SURFER EN TOUTE SÉCURITÉ PENDANT LA CAMPAGNE ÉLECTORALE

Recommandations pour une campagne cybersécurisée

Ce guide 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).

Février 2019

CENTRE FOR CYBER SECURITY 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 cybersécurisée

Bruxelles, février 2019

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. Citons par exemple les e-mails du Parti démocrate qui ont été dévoilés lors de la course à l'élection présidentielle aux États-Unis en 2016, ou encore ceux de l'équipe de campagne du président français actuel, Emmanuel Macron, pendant la campagne électorale de 2017.

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.

Cordialement,

Miguel DE BRUYCKER,
Directeur du Centre pour
la Cybersécurité Belgique

Jaak RAES,
Administrateur général
de la Sûreté de l'État

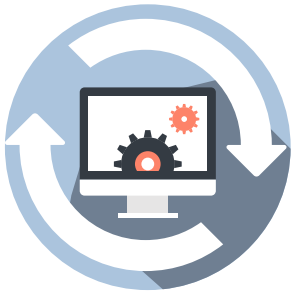
Claude VAN DE VOORDE,
Lieutenant général aviateur,
chef du Service Général
du Renseignement et
de la Sécurité

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

TABLE DES MATIÈRES

MES APPAREILS ET MES PROGRAMMES SONT À JOUR ET OFFICIELS

NE LAISSEZ PAS AUX CYBERCRIMINELS OU D'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 DE 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 uniquement depuis le site officiel de son fabricant.

› **Ne contournez pas le système de sécurité par défaut de votre appareil** (par exemple en jailbreakant[1] ou par routage[2]). 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.

1 : *Jaibreaker :* permettre à un iPhone, un iPod touch, un iPad ou une Apple TV de charger des applications logicielles qui ne sont pas reconnues par la société Apple.

2 : 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.

2

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 code PIN pour ma carte SIM.** Lorsque vous recevez une nouvelle carte SIM, choisissez un code pin adéquat et sans lien direct avec vous. Veillez donc à éviter des codes PIN comme « 0000 », « 1111 » ou « 1234 », et à ne pas utiliser votre date de naissance ou le code PIN de votre e-ID ou de votre carte de banque.

› **Un bon verrouillage.** Activez le verrouillage automatique de votre smartphone lorsqu'il est inactif (maximum une minute). Préférez un mot de passe solide à un schéma. Ce mot de passe doit être changé régulièrement (de préférence tous les 3 mois). 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*[3] 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.

› **Applications et programmes sécurisés.** Installez uniquement 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.

› **Garder le contrôle de votre appareil.** Ne le laissez pas sans surveillance. Si vous devez vous en séparer, enlevez la batterie et la carte SIM et conservez-les.

› **Un appareil à jour.** Mettez régulièrement votre smartphone à jour. Nous vous conseillons de régulièrement redémarrer votre système ou votre appareil.

3 : 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.

3

MES DONNÉES SONT CORRECTEMENT SÉCURISÉES

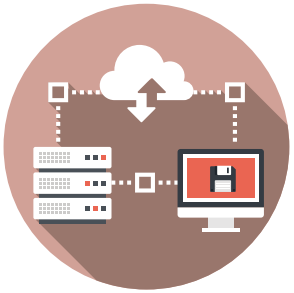
VOUS DEVEZ ÉGALEMENT MANIPULER LES DONNÉES QUE VOUS CONSERVEZ SUR VOS APPAREILS AVEC BEAUCOUP DE PRUDENCE. EN CAS DE PERTE DE VOS DONNÉES, CE SERA NON SEULEMENT ENNUYEUX À TITRE PERSONNEL, MAIS VOUS POUVEZ AUSSI AVOIR DES ENNUIS SI DES PERSONNES MAL INTENTIONNÉES VOLENT ET EXPLOITENT LES DONNÉES DES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

› **Réalisez des back-up.** 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.

› **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 (Wi-Fi, *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.

4

JE PROTÈGE MES COMPTES
À L'AIDE D'UN MOT DE PASSE SÛR

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 E-MAILS OU LES MÉDIAS SOCIAUX, P. EX.).

› **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 e-mail, votre accès aux réseaux sociaux…). De la sorte, si un de vos mots de passe était compromis, un seul service serait affecté.

› **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.

› **Optez pour une double protection ou une authentification en deux étapes** *(« Two Factor Authentication », 2FA).* En outre, pour limiter les risques, nous vous conseillons d'assortir un mot de passe sûr à une authentification en deux étapes, si possible.

› **Veillez à ce que votre mot de passe ne soit pas en lien avec vous.** Évitez d'utiliser votre prénom, votre nom, votre date de naissance ou celle de proches. N'utilisez pas les questions secrètes : les réponses sont généralement trop faciles à trouver.

› **Sans traces.** Ne laissez pas votre mot de passe sur un post-it à côté de votre ordinateur, dans un e-mail, dans un fichier informatique. N'enregistrez pas les mots de passe dans votre navigateur.

› **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 effectuées au nom de l'utilisateur.

› **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 plutôt des combinaisons de plusieurs mots sans lien apparent mais faciles à retenir.

› **Attention à la date de péremption.** Changez vos mots de passe régulièrement (tous les 3 mois est une fréquence raisonnable). Si vous n'utilisez plus un service, supprimez votre compte pour éviter une compromission ultérieure.

5

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 UN 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.

› **Une clé d'accès solide.** Pour le choix de la clé d'accès de votre réseau Wi-Fi, 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.

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

› **Désactivez le WPS *(Wi-Fi Protected Setup).***

› **Utilisez le Wi-Fi uniquement lorsque c'est indispensable.** Éteignez votre connexion Wi-Fi quand vous ne l'utilisez pas.

› **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.

› **Effacez régulièrement la liste des réseaux Wi-Fi enregistrés.** Votre appareil les enregistre en effet tous et envoie des signaux en permanence afin d'établir plus rapidement une connexion à un réseau connu.

JE RECONNAIS
LES MESSAGES SUSPECTS

LE TERME « *PHISHING* » RECOUVRE LES ACTES D'ESCROQUERIE EN LIGNE PAR L'INTERMÉDIAIRE D'E-MAILS, DE SITES WEB OU DE MESSAGES FRAUDULEUX. DE TELS E-MAILS 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 mail semble-t-elle légitime ? Est-ce que cette personne ou organisation vous envoie fréquemment ce type de document ? Dans le doute, appelez la personne ou l'organisation qui vous a envoyé le mail.

› **La nature de la demande.** Est-ce que des informations personnelles ou sensibles vous sont demandées ? Est-ce qu'un sentiment d'urgence est créé ? En cas de doute, ne communiquez jamais des données personnelles ou sensibles.

› **La formulation du mail.** Est-ce que le mail comporte des fautes d'orthographe ou de grammaire ? Est-ce qu'on essaie d'éveiller votre curiosité ? Vous fait-on des promesses trop belles pour être vraies ? Vous demande-t-on de l'argent ? En cas de doute, abstenez-vous de cliquer.

› **Ne cliquez pas sur les liens ou les images contenus 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.

› **Ne transférez pas le message** à vos contacts et ne complétez jamais vos données personnelles.

› Transférez vos messages suspects à suspect@safeonweb.be.

J'UTILISE LES MÉDIAS SOCIAUX AVEC PRÉCAUTION

LA VIE PRIVÉE D'UNE PERSONNALITÉ 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 autant que possible les appareils que vous utilisez pour vos activités politiques ou professionnelles de ceux que vous utilisez pour votre vie privée.

› **Ayez plusieurs adresses mails.** Par exemple, vous pourriez avoir une adresse mail destinée à des services sensibles (votre banque, l'administration…) et une autre destinée à des services qui le sont moins (vidéo à la demande, forum, jeux…). Il est sage d'avoir une adresse mail 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 plate-forme 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.

8

JE SUIS VICTIME D'UNE CYBERATTAQUE : 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 rapidement.

› Vous pouvez signaler l'incident auprès de CERT.be via le formulaire disponible sur le site www.cert.be ou par e-mail : cert@cert.be. Vous trouverez davantage de modes de signalement d'un incident sur le site suivant : https://cert.be/fr/signaler-un-incident. En cas d'urgence, vous pouvez également joindre CERT.be 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.

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.

› Lancez votre antivirus pour qu'il effectue un scan 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 070 344 344.

› 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.

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. e-mail, 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 Cardstop (www.cardstop.be ou 070/ 344 344).

› 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.

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. Entre-temps, n'entrez aucune donnée personnelle ni donnée de paiement, car certains virus peuvent transmettre de telles informations.

CONTACT

1. CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE (CCB)

› CERT.be, le service opérationnel du CCB, est votre interlocuteur pour signaler tout cyberincident et poser vos questions, tant avant, pendant qu'après les élections.

Pour joindre ce service, envoyez un e-mail à cert@cert.be ou signalez un incident sur le site www.cert.be.

En cas d'urgence, CERT.be 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 savoir davantage sur le rôle et les responsabilités du SGRS en matière de cyber, prenez contact avec ce service à l'adresse suivante : csoc@cyber.mil.be.

PLUS D'INFORMATIONS

CYBERATTAQUES :

› CERT.be :
www.cert.be

› Cyberguide :
https://cyberguide.ccb.belgium.be/fr

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

› Cybersecurity kit :
https://www.ccb.belgium.be/fr/actualité/cyber-security-kit-assurez-la-cybersécurité-de-votre-entreprise-et-de-votre-personnel

› Cybersecurity scan :
https://www.cybersecurityscan.be/fr-be/accueil/

› Autorité de protection des données :
https://www.autoriteprotectiondonnees.be/

› Point de contact fraude :
https://pointdecontact.belgique.be/meldpunt/fr/bienvenue

› Safeonweb :
www.safeonweb.be

INFORMATION SUR L'INGÉRENCE ÉTRANGÈRE POTENTIELLE

› VSSE :
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/2019/7951/FR/1186

Surfer en toute sécurité pendant la campagne électorale

Recommandations pour une campagne cybersécurisée

Éditeur responsable : Jaak Raes
Boulevard du Roi Albert II, 6 – 1000 Bruxelles

CENTRE FOR CYBER SECURITY BELGIUM

ADIV-SGRS

VSSE veiligheid van de staat sûreté de l'état

.be