|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Document d’information *Call to action*** **Le PME cyber security scan et kit****CSIPME-JC-13/3/2019** |  |  |
|  |  |  |

Via ce document, nous souhaitons vous aider à faire connaître le scan et le kit à vos membres. Vous trouverez tous les instruments ainsi que le matériel promotionnel dans ce document. Pour les outils et informations, nous renvoyons principalement à la Cyber Security Coalition (CSC), à laquelle le CSIPME est affilié. Nous reprenons toujours les liens vers des outils et documents en néerlandais (N) et en français (F). Sur le site de la CSC, ceux-ci sont également disponibles en anglais.

**1. Objectif du *call to action***

* Faire connaître le PME cyber security scan et le PME cyber security kit au plus grand nombre possible d’indépendants et de PME via les organisations professionnelles et interprofessionnelles.
* Les sensibiliser ainsi aux cyberrisques et les inciter à mieux se protéger, en effectuant avant tout des démarches simples mais qui ont pourtant un impact important.

**2. Le scan et le kit expliqués**

**Le PME cyber security scan**

* Ce scan répond à deux questions: où en est votre cyberprotection et que pouvez-vous faire afin de l’améliorer? En effet, le scan est un questionnaire bref et dynamique, par lequel les entrepreneurs ou les titulaires d’une profession libérale peuvent évaluer à quel point leurs fichiers et leur infrastructure informatique sont protégés. Sur base des réponses données, on reçoit un certain nombre de conseils pratiques.
* Où trouve-t-on le scan?

 en F: [www.cybersecuritycoalition.be/fr/pme-security-scan](http://www.cybersecuritycoalition.be/fr/pme-security-scan)

 en N: [www.cybersecuritycoalition.be/nl/kmo-security-scan](http://www.cybersecuritycoalition.be/nl/kmo-security-scan)

**Le PME cyber security kit**

* Ce kit fournit un certain nombre d’instruments pratiques aux PME pour informer et sensibiliser leurs collaborateurs et leurs clients au sujet de la cybersécurité. Les organisations professionnelles et interprofessionnelles peuvent également avoir recours au kit pour informer et sensibiliser leurs membres.
* Le Cyber Security KIT aborde quatre thèmes :
	1. Comment renforcer ses mots de passe ?
	2. Comment reconnaître les courriels de phishing ?
	3. Comment lutter contre l’ingénierie sociale ?
	4. Comment vos équipes gèrent-elles les données personnelles de vos clients ?
* Pour chaque thème, vous trouverez dans le kit :
1. un courriel ;
2. une courte présentation PowerPoint ;
3. une affiche/un économiseur d’écran.
* Le kit contient également un courriel standard ainsi qu'un carnet de route et un planning, bien que ces derniers outils soient moins utilisables pour la majorité des PME.
* Les organisations professionnelles et interprofessionnelles ainsi que les PME peuvent aussi utiliser le matériel du kit et y ajouter leur propre logo, à côté du logo de la Cyber Security Coalition. À cet effet, le kit contient également les fichiers vectorisés (modifiables).
* Où trouve-t-on le kit?

 en F: [www.cybersecuritycoalition.be/fr/resource/cyber-security-kit](http://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit)

 en N: [www.cybersecuritycoalition.be/nl/resource/cyber-security-kit](http://www.cybersecuritycoalition.be/nl/resource/cyber-security-kit)

**3. Que faut-il promouvoir auprès de vos membres : le scan, le kit, les deux, d’autres outils ?**

**Cela dépend de la situation de vos membres.**

* En règle générale, il convient de leur proposer les **deux instruments.** Si la majorité de vos membres n’ont toutefois pas de personnel et s’il est peu utile pour eux de s’adresser à leurs clients à ce sujet, il y a donc peu d'intérêt de leur proposer le kit.

* Il n’est utile de fournir d'entrée de jeu des informations supplémentaires, telles qu’une brochure, que si vos membres ont un intérêt ou un besoin particulier en matière de cybersécurité. Ci-après, le présent document fait référence à des informations et des outils supplémentaires. **Il est préférable de ne pas fournir trop d’informations en même temps à vos membres.**
* Quand votre secteur professionnel est confronté à une forme spécifique de cybercriminalité comme le phishing, par exemple, **il peut être utile de ne diffuser que cette partie spécifique du kit** à vos membresau lieu du kit entier, afin qu’ils puissent se focaliser sur cette problématique spécifique.

**Votre organisation peut également elle-même utiliser le kit pour sensibiliser ses membres.**

* Vous pouvez porter le kit à l’attention de vos membres pour qu’ils puissent le diffuser à leurs collaborateurs et leurs clients, mais en même temps ou au lieu de cela, il est possible d’utiliser vous-même les contenus du kit afin de sensibiliser vos membres à un ou plusieurs des thèmes qui y sont traités.
* Vous pourriez, par exemple, commencer en les informant du scan et du kit et ensuite, au cours des mois suivants, attirer leur attention sur les différents thèmes du kit de manière progressive, en utilisant vous-même les matériels inclus dans le kit.

**4. Comment diffuser le scan et le kit parmi vos membres ?**

Il existe plusieurs canaux appropriés pour inciter vos membres à se lancer dans l'utilisation du scan et du kit. Il est préférable de combiner plusieurs canaux. Vous pouvez avoir recours aux mêmes canaux afin d’informer et de sensibiliser vous-même vos membres, à partir du matériel du kit. Tant sur les affiches promotionnelles du scan et du kit que sur les documents inclus dans le kit, il vous est loisible d’ajouter le logo de votre organisation.

1. **Via un courriel adressé à vos membres**
* À la fin du présent document, un modèle de courriel est annexé, que vous pouvez adapter et utiliser.
* Si vous souhaitez uniquement attirer l’attention sur le scan et pas sur le kit, le courriel est aisément adaptable.
* Si vous souhaitez vous-même mettre l'accent sur un des thèmes du kit, le kit comprend des courriels que vous pouvez adapter et utiliser.
1. **Via un article dans votre magazine ou newsletter**
* Pour une communication succincte, le texte du courriel en annexe peut être utilisé ou retravaillé.
* Pour des articles plus longs, il est possible de nous contacter afin d’évaluer ensemble quel contenu vous souhaitez exactement et ce que nous pouvons vous fournir à cette fin.
* Un format intéressant pour un article sur ce thème est l'interview, prenant par exemple la forme d’un témoignage d’une victime (bien qu’il ne soit certainement pas facile de trouver quelqu’un qui est prêt à témoigner dans tous les secteurs) avec une annonce (cf. point suivant).
* Les courriels inclus dans le kit peuvent également être convertis en de brefs articles informatifs pour un magazine ou une newsletter.
* Dans les numéros successifs de votre magazine ou votre newsletter, vous pouvez vous pencher sur les différents sous-thèmes de la cybersécurité.
1. **Via une annonce dans votre magazine ou newsletter**
* Vous trouverez les affiches conçues pour la promotion du scan et du kit via le lien suivant :

[www.cybersecuritycoalition.be/fr/pme-cyber-security-scan-kit-2-outils-pour-renforcer-votre-securite-informatique/](http://www.cybersecuritycoalition.be/fr/pme-cyber-security-scan-kit-2-outils-pour-renforcer-votre-securite-informatique/)

Vous y trouverez également les fichiers vectorisés. Il vous est loisible d’ajouter le logo de votre organisation à ces affiches.

* Les affiches du kit peuvent également être reproduites dans votre magazine. Il vous est également loisible d’y ajouter votre propre logo.
1. **Via votre site web**
* Afin de diffuser le scan et le kit sur votre site web, vous pouvez utiliser les fonds d’écran disponibles via le site web mentionné ci-dessus sous le point 3). Il vous appartient également d’ajouter votre logo aux fonds d’écran.
* En outre, vous pouvez prévoir une page séparée sur votre site web, consacrée à la cybersécurité de vos membres. Si vous avez des questions relatives aux contenus éventuels de cette page, n’hésitez pas à nous contacter.
1. **Via les réseaux sociaux**
* L'utilisation des réseaux sociaux constitue également une manière appropriée d’informer vos membres sur la cybersécurité. Le texte du courriel ci-joint et les fonds d’écran susmentionnés peuvent également être utilisés dans ce cadre.
* Le matériel inclus dans le kit peut également être diffusé via les réseaux sociaux.
* Les réseaux sociaux constituent sans aucun doute une bonne solution si vous souhaitez attirer l’attention sur différents sous-thèmes de manière progressive.
1. **Comme point à l’ordre du jour des réunions**
* Il est indiqué d'envisager de mettre la cybersécurité ou un de ses sous-thèmes à l’ordre du jour des réunions prévues / commissions existantes au sein de votre organisation.
* Un collaborateur de votre organisation ou un orateur externe peut y donner des explications.
* Le kit comprend, pour chaque thème, une présentation PowerPoint toute faite, avec des notes pour l’orateur.
1. **Comme sujet lors d’un événement**
* Cela vaut assurément la peine d’organiser un événement relatif à la cybersécurité pour vos membres. Les indépendants et les PME s’intéressent de plus en plus à ce sujet. Un tel événement ne doit certainement pas être trop technique.
* Le scan et le kit pourront être des éléments centraux lors de cet événement.
* Besoin d’idées et d'input pour un événement ? N’hésitez pas à nous contacter.

**8) Des affiches dans vos locaux et à vos événements**

* Pourquoi ne pas apposer quelques affiches promotionnelles du scan et du kit dans vos locaux, dans vos salles de réunion et lors de vos événements?
* Il est également possible d’utiliser les affiches du kit.
* Il vous est loisible d’ajouter votre propre logo aux deux affiches.

**5. Informations et outils supplémentaires**

Veuillez trouver ci-dessous les liens vers des informations supplémentaires. Il est préférable de ne pas abasourdir vos membres par un excès d’information.

**Des brochures intéressantes sont :**

* Le *Cyber security guide* pour les PME

 (qui a été distribué aux personnes présentes lors de la séance d’information du 13/3/2019)

 F: [www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-FR.pdf](http://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-FR.pdf)

 N: [www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-NL.pdf](http://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-NL.pdf)

* Les *Cyber Security Basics* pour les Starters

F: [www.cybersecuritycoalition.be/content/uploads/CSC-FR-Cyber-Security-Basics-pour-les-Starters.pdf](http://www.cybersecuritycoalition.be/content/uploads/CSC-FR-Cyber-Security-Basics-pour-les-Starters.pdf)

N: [www.cybersecuritycoalition.be/content/uploads/CSC-NL-Cyber-Security-Basics-voor-Starters.pdf](http://www.cybersecuritycoalition.be/content/uploads/CSC-NL-Cyber-Security-Basics-voor-Starters.pdf)

**Pour plus d’informations et d’outils, consultez également les sites web suivants :**

* [www.cybersecuritycoalition.be](http://www.cybersecuritycoalition.be)
* [www.safeonweb.be](http://www.safeonweb.be)
* <https://economie.fgov.be/fr/publications/cybersecurite-votre-entreprise>

**6. Au secours!**

**Si vous avez des questions**, si vous ne savez pas exactement comment aborder certains éléments, si vous cherchez plus d’informations, si vous avez besoin d’input pour un article ou si vous souhaitez organiser un événement et vous cherchez de l’inspiration ou des orateurs, … **n’hésitez pas à nous contacter**. En dépit de nos propres limites en termes de temps et de ressources, nous essaierons de vous aider le plus possible.

Si vous souhaitez être associé plus étroitement aux efforts visant une meilleure cyberprotection pour les PME, vous êtes certainement le bienvenu au **groupe de travail *Cybersécurité* du CSIPME**.

**Coordonnées :**

* Jef Cools, CSIPME, jef.cools@economie.fgov.be, 02/277 90 18
* Ellen Stuer, ellen.stuer@economie.fgov.be, 02/277 64 98

**Annexe – Modèle de courriel à l’intention de vos membres**

**Version F**

Sujet : Améliorez votre protection contre les cybercriminels

Cher membre de [abréviation de l’organisation],

Il est quasi certain qu’au cours de l’année dernière, vous avez entendu parler de cyberattaques et de cybercriminalité. La cybercriminalité ne menace pas seulement les grandes entreprises, mais de plus en plus souvent aussi les indépendants [, les professions libérales] et les PME. De surcroît, ceux-ci sont beaucoup moins protégés. Pourtant, la cybercriminalité peut engendrer des coûts importants pour votre entreprise. La cybersécurité joue également un rôle important dans le cadre de la protection des données (RGPD).

Via quelques démarches simples, vous pouvez améliorer sensiblement votre cyberprotection. En tant qu' [organisation professionnelle / interprofessionnelle], nous souhaiterions vous faciliter la tâche. Voilà pourquoi nous vous présentons deux instruments concrets et simples : le PME cyber security scan et kit.

* Le scan vous informe sur votre niveau de cyberprotection et de ce que vous pouvez faire afin de l’améliorer. Il s’agit d’un bref questionnaire en ligne qui vous offre des conseils pratiques et adaptés à votre situation sur base de vos réponses. Faites le scan ici :

<https://www.cybersecuritycoalition.be/fr/pme-security-scan/>

* Le kit vous offre un certain nombre d’outils pratiques pour informer et sensibiliser vos collaborateurs et vos clients. À cet effet, il contient une affiche, un courriel et une présentation sur quatre thèmes différents (phishing, mots de passe, ingénierie sociale et RGPD). Le kit est disponible sur :

<https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/>

La conscience des cyberrisques constitue un premier pas, mais la protection nécessite des actions effectives. Afin d‘augmenter votre sécurité, commencez déjà par ces deux outils simples.

Bonne chance !

**N-versie**

Onderwerp: Bescherm uzelf beter tegen cybercriminelen

Beste [afkorting organisatie] lid,

Het kan bijna niet anders of u heeft het voorbije jaar wel eens iets gehoord over cyberaanvallen en cybercriminaliteit. Cybercriminaliteit is niet alleen een probleem voor grote ondernemingen maar steeds vaker ook voor zelfstandigen[, vrije beroepen] en kmo’s. Tegelijkertijd weten we dat zij veel minder beschermd zijn. Cybercriminaliteit kan nochtans erg belangrijke kosten voor u tot gevolg hebben. Ook in het kader van de gegevensbescherming (GDPR) speelt cyberveiligheid een belangrijke rol.

U kan door een aantal eenvoudige handelingen uw cyberbescherming reeds gevoelig verhogen. Als uw [beroepsorganisatie / interprofessionele organisatie] willen we u daarmee op weg helpen. Daarom stellen we u twee concrete, eenvoudige instrumenten voor: de KMO Cyber Security scan en kit.

* De scan leert u hoe het met uw cyberbescherming gesteld is en wat u kan doen om die te verbeteren. Het is een korte, online vragenlijst die u op basis van uw antwoorden een praktisch en op uw situatie afgestemd advies geeft. Doe de scan hier: [www.cybersecuritycoalition.be/nl/kmo-security-scan](http://www.cybersecuritycoalition.be/nl/kmo-security-scan)
* De kit biedt u een aantal handige hulpmiddelen om uw personeel en uw klanten te informeren en te sensibiliseren. De kit bevat daartoe voor vier verschillende thema's (phishing, paswoorden, social engineering en GDPR) telkens een affiche, een e-mail en een presentatie. Bekijk de kit hier: [www.cybersecuritycoalition.be/nl/resource/cyber-security-kit](http://www.cybersecuritycoalition.be/nl/resource/cyber-security-kit)

Zich bewust zijn van cyberrisico’s is een eerste stap maar zich beschermen vergt daadwerkelijke actie. Begin alvast met deze twee eenvoudige instrumenten om uw veiligheid te verhogen.

Succes!