Bonjour et bienvenue à tous!

Travailler à domicile peut être un défi!

CYBER SECURITY COALITION.be

Ça vous dit quelque chose?

Interview de la BBC à domicile avec la collaboration des enfants...

2

Safe homeworking

Il était une fois, un paisible royaume

Qui faisait le bonheur de tous les télétravailleurs

3


Téléchargez
des apps vérifiées
Protégez
votre réseau
domestique
Configurez
un anti-virus
Sécurisez
le wifi
Protégez
votre routeur
Scindez les outils
privés et pros
4

(Sources: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)

Nous utilisons Internet chaque jour sur notre smartphone, tablette, ordinateur, mais aussi avec des appareils «°intelligents°» tels que caméras, télévisions et solutions de domotique. Cependant, cette dépendance comporte des risques. Comment protéger mon réseau domestique contre les utilisateurs indésirables ?

Un réseau bien sécurisé signifie:

- Installez un **Virtual Private Network** (VPN). Il s'agit de votre **tunnel personnel sécurisé par le réseau Wifi.** Toutes les communications passent par un tunnel virtuel crypté qui empêchent les cybercriminels d'intercepter des communications lisibles et ainsi de récupérer les informations. Beaucoup d'employeurs fournissent une connexion VPN fiable à leurs travailleurs afin qu'ils puissent obtenir un accès sécurisé au réseau professionnel. Dans le cas contraire, vous pouvez vous-même installer des services VPN gratuits ou payants en ligne. Différents antivirus proposent p. ex. un VPN.
- Modifiez les mots de passe standard de **tous** vos appareils reliés à votre réseau domestique. Il peut s'agir notamment d'ordinateurs, smartphones, tablettes, imprimantes, mais aussi caméras et systèmes réseau qui connectent facilement tous ces appareils entre eux via votre réseau domestique. "Admin" et "mot de passe", par exemple, sont des mots de passe standard faibles, qui sont malheureusement encore souvent utilisés. Comment renforcer vos mots de passe: voir le module "Mots de passe" dans ce Cyber Security Kit.
- Sécurisez votre routeur: **Le routeur est le port entre Internet et votre réseau domestique: sécurisez-le bien.**
- **Modifiez le nom du réseau de votre WiFi domestique (SSID)** et n'y intégrez aucun élément évident comme votre adresse. Un cybercriminel peut voir depuis la voie publique quel réseau correspond à votre domicile. Parfois, le producteur de vos appareils figure également dans le nom du réseau, ce qui ouvre la porte aux hackers.
- **Modifiez vos mots de passe réseau** (y compris le mot de passe qui figure sur votre routeur).
- **Utilisez la sécurisation WPA2.** Votre routeur a probablement la possibilité de configurer un **cryptage** WPA3, WPA2, WPA ou WEP. Choisissez le WPA2 ou WPA3 (**Wi**Fi **P**rotected **A**ccess) sécurisé et configurez-le immédiatement à l'aide d'un mot de passe long si cela n'a pas encore été fait. Ainsi, vous avez la certitude que **seules les personnes de confiance peuvent se connecter** à votre réseau domestique. Car elles sont obligées de saisir un mot de passe.
  En outre, toutes les activités en ligne sont alors cryptées.
- **Mettez tous vos appareils à jour.** Votre routeur est aussi un ordinateur et bénéficie de mises à jour tout comme lui. Veillez à installer les dernières mises à jour sur votre° routeur et autres appareils réseau.

(*) **Comment modifier les paramètres de votre routeur?**

Proximus

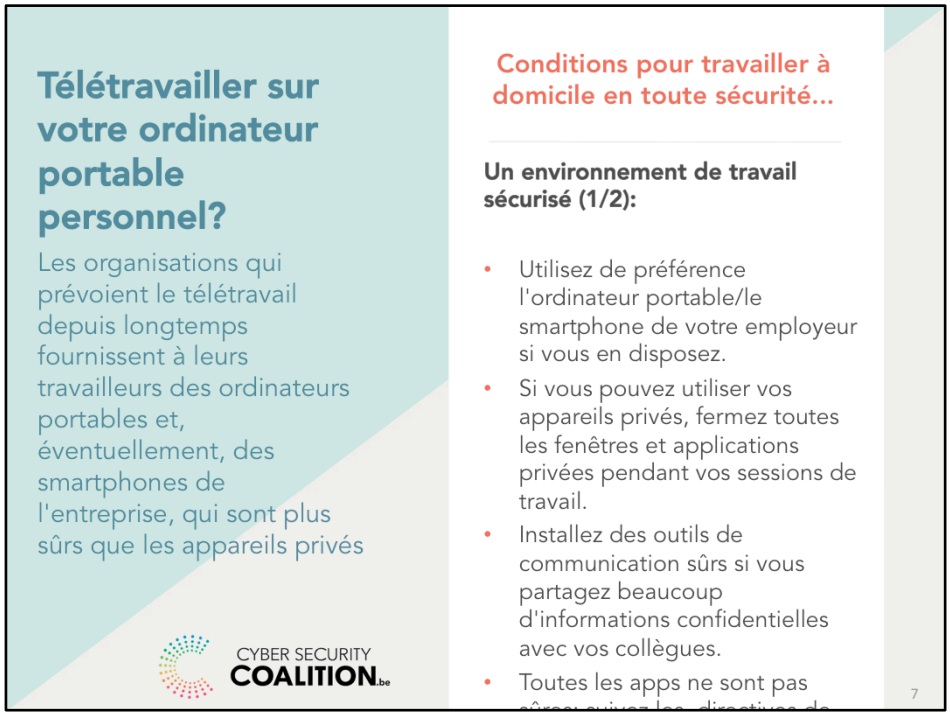
Telenet

- **Activez le pare-feu et utilisez toujours un antivirus.**

- **Désactivez WPS (Wi-Fi Protected Setup)**. WPS est une fonction qui permet aux appareils de se connecter facilement à un réseau WiFi sans devoir saisir de mot de passe. Les criminels peuvent la détourner pour établir une connexion avec votre réseau. Si vous n'êtes pas chez vous pour une longue période, éteignez votre réseau WiFi.

(Sources: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)

- **Créez un réseau invité.** Un réseau invité est un réseau WiFi distinct strictement séparé du réseau personnel. Vos invités ont bien accès à votre connexion Internet, mais pas aux fichiers et appareils partagés tels que les imprimantes et les disques durs réseau. Vous pouvez donc partager le mot de passe de votre réseau invité en toute tranquillité. De nombreux routeurs offrent cette possibilité via les paramètres. Sécurisez encore davantage votre réseau en permettant à vos appareils intelligents IoT (Internet of Things, soit les appareils connectés à Internet et à commander à distance tels que lampes, thermostat...) de se connecter uniquement au réseau invité. Ainsi, les hackers qui exploitent une fuite IoT ont moins facilement accès à l'ensemble de votre réseau.
- **Utilisez la "ligne fixe Internet" ou Ethernet.** Utilisez un câble Ethernet au lieu du WiFi pour les appareils que vous ne déplacez pas, comme ordinateurs de bureau, télévisions ou imprimantes. Un réseau sans fil, même quand il est sécurisé, peut être piraté par une personne dont il est à portée. Le WiFi émet et reçoit des signaux radio dans l'espace d'une portée assez longue, ce qui représente un risque de sécurité potentiel. Les données qui passent par un câble sont beaucoup plus difficiles à intercepter pour les hackers, car ils ont alors besoin d'un accès physique.
- **Évitez le WiFi public à l'extérieur** dans les hôtels, aéroports, gares et cafés
- Si nécessaire, installez un **booster de WiFi pour garantir une connexion Internet puissante** dans votre bureau à domicile.
- Achetez des applications uniquement dans les **app stores officiels** (App Store, Google Play).
- Veillez à ce que **votre système d'exploitation, tous vos programmes et applications soient à jour.** Un logiciel qui n'est plus supporté par le fournisseur ne bénéficie plus de mises à jour de sécurité. Les anciens systèmes d'exploitation tels que Windows XP ou Windows 7, par exemple, les anciens programmes de messagerie électronique ou tout autre logiciel qui n'est plus supporté représentent un risque de sécurité élevé. Veillez à ce que votre antivirus **installe automatiquement les mises à jour.**



(Sources: www.safeonweb.be, Vrije Universiteit Brussel, US Department of Homeland Security et BNP Paribas Fortis)

- Utilisez de préférence l'ordinateur portable/le smartphone de votre employeur. Ils sont **mieux sécurisés et contrôlés** que vos propres appareils. En outre, votre employeur peut **immédiatement intervenir** en cas de problème. Les appareils de votre employeur sont généralement équipés d'un antivirus et les mises à jour sont automatiques. En tant que travailleur, vous n'en avez pas toujours conscience. Pour vos appareils privés, c'est vous qui en assumez la responsabilité et un oubli est vite arrivé.
- Si vous pouvez utiliser vos appareils privés, suivez les instructions de votre employeur et **fermez toutes les fenêtres et applications privées pendant vos sessions de travail.**
- **Installez des outils de communication sûrs (suivez les directives de votre département IT ou demandez conseil à votre fournisseur IT) si vous partagez beaucoup d'informations confidentielles avec vos collègues.** Pour envoyer des messages, les collègues ont souvent recours à WhatsApp. Threema ou Telegram p. ex. sont des alternatives moins connues mais plus sécurisées. Pour les appels vidéo, il existe des alternatives à Skype (Zoom, Teams, Webex…). Lisez l'avis de NVISO sur Zoom: to Zoom or not to Zoom
- **Toutes les applications ne sont pas sûres°: suivez les directives de votre département IT ou demandez conseil à votre fournisseur IT.** Si votre département IT vous interdit, p. ex., de partager des informations confidentielles via WhatsApp ou d'envoyer des fichiers volumineux par WeTransfer, suivez ces directives: elles sont bien réfléchies et visent à limiter le risque de fuites d'informations, notamment. Dans la plupart des cas, des alternatives valables sont également disponibles.

(Sources: www.safeonweb.be, Vrije Universiteit Brussel et BNP Paribas Fortis)

Un environnement de travail sécurisé signifie que vous surveillez votre vie privée et votre confidentialité dans votre bureau à domicile. Concrètement, c'est possible de la sorte:

- **N'imprimez aucun contenu lié au travail chez vous** sauf accord explicite de votre département IT.
- **Verrouillez votre ordinateur quand vous quittez votre poste de travail:** À domicile comme au bureau, prenez la bonne habitude de toujours verrouiller votre ordinateur lorsque vous quittez votre poste de travail afin que personne n'ait la possibilité d'aller fouiller dans vos fichiers. De même, avec des enfants qui jouent dans les parages, des adolescents curieux ou un chat fou de votre clavier, il est prudent de verrouiller votre appareil lorsque vous vous en absentez. Pour ce faire, utilisez les touches WIN + L ou Ctrl + Shift + Power pour les utilisateurs de Mac. Activez également une sécurisation PIN sur votre smartphone.
- **Éteignez votre ordinateur tous les soirs.** Résistez à la tentation de mettre votre ordinateur en veille le soir pour pouvoir reprendre rapidement le travail le lendemain matin. Si vous éteignez votre ordinateur, les nouvelles mises à jour seront exécutées. Une partie de ces mises à jour signifie une amélioration de la sécurité. Il est donc important d'exécuter régulièrement ces mises à jour.
- **Ne laissez traîner aucun mot de passe:** Il va de soi que vous n'apposerez aucun post-it avec des mots de passe sur votre écran. Glisser un morceau de papier discret sous votre clavier n'est pas non plus une bonne idée.

Évidemment, il est difficile de retenir les mots de passe de vos comptes personnels et professionnels. Dès lors, conservez vos mots de passe dans un coffre à mots de passe en ligne (un gestionnaire de mots de passe) que vous sécurisez à l'aide d'une phrase secrète forte. Vous ne devez plus retenir qu'un seul mot de passe. Lorsque vous le pouvez, utilisez la Two-Factor Authentication (2FA) https://www.safeonweb.be/fr/utilisez-des-mots-de-passe-surs

- **Menez les entretiens confidentiels loin des oreilles indiscrètes.** Si vous menez des entretien chez vous ou dans le train, veillez à ce que des tiers ne puissent pas vous écouter. Le but n'est pas de rendre publiques des informations sur votre travail, vos clients ou votre entreprise. Veuillez à avoir un endroit où appeler en toute discrétion chez vous aussi.

N'autorisez pas vos enfants ou des visiteurs à accéder à votre ordinateur ou smartphone de travail. Il peut être tentant de laisser vos enfants travailler/jouer/suivre des cours sur votre ordinateur de travail, mais cela accroît les risque de sécurité. Au bureau, vous ne devez pas vous soucier des enfants, invités ou autres membres de la famille qui utilisent votre ordinateur de travail ou les systèmes de votre employeur. En cas de télétravail, faites savoir clairement à votre famille et vos amis qu'ils ne peuvent pas utiliser vos systèmes de travail. Les informations pourraient être supprimées ou modifiées par accident, ou le système peut, dans le pire des cas, être infecté par accident.

(Sources: www.safeonweb.be & BNP Paribas Fortis)

Reconnaissez les messages frauduleux à temps

Faites particulièrement attention aux e-mails que vous recevez. Le remède au coronavirus p. ex. n'est pas fourni par e-mail. Le Centre pour la Cybersécurité Belgique (CCB) reçoit actuellement différents signalements de messages frauduleux sur le coronavirus:

- avec des offres de masques buccaux
- avec des fausses actions de collecte de fonds pour les victimes du virus
- avec des liens renvoyant vers des faux sites d'information
- avec des offres de vaccins

Recherchez les informations exactes. Vous trouverez les messages officiels du SPF Santé publique sur le site web info-coronavirus.be.

Que faire si vous recevez un message frauduleux?

- Ne cliquez pas sur les liens ou images des messages frauduleux et n'ouvrez aucune pièce jointe. **Téléchargez les pièces jointes ou ouvrez les liens** des e-mails uniquement lorsqu'ils proviennent de **sources connues et fiables.** Ne le faites pas s'ils viennent d'autres sources, même si le message semble urgent ou séduisant.
- En cas de doute, recherchez le site web via un moteur de recherche.
- N'ouvrez certainement pas des documents et pièces jointes de sources officielles non confirmées sur le COVID-19, sur aucun appareil.
- Ne téléchargez pas de logiciel non officiel sur votre ordinateur ou d'app sur votre smarphone en dehors de l'App Store officiel pour en savoir plus sur le COVID-19.
- Ne contribuez pas à la diffusion de messages frauduleux qui ne feront qu'effrayer vos amis et votre famille.
- **Transférez les messages suspects à** suspect@safeonweb.be ou à la mailbox phishing de votre banque.

Que faire si vous avez cliqué sur une pièce jointe dans un message suspect?

Vous suspectez quelqu'un de connaître votre de passe, ou d'avoir reçu un e-mail de phishing à votre adresse e-mail ou sur le téléphone de votre employeur? Vous avez ouvert le lien ou la pièce jointe d'un message suspect? Vous avez perdu votre ordinateur portable, smartphone ou tablette de votre employeur, ou il a été volé? Signalez-le immédiatement à votre employeur.

(Sources: Vrije Universiteit Brussel & BNP Paribas Fortis)

Utilisez des canaux de communication sécurisés

- Pour votre communication professionnelle, utilisez **les applications sélectionnées par votre département ou fournisseur IT.**

Les moyens de communication sont importants dans le télétravail. Le VPN de votre employeur (voir slide 4) vous permet de vous connecter au réseau de votre employeur depuis votre domicile. Mais il existe de nombreux autres moyens de communication. Ce qui est primordial, c'est de faire une distinction claire entre la communication privée et professionnelle et surtout de ne pas les mélanger. Pour votre communication professionnelle, il est préférable d'utiliser uniquement des applications sélectionnées par votre employeur. Utilisez des produits reconnus d'une appstore officielle et veillez à les mettre à jour.

- N'envoyez pas d'e-mails professionnels vers votre compte G-mail/Hotmail privé: **risque de fuite d'informations**

Si vous envoyez un e-mail pour le travail, utilisez uniquement votre compte professionnel. Parfois, il peut sembler pratique d'envoyer un fichier vers votre propre compte Gmail/Hotmail pour imprimer le document à domicile. N'oubliez pas que cela peut provoquer une fuite d'informations sensibles liées au travail. En effet, l'imprimante que vous avez chez vous ne répond pas toujours aux exigences de sécurité de votre employeur. Autrement dit, ne le faites jamais! Soyez particulièrement su vos gardes lorsque vous communiquez en externe et échangez des informations. Recourez uniquement aux solutions approuvées.

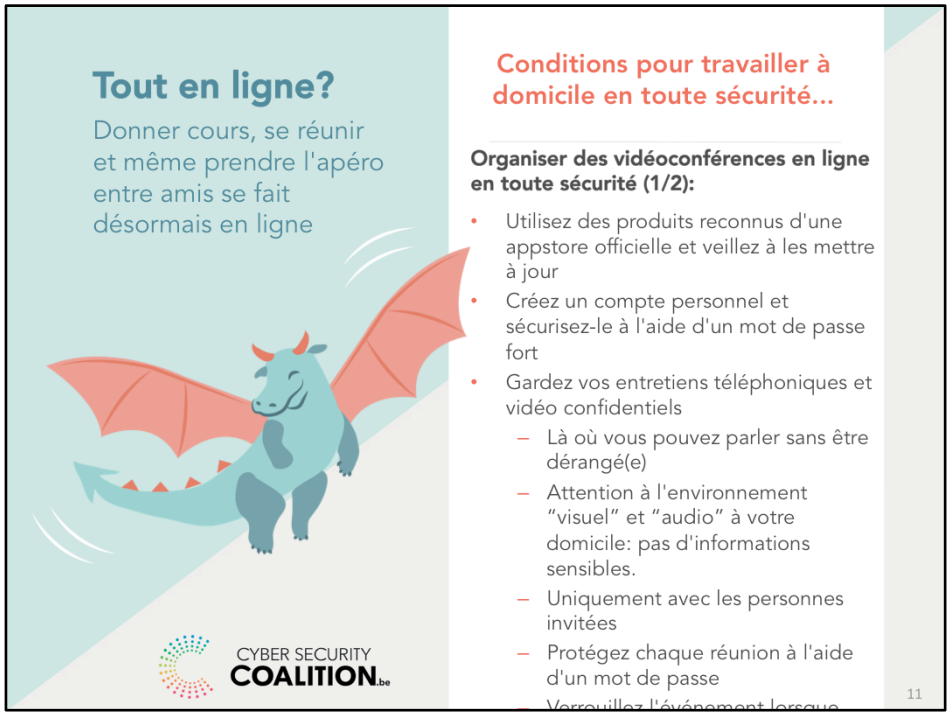
- Utilisez toujours une connexion **HTTPS**

Si vous naviguez sur des sites web, veillez à ce que votre navigateur utilise **toujours une connexion HTTPS et non HTTP** Pensez-y surtout lorsque vous devez saisir votre données personnelles sur ce site web, comme vos nom d'utilisateur et mot de passe. HTTPS utilise une communication cryptée et sécurisée. Ce n'est pas le cas d'une connexion HTTP, où toutes les données que vous avez saisies sont intégralement envoyées non cryptées sur internet et, par conséquent, peuvent être interceptées par des cybercriminels.

- Ne publiez **pas d'informations professionnelles sur les réseaux sociaux**

Dans le cadre du télétravail, la frontière entre l'utilisation de vos réseaux sociaux (privés) et activités professionnelles est évidemment plus mince qu'au bureau. Mettre en ligne des petits détails professionnels ou votre routine quotidienne est étrange lorsqu'il n'y a pas de collègues avec qui les partager. Les télétravailleurs doivent cependant prendre garde, car ces mises à jour donnent souvent des informations précieuses pour mettre en place des campagnes de phishing.

- Rangez les **documents confidentiels** en attendant de les ramener au travail. Ne les jetez jamais dans votre poubelle ménagère de déchets papier. Au travail, vous pouvez bien souvent détruire/traiter ces documents discrètement.



(Sources: www.safeonweb.be & US Department of Homeland Security)

Organiser des vidéoconférences en ligne en toute sécurité

- Utilisez des produits reconnus d'une appstore officielle et veillez à les mettre à jour.
    - Si vous téléchargez une app d'un appstore, utilisez uniquement les **appstores officielles** (App Store/Google Play)
    - Quelle que soit la plateforme que vous utilisez, veillez à toujours faire les **mises à jour.** Une mise à jour permet de fournir davantage de fonctionnalités et de résoudre les problèmes. En outre, les failles de sécurité sont corrigées. C'est pourquoi il est important de toujours exécuter les mises à jour lorsqu'elles sont disponibles.
- Créez votre **propre compte** et sécurisez-le à l'aide d'un **mot de passe fort.**
- Gardez vos entretiens téléphoniques et vidéo **confidentiels.**
    - Menez vos entretiens vidéo **à un endroit où vous pouvez parler sans être dérangé(e).** Si vous faites la réunion sur votre terrasse, vos voisins pourront peut-être entendre chaque mot prononcé, et ce n'est pas ce qui est souhaité. Il en va de même pour le train ou tout autre lieu public.
    - Attention à l'**environnement "visuel" et "audio"** à votre domicile°: pas d'informations sensibles. Pensez à remplacer ou flouter ("blurring") l'arrière-plan.
    - **Partagez le lien vers la réunion uniquement avec les personnes invitées** et pas en public (p. ex. sur Facebook). Vous évitez ainsi la présence de participants indésirables. En tant que "host", veillez à pouvoir mettre sur "mute" (désactiver le micro) toutes les personnes présentes (de préférence au début) et déterminer qui partage des écrans.
    - **Protégez chaque réunion à l'aide d'un mot de passe.** Utilisez la "salle d'attente" pour vérifier l'accès de vos invités. En tant qu'hôte/hôtesse, soyez le ou la première, n'autorisez pas d'autres participants avant vous.
    - "Verrouillez" l'événement lorsque tous les invités sont présents afin d'éviter les voyeurs indésirables.
    - Utilisez votre **casque** et désactivez les éventuelles caméras de sécurité de votre habitation.
    - **Utilisez un cache pour webcam.** Veillez à ce que votre webcam soit toujours couverte si vous ne l'utilisez pas.
    - **Protégez vos données** de manière optimale.
        - Pour partager des informations très sensibles, vous avez peut-être besoin d'une protection renforcée. Consultez à cet effet les **spécifications et paramètres.**
        - Demandez à votre employeur d'installer des **canaux de communication sécurisés** si vous partagez beaucoup d'informations confidentielles avec vos collègues.
    - Si **vous partagez des fichiers, écrans ou lorsque vous enregistrez la réunion:** veillez aussi à ce que tout soit particulièrement contrôlé. Sachez qui regarde/écoute. Faites preuve de vigilance si vous partagez tout votre écran ou une application individuelle.
    - Pensez bien à la sensibilité des informations avant de les partager via votre écran. **Ne discutez pas d'informations que vous ne communiqueriez pas non plus par téléphone.**

(Sources: www.safeonweb.be & US Department of Homeland Security)

Organiser des vidéoconférences en ligne en toute sécurité

- **Protégez vos données** de manière optimale.

  - Pour partager des informations très sensibles, vous avez peut-être besoin d'une protection renforcée. Consultez à cet effet les **spécifications et paramètres.**

  - Demandez à votre employeur d'installer des **canaux de communication sécurisés** si vous partagez beaucoup d'informations confidentielles avec vos collègues.

- Si **vous partagez des fichiers, écrans ou lorsque vous enregistrez la réunion:** veillez aussi à ce que tout soit particulièrement contrôlé. Sachez qui regarde/écoute. Faites attention si vous partagez tout votre écran ou une application individuelle.

- Pensez bien à la sensibilité des informations avant de les partager via votre écran. **Ne discutez pas d'informations que vous ne communiqueriez pas non plus par téléphone.**

Restez vigilant(e) et signalez immédiatement toute irrégularité à votre employeur:

- Smartphone, ordinateur portable, tablette perdu/volé?
- Message suspect?
- Vous avez cliqué sur un lien ou une pièce jointe d'un message suspect?
- Informations importantes perdues/volées?
- Mot de passe piraté?

Signalez les messages suspects à suspect@safeonweb.be. Le CCB fera bloquer les liens vers des sites frauduleux afin que vous et d'autres utilisateurs ne puissiez plus tomber dans le piège... Si le message suspect semble provenir de votre banque, transférez-le à la mailbox phishing de votre banque.

Vérifiez la sécurité de votre façon de télétravailler!

Testez votre santé digitale

faites le test sur
www.safeonweb.be

CYBER SECURITY COALITION

14

Quel est votre avis ?

Avez-vous des remarques?

Qu'avez-vous retenu?

Quelle sera votre première action après cette présentation?

Télétravailler
Points d'attention

CYBER SECURITY COALITION.be

Points d'attention SANS

Sans, référence internationale majeure en matière de cybersécurité, a publié cette vidéo qui résume très bien les principaux messages de ces slides très sérieux:

16

Liens utiles:

Centre pour la Cybersécurité Belgique (CCB):

-www.safeonweb.be : le site web du Centre pour la Cybersécurité Belgique (CCB) avec des conseils de sécurité et tests pratiques.

-suspect@safeonweb.be envoyez les messages suspects (e-mail/SMS/...) à cette adresse. Le CCB fait retirer les liens suspects hors ligne.

-Vérifiez votre santé digitale maintenant!: Faites le test et découvrez si votre santé digitale doit être stimulée. Vous recevez 15 questions sur les mises à jour, sauvegardes, phishing, antivirus et mots de passe.

-Webinaires sur la cybersécurité : Ces webinaires peuvent faire prendre conscience aux organisations des principales cybermenaces et leur donner des conseils pratiques pour se protéger et sécuriser les données clients. Ces webinaires ont pour but d'informer le management, ainsi que tous les travailleurs d'une organisation.

Europol: https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know contient 4 infographies (ANG) sur le Covid-19°:

- You can go outside again, criminals can too
- At home, still spending plenty of time online?
- Children's safety, a priority
- Protect your finances

Febelfin

US Department of Homeland Security

NVISO: to Zoom or not to Zoom
SANS: work from home deployment kit

Merci pour votre attention!