



CYBER SECURITY
COALITION.be



Home sweet home

Travaillez en toute sécurité chez vous aussi

Bruxelles, Septembre 2020

Travailler à domicile peut être un défi!



Ça vous dit quelque chose?

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



CYBER SECURITY
COALITION.be

Safe homeworking

Il était une fois, un paisible royaume

Qui faisait le bonheur de tous les télétravailleurs





Télétravailler

ne doit pas signifier que vous et l'organisation courez un plus grand risque d'être la proie d'une cyberattaque



Check the 'Passwords' module
in the Cyber Security Kit



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Une connexion réseau puissante et bien sécurisée (1/2):

- Installez un VPN (Virtual Private Network)
- Modifiez les mots de passe standard de tous vos appareils, y compris la domotique. Comment renforcer vos mots de passe: voir le module "Mots de passe" dans ce Cyber Security Kit.
- Sécurisez votre routeur
- Activez le pare-feu et protégez votre ordinateur et votre smartphone à l'aide d'un antivirus
- Désactivez le WPS (Wi-Fi Protected Setup)

Télétravailler



Consultez le module “Mots de passe”
dans ce Cyber Security Kit



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Une connexion réseau puissante et bien sécurisée (2/2):

- Créez un réseau invité
- Si possible, utilisez la ligne fixe Internet ou Ethernet
- Évitez le WiFi public à l'extérieur dans les hôtels, aéroports, gares et cafés
- Si nécessaire, installez un booster de WiFi
- Achetez des applications uniquement dans les app stores officiels
- Veillez à ce que votre système d'exploitation, tous vos programmes et applications soient à jour et à ce que les mises à jour soient automatiquement installées

Télétravailler sur votre ordinateur portable personnel?

Les organisations qui prévoient le télétravail depuis longtemps fournissent à leurs travailleurs des ordinateurs portables et, éventuellement, des smartphones de l'entreprise, qui sont plus sûrs que les appareils privés



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Un environnement de travail sécurisé (1/2):

- Utilisez de préférence l'ordinateur portable/le smartphone de votre employeur si vous en disposez.
- Si vous pouvez utiliser vos appareils privés, fermez toutes les fenêtres et applications privées pendant vos sessions de travail.
- Installez des outils de communication sûrs si vous partagez beaucoup d'informations confidentielles avec vos collègues.
- Toutes les apps ne sont pas sûres: suivez les directives de votre département IT ou demandez conseil à votre fournisseur IT

Télétravailler sur votre ordinateur portable personnel?



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Un environnement de travail sécurisé (2/2): surveillez votre vie privée et votre confidentialité dans votre bureau à domicile

- 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, sécurisez votre smartphone à l'aide d'un code PIN.
- Éteignez votre ordinateur tous les soirs
- Ne laissez traîner aucun mot de passe
- Menez les entretiens confidentiels loin des oreilles indiscrètes
- N'autorisez pas vos enfants ou des visiteurs à accéder à votre ordinateur ou smartphone de travail

Fake news et phishing

Les cybercriminels exploitent l'actualité et savent quels thèmes nous intéressent



Consultez le module “Phishing” dans ce Cyber Security Kit



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Reconnaissez les messages frauduleux à temps:

- Ne cliquez pas sur les liens ou images des messages frauduleux et n'ouvrez aucune pièce jointe. En cas de doute, recherchez le site web via un moteur de recherche. Consultez le module “Phishing” dans ce Cyber Security Kit.
- Ne téléchargez pas de logiciel non officiel sur votre ordinateur ou d'app sur votre smartphone en dehors de l'App Store/du Google Play officiel.
- Contactez immédiatement votre département ou fournisseur IT si vous avez cliqué sur une pièce jointe dans un message suspect.
- 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.

Travail ou vie privée?

En tant que télétravailleur, vous devez également continuer à différencier votre communication privée et professionnelle



Check the 'Social Engineering' module
in the Cyber Security Kit



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Utilisez des canaux de communication sécurisés:

- Pour la communication professionnelle, utilisez uniquement les applications sélectionnées par votre département ou fournisseur IT.
- N'envoyez pas d'e-mails professionnels vers votre compte Gmail/Hotmail privé: risque de fuite d'informations
- Utilisez toujours une connexion HTTPS
- Ne publiez pas d'informations professionnelles sur les réseaux sociaux
- Rangez les documents confidentiels en attendant de les ramener au travail.

Tout en ligne?

Donner cours, se réunir et même prendre l'apéro entre amis se fait désormais en ligne



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Organiser des vidéoconférences en ligne en toute sécurité (1/2):

- Utilisez des produits reconnus d'une appstore officielle et veillez à les mettre à jour
- Créez un compte personnel et sécurisez-le à l'aide d'un mot de passe fort
- Gardez vos entretiens téléphoniques et vidéo confidentiels
 - Là où vous pouvez parler sans être dérangé(e)
 - Attention à l'environnement “visuel” et “audio” à votre domicile: pas d'informations sensibles.
 - Uniquement avec les personnes invitées
 - Protégez chaque réunion à l'aide d'un mot de passe
 - Verrouillez l'événement lorsque tous les invités sont présents
 - Utilisez votre casque ou vos écouteurs
 - Utilisez un cache pour webcam

Tout en ligne?

Conditions pour travailler à domicile en toute sécurité...

Organiser des vidéoconférences en ligne en toute sécurité (2/2):

- Protégez vos données de manière optimale
 - Installez des canaux de communication sécurisés
 - Partage d'écran/de fichiers: pas avec n'importe qui.
 - Ne partagez pas de données que vous ne communiqueriez pas non plus par téléphone.



Télétravailler

Et si ça se passe mal?



CYBER SECURITY
COALITION.be

Conditions pour travailler à domicile en toute sécurité...

Restez vigilant(e) et signalez immédiatement toute irrégularité à votre département ou fournisseur IT, à votre banque:

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

Vérifiez la sécurité de votre façon de télétravailler!

Testez votre santé digitale

[faites le test](#) sur www.safeonweb.be



Télétravailler en toute sécurité: parlez-en !

Quel est votre avis?

Avez-vous des remarques?

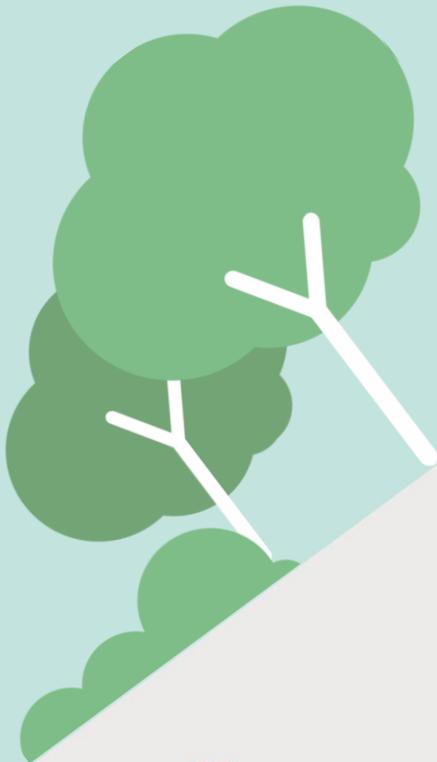
Qu'avez-vous retenu?

Votre première action?



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:



Liens utiles

- www.safeonweb.be : Centre pour la Cybersécurité Belgique (CCB) avec des conseils de sécurité et des tests pratiques.
- suspect@safeonweb.be : envoyez les messages suspects (e-mail/SMS/...) à cette adresse.
- [Vérifiez votre santé digitale maintenant!](#)
- [Webinaires sur la cybersécurité \(CCB\)](#)
- [Europol^o : infographies on Covid-19 threats \(ANG\)](#)
- [Febelfin](#)
- [US Department of Homeland Security](#)
- NVISO: [to Zoom or not to Zoom](#)
- SANS: [work from home deployment kit](#)





CYBER SECURITY
COALITION.be

*Ajoutez ici le logo de
votre
organisation/
entreprise*

Une initiative de la Cyber Security Coalition

Son objectif? Renforcer la sécurité IT en Belgique. Elle rassemble des experts du monde académique, les autorités et les entreprises pour mieux lutter contre la cybercriminalité.

www.cybersecuritycoalition.be



Tous droits réservés© 2020 Cyber Security Coalition