SURFER EN TOUTE SÉCURITÉ PENDANT LA CAMPAGNE ÉLECTORALE

Recommandations pour une campagne sous le signe de la cybersécurité

MARS 2024

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

SURFER EN TOUTE SÉCURITÉ PENDANT LA CAMPAGNE ÉLECTORALE

Recommandations pour une campagne sous le signe de la cybersécurité

Le guide « *Surfer en toute sécurité pendant la campagne électorale* » contient des recommandations en vue de mieux sécuriser les différents outils numériques que vous utilisez au quotidien.

Les élections sont la clé de voûte du processus démocratique. Des groupes terroristes, des criminels ou des instances politisées peuvent essayer d'en influencer le résultat. Les partis politiques et leurs candidats constituent dès lors une cible potentielle non négligeable. L'Agence de Cybersécurité de l'Union européenne (ENISA)[1] a ainsi mis en évidence les effets perturbateurs de *chatbots* et de la manipulation d'informations par l'intelligence artificielle (IA). Elle a enregistré environ 2 580 incidents entre juillet 2022 et juin 2023, dont un grand nombre visait les administrations publiques.

Par le biais de ce guide, nous entendons vous donner toutes les clés nécessaires pour améliorer votre niveau de cybersécurité, limiter les dangers liés à la cybersécurité et réduire les vulnérabilités numériques.

La plupart de ces trucs et astuces vous paraîtront couler de source et peut-être les appliquez-vous déjà. Si ce n'est pas le cas, ce document vous aidera à améliorer la protection de vos intérêts et de votre sécurité numérique. Par ailleurs, il est primordial que votre entourage se protège rigoureusement lui aussi. Partagez donc ces trucs et astuces avec votre famille et vos amis !

Le guide « Surfer en toute sécurité pendant la campagne électorale » est une initiative de la Sûreté de l'État (VSSE), du Centre pour la Cybersécurité Belgique (CCB) et du Service général du renseignement et de la sécurité (SGRS). Fort d'une expertise propre, chaque service a apporté sa pierre à l'édifice et a permis l'élaboration de ce guide.

Bruxelles, mars 2024
Cordialement,

Miguel DE BRUYCKER
Directeur général du Centre pour la Cybersécurité Belgique

Francisca BOSTYN
Administratrice générale a.i. de la Sûreté de l'État

Stéphane DUTRON
Général-major, Chef du Service général du Renseignement et de la Sécurité

1 : The ENISA Threat Landscape 2023, *Impact of social engineering & information manipulation campaigns*. Voir également le Chapitre 4 "Addressing FIMI during electoral processes" dans *2nd EEAS Report on Foreign Information Manipulation and Interference Threats* (janvier 2024).

TABLE DES MATIÈRES

1

JE RECONNAIS LES MESSAGES SUSPECTS

LE TERME « PHISHING » RECOUVRE LES ACTES D'ESCROQUERIE EN LIGNE PAR L'INTERMÉDIAIRE D'EMAILS, DE SITES WEB OU DE MESSAGES FRAUDULEUX. DE TELS EMAILS, LEURS LIENS ET LEURS PIÈCES JOINTES OUVRENT SOUVENT LA PORTE À UNE CYBERATTAQUE. VOICI QUELQUES INDICES AUXQUELS PRÊTER ATTENTION AVANT DE DÉCIDER DE CLIQUER SUR UN LIEN OU UNE PIÈCE JOINTE.

> **L'expéditeur.** Connaissez-vous personnellement l'expéditeur ? Est-ce son adresse mail habituelle ? L'adresse électronique a-t-elle l'air légitime ? Est-ce que cette personne ou organisation m'envoie fréquemment ce type de document ? Dans le doute appelez la personne ou l'organisation qui vous a envoyé l'email.

> **La nature de la demande.** Est-ce que des informations personnelles ou sensibles vous sont demandées ? En cas de doute, ne communiquez jamais des données personnelles ou sensibles.

> **La formulation du message.** Est-ce que l'email comporte des fautes d'orthographe ou de grammaire ? Le message tente-t-il d'éveiller votre curiosité ? Vous fait-on des promesses trop belles pour être vraies ? Vous demande-t-on de l'argent ? Est-ce qu'un sentiment d'urgence est créé ? En cas de doute, abstenez-vous de cliquer.

> **Ne cliquez pas sur les liens ou codes QR dans des messages frauduleux et n'ouvrez aucune pièce jointe.** Si vous avez des doutes, effectuez une recherche à propos du site via un moteur de recherche.

> **Apprenez à repérer un faux lien** grâce au module d'apprentissage en ligne « Surfer sans soucis » https://surfersanssoucis.safeonweb.be/fr/modules/1

> **Ne complétez jamais vos données personnelles.**

> **Transférez vos messages suspects** à suspect@safeonweb.be

> **Installez l'extension de navigateur Safeonweb.** L'extension Safeonweb est un outil permettant d'évaluer la fiabilité d'un site web. L'extension de navigateur Safeonweb vous indique, pour chaque site web que vous visitez, si le propriétaire a été validé (vert) ou non (orange).

Pour plus d'informations :

- www.safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux
- https://surfersanssoucis.safeonweb.be/fr/modules/1

2

JE PROTÈGE MES COMPTES AVEC L'AUTHENTIFICATION À DEUX FACTEURS (2FA)

IL EST INDISPENSABLE DE FAIRE PREUVE DE PRUDENCE EN CHOISISSANT VOS MOTS DE PASSE. VOUS AVEZ TOUJOURS BESOIN DE MOTS DE PASSE POUR SÉCURISER VOS APPAREILS, VOS DONNÉES, VOS RÉSEAUX (LE WI-FI, P. EX.) ET VOS COMPTES (VOS EMAILS OU LES MÉDIAS SOCIAUX, P. EX.). CEPENDANT, MÊME LE MOT DE PASSE LE PLUS FORT NE GARANTIT PAS UNE SÉCURITÉ TOTALE.

L'authentification à deux facteurs renforce la sécurité lors de l'accès à vos comptes et appareils. De cette façon, même si un cybercriminel parvient à obtenir votre mot de passe, il ne pourra pas accéder à vos comptes sans franchir les autres niveaux de sécurité.

> **Activez l'authentification à deux facteurs (2FA) chaque fois que cela est possible.** La plupart des services proposés par les grandes plateformes digitales (comme les réseaux sociaux) ainsi que de nombreux équipements offrent cette possibilité (p. ex. par le biais de l'empreinte digitale et/ou reconnaissance faciale).

> **Utilisez plusieurs mots de passe.** La pratique la plus sûre est d'avoir un mot de passe différent pour chaque service sensible (votre banque, votre email, votre accès aux réseaux sociaux…). Ainsi si un de vos mots de passe était compromis, un seul service serait affecté.

> **Long et original.** Plus votre mot de passe est long, plus il est sûr. Évitez de choisir un mot unique figurant dans le dictionnaire. Préférez des combinaisons de plusieurs mots sans lien apparent mais faciles à retenir.

> Vous pouvez opter pour **un gestionnaire de mots de passe.** C'est un programme qui gère l'ensemble de vos mots de passe, lui-même bien protégé.

> **Sans traces.** Ne laissez pas votre mot de passe sur un post-it à côté de votre ordinateur, dans un email ou dans un fichier informatique.

> **Ne partagez pas vos mots de passe et comptes avec des tierces personnes.** En partageant vos comptes, vous risquez de diluer la responsabilité des comptes en question et d'ainsi réduire la traçabilité des actions prises au nom de l'utilisateur.

Pour plus d'informations :

- www.safeonweb.be/fr/utilisez-des-mots-de-passe-surs
- https://safeonweb.be/fr/utilisez-lauthentification-deux-facteurs
- https://atwork.safeonweb.be/fr/MFA

3

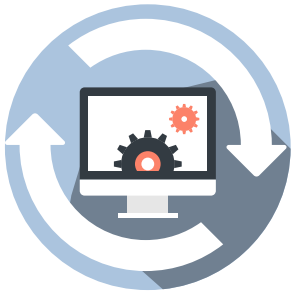
MES APPAREILS ET MES PROGRAMMES SONT À JOUR ET OFFICIELS

NE LAISSEZ PAS AUX CYBERCRIMINELS OU AUTRES INTRUS L'OCCASION D'ACCÉDER À VOTRE APPAREIL OU À VOS DONNÉES EN RÉALISANT RÉGULIÈREMENT DES MISES À JOUR DE SÉCURITÉ ET CE, TANT POUR VOS SYSTÈMES D'EXPLOITATION QUE POUR VOS PROGRAMMES ET VOS APPLICATIONS. EN EFFET, TOUS LES PROGRAMMES CONTIENNENT DES VULNÉRABILITÉS QUI PERMETTENT AUX CYBERCRIMINELS DE VOUS PORTER ATTEINTE OU DE PRENDRE LE CONTRÔLE DE VOTRE APPAREIL. CES VULNÉRABILITÉS SONT DÉCOUVERTES ET RÉSOLUES QUAND VOUS EFFECTUEZ UNE MISE À JOUR.

> **Activez la mise à jour automatique des appareils et logiciels.** Cela permet de garantir que dès qu'une vulnérabilité est détectée votre appareil est mieux protégé.

> **N'utilisez que les sites officiels.** Si vous devez télécharger un logiciel ou sa mise à jour, faites-le seulement depuis le site officiel de son fabricant.

> **Installez uniquement des applications et programmes sécurisés.** Installez des applications qui proviennent d'un magasin d'applications standard (Google Play, App Store) et des programmes d'un vendeur officiel. Limitez l'accès de vos applications au strict nécessaire. Par exemple, une application servant de calculatrice ne doit en rien accéder à votre localisation ou à vos contacts. Contrôlez régulièrement les données qu'utilisent vos applications afin de détecter tout trafic illégitime.



> **Ne contournez pas le système de sécurité par défaut de votre appareil** (par exemple en jailbreakant[2] ou par routage[3]). Si de telles manipulations peuvent vous donner l'impression d'avoir davantage le contrôle de votre appareil et de toujours avoir accès à des fonctions de sécurisation, elles augmentent sérieusement les risques.

> **Éteignez votre appareil tous les jours.** En effet, les mises à jour sont en général réalisées automatiquement au démarrage de l'appareil.

Pour plus d'information sur les mises à jour :

- www.safeonweb.be/fr/procedez-regulierement-des-mises-jour
- https://atwork.safeonweb.be/fr/tools-resources/comment-gerer-les-mises-jour

2: Jailbreaker : permettre à un iPhone, un iPod touch, un iPad ou une Apple TV de charger des applications logiciel qui ne sont pas reconnues par la société Apple.

3: Le routage d'un smartphone ou d'une tablette consiste à réaliser une mise à jour du logiciel en vue d'accéder au compte administrateur de l'appareil qui a accès à toutes les fonctionnalités et paramètres.

4

MES APPAREILS SONT CORRECTEMENT SÉCURISÉS

SI UN DE VOS APPAREILS ATTERRIT DANS DE MAUVAISES MAINS, VOUS POUVEZ AVOIR DE GROS PROBLÈMES. VEILLEZ DÈS LORS À BIEN SÉCURISER VOTRE SMARTPHONE, VOTRE TABLETTE, VOTRE ORDINATEUR PORTABLE, ETC.

> **Un bon verrouillage.** Activez le verrouillage automatique de votre smartphone lorsqu'il est inactif (maximum une minute). Préférez un code à un schéma. Lorsque ce service est offert, programmez un blocage temporel de votre smartphone après plusieurs essais erronés et un effacement des données lorsque de trop nombreuses tentatives d'accès ont été enregistrées. Assurez-vous bien entendu de la disponibilité de back-up de qualité.

> **Cryptez vos appareils.** Si vous en avez la possibilité, cryptez vos appareils, de même que vos clés USB et vos disques durs externes. Si vous utilisez une carte SD, cryptez-là également.

> **Limitez l'accès.** Veillez à uniquement activer l'accès au Wi-Fi, au Bluetooth, la *Near Field Communication*[4] ou NFC, vos données, la géolocalisation, etc. lorsque vous en avez besoin. N'activez pas les fonctions d'auto-activation (p. ex. pour le Wi-Fi). Vérifiez régulièrement les droits d'accès des applications.

> **Gardez le contrôle de votre appareil.** Ne le laissez pas sans surveillance.

4: La « Near Field Communication » ou « NFC » consiste en une communication sans fil permettant d'échanger de petites quantités d'informations dans un rayon de dix centimètres, par exemple pour se connecter avec un système de paiement ou un smartphone.

5

MES DONNÉES SONT CORRECTEMENT SÉCURISÉES

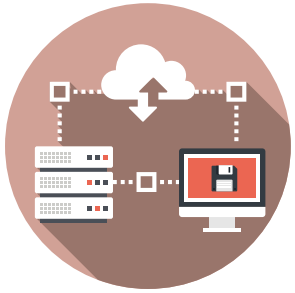
VOUS DEVEZ ÉGALEMENT MANIPULER LES DONNÉES QUE VOUS CONSERVEZ SUR VOTRE ORDINATEUR EN FAISANT PREUVE DE PRUDENCE. EN CAS DE PERTE DE VOS DONNÉES, CE SERA NON SEULEMENT ENNUYEUX À TITRE PERSONNEL, MAIS VOUS POUVEZ AUSSI AVOIR DES ENNUIS SI DES PERSONNES MAL INTENTIONNÉES VOLENT ET EXPLOITENT LES DONNÉES DES MEMBRES DE VOTRE PARTI, PAR EXEMPLE.

> **Réalisez des back-ups.** Un back-up est une copie de sauvegarde des données importantes pour vous. Le back-up vous permettra de réinstaller les données sur votre appareil si vous êtes touché par un virus. Par ailleurs, en cas de vol, de perte ou de problème technique, il est rassurant de disposer d'un back-up. Vous pouvez alors (faire) réinstaller tout votre système et réintroduire vos données dans votre ordinateur. **Ceci s'applique bien entendu aussi à vos appareils mobiles.**

> **Sauvegardez.** Mettez en place un système pour sauvegarder régulièrement vos données de manière automatique. Des solutions décentralisées (cloud) peuvent présenter un avantage certain pour autant que votre fournisseur soit de confiance.

> **Utilisez un scanner antivirus.** Un scanner antivirus rendra votre ordinateur imperméable aux virus. Il s'agit du plus important logiciel de protection de votre ordinateur et de vos données.

> **Éteignez.** Éteignez vos appareils lorsque vous ne les utilisez pas (vacances, week-end, jours fériés…) et désactivez les fonctions que vous n'utilisez pas (wifi, Bluetooth, NFC, géolocalisation).



> **Soyez vigilant si vous utilisez des clés USB.** Une clé USB est pratique pour transporter des données, mais elle se perd également facilement. Faites surtout attention aux clés USB que vous recevez d'autres personnes ou que vous pourriez trouver par terre, par exemple. Elles peuvent en effet contenir des virus. Nous vous conseillons dès lors de faire réaliser (par un professionnel) un scan des virus potentiels avant d'utiliser la clé USB en question. Sauvegardez régulièrement le contenu de vos clés USB et supprimez régulièrement les documents non nécessaires sur celles-ci.

Pour plus d'informations sur les back ups :
- www.safeonweb.be/fr/pensez-aux-sauvegardes
- https://atwork.safeonweb.be/fr/tools-resources/comment-gerer-les-copies-de-sauvegarde

Pour plus d'informations sur la recherche de virus :
- www.safeonweb.be/fr/scannez-votre-ordinateur
- https://atwork.safeonweb.be/fr/tools-resources/logiciel-antivirus

Pour plus d'informations sur les clés USB :
- https://cyfun.be (Cyberfondamentaux - niveau 'Small', sous « 3. Installer un antivirus »).

6

J'UTILISE UN RÉSEAU (WI-FI) SÉCURISÉ

UN RÉSEAU BIEN SÉCURISÉ EST UNE CONDITION *SINE QUA NON* À UNE PRÉVENTION DE QUALITÉ. SI UN CYBERCRIMINEL OU AUTRE INTRUS PARVIENT À ACCÉDER À VOTRE RÉSEAU, IL AURA EN MÊME TEMPS ACCÈS À TOUS LES APPAREILS QUI Y SONT CONNECTÉS. LE SYSTÈME SANS FIL WI-FI A CONSIDÉRABLEMENT SIMPLIFIÉ LES CONNEXIONS DES APPAREILS ÉLECTRONIQUES AUX DIFFÉRENTS RÉSEAUX (INTERNET, RÉSEAU PRIVÉ, RÉSEAU D'ENTREPRISE…). COMMENT SÉCURISER AU MAXIMUM VOTRE WI-FI ?

> **Sécurisez votre routeur personnel.** Lorsque vous recevez un nouveau routeur Wi-Fi (ou une nouvelle box Wi-Fi), ne gardez pas les paramètres par défaut. Modifiez le nom du réseau (SSID) et n'y intégrez pas d'éléments évidents. Modifiez également les mots de passe (en ce compris le mot de passe qui sécurise votre routeur).

> **Utilisez une sécurisation WPA2.** Votre routeur aura vraisemblablement la possibilité d'être crypté à l'aide de WPA2, WPA ou WEP. Optez pour WPA2 et installez-le immédiatement si ce n'est pas encore fait.

> **Activez le firewall (pare-feu).**

> **Une clé d'accès solide.** Pour le choix de la clé d'accès de votre réseau wifi, référez-vous aux conseils donnés plus haut pour les mots de passe. Ne divulguez cette clé qu'à des personnes de confiance. Changez-la régulièrement.

> **Évitez d'utiliser les réseaux Wi-Fi publics.** Nous vous conseillons de ne pas réaliser de transactions bancaires ou autres opérations importantes via un réseau Wi-Fi public. Évitez de créer des comptes avec un mot de passe via un réseau Wi-Fi public.

> **Installez un *Virtual Private Network* (VPN).** Il s'agit d'un tunnel personnel et sécurisé qui fonctionne à l'aide du réseau Wi-Fi. Vous pouvez installer en ligne les services VPN gratuitement ou moyennant paiement. Plusieurs scanners antivirus proposent également un VPN.

Pour plus d'informations sur le Wi-Fi :
- www.safeonweb.be/fr/actualite/est-ce-quil-y-aussi-le-wifi
- https://atwork.safeonweb.be/fr/tools-resources/protegez-vos-appareils-mobiles
- https://atwork.safeonweb.be/fr/tools-resources/face-aux-cybermenaces-restons-vigilants

Pour plus d'informations sur la sécurisation WPA2 :
- https://cyfun.be (Cyberfondamentaux - niveau 'Small', sous « 4. Sécuriser votre réseau »).

7

J'UTILISE LES MÉDIAS SOCIAUX AVEC PRÉCAUTION

LA VIE PRIVÉE D'UN DÉCIDEUR POLITIQUE EST PLUS VULNÉRABLE QUE CELLE DES AUTRES CITOYENS. EN ÉTANT ACTIF SUR LES MÉDIAS SOCIAUX, VOUS ENTREZ NON SEULEMENT EN CONTACT AVEC LE MONDE EXTÉRIEUR MAIS CE DERNIER EST ÉGALEMENT EN MESURE DE DRESSER VOTRE PROFIL SUR LA BASE DES INFORMATIONS QUE VOUS PARTAGEZ, QUI VONT DES PHOTOS PERSONNELLES JUSQU'À VOTRE COMPORTEMENT PERSONNEL EN PASSANT PAR VOS CHOIX DE FILMS, TENDANCES ALIMENTAIRES, INFORMATIONS SUR VOTRE FAMILLE, VOS RÉSEAUX, LE LIEU OÙ VOUS VOUS TROUVEZ. CES INFORMATIONS SONT PAR CONSÉQUENT SUSCEPTIBLES D'ÊTRE EXPLOITÉES À DES FINS ABUSIVES. VOICI QUELQUES CONSEILS POUR PROTÉGER VOTRE VIE PRIVÉE.

> **Ayez des appareils séparés.** Si c'est possible, séparez les appareils que vous utilisez pour vos activités politiques ou professionnelles de ceux que vous utilisez pour votre vie privée.

> **Ayez plusieurs adresses électroniques.** Par exemple, vous pourriez avoir une adresse email destinée à des services sensibles (votre banque, l'administration…) et une autre destinée à des services qui le sont moins (vidéo à la demande, forums, jeux…). Il est sage d'avoir une adresse email dédiée à vos activités publiques.

> **Pensez à la sécurité de vos réseaux sociaux.** Vérifiez les paramètres des réseaux sociaux que vous utilisez avant la campagne (notamment certaines publications automatiques). Faites des choix pour la visibilité de vos publications qui soient conformes à ce que vous voulez partager et ceci avant chaque publication. Activez une authentification forte à deux facteurs (2FA) pour l'accès à vos comptes.

> **Soyez vigilant concernant les trolls informatiques.** Leur but principal est de provoquer, d'influencer, de diriger et de faire escalader les discussions en ligne. À cette fin, des comptes de citoyens apparemment ordinaires sont créés à l'avance sur les médias sociaux. Au moment opportun, ils sont ensuite mis en action pour prendre position sur un sujet particulier. Pour arrêter le troll, il est important de ne pas réagir comme il le veut. Ne participez pas à la discussion et ne vous fâchez pas.

> **Dans la mesure du possible, évitez d'établir des liens entre vos comptes.** Certaines plateformes offrent la possibilité de vous connecter avec votre compte existant sur d'autres médias sociaux. Ces comptes liés sont vulnérables puisque toutes vos données personnelles sont concentrées sur une plateforme déterminée.

> **Les paramètres de confidentialité de vos comptes doivent être vérifiés régulièrement.** Les paramètres peuvent parfois être modifiés unilatéralement par le fournisseur, ce qui peut par exemple signifier que les droits de propriété de vos informations personnelles risquent d'être transférés au gestionnaire de la plate-forme.

> **Soyez conscients que certaines plateformes de médias sociaux peuvent avoir des liens avec des pays spécifiques.** TikTok par exemple est un produit chinois. Les données conservées sur cette plateforme pourraient faire l'objet d'abus de la part du gouvernement chinois en raison de la législation chinoise. Réfléchissez à la nécessité d'être présent sur toutes les plateformes de médias sociaux.

8

JE RECONNAIS LA DÉSINFORMATION

LA DÉSINFORMATION EST UN DANGER POUR NOTRE DÉMOCRATIE CAR ELLE PEUT EMPÊCHER LES ÉLECTEURS DE FAIRE UN CHOIX POLITIQUE ÉCLAIRÉ. C'EST LE CAS, NOTAMMENT, POUR LA DIFFUSION DE FAUSSES INFORMATIONS OU D'INFORMATIONS MANIPULÉES, MAIS AUSSI L'EXACERBATION ARTIFICIELLE DES CLIVAGES, LA STIMULATION DE LA DÉFIANCE ENVERS LES ÉLECTIONS OU DE L'EXCLUSION DU DÉBAT DE VOIX LÉGITIMES. EN TANT QUE RESPONSABLE POLITIQUE, VOUS POURRIEZ EN ÊTRE LA CIBLE, MAIS AUSSI ALIMENTER VOUS-MÊME LA DÉSINFORMATION SANS LE SAVOIR.

> **Informez-vous sur la désinformation.** La désinformation n'est pas nécessairement la même chose que la propagande ou les *fake news*. De plus, elle peut se présenter sous de nombreuses formes. Pensez aux faux sites d'information ou aux fausses images, mais aussi aux faux messages audios ou aux vidéos conspirationnistes sur TikTok. Le site web du Centre de crise National explique en détail ce qu'est exactement la désinformation et les différentes techniques d'influence qui sont généralement utilisées : https://centredecrise.be/fr/desinformation

> **Faites preuve de bon sens.** Vous pouvez reconnaître la désinformation en vous posant quelques questions. Qui est l'auteur, le créateur ou le diffuseur ? L'information est-elle véridique ? Dans quel but le message a-t-il été créé ou diffusé ? Autres conseils : lisez au-delà du titre, consultez plusieurs sources, vérifiez la date de rédaction ou de diffusion d'un message et faites preuve d'esprit critique à l'égard de la forme.

> **Méfiez-vous des *deepfakes*.** L'essor rapide de l'intelligence artificielle générative facilite énormément la manipulation d'images ou la création de photos, de vidéos et de sons totalement factices. La lecture d'une vidéo au ralenti peut être le premier moyen de repérer ces *deepfakes*.

> **Vérifiez vous-même les faits.** Pour vérifier l'exactitude des images, vous pouvez également procéder comme suit. En utilisant un moteur de recherche, tel que Google Reverse Image Search, vous pouvez découvrir le véritable contexte. Regardez attentivement et notez les différents éléments environnementaux qui vous en disent plus sur le lieu. Trouver des sources indépendantes pour vérifier les histoires ou les images. Des conseils supplémentaires sont disponibles sur https://belux.edmo.eu/fr/outils/boite-a-outils/

> **Ne partagez pas de contenu douteux.** Vous avez encore des doutes sur l'exactitude ou la fiabilité d'une information ? Dans ce cas, ne diffusez pas cette information ou ce message. Non seulement c'est ce que les propagateurs espèrent mais, en tant qu'homme ou femme politique, vous avez une très grande portée et vous donnez à la désinformation une autorité supplémentaire en la partageant par le biais de vos canaux.

> **Signalez la désinformation.** Êtes-vous sûr d'avoir affaire à de la désinformation ? Dans ce cas, vous pouvez la signaler à l'EDMO BELUX à l'adresse https://belux.edmo.eu/fr/rapports-de-desinformation/

JE SUIS VICTIME: QUE FAIRE ?

1. JE SUIS VICTIME D'UNE CYBERATTAQUE QUI EST ENCORE EN COURS

> Vous pouvez limiter les conséquences d'une cyberattaque si vous réagissez promptement.

> Vous pouvez signaler l'incident auprès du CCB via le formulaire disponible sur le site du CCB ou par email : incident@ccb.belgium.be. Vous trouverez davantage de modes de signalement d'un incident sur le site suivant : https://ccb.belgium.be/fr/cert/signaler-un-incident

En cas d'urgence, vous pouvez également joindre le CCB par téléphone au : **+32 (0)2 501 05 60.**

> N'éteignez PAS votre ordinateur, sinon vous effacerez les traces laissées par les auteurs de la cyberattaque.

> Il vaut également mieux changer les mots de passe depuis un ordinateur sécurisé dans la mesure où l'auteur les a peut-être en sa possession.

> Déposez plainte à la police locale.

Pour plus d'informations :
- https://ccb.belgium.be/fr/cert/premiers-secours-en-cas-de-cyberattaque

2. MON COMPTE A ÉTÉ PIRATÉ

> Changez immédiatement tous vos mots de passe. Pour ce faire, opérez depuis un appareil sécurisé et donc différent de celui sur lequel vos données ont été volées.

> Ajoutez immédiatement l'authentification à deux facteurs (2FA).

> Lancez votre antivirus pour qu'il effectue un scan de votre ordinateur.

> Si vos coordonnées bancaires ou les coordonnées de votre carte de crédit ont été volées, avertissez votre banque et surveillez vos comptes. Contactez « Card Stop » au **078 170 170.**

> Si des données relatives à votre vie politique ont été volées, avertissez au plus vite votre parti et faites une déclaration auprès de l'Autorité de protection des données.

> Informez vos contacts. Ils risquent en effet de recevoir des messages envoyés frauduleusement en votre nom.

Pour plus d'informations :
- www.safeonweb.be/fr/mon-compte-est-pirate

3. J'AI PERDU MON APPAREIL OU IL A ÉTÉ VOLÉ

> Changez immédiatement tous les mots de passe des comptes qui se trouvaient sur votre appareil (p. ex. email, Facebook, WhatsApp, etc.).

> Si vos coordonnées bancaires ou vos données de paiement se trouvaient sur l'appareil volé, avertissez votre banque via votre personne de contact et surveillez bien vos comptes. Faites éventuellement bloquer vos cartes de banque et vos comptes via Card Stop (www.cardstop.be ou **078 170 170**).

> Si des données relatives à votre vie politique ont été volées, avertissez au plus vite votre parti.

> Si votre appareil a été volé, faites une déclaration à la police.

Pour plus d'informations :
- www.safeonweb.be/fr/jai-perdu-mon-smartphonema-tablette

4. MON APPAREIL A ÉTÉ CONTAMINÉ PAR UN VIRUS

> Il est impératif d'éliminer un virus au plus vite.

> Si vous n'avez pas encore de logiciel antivirus et si votre ordinateur n'est pas bloqué, il est temps d'installer un antivirus, d'effectuer un scan et d'éliminer le virus. Pendant ce temps, n'entrez aucune donnée personnelle ni donnée de paiement, car certains virus peuvent transmettre de telles informations

Pour plus d'informations :
- www.safeonweb.be/fr/jai-un-virus

CONTACT

1. CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE (CCB)

> Le CCB est votre interlocuteur pour signaler tout cyberincident et poser vos questions, tant pendant qu'après les élections.

Pour joindre ce service, envoyez un email à incident@ccb.belgium.be ou signalez un incident sur le site https://ccb.belgium.be/fr/cert

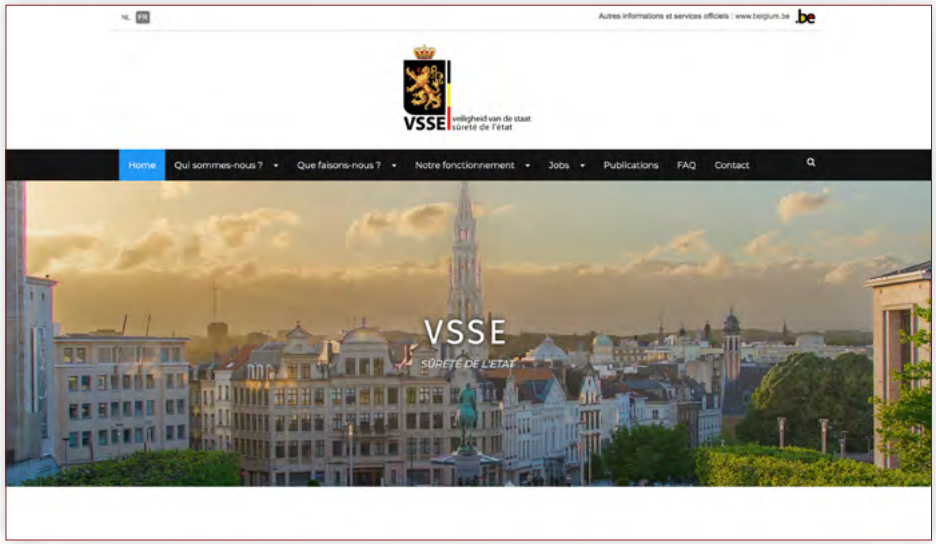
En cas d'urgence, le CCB est également accessible par téléphone au **+32 (0)2 501 05 60.**

2. SÛRETÉ DE L'ÉTAT (VSSE)

> Vous trouverez toutes les informations sur les missions et le fonctionnement de la VSSE sur son site : www.vsse.be

3. SERVICE GÉNÉRAL DU RENSEIGNEMENT ET DE LA SÉCURITÉ (SGRS)

> Pour en apprendre davantage sur le rôle et les responsabilités du SGRS, prenez contact avec ce service à l'adresse suivante : csoc@cyber.mil.be



PLUS D'INFORMATIONS

CYBERATTAQUES :

> **Centre pour la Cybersécurité Belgique :** https://ccb.belgium.be/fr/cert

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

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

> **Cybersecurity Basics pour les starters :** www.cybersecuritycoalition.be/fr/cyber-security-basics-pour-les-starters/

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

> **Autorité de protection des données :** www.autoriteprotectiondonnees.be/

> **Point de contact fraude :** https://pointdecontact.belgique.be/

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

DÉSINFORMATION :

> **Désinformation (Centre de crise National) :** https://centredecrise.be/fr/desinformation

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

INFORMATIONS SUR L'INGÉRENCE ÉTRANGÈRE POTENTIELLE :

> www.vsse.be

Chacun est libre de suivre les recommandations de ce guide en fonction de sa propre analyse des risques. Elles ont été établies en fonction de la menace telle qu'observée au jour de leur publication. Nous ne pouvons pas certifier que ces recommandations garantiront la sécurité d'un système informatique ciblé.

D/2024/7951/FR/1305

Surfer en toute sécurité pendant la campagne électorale

Recommandations pour une campagne sous le signe de la cybersécurité

Éditeur responsable : Francisca BOSTYN
Boulevard du Roi Albert II, 6 - 1000 Bruxelles

CENTRE FOR CYBERSECURITY BELGIUM

ADIV-SGRS

VSSE veiligheid van de staat sûreté de l'état

.be