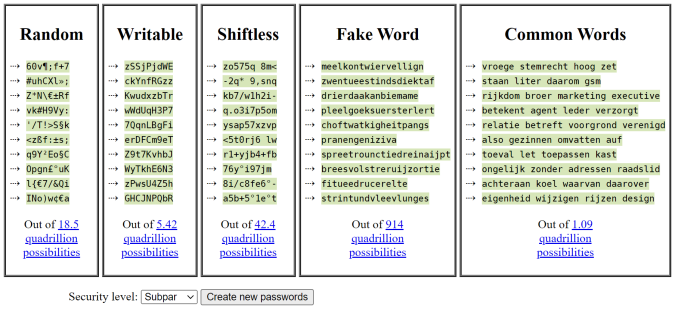
https://diceware.rempe.us/#dutch

Aanbevolen instellingen:

- **5 Words**

*Deze generator zet soms cijfers en symbolen tussen de wachtwoorden, en genereert geen wachtwoorden van minder dan 5 woorden.*




https://passwordcreator.org/nl.html#subpar

Aanbevolen instellingen:

- **Security level:** Subpar

*Kies uit de lijst “Common Words”.*

# Pseudowoord

Een reeks willekeurige lettergrepen, zodat het wachtwoord in principe uitspreekbaar is, en daardoor hopelijk ook makkelijker te onthouden.


https://lastpass.com/nl/features/password-generator

Aanbevolen instellingen:

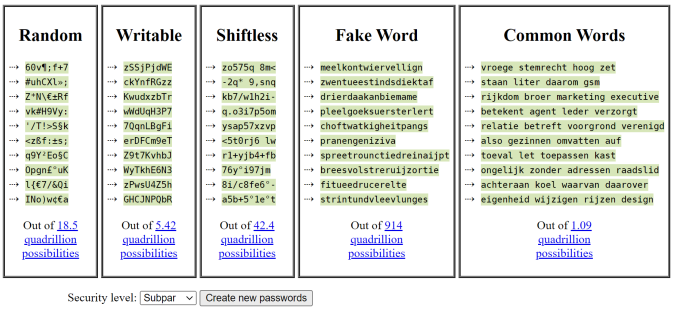
- **Wachtwoordlengte:** 12
- **Eenvoudig uit te spreken**
- Enkel “**Kleine letters**”

https://passwordcreator.org/nl.html#subpar

Aanbevolen instellingen:

- **Security level:** Subpar

*Kies uit de lijst “Fake Word”.*




# Wachtwoordzin

Neem een willekeurige zin uit een willekeurige tekst, bv. een krantenartikel, niets dat speciale betekenis voor jou heeft. Als wachtwoord kan je bijvoorbeeld de eerste letter van ieder woord nemen. Voor een wachtwoord van 12 tekens neem je dan ook best een zin van 12 woorden. Enkele voorbeelden:

**Fantasy Roman**
“Het is te laat op de dag om de poort te openen.” hitloddodpto

**Boek over Tuinieren**
“Plant bij voorkeur een ras dat weerstand biedt aan de schimmel.” pbverdwbads

**Handleiding Koelkast**
“Er kan een probleem met de stroomtoevoer naar het apparaat zijn.” ekepmdsnhaz

# Pincode

Pincodes zijn geschikt voor de beveiliging van toestellen, apps, alarmsystemen, enzovoort. Je probeert beter niet zelf willekeurige pincodes te bedenken, want die blijken vaak niet zo willekeurig als gedacht.


https://password.utwente.io/nl/#generic/numerals:6

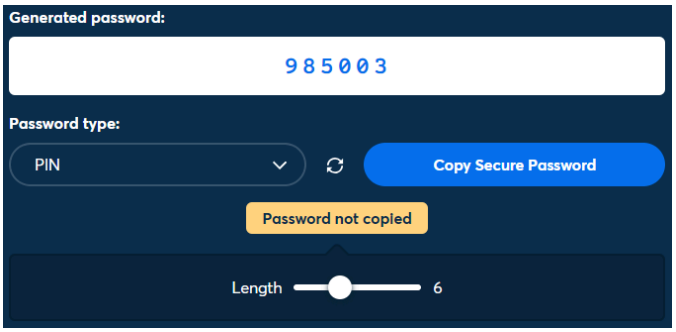
Aanbevolen instellingen:

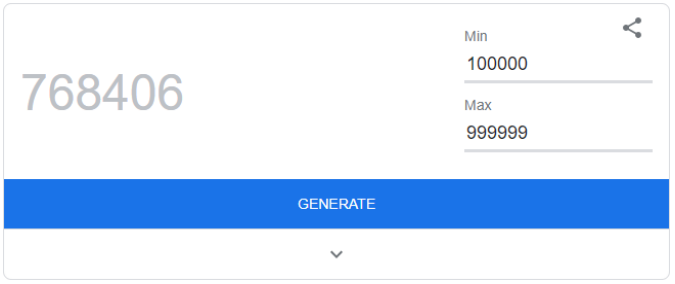
- **Lijst:** Getallen
- **Woorden:** 6

https://1password.com/password-generator

Aanbevolen instellingen:

- **Password type:** PIN
- **Length:** 6




https://google.com/search?q=random+number+between+100000+and+999999

*Je kan nullen en negens toevoegen/weghalen om de lengte van de pincode te wijzigen.*

# Password Managers

Je hebt twee opties: je browser gebruiken als password manager, of zelf een password manager installeren. De eerste optie is makkelijker, de tweede optie biedt meer flexibiliteit.

## Browser

De makkelijkste optie is om je wachtwoorden door je browser te laten beheren, dan hoef je zelf niets te installeren. Zorg enkel dat je op al je toestellen op dezelfde browser account bent ingelogd, zodat je wachtwoorden tussen al je toestellen worden gesynchroniseerd..

Via de volgende links kan je je opgeslagen wachtwoorden en je instellingen beheren:

### Google Chrome

- https://passwords.google.com
  *(werkt in eender welke browser)*
- **chrome://password-manager**
  *(werkt enkel in Chrome)*

### Microsoft Edge

- **edge://wallet/passwords**
  *(werkt enkel in Edge)*

### Apple Safari

- https://support.apple.com/104955
  *(voor iPhone)*
- https://support.apple.com/105115
  *(voor Mac)*

### Mozilla Firefox

- **about:logins**
  *(werkt enkel in Firefox)*

## Zelf Installeren

Je kan ook kiezen om zelf een password manager te installeren. De meest voorkomende redenen daarvoor zijn:

- **Je wilt verschillende browsers naast elkaar gebruiken**, en je wilt je niet binden aan één ecosysteem (zoals dat van Google, Apple of Microsoft).
- **Je wilt bijkomende functies gebruiken, zoals het delen van wachtwoorden met gezinsleden.** Dergelijke functies zijn vaak betalend (tenzij je ze gratis via je werkgever kan krijgen).

Volgende password managers zijn aanbevolen. Klik op het logo om de website te openen.

1Password

bitwarden

Proton Pass

KEEPER

KeePassXC

# Accountbeveiliging

Hieronder een lijst van populaire online platformen. **Al je accounts op de onderstaande platformen zouden een vorm van MFA actief moeten hebben**, naast sterke en unieke wachtwoorden die je best in een password manager bewaart. Ga zeker eens door de onderstaande lijst. Denk ook na of je nog andere accounts hebt die voor jou van bijzonder belang zijn, die gevoelige gegevens bevatten, of waaraan betaalmethoden gekoppeld zijn.

## Email & Browser Accounts

**Google**
https://myaccount.google.com/security

**Microsoft**
https://account.microsoft.com/security

**Apple**
https://appleid.apple.com/account/manage/section/security

**Mozilla**
https://accounts.firefox.com/settings#security

**Yahoo**
https://login.yahoo.com/myaccount/security

*Belgische telecom providers (Telenet, Proximus, Orange, ...) bieden vaak nog geen MFA opties. Het is daarom van zeer groot belang om een sterk en uniek wachtwoord op deze accounts te gebruiken, vooral indien ook je mailbox hieraan gekoppeld is (bv. als je een @telenet.be emailadres hebt).*

## Sociale Media

**Facebook**
https://accountscenter.facebook.com/password_and_security

**Instagram**
https://accountscenter.instagram.com/password_and_security

**TikTok** *(enkel via mobile app)*
https://tiktok.com/safety/youth-portal/keep-your-account-secure

**WhatsApp** *(enkel via mobile app)*
https://faq.whatsapp.com/1095301557782068

**X** (Twitter)
https://x.com/settings/account

**LinkedIn**
https://linkedin.com/mypreferences/d/categories/sign-in-and-security

**Pinterest**
https://pinterest.com/settings/security

# Overige

**CSAM** (Belgische overheid)
https://iamapps.belgium.be/sma/selfManagement/credential

**Doccle**
https://secure.doccle.be/ui/settings/security

**Fluvius** (om enkel login via Itsme/eID toe te laten, kan je “Login via e-mail verwijderen”)
https://mijn.fluvius.be/profiel

**PayPal**
https://paypal.com/myaccount/security

**Amazon**
https://amazon.com/ax/account/manage

**Booking.com**
https://account.booking.com/mysettings/security

**Dropbox**
https://dropbox.com/account/security

# Overige

## Bijzondere Zoekmachines

### Insecam

Insecam toont livestreams van **gehackte internetcamera's** wereldwijd. De camerabeelden zijn doorzoekbaar per land en per type locatie. Er staan een aantal gevoelige soorten locaties tussen, bijvoorbeeld scholen.

- http://insecam.org

### WiGLE

WiGLE is een zogenoemde wardriving site; een website die de **locaties van WiFi netwerken** wereldwijd verzamelt. Je kan de site gebruiken om de naam van een WiFi netwerk te herleiden naar een straatadres, of een straatadres naar het bijbehorende WiFi netwerk. Daarnaast is er ook steeds meer infrastructuur die WiFi netwerken uitzendt, van airco's tot zonnepanelen. Soms is deze infrastructuur vanuit de fabriek slecht beveiligd. Een hacker kan deze interessante doelwitten dan eenvoudig op de kaart terugvinden via WiGLE.

- https://wigle.net

### PimEyes

PimEyes is een **betalende** site voor "**reverse face search**"; als je enkele foto's van een persoon uploadt, dan zoekt de websites andere foto's van dezelfde persoon op het internet. Je mag enkel opzoekingen doen van meerderjarigen, en enkel mits toestemming van de persoon in kwestie, maar dit wordt niet goed afgedwongen. De website werkt opvallend goed en weet soms oude en vergeten foto's te vinden.

- https://pimeyes.com

### RansomWatch & RansomLook

RansomWatch & RansomLook zijn twee gelijkaardige websites die de activiteiten van hacking groepen monitoren. Op deze sites zijn slachtoffers van ransomware terug te vinden, en onrechtstreeks vaak ook de download links naar de data van slachtoffers die het losgeld niet hebben betaald.

- https://ransomwatch.telemetry.ltd
- https://ransomlook.io

# Hacking Hardware

Tijdens de sessie(s) is mogelijk hacking hardware aan bod gekomen. Als je geïnteresseerd bent om zelf dergelijke hardware aan te kopen, dan kan dat onder meer via volgende websites. Deze hardware kan legaal gebruikt worden:

- Om je eigen beveiliging te testen (controleer wel eerst de eventuele gebruiksvoorwaarden van producten die je test).
- Om de beveiliging van anderen te testen, mits toestemming.
- Binnen een strikt wettelijk kader, om de beveiliging van anderen te testen zonder toestemming. Voor meer informatie, zie:
    - https://dnsbelgium.be/nl/nieuws/ethisch-hacken
    - https://vrt.be/vrtnws/nl/2023/02/14/ethische-hackers-mogen-meer-door-nieuwe-wet

*Dit document is geen juridisch advies. Wij aanvaarden geen enkele verantwoordelijkheid of aansprakelijkheid voor de in dit document verstrekte informatie.*

## Lab401

Lab401 is één van de beste webshops om vanuit Europa hacking hardware te bestellen, inclusief de Flipper Zero en Hak5 producten. Ze hebben ook tal van informatieve artikels over hoe hun producten te gebruiken: https://lab401.com/blogs/academy.

- https://lab401.com

## Flipper Zero

De Flipper Zero is het populaire “hacking speelgoed” waarmee je tal van draadloze technologieën kan manipuleren, zoals NFC, RFID, infrarood en sub-GHz signalen. Er is ook laagdrempelige documentatie over hoe de Flipper Zero te gebruiken op https://docs.flipper.net.

- https://flipperzero.one

## Hak5

Hak5 heeft een groot gamma aan producten die reeds in tal van films en series zijn verschenen. Hun meest bekende product, de USB Rubber Ducky, lijkt een onschuldige USB drive, maar is in realiteit een voorgeprogrammeerd toetsenbord dat, in ideale omstandigheden, op enkele seconden een toestel kan hacken. Een dergelijke aanval kwam recent nog aan bod in het VRT-programma Factcheckers: https://vrt.be/vrtnws/nl/2024/01/16/sensibiliseringsactie-van-vrt-programma-factcheckers-met-usb.

- https://hak5.org

# Cybersecurity in Cijfers

- De **CS-barometer** is een studie die de Vlaamse Regering jaarlijks laat uitvoeren om de cybersecurity maturiteit bij Vlaamse bedrijven in kaart te brengen: https://vlaio.be/begeleiding-advies/digitalisering/cybersecurity/waarom-inzetten-op-cybersecurity/cs-barometer

- **Statista** is een onderzoeksbedrijf dat inzichten publiceert over tal van sectoren, waaronder ook cybersecurity: https://www.statista.com/outlook/tmo/cybersecurity/worldwide.