VEILIG ONLINE TIJDENS DE VERKIEZINGSCAMPAGNE

Aanbevelingen voor een cyberveilige campagne

MAART 2024

CENTRE FOR CYBERSECURITY BELGIUM
ADIV - SGRS
VSSE veiligheid van de staat sûreté de l'état
.be

VEILIG ONLINE TIJDENS DE VERKIEZINGSCAMPAGNE

Aanbevelingen voor een cyberveilige campagne

De gids *'Veilig online tijdens de verkiezingscampagne'* bevat aanbevelingen om de verschillende digitale tools die je dagelijks gebruikt beter te beveiligen.

Verkiezingen zijn een cruciaal element in het democratisch proces. Terreurgroepen, criminelen of instanties met politieke motieven kunnen proberen de verkiezingsresultaten te beïnvloeden. Politieke partijen en hun kandidaten zijn daarbij een potentieel belangrijk doelwit. Zo heeft het Europees Agentschap voor Cyberveiligheid (ENISA)[1] gewezen op de ondermijnende effecten van chatbots en de manipulatie van informatie door kunstmatige intelligentie (AI). Het agentschap heeft tussen juli 2022 en juni 2023 ongeveer 2.580 incidenten geregistreerd, waarvan vele gericht waren op overheidsinstanties.

Met deze gids willen we je in staat stellen om je cyberveiligheidsniveau te verhogen, cyberveiligheidsrisico's te beperken en digitale kwetsbaarheden te verminderen.

De meeste van deze tips zijn evident en volg je misschien al op. Zo niet zal dit document je helpen om je belangen en je digitale veiligheid beter te beschermen. Het is belangrijk dat ook je omgeving zich goed beschermt. Deel deze tips met je familie en vrienden.

De gids *'Veilig online tijdens de verkiezingscampagne'* is een initiatief van de Veiligheid van de Staat (VSSE), het Centrum voor Cybersecurity België (CCB) en de Algemene Dienst voor Inlichting en Veiligheid (ADIV). Elke dienst, vertrekkend vanuit haar eigen expertise, heeft een belangrijke bijdrage geleverd aan de totstandkoming van deze gids.

Brussel, maart 2024
Met hoogachting,

Miguel DE BRUYCKER
Directeur-generaal,
Centrum voor Cybersecurity België

Francisca BOSTYN
Administrateur-Generaal a.i.
Veiligheid van de Staat

Stéphane DUTRON
Generaal-majoor,
Hoofd van het Departement
Inlichting en Veiligheid.

1: The ENISA Threat Landscape 2023, *Impact of social engineering & information manipulation campaigns.* Zie ook Hoofdtsuk 4 'Addressing FIMI during electoral processes' in 2nd EEAS *Report on Foreign Information Manipulation and Interference Threats* (Januari 2024).

INHOUD

1

IK HERKEN VERDACHTE BERICHTEN

PHISHING IS ONLINE OPLICHTING DOOR VALSE MAILS, WEBSITES OF BERICHTEN. DERGELIJKE E-MAILS, DE LINKS EN DE BIJLAGEN ZIJN VAAK DE TOEGANGSPOORT VOOR EEN CYBERAANVAL. HIER ZIJN ENKELE AANWIJZINGEN DIE JE AANDACHT MOETEN TREKKEN VOORDAT JE BESLIST OM OP EEN LINK OF BIJLAGE TE KLIKKEN.

> **De afzender.** Ken je de afzender persoonlijk? Is dat het gebruikelijke e-mailadres? Ziet het e-mailadres er legitiem uit? Stuurt deze persoon of organisatie mij regelmatig dit soort documenten? In geval van twijfel, bel de persoon of de organisatie die je de e-mail heeft gestuurd.

> **De aard van de vraag.** Word je om persoonlijke of gevoelige informatie gevraagd? Geef bij twijfel nooit persoonlijke of gevoelige gegevens door.

> **De formulering van de e-mail.** Bevat de e-mail spellings- of grammaticafouten? Probeert men je nieuwsgierigheid te wekken? Maakt men je beloftes die te mooi zijn om waar te zijn? Moet je iets betalen? Is het dringend? Bij de minste twijfel, klik je niet.

> **Klik niet op de links of QR-codes in valse berichten en open geen bijlagen.** Als je twijfelt, zoek de website op via een zoekmachine.

> **Leer een valse link te herkennen** via de e-learningmodule 'Surfen zonder zorgen': https://surfenzonderzorgen.safeonweb.be/nl/modules/1

> **Vul zeker nooit persoonlijke gegevens in.**

> **Stuur verdachte berichten door** naar verdacht@safeonweb.be

> **Installeer de Safeonweb browser extensie. De Safeonweb browser extensie** is een hulpmiddel bij het evalueren van de betrouwbaarheid van een website. De extensie laat je voor elke website die je bezoekt, zien of de eigenaar is gevalideerd (groen) of niet (oranje).

Meer informatie:

- www.safeonweb.be/nl/leer-valse-mails-herkennen
- surfenzonderzorgen.safeonweb.be/nl/modules/1

2

IK BESCHERM MIJN ACCOUNTS MET TWEESTAPSVERIFICATIE (2FA)

EEN GOED GEBRUIK VAN WACHTWOORDEN IS VAN GROOT BELANG. JE HEBT NOG STEEDS WACHTWOORDEN NODIG OM JE TOESTELLEN, JE GEGEVENS, JE NETWERKEN (BV. WIFI) EN JE ACCOUNTS (BV. E-MAIL EN SOCIAL MEDIA) GOED TE BEVEILIGEN. MAAR ZELFS HET STERKSTE WACHTWOORD GARANDEERT GEEN TOTALE VEILIGHEID.

Tweestapsverificatie versterkt de beveiliging voor de toegang tot je accounts en apparaten. Op deze manier kan een cybercrimineel, zelfs als die je wachtwoord weet te achterhalen, geen toegang krijgen tot je accounts zonder de andere beveiligingsniveaus te doorlopen.

> **Activeer waar mogelijk tweestapsverificatie (2FA).** De meeste diensten van de grote digitale platforms (zoals sociale netwerken) en veel apparaten bieden deze optie (bijvoorbeeld via vingerafdruk en/of gezichtsherkenning).

> **Gebruik verschillende wachtwoorden.** Het veiligst is om een verschillend wachtwoord te hebben voor elke gevoelige dienst (je bank, je e-mail, je toegang tot sociale netwerken etc.). Als een van je wachtwoorden gekraakt is, dan wordt er slechts één dienst getroffen.

> **Lang en origineel.** Hoe langer je wachtwoord, hoe veiliger het is. Kies geen wachtwoord dat in het woordenboek te vinden is. Combineer eerder verschillende woorden zonder duidelijk onderling verband maar wel gemakkelijk te onthouden.

> **Gebruik een password manager.** Een password manager is een programma dat al je wachtwoorden beheert en dat zelf goed beschermd is.

> **Zonder sporen.** Laat je wachtwoord niet achter op een post-it naast je computer, in een e-mail of in een computerbestand.

> **Deel je wachtwoorden en accounts niet met anderen.** Met gedeelde accounts loop je het risico dat de verantwoordelijkheid verwatert en dat de acties die in naam van de gebruiker werden uitgevoerd, niet te traceren zijn.

Meer informatie:

- www.safeonweb.be/nl/gebruik-sterke-wachtwoorden
- https://safeonweb.be/nl/gebruik-tweestapsverificatie
- https://atwork.safeonweb.be/fr/MFA

3

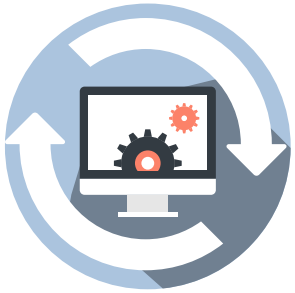
MIJN TOESTELLEN EN PROGRAMMA'S ZIJN UP-TO-DATE EN OFFICIEEL

GEEF CYBERCRIMINELEN NIET DE KANS OM TOEGANG TE KRIJGEN TOT JE TOESTEL OF JE GEGEVENS DOOR REGELMATIG BEVEILIGINGSUPDATES UIT TE VOEREN, ZOWEL VOOR JE BESTURINGSSYSTEEM ALS VOOR JE PROGRAMMA'S EN JE APPS. ELK PROGRAMMA BEVAT IMMERS KWETSBAARHEDEN DIE HET MOGELIJK MAKEN VOOR CYBERCRIMINELEN OM SCHADE TE BEROKKENEN OF DE CONTROLE OVER JE TOESTELLEN TE NEMEN. DEZE KWETSBAARHEDEN WORDEN GELUKKIG ONTDEKT EN HERSTELD. DIT IS PRECIES WAT ER GEBEURT ALS JE EEN UPDATE UITVOERT.

> **Activeer het automatisch updaten van hardware en software.** Dit zorgt ervoor dat zodra er een kwetsbaarheid wordt gedetecteerd, je toestel beter beschermd is.

> **Gebruik alleen officiële websites.** Als je software moet downloaden of updaten, doe dit alleen vanaf de officiële website van de fabrikant.

> **Gebruik veilige apps en programma's.** Installeer alleen apps uit een standaard appstore (Google play, App Store) en programma's van een officiële verkoper. Verwijder regelmatig toepassingen die je niet gebruikt. Beperk de toegang van je apps tot het strikt noodzakelijke. Een rekenmachine-app heeft bv. geen toegang nodig tot je locatie of contacten. Controleer regelmatig de gegevens die door je toepassingen worden verbruikt om ongepast verkeer op te sporen.



> **De standaard beveiliging van je apparaat mag je niet omzeilen** (bijvoorbeeld jailbreaken[2] of rooten[3]). Hoewel dat je de indruk lijkt te geven dat je meer controle over het apparaat hebt en je dan toegang hebt tot beschermde functies, verhoogt dit de risico's aanzienlijk.

> **Sluit je toestellen dagelijks af.** Bij het opstarten worden updates immers meestal automatisch uitgevoerd.

Meer info over updates:

- www.safeonweb.be/nl/doe-regelmatig-updates
- atwork.safeonweb.be/nl/tools-resources/updates-beheren

2: Jailbreaken: het mogelijk maken om op een iPhone, iPod touch, iPad en Apple TV softwaretoepassingen te laden die door de firma Apple niet erkend zijn.
3: Het rooten van een smartphone of tablet betekent dat door een softwarematige update toegang verkregen wordt tot de administrator account van de telefoon die toegang heeft tot alle functionaliteiten en instellingen.

4

MIJN TOESTELLEN ZIJN GOED BEVEILIGD

WANNEER EEN TOESTEL IN VERKEERDE HANDEN TERECHTKOMT, KAN JE DAT VEEL SCHADE TOEBRENGEN. ZORG DAAROM VOOR EEN GOEDE BEVEILIGING VAN JE SMARTPHONE, TABLET, LAPTOP EN PC.

> **Een goede vergrendeling.** Activeer de automatische vergrendeling van je smartphone wanneer deze inactief is (maximaal 1 minuut). Kies een code en geen patroon. Wanneer deze dienst wordt aangeboden, stel dan een tijdslot na een aantal mislukte pogingen op je smartphone in en stel het automatisch wissen van gegevens na te veel toegangspogingen in. Let uiteraard wel op dat goede back-ups voorhanden zijn.

> **Versleutel je toestellen.** Versleutel indien mogelijk je toestellen, ook je USB en draagbare harde schijven. Als je een SD-kaart gebruikt, dan versleutel je deze ook.

> **Beperk de toegang.** Activeer de toegang van wifi, Bluetooth, Near Field Communication[4] of NFC*, data, geolocatie etc.) alleen wanneer je deze nodig hebt. Activeer de automatische-activeringsfuncties (bv. voor wifi) niet. Controleer regelmatig de toegangsrechten voor applicaties.

> **Behoud de controle over je toestellen.** Laat ze niet onbeheerd achter.

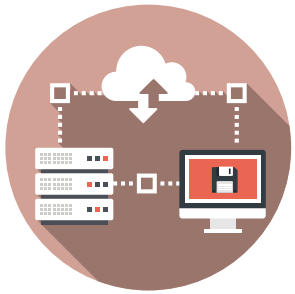
4: "Near Field Communication" of "NFC" is een draadloze manier om kleine hoeveelheden informatie uit te wisselen binnen een straal van 10 centimeter, om bv een connectie te maken met betaalsystemen of smartphones.

5

MIJN GEGEVENS ZIJN GOED BEVEILIGD

OOK MET DE GEGEVENS DIE JE BEWAART OP JE TOESTELLEN MOET JE HEEL ZORGVULDIG OMSPRINGEN. ALS JE JE GEGEVENS KWIJTRAAKT, IS DAT NIET ALLEEN ZEER VERVELEND VOOR JEZELF, JE KAN OOK IN DE PROBLEMEN KOMEN ALS KWAADWILLIGE PERSONEN GEGEVENS VAN BV. JE PARTIJLEDEN STELEN EN MISBRUIKEN.

> **Maak back-ups.** Een back-up is een reservekopie van gegevens die belangrijk zijn voor jou. Met een back-up kan je je gegevens terugzetten als je een virus hebt. Ook bij diefstal, verlies of technische problemen, is het een geruststelling om een back-up te hebben. Je kan dan het hele systeem opnieuw (laten) installeren en je gegevens terugplaatsen. **Dit geldt natuurlijk ook voor je mobiele toestellen.**



> **Automatiseer back-ups.** Voer een systeem in om regelmatig automatisch een back-up van je gegevens te maken. Gedecentraliseerde (cloud-) oplossingen kunnen een voordeel zijn op voorwaarde dat je leverancier betrouwbaar is.

> **Gebruik een virusscan.** Een virusscan zorgt ervoor dat je computer niet vatbaar is voor virussen. Het is het belangrijkste stukje software om je computer en je gegevens te beschermen.

> **Uitschakelen.** Zet je apparaten uit wanneer je ze niet gebruikt (vakantie, weekend, feestdagen etc.) en schakel de functies die je niet gebruikt uit (wifi, Bluetooth, NFC, geolocatie).

> **Kijk uit met het gebruik van USB-sticks.** Een USB memory stick is handig om mee te nemen maar kan je gemakkelijk kwijtspelen. Kijk vooral uit met USB memory sticks die je van anderen krijgt of die je op straat of elders zou vinden. Deze kunnen virussen bevatten. Laat daarom een virusscan uitvoeren (door een ICT professional) vooraleer de USB memory stick te gebruiken. Bewaar regelmatig de inhoud van de USB memory stick en verwijder regelmatig de documenten die overbodig zijn.

Meer informatie over back-ups:
- www.safeonweb.be/nl/maak-back-ups
- https://atwork.safeonweb.be/nl/tools-resources/back-ups-beheren

Meer informatie over virusscans:
- www.safeonweb.be/nl/scan-je-computer
- https://atwork.safeonweb.be/nl/tools-resources/antivirussoftware

Meer informatie USB:
- https://cyfun.be (Cyberfundamentals - niveau 'Small', onder "3. Installeer antivirus").

6

IK GEBRUIK EEN VEILIG (WIFI) NETWERK

EEN GOED BEVEILIGD NETWERK IS DE BASIS VAN EEN GOEDE CYBERPREVENTIE. ALS EEN CYBERCRIMINEEL TOEGANG KAN KRIJGEN TOT JE NETWERK, DAN HEEFT DIE TEGELIJKERTIJD OOK TOEGANG TOT ALLE TOESTELLEN DE ER OP AANGESLOTEN ZIJN. HET DRAADLOZE WIFISYSTEEM HEEFT DE CONNECTIE VAN ELEKTRONISCHE APPARATEN MET DE VERSCHILLENDE NETWERKEN (INTERNET, PRIVÉNETWERK, BEDRIJFSNETWERK ETC.) AANZIENLIJK VEREENVOUDIGD. HOE BEVEILIG JE JE WIFI ZO GOED MOGELIJK?

> **Beveilig je persoonlijke router.** Wanneer je een nieuwe wifirouter (of box) ontvangt, behoud dan niet de standaardinstellingen. Wijzig je netwerknaam (SSID) en verwerk er geen evidente elementen in. Wijzig je netwerkwachtwoorden (inclusief het wachtwoord dat op je router staat).

> **Gebruik WPA2 beveiliging.** Je router heeft waarschijnlijk de mogelijkheid om WPA2, WPA of WEP encryptie in te stellen. Kies WPA2 en stel dit onmiddellijk in als dit nog niet gebeurd is.

> **Activeer de firewall.**

> **Kies een sterke toegangssleutel.** Om de toegangssleutel voor je wifinetwerk te kiezen, raadpleeg de bovenstaande instructies voor wachtwoorden. Maak deze sleutel alleen bekend aan vertrouwenspersonen. Verander hem regelmatig.

> **Vermijd openbare wifinetwerken.** Bankverrichtingen of andere belangrijke zaken doe je niet via een open wifinetwerk. Vermijd het om via een open wifinetwerk accounts te creëren waarbij je een wachtwoord moet invoeren.

> **Installeer een Virtual Private Network (VPN).** Dit is je persoonlijke beveiligde tunnel door het wifinetwerk. Je kan online gratis of betalend VPN diensten installeren. Verschillende virusscanners bieden ook VPN aan.

Meer informatie over wifi:
- www.safeonweb.be/nl/actueel/er-ook-wifi
- https://atwork.safeonweb.be/nl/tools-resources/bescherm-je-mobiele-toestellen
- https://atwork.safeonweb.be/nl/tools-resources/hoe-blijf-je-waakzaam-voor-cyberbedreigingen

Meer informatie over WPA2:
- https://cyfun.be (Cyberfondamentals - niveau 'Small', onder "4. Beveilig uw netwerk").

7

IK MAAK VERSTANDIG GEBRUIK VAN SOCIAL MEDIA

HET PRIVÉLEVEN VAN EEN POLITICUS IS MEER BLOOTGESTELD DAN DAT VAN ANDERE BURGERS. VIA DE SOCIALE MEDIA VERZORG JE NIET ALLEEN RECHTSTREEKSE CONTACTEN MET DE BUITENWERELD, DE BUITENWERELD IS IN STAAT OM EEN PROFIEL VAN JOU TE SCHETSEN OP BASIS VAN INFORMATIE DIE JE DEELT, GAANDE VAN PERSOONLIJKE FOTO'S, VOORKEUREN INZAKE FILMS, VOEDING, JE FAMILIE, JE NETWERKEN, JE LOCATIE TOT ZELFS JE GEDRAG. DEZE INFORMATIE KAN BIJGEVOLG MISBRUIKT WORDEN.
HIER VIND JE EEN AANTAL AANBEVELINGEN OM JE PRIVACY TE BESCHERMEN.

> **Gebruik afzonderlijke apparaten.** Scheid zoveel mogelijk de apparaten die je gebruikt voor je politieke of professionele activiteiten van de apparaten voor je privégebruik.

> **Gebruik verschillende e-mailadressen.** Je kan bijvoorbeeld één e-mailadres hebben voor gevoelige diensten (je bank, administratie etc.) en een ander voor minder gevoelige diensten (video on demand, forum, spelletjes etc.). Het is verstandig om een e-mailadres voor je openbare activiteiten te hebben.

> **Denk aan de veiligheid van je sociale netwerken.** Controleer de instellingen van de sociale netwerken die je voor de campagne gebruikt (inclusief bepaalde automatische publicaties). Maak vóór elke publicatie keuzes voor de zichtbaarheid van je publicaties, afhankelijk van wat je wil delen. Gebruik tweestapsverificatie (2FA) voor de toegang tot je accounts.

> **Wees waakzaam voor internettrollen.** Zij hebben als voornaamste doel online discussies uit te lokken, te beïnvloeden, te sturen en te laten escaleren. Hiervoor worden op voorhand op sociale media accounts aangemaakt van ogenschijnlijk gewone burgers. Op gepaste tijden worden deze dan ingeschakeld om een positie in te nemen bij een bepaald onderwerp. Om de internettrol te doen stoppen is het belangrijk dat je niet reageert zoals de trol wil. Ga niet mee in de discussie en word niet boos.

> **Vermijd waar mogelijk het koppelen van accounts.** Sommige platformen bieden de mogelijkheid aan in te loggen met je bestaande account op andere sociale media. Deze gekoppelde accounts zijn kwetsbaar omdat al je persoonlijke informatie geconcentreerd bij een bepaald platform terecht komt.

> **De privacy instellingen van je accounts dienen regelmatig nagekeken te worden.** Instellingen kunnen door de provider soms eenzijdig gewijzigd worden waardoor bijvoorbeeld de eigendomsrechten van je persoonlijke informatie bij de platformbeheerder komen te liggen.

> **Wees je ervan bewust dat sommige sociale media platformen banden kunnen hebben met specifieke landen.** TikTok bijvoorbeeld is een Chinees product. De bewaarde gegevens op dit platform zouden als gevolg van de Chinese wetgeving door de Chinese overheid misbruikt kunnen worden. Maak de bedenking of je echt op elk social media platform aanwezig moet zijn.

8

IK HERKEN DESINFORMATIE

DESINFORMATIE IS EEN GEVAAR VOOR ONZE DEMOCRATIE OMDAT HET KIEZERS KAN VERHINDEREN EEN GEÏNFORMEERDE POLITIEKE KEUZE TE MAKEN. DIT BIJVOORBEELD DOOR DE VERSPREIDING VAN VALSE OF GEMANIPULEERDE INFORMATIE, MAAR OOK DOOR HET KUNSTMATIG OPSTOKEN VAN VERDEELDHEID, HET ONDERMIJNEN VAN HET VERTROUWEN IN DE VERKIEZINGEN OF HET WEREN VAN LEGITIEME STEMMEN UIT HET DEBAT. ALS POLITICUS KAN JE EEN DOELWIT ZIJN, MAAR ONBEWUST OOK ZELF DESINFORMATIE VERSTERKEN.

> **Informeer je over desinformatie.** Desinformatie is niet noodzakelijk hetzelfde als propaganda of nepnieuws. Het kan zich bovendien in vele gedaanten voordoen. Denk aan nagemaakte nieuwssites of vervalste beelden, maar net zo goed aan artificiële audioberichten of complotfilmpjes op TikTok. Op de website van het Nationaal Crisiscentrum vind je meer informatie over wat desinfo precies is en de diverse beïnvloedingstechnieken die vaak worden ingezet: www.crisiscentrum.be/nl/desinformatie

> **Gebruik je gezond verstand.** Je kan desinformatie herkennen door een aantal vragen te stellen. Wie is de auteur, maker of verspreider? Is de informatie waarheidsgetrouw? Met welk doel is het bericht gemaakt of verspreid? Bijkomende tips: lees verder dan de titel, raadpleeg meerdere bronnen, check wanneer een bericht geschreven of gedeeld is en wees kritisch over de vorm.

> **Wees beducht voor deepfakes.** De snelle opkomst van Generatieve Artificiële Intelligentie maakt het enorm makkelijk om beelden te manipuleren of compleet artificiële foto's, video's en audio te creëren. Een video vertraagd afspelen kan een eerste manier zijn om dergelijke deepfakes te herkennen.

> **Doe zelf een factcheck.** Om na te gaan of beelden kloppen, kan je ook het volgende doen. Met een zoekmachine, zoals Google Reverse Image Search, kan je de werkelijke context achterhalen. Kijk aandachtig en let op diverse omgevingselementen die je meer vertellen over de locatie. Zoek onafhankelijke bronnen om verhalen of beelden te verifiëren. Extra tips vind je op belux.edmo.eu/nl/factchecking-toolkit

> **Deel geen twijfelachtige content.** Ben je nog steeds niet zeker of de informatie wel correct en betrouwbaar is? Verspreid de informatie of het bericht dan zeker niet verder. Niet alleen is dat net waar de verspreiders op hopen. Bovendien heb je als politicus of politica een erg groot bereik en geef je desinformatie extra gezag door het via jouw kanalen te delen.

> **Meld desinformatie.** Ben je zeker dat je met desinformatie te maken hebt? Dan kan je dit melden aan EDMO BELUX op belux.edmo.eu/nl/verslaggeving-over-desinformatie

IK BEN SLACHTOFFER: WAT NU?

1. IK BEN SLACHTOFFER VAN EEN CYBERAANVAL EN DE AANVAL IS NOG AAN DE GANG

> Je kan de gevolgen van een cyberaanval beperken als je snel handelt.

> Je kan het incident melden bij het CCB via het formulier op de website van het CCB of per e-mail: incident@ccb.belgium.be. Meer info over de mogelijkheden om een incident te melden vind je op https://ccb.belgium.be/nl/cert/een-incident-melden

Bij een noodgeval kan het CCB ook telefonisch bereikt worden op: **+32 (0)2 501 05 60.**

> Je zet de computer NIET uit, want op die manier wis je sporen die de daders achterlaten.

> Het is ook raadzaam om de wachtwoorden te veranderen vanop een veilig toestel omdat de dader die mogelijks in zijn of haar bezit heeft.

> Dien een klacht in bij de lokale politie.

Meer informatie:

- https://ccb.belgium.be/nl/cert/eerste-hulp-bij-een-cyberaanval

2. MIJN ACCOUNT IS GEHACKT

> Vervang onmiddellijk al je wachtwoorden. Werk daarvoor vanop een veilig toestel, dus niet hetzelfde als waar je gegevens werden gestolen.

> Voeg onmiddellijk tweestapsverificatie toe (2FA).

> 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.**

> Zijn er gegevens uit je politieke leven gestolen, breng dan zo snel mogelijk je partij op de hoogte en doe aangifte bij de Gegevensbeschermingsautoriteit.

> Informeer je contactpersonen. Zij lopen immers het risico om berichten te ontvangen die zogezegd uit jouw naam verstuurd werden.

Meer informatie:

- www.safeonweb.be/nl/mijn-account-gehackt

3. MIJN TOESTEL IS GESTOLEN OF VERLOREN

> Vervang onmiddellijk al je wachtwoorden van de accounts die op je toestel stonden (bv. e-mail, Facebook, WhatsApp…)

> Stonden je bank- of betaalgegevens op het gestolen toestel, verwittig de contactpersoon bij je bank en houd je rekeningen nauwlettend in het oog. Laat eventueel je bankkaarten en rekeningen blokkeren via Card Stop (www.cardstop.be of **078 170 170**).

> Stonden er gegevens uit je politieke leven op het toestel, breng dan zo snel mogelijk je partij op de hoogte.

> Als je toestel werd gestolen, doe dan aangifte bij de politie.

Meer informatie:

- www.safeonweb.be/nl/ik-ben-mijn-smartphone-tablet-kwijt

4. MIJN TOESTEL IS GEÏNFECTEERD DOOR EEN VIRUS

> Een virus moet zo snel mogelijk verwijderd worden.

> Als je nog geen virusscanner had en je toestel is niet geblokkeerd, dan is dit het moment om er een te installeren, een scan te doen en het virus te verwijderen. Geef ondertussen geen persoonlijke gegevens of betaalgegevens in, want sommige virussen kunnen deze info doorsturen.

Meer informatie:

- www.safeonweb.be/nl/help-ik-heb-een-virus

CONTACT

1. CENTRUM VOOR CYBERSECURITY BELGIË (CCB)

> Je kan je cyberincidenten melden bij het CCB en bijstand vragen, zowel voor, tijdens als na de verkiezingen.

Dit doe je door een mail te sturen naar incident@ccb.belgium.be of een melding te doen op https://ccb.belgium.be/fr/cert

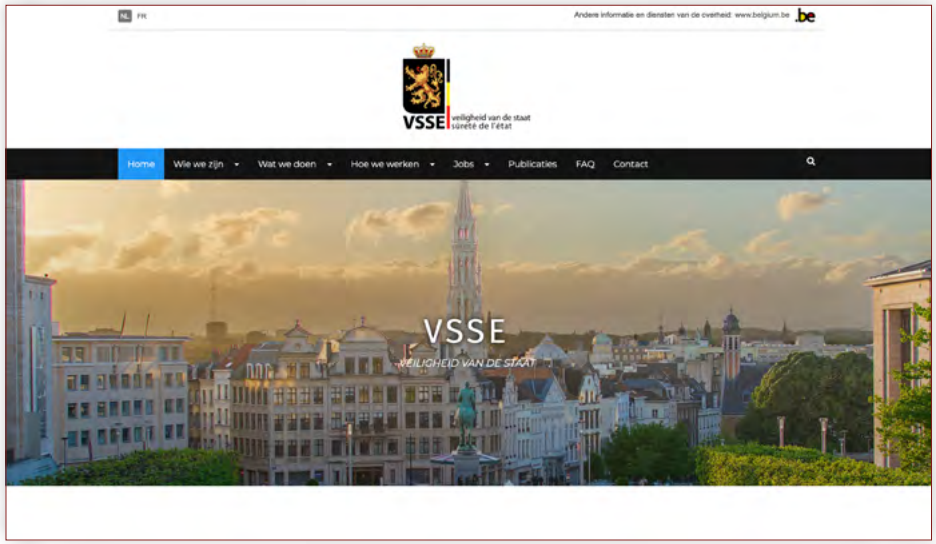
Bij een noodgeval kan het CCB ook telefonisch bereikt worden op: **+32 (0)2 501 05 60.**

2. VEILIGHEID VAN DE STAAT (VSSE)

> Alle info over de opdrachten en de werking van de VSSE vind je op de website www.vsse.be

3. ALGEMENE DIENST INLICHTING EN VEILIGHEID (ADIV)

> Voor meer informatie over de rol en verantwoordelijkheden van ADIV kan je csoc@cyber.mil.be contacteren.



MEER INFORMATIE

CYBERAANVALLEN:

> **Centrum voor Cybersecurity België:** https://ccb.belgium.be/nl/cert

> **Safeonweb at work:** https://atwork.safeonweb.be/nl

> **Cyberfundamentals:** https://cyfun.be

> **Cybersecurity Basics voor starters:** www.cybersecuritycoalition.be/nl/cyber-security-basics-voor-starters/

> **Cybersecurity scan (FOD Economie):** https://economie.fgov.be/cybersecurity

> **Gegevensbeschermingsautoriteit:** www.gegevensbeschermingsautoriteit.be/

> **Meldpunt fraude:** https://meldpunt.belgie.be/meldpunt/

> **Safeonweb:** www.safeonweb.be

DESINFORMATIE:

> **Desinformatie (Nationaal Crisiscentrum):** https://crisiscentrum.be/nl/desinformatie

> **The European Centre of Excellence for Countering Hybrid Threats:** www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

INFORMATIE OVER POTENTIËLE BUITENLANDSE INMENGING:

> www.vsse.be

Iedereen is vrij de aanbevelingen uit deze gids te volgen volgens zijn/haar eigen risicoanalyse. Ze zijn opgesteld in functie van de dreiging zoals deze is waargenomen op de dag van de publicatie ervan. We kunnen niet garanderen dat deze aanbevelingen op zichzelf de veiligheid van een gericht informatiesysteem kunnen waarborgen.

D/2024/7951/NL/1306

Veilig online tijdens de verkiezingscampagne

Aanbevelingen voor een cyberveilige campagne

Verantwoordelijke uitgever: Francisca BOSTYN
Koning Albert II laan, 6 - 1000 Brussel

CENTRE FOR CYBERSECURITY BELGIUM

ADIV - SGRS

VSSE veiligheid van de staat sûreté de l'état

.be