De waarde en kwetsbaarheid die online gegevens bieden voor good and bad guys

Ricardo Nieuwkamp PhD

Agenda

- Gevaren en gevolgen
- Belang van datalekken voor boeven
- Belang van datalekken voor opsporingsdiensten
- Wat kunnen we eraan doen?
- Usecase

Gevaren

el je vraag

vrt nws

Kostbare passagiersgegevens gestolen

"Eigenlijk sta je als bedrijf met je rug tegen de muur. Nog belangrijker dan je systemen opnieuw online te krijgen, zijn de vele gegevens die dreigen te worden gelekt."

"Ik ga ervan uit dat er in dit geval duizenden passagiersgegevens zijn gestolen. Dat gaat over namen, adressen, geboortedata, telefoonnummers ... Eigenlijk alle identiteitsgegevens die je doorgeeft als je een vlucht boekt."

"Als je geen deal kan sluiten met de hackers, zullen al die identiteitsgegevens, die extreem veel geld waard zijn, verkocht worden aan andere cybercriminelen. Met alle gevolgen van dien."

"Op basis van die data kunnen criminelen slachtoffers veel gerichter proberen op te lichten. Dat is ook wat er een paar jaar geleden is gebeurd met de cyberaanval op afvalintercommunale Limburg.net. Toen zijn de gegevens van meer dan 400.000 Limburgers op het dark web terechtgekomen en zijn veel van die mensen het doelwit geworden voor phishing."

orange Menu Klantenzone

Belangrijke informatie

De bescherming van uw gegevens is onze prioriteit

Bij Orange Belgium staat de bescherming van je persoonlijke gegevens altijd voorop.

Eind juli hebben we een cyberaanval ontdekt waardoor ongeoorloofde toegang werd verkregen tot een van onze IT-systemen.

Op deze pagina leggen we je duidelijk uit wat er gebeurd is, welke maatregelen we genomen hebben en hoe u het beste uw gegevens kan beschermen.

Laatste update: 20 augustus 2025 – 16:30

Je meest gevoelige gegevens zijn beschermd

We willen u eerst en vooral geruststellen, de **volgende gegevens zijn niet geraadpleegd**:

- wachtwoorden
- e-mailadres
- adres
- bankgegevens

Wat we ontdekt hebben

Tijdens het incident werden **bepaalde gegevens geraadpleegd**:

- voor- en achternaam
- telefoonnummer
- simkaartnummer
- PUK-code
- tariefplan

20/08/2025

De Belgische politiediensten zijn vorige week geconfronteerd geweest met een grote phishingcampagne, waarbij een heel aantal valse mails verstuurd zijn vanop @police.belgium.eu-adressen, de domeinnaam die door alle Belgische politiemensen wordt gebruikt. Dat meldt de persdienst van de federale politie. Volgens de federale politie is er geen operationele schade.

Belga

ma 22 sep. 18u53

"De Geïntegreerde Politie werd afgelopen week geconfronteerd met een phishingcampagne", zegt An Berger, woordvoerder van de federale politie. "Op donderdag 18 september werden een heel aantal valse mails verstuurd vanuit @police.belgium.eu-adressen, de domeinnaam die door alle politiemensen van de Geïntegreerde Politie wordt gebruikt. Via deze phishingmails werd gevraagd om op een frauduleuze link te klikken en er identificatiegegevens in te vullen."

Online gegevens

- Bronnen: data lekken, door anderen geplaatst, zelf geplaatst

Gevaren en gevolgen. Wat is een datalek?

- verlies van controle,
- vertrouwelijkheid,
- integriteit,
- beschikbaarheid.

Maastricht University Onderwijs Onderzoek Over de UM

Cyberaanval - een samenvatting

Op maandag 23 december werd de Universiteit Maastricht getroffen door een serieuze cyberaanval. Bijna alle Windows-systemen bleken te zijn geraakt en onder andere ook e-mail kon vanaf dat moment niet meer worden gebruikt.

Type datalekken

- Menselijke fout (bv. verkeerd geadresseerde mail)
- Technisch lek (configuratiefout, bug)
- Kwaadwillige aanval (hack, ransomware)

De kettingreactie van één lek

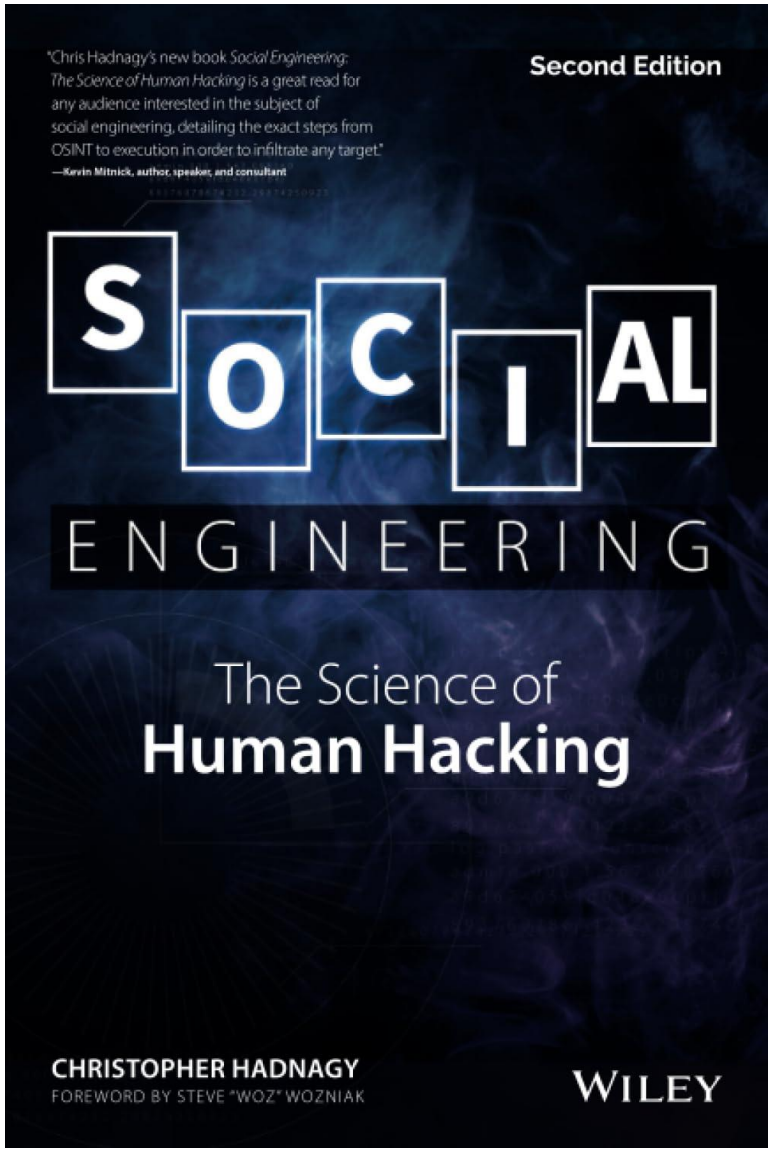
- Van e-mailadres → phishing → identiteitsdiefstal → financieel of reputatieschade

Maatschappelijke impact

- Vertrouwen in instellingen daalt
- Economische schade (bedrijven, burgers)
- Politie en overheid zijn ook het doelwit

Psychologische dimensie

- Social engineering
  - Michael McIntyre → Password1!

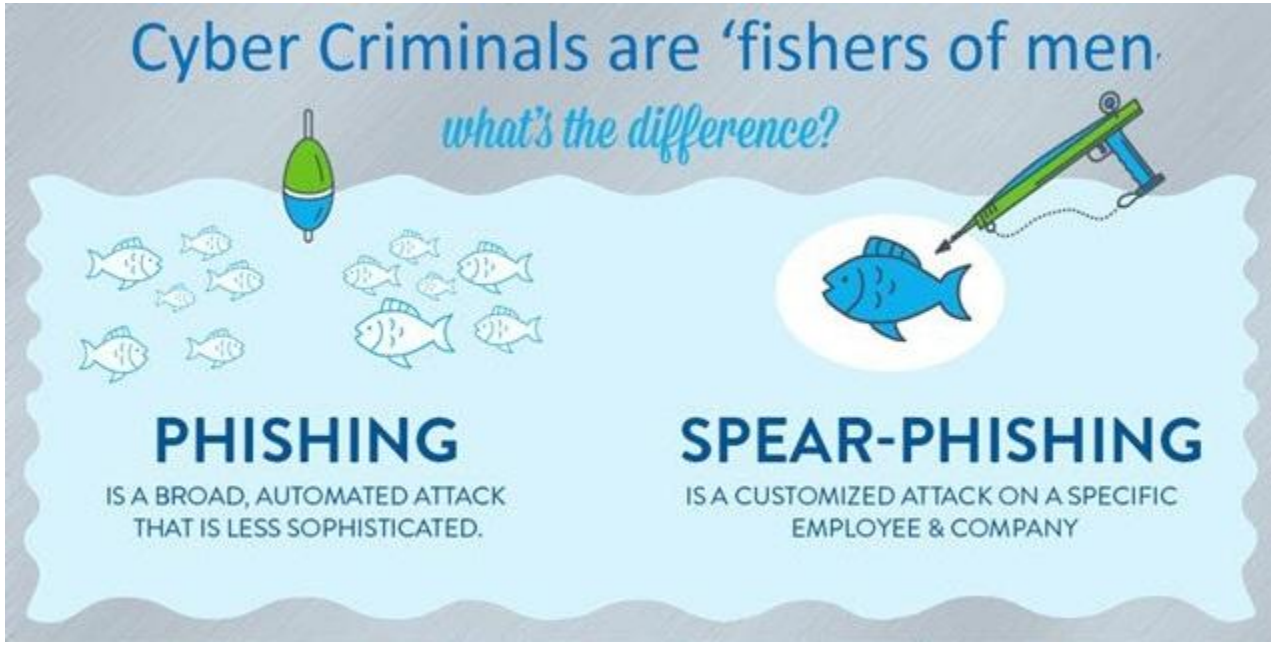


Deel 2: belang van datalekken voor boeven

- Geldgewin
- afpersing
- identiteitsfraude
- reputatieschade.

Van data naar daden

- Hoe gelekte data wordt gebruikt in phishing & spear phishing



Ransomware en dataverkoop

- Dubbele afpersing: betalen of data wordt gepubliceerd.

HOW TO BACK FILES.txt - Notepad

File Edit Format View Help

```
Hello

Your files are encrypted and can not be used
We have downloaded your confidential data and are ready to publish it on our blog
To return your files in work condition you need decryption tool
Follow the instructions to decrypt all your data

Do not try to change or restore files yourself, this will break them
If you want, on our site you can decrypt one file for free. Free test decryption allowed only for not valuable file with size less than 3MB

How to get decryption tool:
1) Download and install TOR browser by this link: https://www.torproject.org/download/
2) If TOR blocked in your country and you can't access to the link then use any VPN software
3) Run TOR browser and open the site: [redacted]
4) Copy your private ID in the input field. Your Private key: [redacted]
5) You will see payment information and we can make free test decryption here
6)After payment, you will receive a tool for decrypting files, and we will delete the data that was taken from you

Our blog of leaked companies:
[redacted]

If you are unable to contact us through the site, then you can email us: [redacted]
Waiting for a response via mail can be several days. Do not use it if you have not tried contacting through the site.
```

LOCKBIT 2.0 LEAKED DATA CONDITIONS FOR PARTNERS AND CONTACTS

ENCRYPTED FILES ARE PUBLISHED

28 Apr, 2022 13:32:00

ekz.de

EKZ Bibliotheksservice is a service company based in Reutlingen, whose services are primarily aimed at libraries. It maintains a network of editors, known as the Lektoratskooperation, which sifts through the approximately 90,000 new German-language publications published each year and selects up to 20,000 titles for "library stock building." The EKZ is one of the largest library service providers in Germany.

ALL AVAILABLE DATA PUBLISHED !

RETURN BACK

NAME	DATE	SIZE
DESK	21 Apr, 2022	—

Dark web-ecosysteem

- Marktplaatsen voor gestolen gegevens.

Digital Thrift Shop

Best digital stuff in Tor network!

Shop Announcements About Terms and conditions My account Help

Home › Data Leak › NordVPN accounts

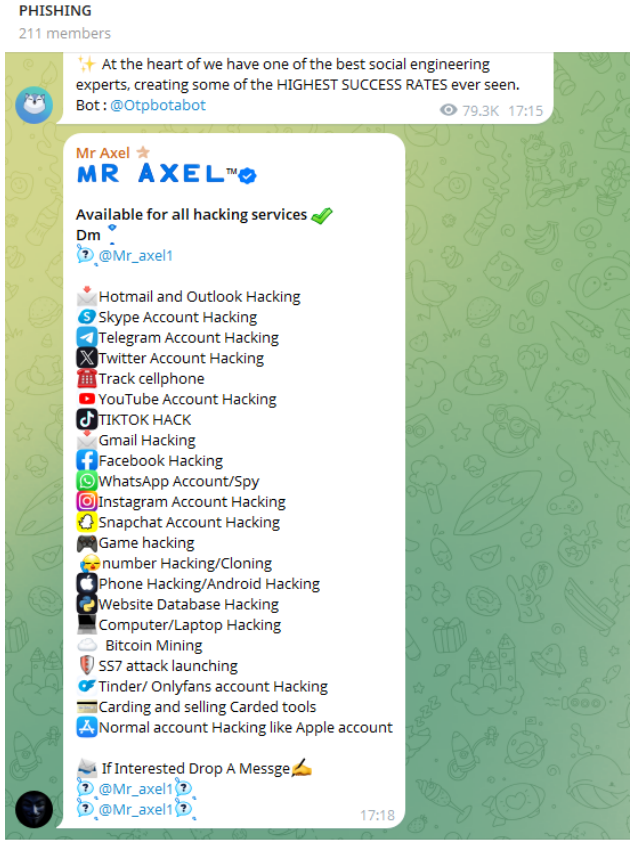
NordVPN accounts

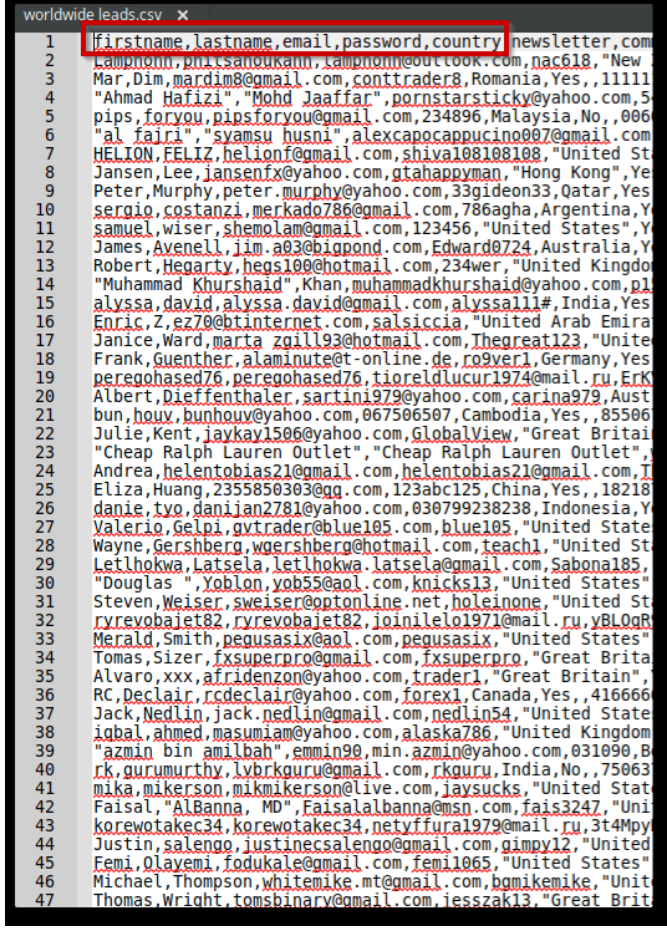
$2.00

0.00001824	0.00390163	10.189043
109,658.82 USD/BTC	512.61 USD/BCH	0.2 USD/DOGE
0.0219475	0.00660388	
91.13 USD/LTC	302.85 USD/XMR	

1830 NordVPN accounts.

Add to cart





Deel 3: belang van datalekken voor opsporingsdiensten

- Datalekken als bron van inlichtingen (OSINT)

OSINT

- Wat kan legaal, wat niet
- Waarde van correlatie tussen datasets - identifiers
  - Selectoren
    - Oproepnummer
    - Gebruikersnaam
    - Emailadres
    - Cryptowallet
    - …

Samenwerking met bedrijven en burgers

- Publiek-private samenwerking
- meldplicht
- CERT-beleid

GDPR & ethisch kader

- Wat is openbaar?
- Datalekken vs heling

International Journal of Intelligence and CounterIntelligence

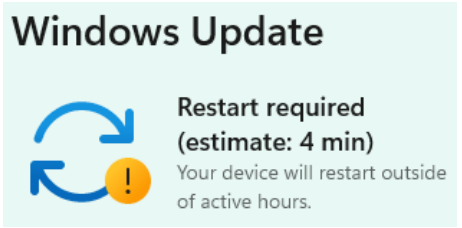
ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: www.tandfonline.com/journals/ujic20

Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices

Jan-Jaap Oerlemans & Sander Langenhuijzen

Deel 4 wat kunnen wij doen?

- Detectie & respons
  - Hoe snel we reageren bepaalt (doorgaans) de schade
    - Zero days exploits
    - Updates!
  - Incidentrespons, communicatie, herstel.

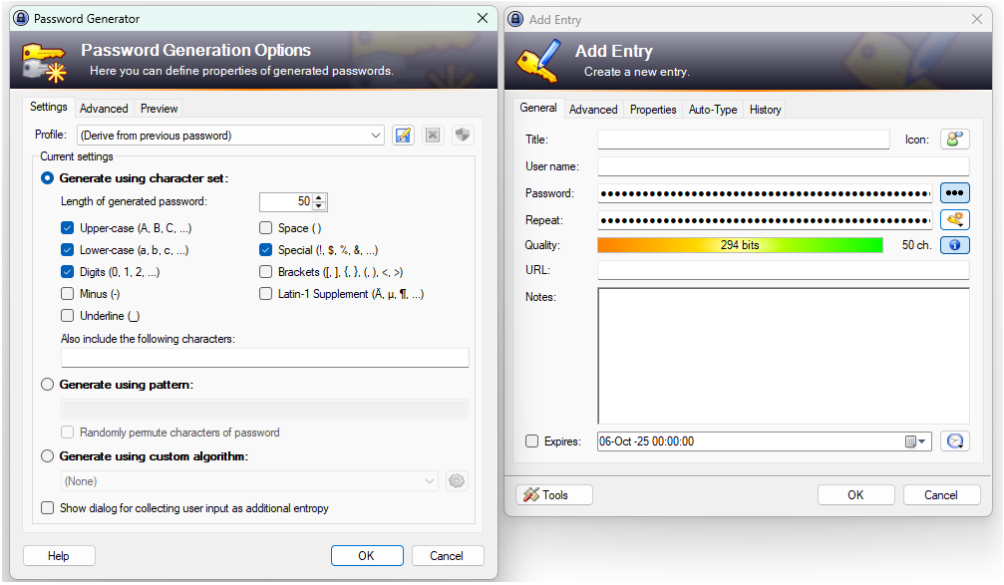


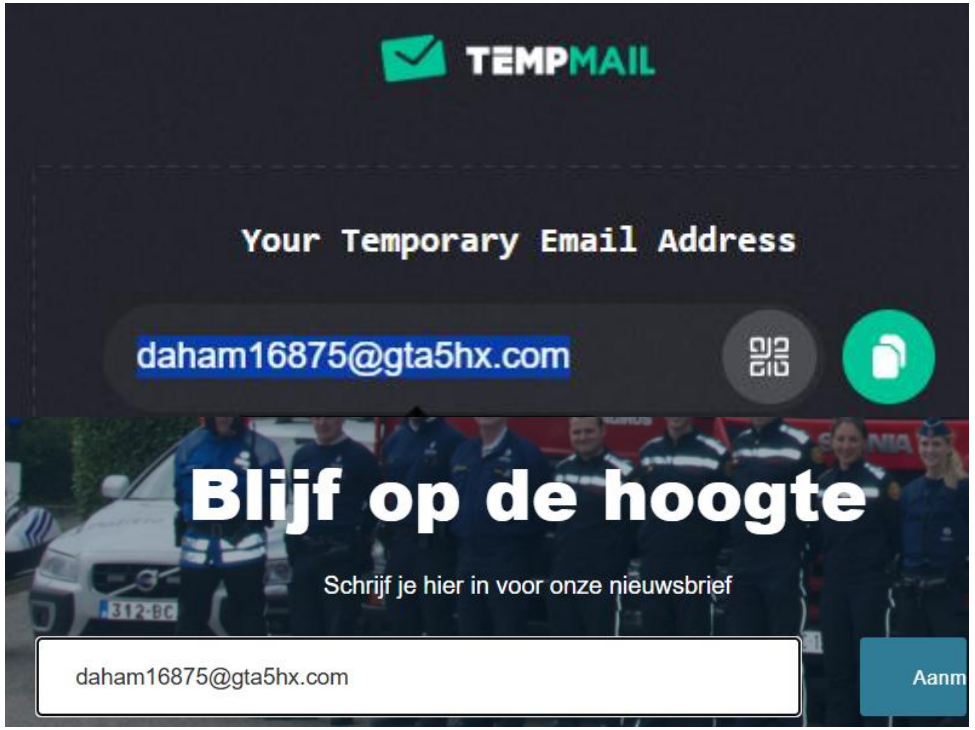
CPS opleidingen OSINT

- Onderzoek
- Bewustwording
- Veilige opzoekingen voor diensten

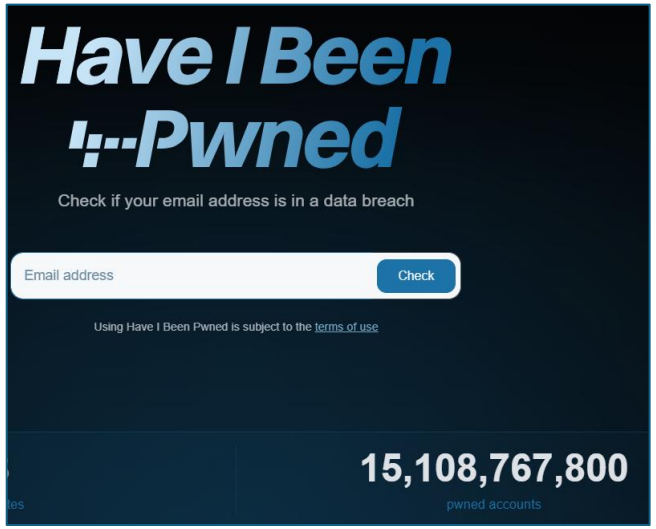
Bescherming van gegevens

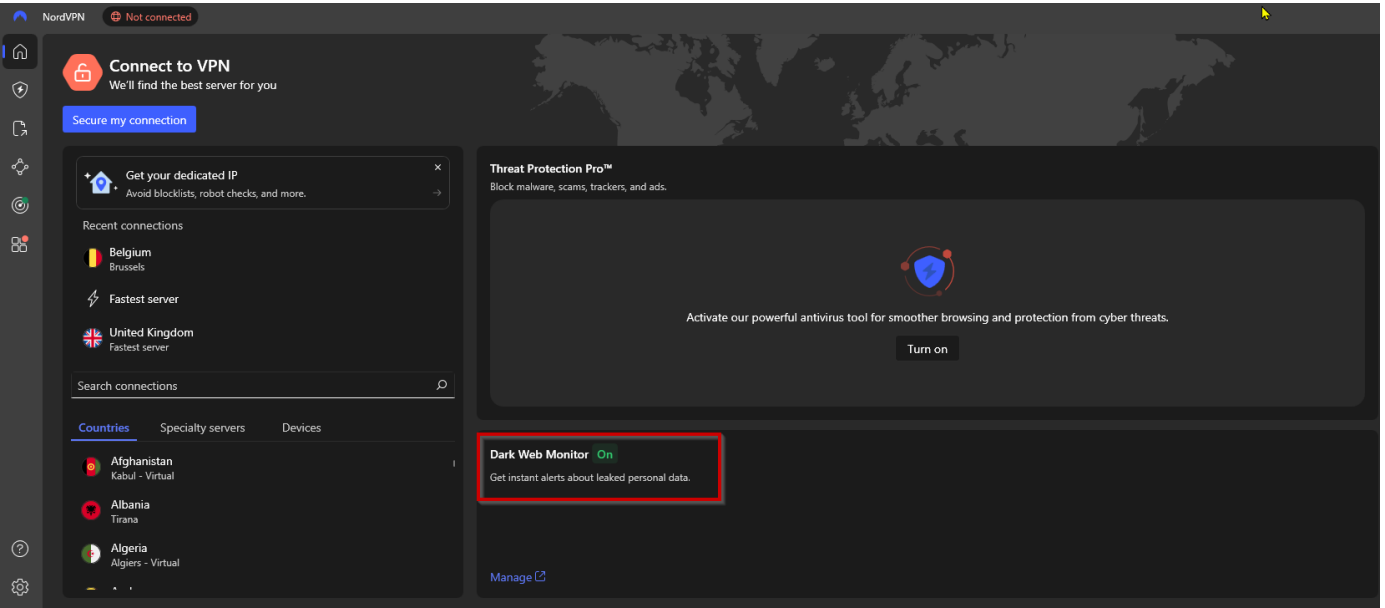
- Sterke wachtwoorden
- Passwordmanager
- MFA
- -> Safety vs comfort <-
- Bewust omgaan met data

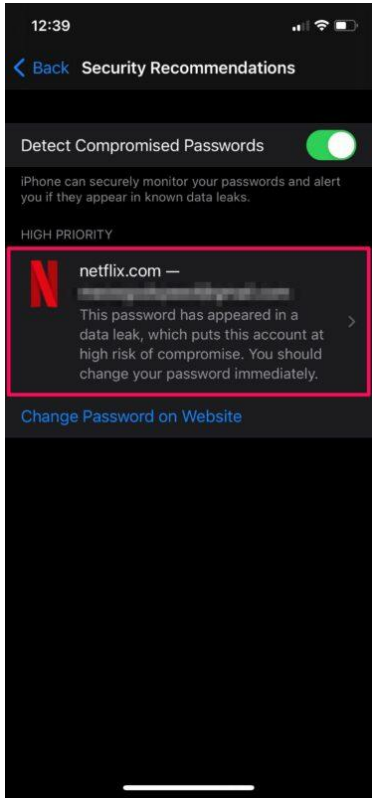


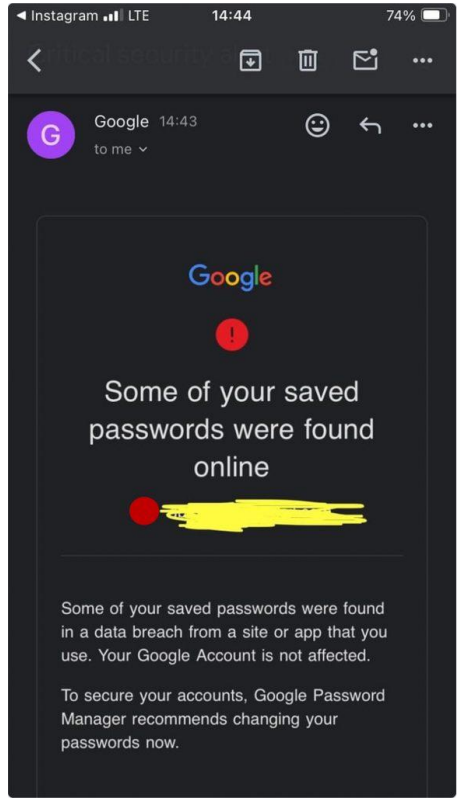


Monitor


Have I Been Pwned
Check if your email address is in a data breach
Email address
Check
Using Have I Been Pwned is subject to the terms of use
15,108,767,800
pwned accounts


NordVPN
Not connected
Connect to VPN
We'll find the best server for you
Secure my connection
Get your dedicated IP
Avoid blocklists, robot checks, and more.
Recent connections
Belgium
Brussels
Fastest server
United Kingdom
Fastest server
Search connections
Countries
Specialty servers
Devices
Afghanistan
Kabul - Virtual
Albania
Tirana
Algeria
Algiers - Virtual
Threat Protection Pro™
Block malware, scams, trackers, and ads.
Activate our powerful antivirus tool for smoother browsing and protection from cyber threats.
Turn on
Dark Web Monitor On
Get instant alerts about leaked personal data.
Manage


12:39
Back
Security Recommendations
Detect Compromised Passwords
iPhone can securely monitor your passwords and alert you if they appear in known data leaks.
HIGH PRIORITY
netflix.com —
This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.
Change Password on Website


Instagram LTE
14:44
74%
Google 14:43
to me
Google
Some of your saved passwords were found online
Some of your saved passwords were found in a data breach from a site or app that you use. Your Google Account is not affected.
To secure your accounts, Google Password Manager recommends changing your passwords now.

Bewustwording

- Security culture
  - Human
  - Tech

Usecase dagvoorzitter

Take home messages

- Meer data dan je denkt
- Good guys
- Bad guys

- Preventie (human & tech)
- Opleiding
- Monitor & react

PODCAST SCHADUWOORLOG

De Volkskrant presenteert ‘Schaduwoorlog’, een nieuwe podcast over spionage en sabotage

Spionage, sabotage, beïnvloeding en cyberaanvallen: in de tweewekelijkse podcast *Schaduwoorlog* duikt adjunct-hoofdredacteur van *de Volkskrant* Annieke Kranenberg met onderzoeksjournalist Huib Modderkolk in de wereld van hybride oorlogsvoering.

Huib Modderkolk en **Annieke Kranenberg**

Q & A

“Wat gelekt is, kunnen we niet wissen — maar we kunnen wél leren.”