



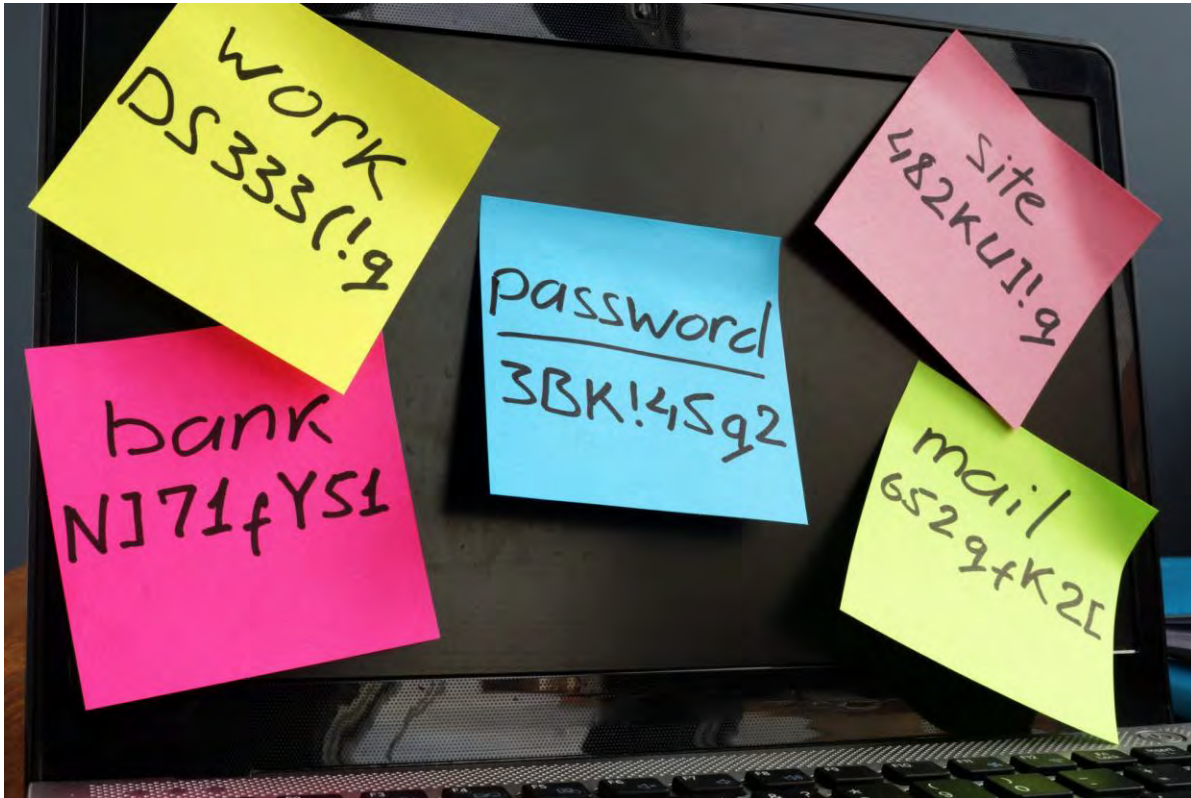
Cyberpreventie- advies (CPA)

Cruciaal in dit verhaal: de 10 tips!

1. Wachtwoorden
2. Tweestapsverificatie
3. Websites controleren
4. Opletten met vreemde berichten
5. Ongevraagde helpdeskmedewerkers
6. Openbare wifi en QR
7. Software updates
8. Officiële app stores
9. Anti virus
10. Privacy op sociale media



Tip 1: wachtwoorden



- complex/wachtwoordzinnen
- nooit hetzelfde
- niet hergebruiken
- verander regelmatig
- wachtwoordkluis (digitaal) of wachtwoordboekje (papier)

Tip 1: wachtwoorden

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	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

**Time it takes
a hacker to
brute force
your password
in 2025**

**Hardware: 12 x RTX 5090
Password hash: bcrypt (10)**



Hive Systems

**Read more and download at
hivesystems.com/password**

Benieuwd of jouw e-mail gelekt is?

Check het via

→ haveibeenpwned.com

Wat moet je doen als je merkt dat je gegevens gelekt zijn?

Je gegevens weer laten verdwijnen van het internet is onmogelijk.

- wachtwoorden die je gebruikte op de getroffen platformen onmiddellijk veranderen.
- Nergens hetzelfde wachtwoord gebruiken
- Gebruik voortaan overal waar dat kan tweestapsverificatie.



Tip 2: tweestapsverificatie

Om toegang te krijgen tot je account moet je bewijzen dat je bent wie je beweert te zijn.



Bescherm je online accounts met tweestapsverificatie.
Surf snel naar safeonweb.be

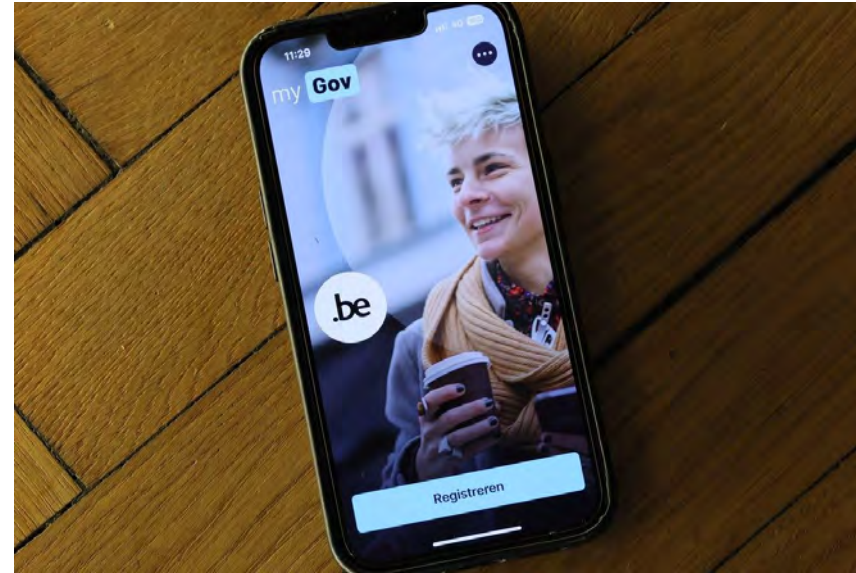
- JOUW WACHTWOORD OF PINCODE**
Met iets dat jij alleen weet
- EEN CODE DIE JE ONTVANGT OP JOUW TELEFOON OF AUTHENTICATIEAPP**
Met iets dat jij alleen hebt
- JOUW VINGERAFDRUK, GELAAT, IRIS...**
Met iets dat jij bent

Itsme en MyGov



itsme[®] is een app op uw smartphone waarmee u uw identiteit kunt aantonen en transacties kunt bevestigen.

→ **Check de pop-up**



MyGov.be is een app van de federale overheid die u kunt gebruiken als digitale sleutel om eenvoudig aan te melden bij online overheidsdiensten.

Tip 3: websites controleren



- Via allerhande wegen komen die binnen:
 - E-mail
 - Sociale media
 - SMS
 - Whatsapp
- Controleer het adres van websites op onregelmatigheden
- Bij twijfel, surf dan zelf naar het adres dat je kent
- [Scamadviser.com](https://www.scamadviser.com)

Tip 3: websites controleren

Cybercriminelen gebruiken webadressen die erg lijken op de echte naam, met kleine foutjes of toevoegingen.

- belfuis.be
- safeonweb-be.com
- safe.onweb.be
- rnicrosoft.com
- online.be/ing

**Kijk goed, kun jij de
de fout vinden?**

1 2 3 4 5 6 7 8 9

Check de link

The screenshot shows a web browser window with the URL <https://www.scamadviser.com/nl/check-website/financien.be-vergoedingsaanvraag.info>. The page header includes the Scam Adviser logo (10 years), a search bar, and navigation links: [Rapporteer](#), [Hulp & Info](#), [Chat with Us](#), and a language selector set to [NL](#).

financien.be-vergoedingsaanvraag.info Reviews

is financien.be-vergoedingsaanvraag.info betrouwbaar of oplichting?

De site lijkt niet beschikbaar. We tonen daarom data van een eerdere analyse (foutmelding: 503)

Trust Score
15 / 100

[Wat is dit?](#)

[Disclaimer](#)

Wat is jouw gevoel bij financien.be-vergoedingsaanvraag.info

0 0 0 0 0

Geen reviews beschikbaar. wees de eerste om deze site te beoordelen

[Meld een Scam](#)

Tip 4: vreemde berichten



Tip 4: vreemde berichten

#7 Word je persoonlijk aangesproken?

Mails die beginnen met beste, mevrouw, meneer ... zijn vaak niet te vertrouwen als ze niet gevolgd worden door je naam.

#8 Bevat het bericht veel taalfouten?

Ook taalfouten of vreemde zinsconstructies kunnen wijzen op een verdacht bericht.

Gephisht! Wat nu?

Deelde je je bankgegevens?
Bel Cardstop via 078 170 170.
Vraag aan de bank om je rekening
of bankapp te blokkeren.

Denk je dat iemand
je wachtwoord heeft
gekraakt? Verander
het zo snel mogelijk.

Is er geld van je rekening
gestolen? Dan kan je altijd
klacht indienen bij de politie.

Meld het bericht via
verdacht@safeonweb.be

Meer weten? Surf naar www.safeonweb.be
en www.mediawijs.be/cybersecurity

Tip 4: vreemde berichten

----- Doorgestuurd bericht -----

Onderwerp: Een nieuw document van CM: CM-Hospitaalplan

Datum: Thu, 3 Jul 2025 00:05:25 +0000

Van: persoonlijk_dossier_cm@jkotypc.com

PHISHING

Geachte heer/mevrouw,

Wij nemen contact met u op in verband met uw aanvraag voor de **verhoogde tegemoetkoming**. Om uw aanvraag correct te verwerken, vragen wij u vriendelijk om uw e-mailadres te bevestigen.

Wat moet u doen?

Klik op onderstaande knop om uw e-mailadres te bevestigen:

[\[Bevestig mijn e-mailadres\]](#)

Zodra uw e-mailadres is bevestigd, kunnen wij uw aanvraag verder behandelen en u op de hoogte houden van de verdere stappen.

Heeft u vragen of hulp nodig? Neem gerust contact op met uw CM-kantoor of bezoek onze website

Met vriendelijke groet,

Tip 4: vreemde berichten

Van: "website noreply" <dewatergroep@aol.com>
Verzonden: Woensdag 18 juni 2025 02:15:16
Onderwerp: Uw meterstand kan niet worden geregistreerd



PHISHING

Beste klant,

Bij het verwerken van uw meterstand merken we dat er nog enkele gegevens ontbreken. Daardoor konden we de registratie momenteel niet afronden.

Om uw waterverbruik correct te kunnen verwerken en een nauwkeurige facturatie te garanderen, vragen we u vriendelijk om de ontbrekende informatie aan te vullen.

U kunt uw gegevens eenvoudig [hier](#) aanvullen

Heeft u vragen of hulp nodig? Onze klantendienst helpt u graag verder.

Tip 4: vreemde berichten

Jaarverslag 2025 Federale Gerechtelijke Politie

88266489039/2025
Kennisgeving LI.45.99.000559/2025

Onderzoeksafdeling 1
Koningsstraat 202 A,
1000 Brussel, België

PARKET ALGEMEEN BRUSSEL

 Federale Politie

Geachte heer/mevrouw;

In het kader van het vooronderzoek nr. 88266489039/2025, afgeleverd door de rechter, de **heer** Frédéric Van LEEUW, de procureur-generaal van het Federaal Parket van Brussel, wegens vermoedelijke daden van aanranding van de eerbaarheid, geregistreerd bij de DCSP met referentie. Nr. 2025/1702.

In toepassing van de bepalingen van artikel 372 van het Wetboek van Strafrecht luidt: “Elk misdrijf van bescheidenheid gepleegd zonder geweld of bedreiging tegen de persoon of met de hulp van de persoon van een kind van het ene of het andere geslacht, jonger dan 16 jaar, zal worden gestraft met gevangenisstraf.

Artikel 227-23 van het Wetboek van Strafrecht bepaalt: “Het feit, met het oog op de verspreiding ervan, van het vastleggen, opnemen of doorgeven van een afbeelding of afbeelding van een minderjarige, terwijl deze afbeelding of afbeelding van pornografische aard is, wordt bestraft met 5 jaar gevangenisstraf en een boete van 955.000,00 euro.

Volgens de voorwaarden van artikel 331 “vormt een aanval op de bescheidenheid elke daad van seksuele aard, in strijd met de goede zeden, die rechtstreeks en opzettelijk tegen een persoon wordt uitgevoerd, met of zonder geweld, dwang of verrassing”. Het slachtoffer kan met name minderjarig of volwassen zijn.

Tip 4: vreemde berichten

Hoe reageer je?

1. Bij twijfel nooit oversteken
 - Antwoord niet, open geen bijlage en klik niet op de links.
 - Deel nooit bankgegevens
2. Rechtstreeks contact met afzender
3. Meld de poging tot phishing en verwijder de e-mail/tekst.

Tip 4: vreemde berichten

Wat als je toch geklikt hebt op een verdachte link?

- Geef geen persoonlijke gegevens in
- Niets downloaden en geen codes invoeren
- Sluit de nepwebsite direct
- Sluit je internetconnectie af
- Gegevens niet invoeren
- Virusscan uitvoeren
- Wachtwoorden aanpassen
- Twee-factor-authenticatie inschakelen



Smishing – sms phishing

Smishing = SMS phishing

- Mensen zijn vaak eerder geneigd om een sms te vertrouwen dan een e-mail
- Echter kan ook met de telefoon *'gespoofed'* worden (het scherm laat een ander nummer zien)
- Kortom: klik nooit zomaar op links en geef geen persoonlijke informatie via sms



Betaalverzoekfraude (WhatsApp/vriend in nood)



Vriendschapsfraude

- Aanvaard niet zomaar vriendschapsverzoeken van een wildvreemde.
- Controleer altijd de echtheid van een profiel.
- Vertrouw niet zomaar iedereen
- Wees op je hoede voor “zielige” verhalen
- Houd je portemonnee dicht



Te mooi om waar te zijn

Onderwerp: Re: Uw gratis staatslot
Datum: Thu, 21 Jan 2016 21:23:57 +0000
Van: Staatsloterij Spel <staatsloterij@nieuws.email-aanbieding.nl>

Gefeliciteerd

Jij ontvangt een 100% gratis staatslot!

Jouw emailadres is geselecteerd en daarom ontvang jij een 100% GRATIS STAATSLOT!

Volg de stappen op de speciale actiepagina om aanspraak te maken op jouw 100% gratis staatslot.

Maak jij gratis kans op de een van de vele prijzen van de Staatsloterij? Klik hieronder op "ga verder" om je deelname te bevestigen!

GA VERDER

Ontvang nu een
100% gratis staatslot



Meld je nu aan, speel mee en ontvang een gratis staatslot!

winnen nu een cadeaubon ter wa...
30255 KEER GEDEELD

Krijg nu een GRATIS cadeaubon ter waarde van € 500 voor het IKEA (slechts tijdelijk beschikbaar)



Volg hieronder deze twee eenvoudige stappen op om in aanmerking te komen voor jouw IKEA cadeaubon ter waarde van € 500:

Aantal nog beschikbare cadeaubonnen:
359

Doe de test

Zeker de moeite

Phishingtest → <https://safeonweb.be/nl/quiz/phishingtest>



Helpdeskfraude



- Verbreek de verbinding
- Laat je niet onder druk zetten
- Dit zal je bank nooit vragen:
 - geld overschrijven naar een (veilige) rekening
 - pincodes, wachtwoorden, responsecodes, saldo
 - toegang tot je computer /smartphone
 - medewerker langs te sturen

Te onthouden:

- afgedankte bankkaart doorknippen, dwars door de kopergouden betaalchip
- de pincode moet je nooit op een website intikken

Tip 6: openbare wifi en QR



Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifinetwerken.

- dataverbinding smartphone
(3G, 4G, 5G)
- kostaspect (let op in Zwitserland!)
- meeluisteren?
- wifi hotspot kan fake zijn

Valse QR-codes



Via de valse QR-code kom je op een phishingwebsite terecht.
Foto: stad Brugge

Stad Brugge ontdekt op tijd poging tot oplichting met valse QR-codes op parkeerautomaten

In Brugge is een poging tot fraude via de parkeerautomaten ontdekt. Op 17 automaten was een valse QR-code gekleefd. Die leidde naar een phishingwebsite, waar de gebruikers de gegevens van hun bankkaart moesten invoeren. Gelukkig werd de poging tot oplichting snel ontdekt. Er hebben zich nog geen gedupeerden gemeld.

Een QR code in het openbaar:
wees voorzichtig

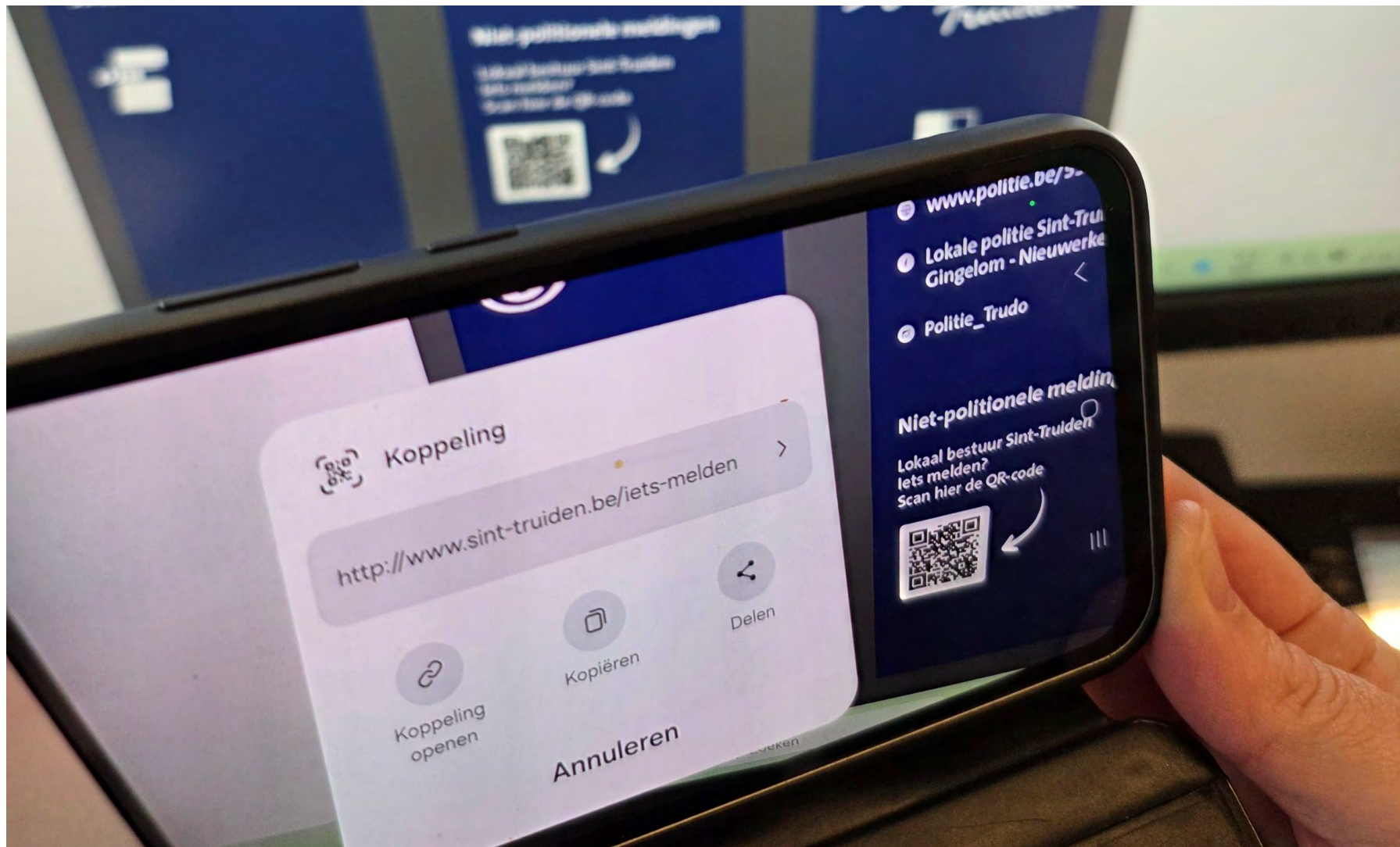
- terrastafeltjes (binnen- en buitenland)
- parkeermeter
- laadpaal
- affiche, flyer, enz

Valse QR-codes

Wat is quishing?

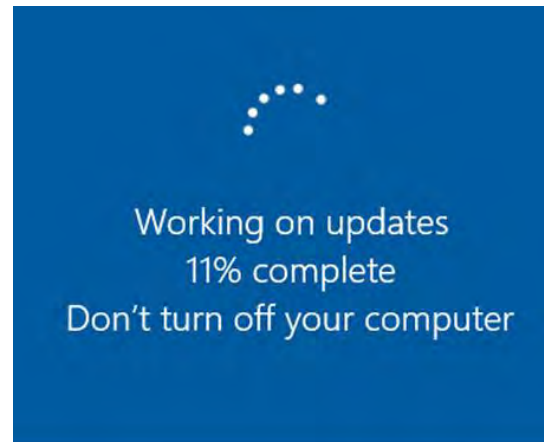


Valse QR-codes



Tip 7: software updates

- Update = gekend lek dat gedicht wordt!
- Installeer altijd de officiële software-updates. Zo verklein je de kans dat je gehackt wordt.
- Maak regelmatig back-ups van je bestanden.



Stel updates niet langer uit dan nodig...



Je zou het waarschuwingslampje in je auto toch ook niet negeren?

CyberPilot

Tip 8: officiële app stores

- Officiële applicatiewinkels
 - Google Play Store
 - Apple App Store
 - Windows App store
- Verwijder ongebruikte apps
- Ervaringen van anderen
- Wie is de uitgever/maker?
- Aantal downloads?
- Spelling (Gmeel i.p.v. Gmail)



Tip 9: anti virus



Nog steeds zeer belangrijk



Uiteraard up to date te houden graag



Zoekt ook in je mailbox vaak



Bevat vaak (zeker de betalende) een ingebouwde firewall

- Installeer een antivirusprogramma op al je toestellen en niet alleen op je computer/laptop.
- Schakel automatische updates in.
- Maak gebruik van een firewall.
- Gratis of betalend pakket? Betalend is niet “beter” maar vaak wel “meer”

Tip 10: privacy op sociale media

Hoe meer details je achterlaat, hoe beter men een poging tot phishing er kan laten uitzien, waardoor de kans dat je erin trapt stijgt.

Tip 10: sociale media

- Privacyinstellingen (zien, delen, posten) + regelmatig checken
- Accepteer wie je kent.
- Deel zo weinig mogelijk buiten je vriendenkring
- Een bericht van een vriend is niet 100% betrouwbaar (hacking)
- Sla nooit inloggegevens op
- 2FA

Voorkom dat je wordt gehackt op sociale media



Vertrouw niemand op sociale media voor 100%. Zelfs van mensen die je kent, kan het account zijn overgenomen door een hacker.

Als je vermoedt dat iemand in je netwerk is gehackt, bedenk dan dat je zijn of haar identiteit niet kan bevestigen door terug te schrijven. Neem in plaats daarvan via andere kanalen contact op met de persoon, bijv. door hem of haar op te bellen.



Multi-factor authenticatie is de beste verdediging tegen het hacken van jouw accounts door cybercriminelen.



Wat als het toch
fout loopt?

Doe aangifte



Politie

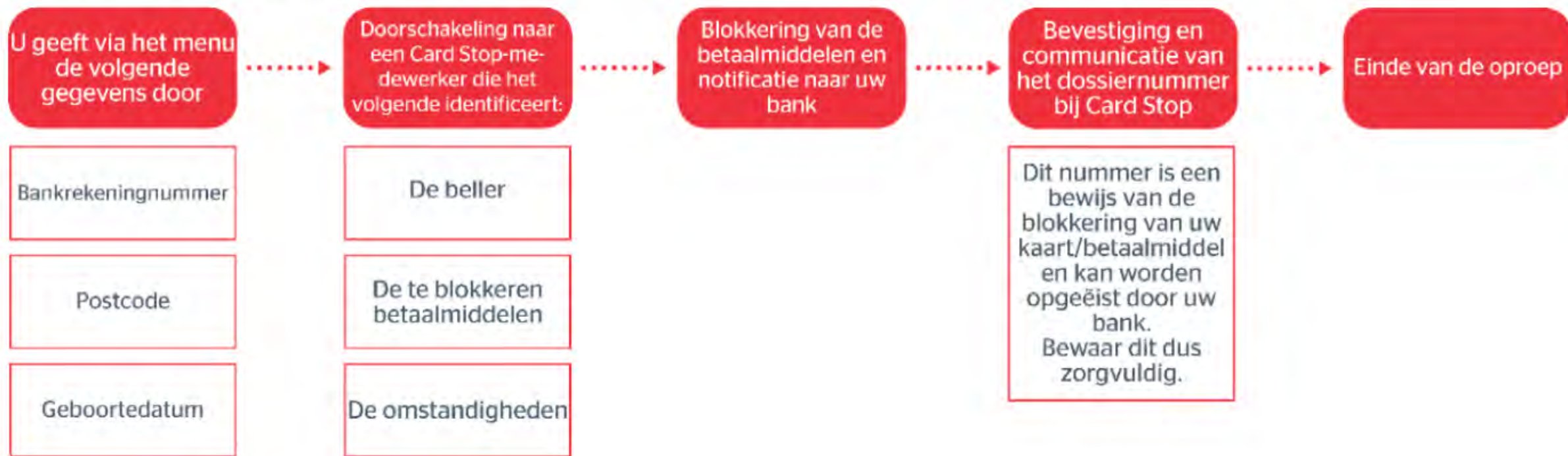
- Schaam je niet!
- Onmiddellijk, de klok tikt.
- Verzamel bewijs (mails, data, profielen, afschriften, ...)
- Aangifte
 - Online: <https://my.police.be/app/nl/home>
 - Afspraak via www.politie.be/5376
(Bel eerst even 011-70 19 10 om te situatie uit te leggen.)

Cardstop



Cardstop

Hoe verloopt een oproep naar Card Stop?



Vergeet niet je rekening te blokkeren rechtstreeks via de bank(app)!

Je bank



Geld gestolen van je rekening of vermoed je misbruik van je bankgegevens?

Banken zijn 24/7 bereikbaar om je te helpen.

→ zie flyer

Hieronder vind je de telefoonnummers die je kunt bellen om je bankapplicaties onmiddellijk te laten blokkeren:

Je bank	Binnen openingsuren	Buiten openingsuren
Argenta	00 32 3 285 53 33	00 32 3 285 53 33
Bank de Kremer	00 32 3 245 00 11	00 32 3 245 00 11
Bank Van Breda	00 32 3 245 00 11	00 32 3 245 00 11
Belfius	00 32 2 222 46 00	00 32 2 222 46 00
Beobank	00 32 2 622 20 00	00 32 78 170 170**
BNP Paribas Fortis	00 32 2 762 60 00	00 32 2 433 43 80
CBC	00 32 16 43 20 00	00 32 16 43 20 00

1



Bel onmiddellijk je bank via een van de nummers hiernaast (sommige banken zijn ook online bereikbaar via hun website of bankapp).*

Kaarten

- Wees steeds voorzichtig waar je je kaartnummer achterlaat
- Sla je kaartgegevens niet op in een webshop
- Geef je kaart niet zomaar mee met een vreemde
- Schakel enkel de landen in die je ook effectief nodig hebt
- Zet je limiet zo laag mogelijk. En verhoog je limiet slechts tijdelijk indien nodig (via de app)

SafeOnWeb

verdacht@safeonweb.be (mail, sms, QR)

- 2024 werden er 9 miljoen berichten doorgestuurd naar SafeOnWeb
- verdachte link -> Google SafeBrowsing en Microsoft SmartScreen.

App met actuele info.



CCB

Het **Centrum voor Cybersecurity België (CCB)** ontvangt dagelijks meer dan 12.000 meldingen... Het CCB laat de verdachte linken in deze berichten blokkeren en meldt frauduleuze websites aan bijvoorbeeld Google en Microsoft.



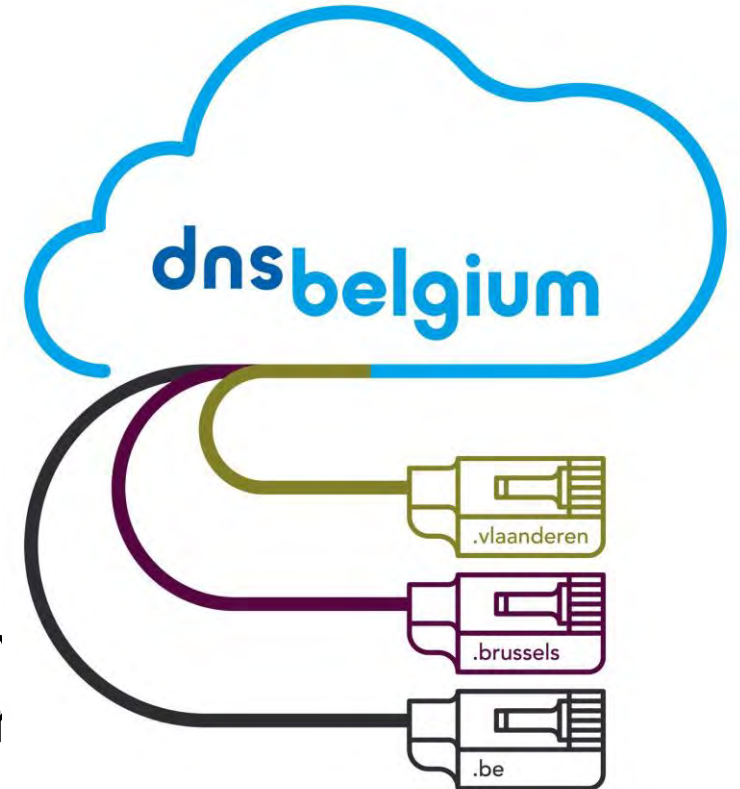
CENTRE FOR
CYBERSECURITY
BELGIUM

Samen veilig online

DNS Belgium is een organisatie die verantwoordelijk is voor het beheer van de Belgische internetdomeinen, zoals .be, .vlaanderen en .brussels. Ze werken samen met andere organisaties om online veiligheid te bevorderen en cyberaanvallen te bestrijden

→ Samen veilig online

Op deze pagina ontdek je hoe jij anderen kan helpen om beschermen. Lees de verhalen, herken de risico's en leer www.dnsbelgium.be/nl/samen-veilig-online



Digipunten – Truiers Digicenter

Om digitale problemen aan te pakken, biedt het Truiers Digicenter gratis ondersteuning en opleidingen in Sint-Truiden, Gingelom en Nieuwerkerken.

→ www.truiersdigicenter.be





Om af te sluiten,
nog dit!

In het kort

- Train enkele reflexen:
 - Vreemde berichten
 - Vreemde vrienden
- Wees gezond argwanend: de bank belt niet
- Laat u niet meeslepen
- Durf hulp te zoeken
- Vraagt men geld? Waarom? En wie!
- Doe aangifte!

Vragen

Carolien Motmans

Coördinator preventie & handhaving
carolien.motmans@police.belgium.eu
011-70 19 85

Evi Lennertz

Adviseur communicatie lokale politie Sint-Truiden - Gingelom - Nieuwerkerken
evi.lennertz@police.belgium.eu
011-70 19 03

Een project van:

*Sint
Truiden*

