

Doe zoals Herstappe: Hou cybercriminelen buiten

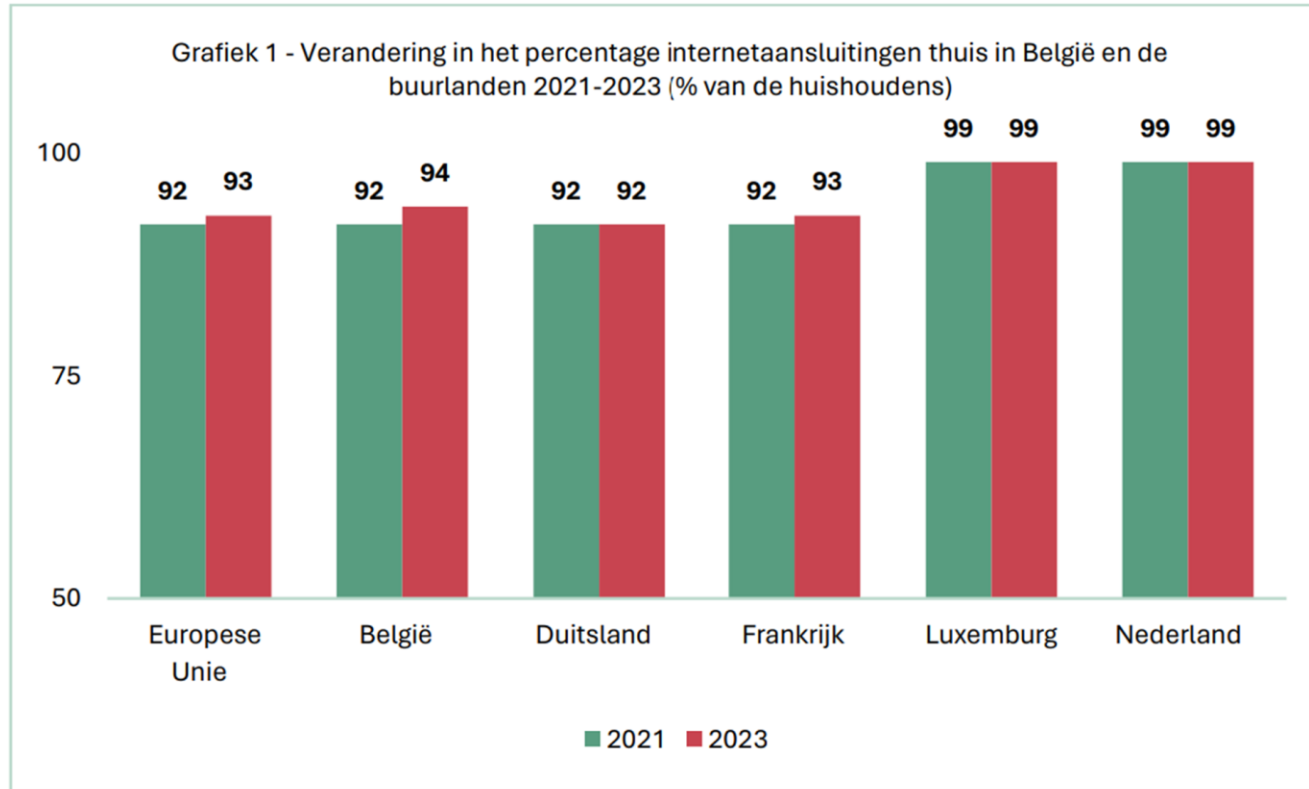
Wat is tweestapsverificatie en waarom
moet iedereen het overal gebruiken?

Wie kan het internet nog missen?

- Alle informatie altijd bij de hand:
 - Openingsuren
 - Weerbericht
 - Wegbeschrijving
- Het is handig en snel:
 - Bankzaken kan je digitaal regelen
 - Niet aanschuiven aan het gemeenteloket
 - Geen boete bij de bib
 - Dokter, tandarts, apotheker in een vingerknip
- Je bent altijd met iedereen in contact:
 - Familie en vrienden die ver weg wonen, zijn nu altijd een beetje dichtbij
 - Snel afspreken om samen uit te gaan eten



Het internet is niet meer weg te denken



Bron: berekeningen IACCHOS, UCLouvain, op basis van Statbel-enquêtes 2021 en 2023.

Ook cybercriminelen vinden hun weg

- **Phishing, smishing**

- Oplichting via verdachte e-mails of tekstberichten: je geeft je bankgegevens weg of schrijft een bedrag over op de rekening van oplichters

- **Hacking**

- Hackers hebben toegang tot je accounts (Facebook, e-mail, enz...), Ze sturen berichten in jouw naam, doen bestellingen in jouw naam, enz...

- **Crypto investment scam**

- Oplichters moedigen je aan om te investeren in crypto via valse tradingplatformen, Je verliest al het geld dat je hierin 'investeerde'.



Ook cybercriminelen vinden hun weg

- **Sextortion scam**

- De oplichter beweert seksueel getinte beelden van jou te bezitten. Dit is bluf. Hij dreigt ermee de beelden te delen als jij niet betaalt.

- **Microsoft scam**

- Je wordt opgebeld door iemand die zich voordoeft als een medewerker van Microsoft, Apple, Proximus. De persoon beweert dat er een probleem is met toestel en wil je helpen, als je betaalt.

- **En vele andere vormen van online fraude floreren...**





5 tips om je online te beschermen

5 tips om je online te beschermen

Leer phishing
herkennen

Download
enkel uit
erkende shops

Maak back-ups

Voer updates
uit

Gebruik een
antivirus



An aerial photograph of a street scene. A dark-colored van is parked on the left side of the road, and a dark-colored sedan is parked on the right side. The road is paved with light-colored material and has a cobblestone curb. There are green bushes and trees on both sides of the road. Two green text boxes are overlaid on the image. The first box contains the text "De zesde tip = de beste tip" in white. The second box contains the text "Gebruik tweestapsverificatie overal waar het kan!" in white. A white horizontal line is drawn across the road between the two cars.

De zesde tip = de beste tip

**Gebruik tweestapsverificatie
overal waar het kan!**



Safeonweb.be

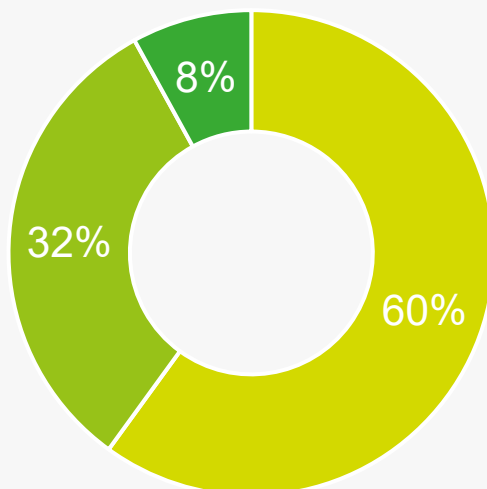


en te scrollen op sociale media.

Belangrijke cijfers

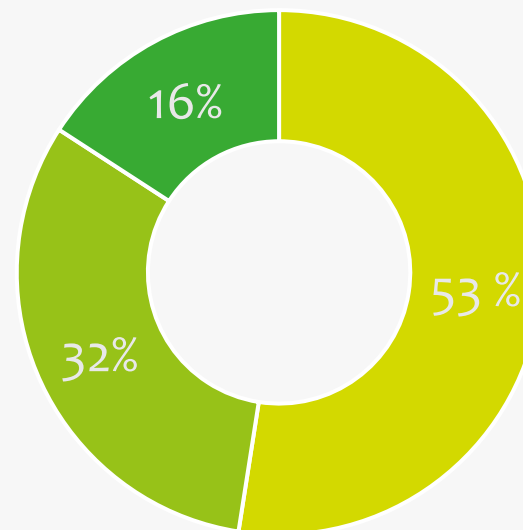
Ik gebruik verschillende wachtwoorden

- Ja
- Nee, maar ik ben me bewust van de risico's
- Nee, maar ik wist niet dat het gevaarlijk was.



Ik gebruik tweestapsverificatie

- Ja
- Nee, maar ik ben me bewust van de risico's
- Nee, maar ik wist niet dat het gevaarlijk was.





Belangrijke cijfers

- 2FA vermindert het hacken van accounts met 99%:
- Wachtwoorden die zijn gestolen door hacken zijn nutteloos met 2FA.
- Malware en virussen kunnen niet langer een impact hebben op de veiligheid van accounts die 2FA gebruiken.
- Accounts die zijn ingesteld met 2FA worden aanzienlijk minder snel gehackt.

• Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits; 12/2023;
<https://www.enterpriseappstoday.com/stats/two-factor-authentication-statistics.html#:~:text=According%20to%20TechCrunch%2C%20Facebook%20FA,more%20than%201.5%20million%20accounts.&text=95%25%20of%20companies%20that%20used,benefits%20of%20software%2Dbased%20authentication>



Tweestapsverificatie, of...

2FA

MFA

Twee Factor
Authenticatie

Tweestapsvalidatie



Tweestapswatte? Wat is 2FA?

Het is een beveiligingsmaatregel om te voorkomen dat hackers of oplichters toegang krijgen tot je accounts door twee verschillende vormen van identificatie te gebruiken:

- Iets wat je weet: wachtwoord
- Iets dat je hebt: smartphone
 - Code ontvangen via sms,
 - Toepassing (Itsme, Authenticator App, enz.),
- Iets dat je bent: vingerafdruk, gezichtsherkenning, ...

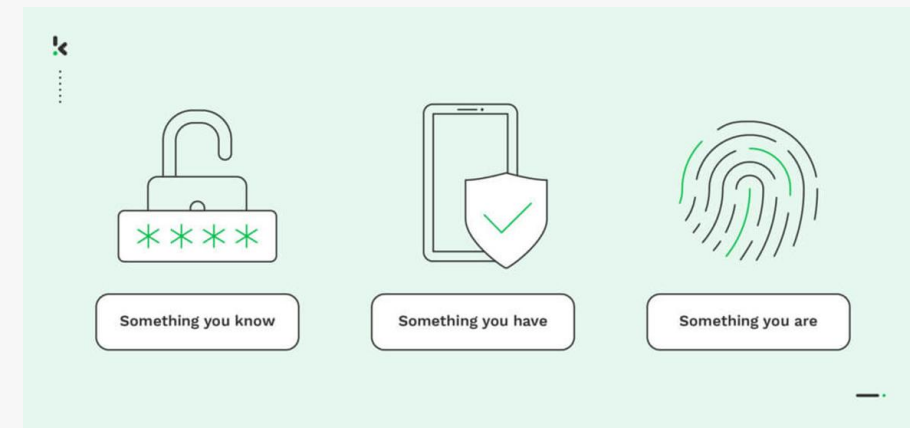


Image : Kaspersky



En wat is MFA dan?

Als je niet 2 maar meer beveiligingsfactoren gebruikt, dan spreken we over MFA

Als ze maar tweestapsverificatie hadden gebruikt...



Facebook-account burgemeester Bilzen gehackt door criminelen: "Ga niet in op vraag om geld over te maken"

Mailbox burgemeester van Vilvoorde Hans Bonte gehackt, enkele duizenden valse mails verstuurd

Waarom je online accounts beschermen?

Internetcriminelen die toegang hebben tot je accounts:

- Kunnen je **financiële nachtmerries** bezorgen
 - toegang tot jouw online betaalaccounts
 - aankopen in jouw naam
 - fraude in jouw naam
- Kunnen je **online identiteit** overnemen
 - Reputatieschade
 - Vrienden en familie oplichten in jouw naam
 - Toegang tot persoonlijke informatie



Hoe weet je dat je account gehackt is?

- Je ontvangt een e-mail over loginpoging met een nieuw apparaat
- Je merkt een frauduleuze betaling op je account op
- Er verschijnen vreemde berichten op je sociale netwerken
- Je merkt verdachte activiteiten op: bijv. laatste films gezien op Netflix
- Je vrienden vertellen je dat ze een vreemde e-mail van je hebben ontvangen



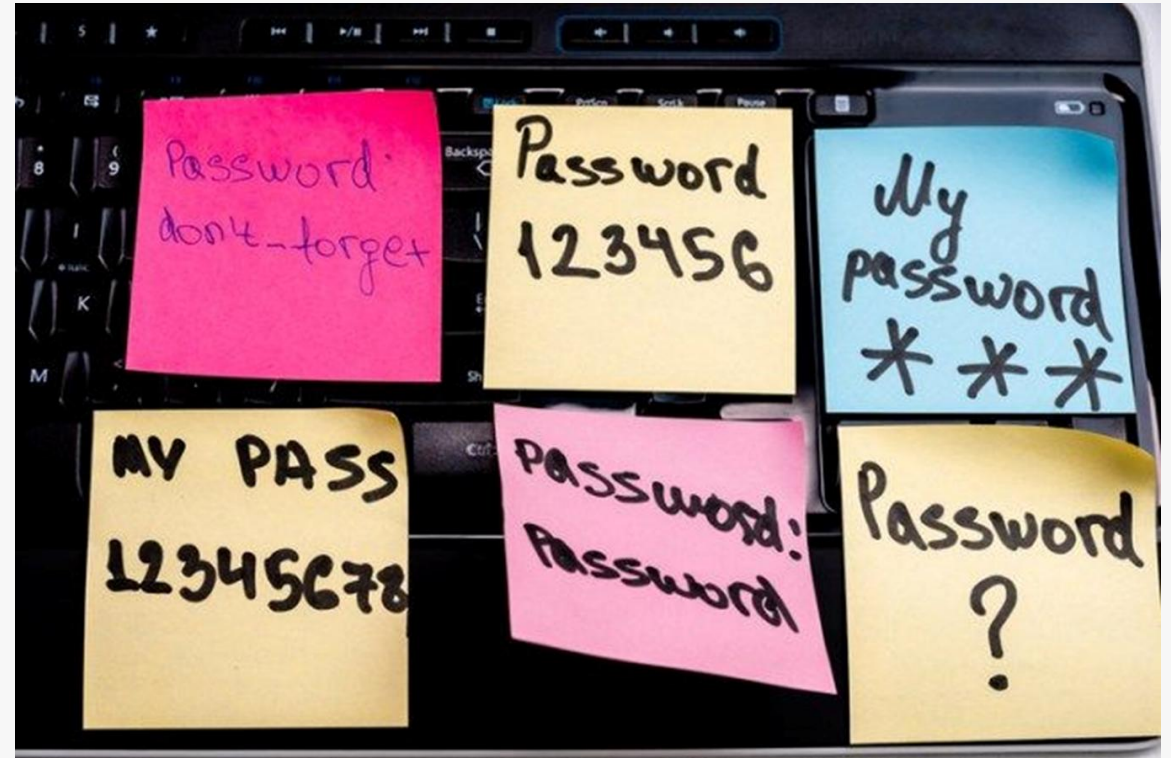
Mijn account is gehackt, wat moet ik doen?

- Hoe krijg je weer controle over je account?
 - Heb je nog altijd toegang tot de account? Verander dan meteen het wachtwoord van die account en van je andere accounts,
 - Heb je geen toegang meer? Gebruik de herstelopties om opnieuw toegang te krijgen en verander daarna al je wachtwoorden.
- Wat moet je nog meer doen?
 - Scan je computer op virussen.
 - Zijn je bank- of kredietkaartgegevens gestolen, verwittig je bank en houd je rekeningen nauwlettend in het oog. Contacteer [Card Stop](#) op 078 170 170 als je verdachte transacties opmerkt.
- Zijn er gegevens uit je professionele leven gestolen, breng dan zo snel mogelijk je werkgever op de hoogte.
- Activeer 2FA



Wachtwoorden zijn niet van deze tijd

- Wachtwoorden zijn frustrerend
- We blijven zwakke wachtwoorden gebruiken
- Maar ook sterke wachtwoorden zijn niet veilig...



50 Most Commons Passwords

50 Most Common Passwords

THE READER'S DIGEST VERSION

1	123456	26	ubnt
2	admin	27	abc123
3	12345678	28	Aa@123456
4	123456789	29	abcd1234
5	1234	30	1q2w3e4r
6	12345	31	123321
7	password	32	qwertyuiop
8	123	33	87654321
9	Aa123456	34	987654321
10	1234567890	35	Eliska81
11	1234567	36	123123123
12	123123	37	11223344
13	111111	38	0987654321
14	Password	39	demo
15	12345678910	40	12341234
16	000000	41	qwerty123
17	admin123	42	Admin@123
18	1111	43	1q2w3e4r5t
19	P@ssw0rd	44	11111111
20	root	45	pass
21	654321	46	Demo@123
22	qwerty	47	azerty
23	Pass@123	48	admintelecom
24	112233	49	Admin
25	102030	50	123meklozed



Ook een sterk
wachtwoord is
niet veilig

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



> Learn how we made this table at hivesystems.io/password

Hoe stelen hackers je wachtwoord?

- Ze stelen je wachtwoord via **phishing** of valse berichten
- Een **datalek** bij een bedrijf online dienst kan je wachtwoord te grabbel gooien op het internet
- Met **virussen** die wachtwoorden stelen



We maken het hackers heel gemakkelijk!

- We schrijven wachtwoorden op post-it
- We geven wachtwoorden prijs aan de telefoon
- We geven een wachtwoord op bij een valse wedstrijd online

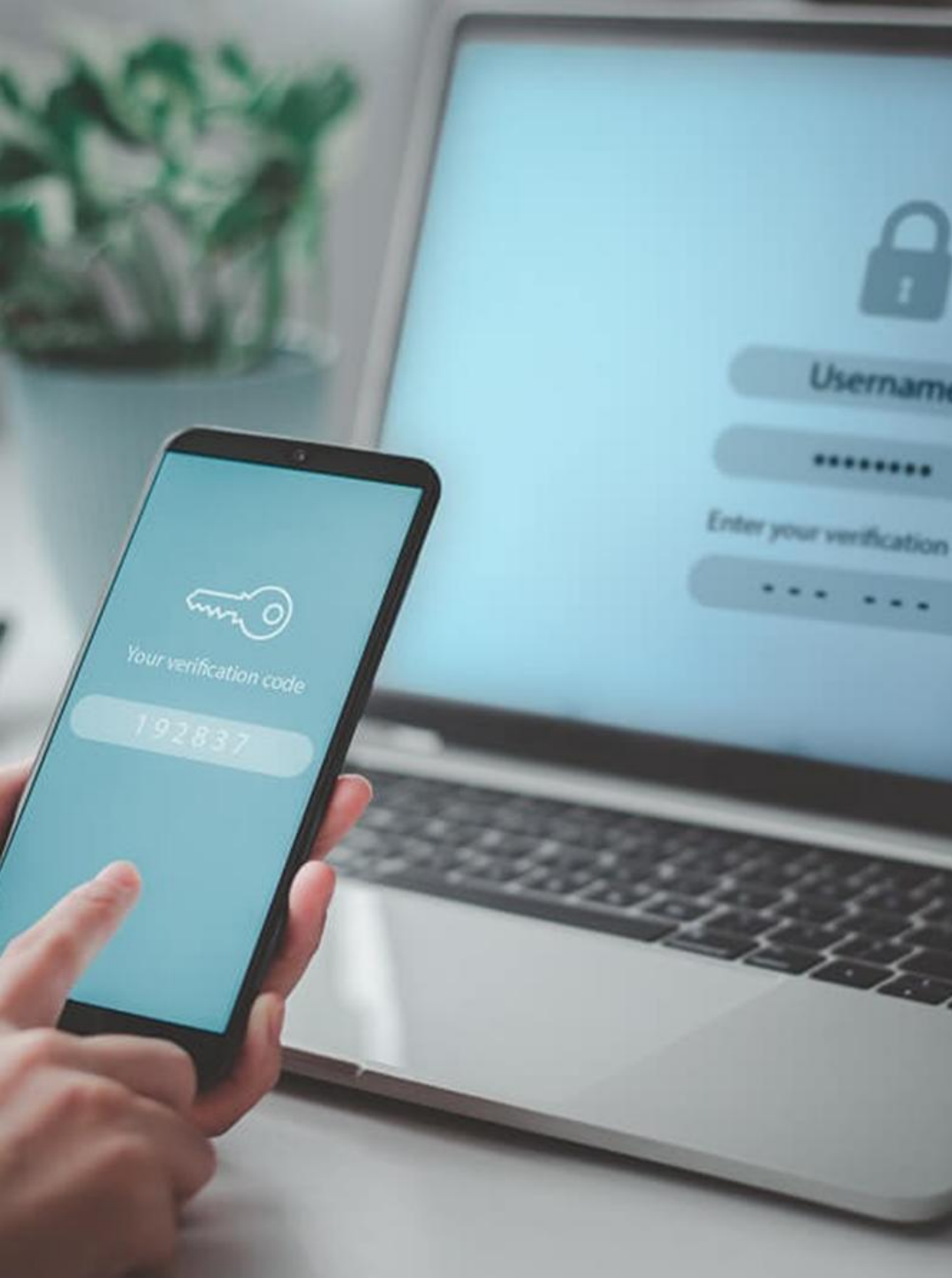


Hoe kan je dat voorkomen?

- Gebruik tweestapsverificatie waar mogelijk
 - Begin met je e-mail account
- Gebruik het op websites waar je je bankgegevens achterlaat: webshops, reservatieplatformen, sites voor aankoop van tickets, tweedehandswebsites...
- Bescherm je social media met 2FA

Kortom: maak er een gewoonte van om het overal te gebruiken waar het beschikbaar is





Hoe stel je 2FA in?

Het instellen van 2FA verschilt per platform, maar over het algemeen zijn de stappen vrij gelijkaardig:

- Ga naar de beveiligingsinstellingen van de account die je wil beveiligen.
- Zoek naar de optie om 2FA in te schakelen en selecteer deze.
- Kies de tweede factor die je wilt gebruiken (bijvoorbeeld SMS, authenticatie-app, etc.).
- Volg de instructies op het scherm om de tweede factor te configureren.
- Test of alles goed is ingesteld door uit te loggen en opnieuw in te loggen met de tweede factor.

Welke 2^{de} factor is de beste?

- Het maakt niet uit welke 2^{de} factor je gebruikt*.
2 beveiligingsfactoren zijn altijd beter dan 1.
- Gebruik wel 2 verschillende soorten factoren, dus niet bv, 2 keer iets dat je weet

** Een code die per sms wordt toegestuurd is gemakkelijk en veel mensen kennen dit al. Het is misschien wel de meest laagdrempelige oplossing, maar... oplichters proberen die te bemachtigen via SIM-swapping. Als de oplichter je telefoon kan bemachtigen, en die is niet vergrendeld of die toont de boodschappen ook bij vergrendeling, dan kan de oplichter de code gebruiken...*



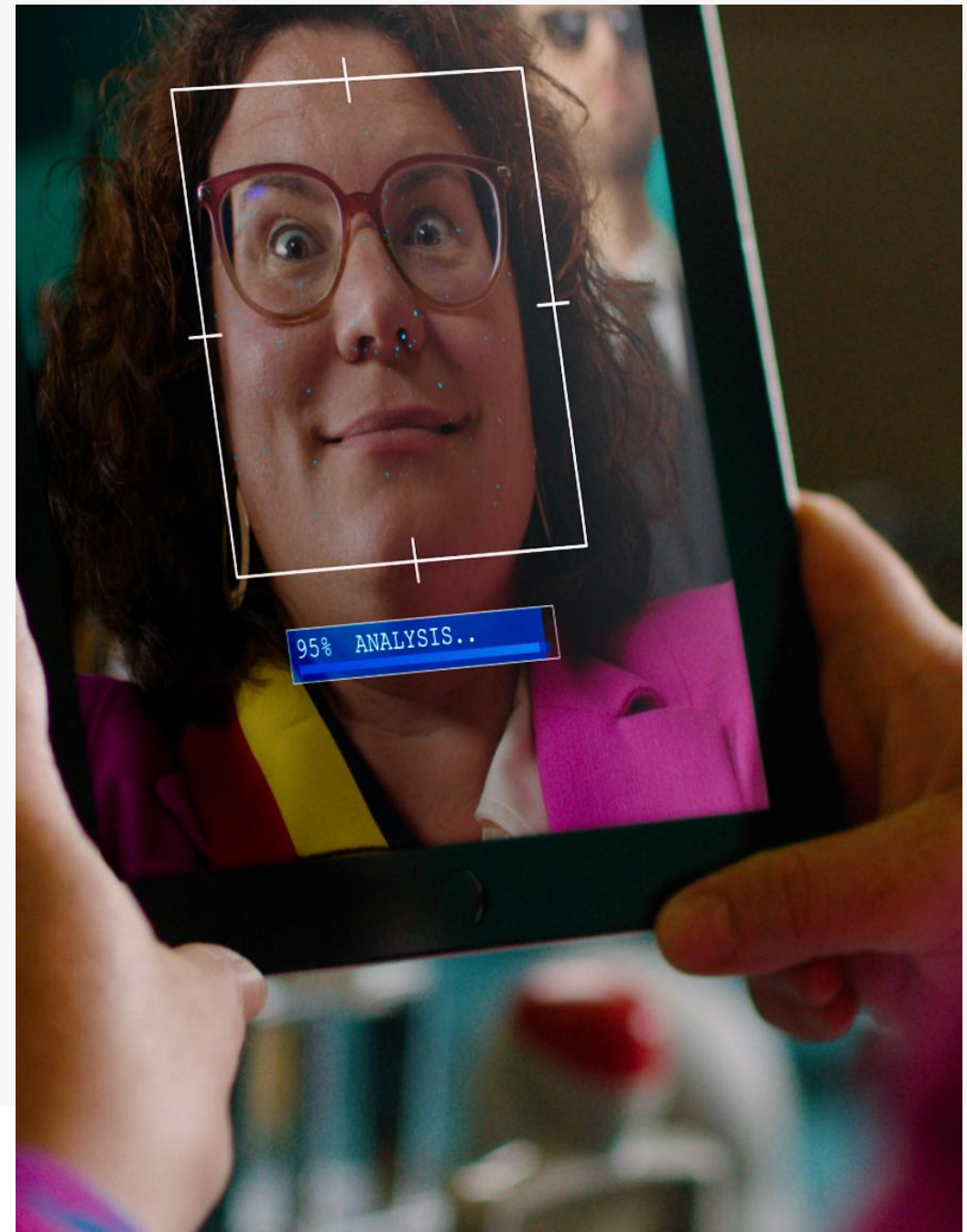
Sms of authenticator app?

- Sms: je geeft je telefoonnummer in je krijgt vervolgens een sms'je toegestuurd met een code die je vervolgens moet intypen op de aangegeven plaats
- Authenticator app: de downloadt een app via App Store of Google Play (bv. Google Authenticator of Microsoft Authenticator). Via een QR code goeg je de account toe aan je app. Telkens wanneer je inlogt zal de app een eenmalige code genereren die je invoegt op de aangegeven plaats
- Het is een vrije keuze, in functie van de maturiteit van het doelpubliek
- Opgepast: deel nooit je codes met derden!



Twijfel je?

- Bekijk op Safeonweb hoe je 2FA gebruikt op de meest gebruikte accounts
- <https://safeonweb.be/nl/2FA>
- Vraag hulp aan iemand die je vertrouwt: een familielid, een vriend of een medewerker van een van de vele Digipunten



Domme excuses om geen 2FA te gebruiken

- Daar verlies ik te veel tijd mee!
 - Slechts enkele seconden. Verwaarloosbaar tegenover de tijd die je verliest als je gehackt bent
- Wat als ik mijn telefoon verlies?
 - Je kan steeds een herstel e-mailadres ingeven, of codes opvragen en bewaren.



Geen goed idee

- Als ik een 2^{de} factor gebruik, mag ik dan een zwak wachtwoord kiezen?
- Geen goed idee. Het is net de bedoeling dat je 2 veilige methodes kiest. Een zwak wachtwoord is nooit een goed idee.



Wat als 2FA niet beschikbaar is op een bepaalde dienst?

- Gebruik sterke, unieke wachtwoorden: Zorg ervoor dat je wachtwoord complex is en verschilt van wachtwoorden die voor andere accounts worden gebruikt.
- Controleer je account regelmatig op ongewone activiteiten of ongeautoriseerde toegang.
- Stel meldingen in voor accountactiviteiten zoals aanmeldingen of wijzigingen in instellingen.
- Gebruik andere beveiligingsfuncties van de service, zoals beveiligingsvragen of opties voor accountherstel.
- Overweeg over te stappen naar een serviceprovider die wel 2FA aanbiedt.
- Neem contact op met de huidige serviceprovider om interesse te tonen in 2FA of informeer naar andere beveiligingsopties die ze bieden.



Is 2FA echt niet te kraken?

- Oplichters kunnen proberen om ook je 2^{de} beschermingsfactor te bemachtigen:
 - door je op te bellen en met een smoes je te overtuigen om je code te delen of om Itsme te gebruiken (voor een authenticatie die de oplichter zelf aangevraagd heeft!)
 - door je een phishingbericht te sturen
 - door je telefoon te stelen en daar de codes op te vragen
- Deel daarom nooit je codes met iemand die er om vraagt!



Veel materiaal beschikbaar via Safeonweb YouTube



Tutorials: 2FA op Insta

STAP 7: VOLG DE INSTRUCTIES

AUTHENTICATOR



Ook vorige campagnes



Doe de wachtwoord test

Test je kennis

Hackers maken tegenwoordig gebruik van allerlei technieken om je wachtwoord te raden en toegang te krijgen tot je account. Daarom is een goede beveiliging belangrijker dan ooit. Hoe goed ga jij om met wachtwoorden? Zijn jouw accounts goed beveiligd of loop je meer risico dan je denkt? Test je kennis!

Doe de test

Geen tijd voor de test?

Leer hoe je jouw account beter kan beveiligen.

Ontdek onze tips



Meer weten over 2FA ?

<https://safeonweb.be/nl>

Volg ons !



[Facebook - Safeonweb.be](#)



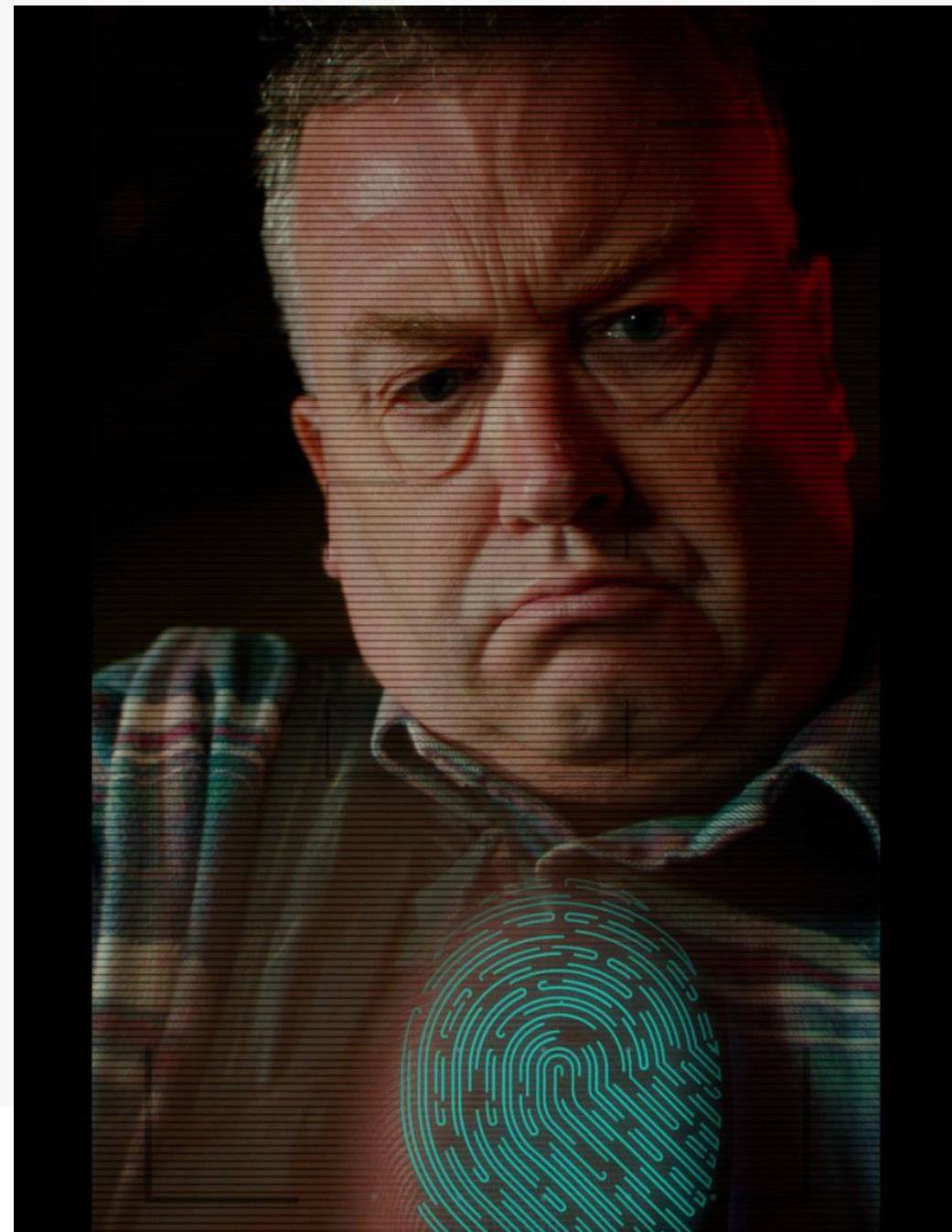
[Instagram - Safeonweb.be](#)



X – Safeonweb



[YouTube - @safeonwebbe](#)







**Een presentatie aangeboden door Safeonweb naar
aanleiding van de campagne 2024**