Cyber Challenge

PROTÉGER SON ENTREPRISE À L'ÈRE DU NUMÉRIQUE :

Enjeux et **bonnes pratiques**

CYBERSCAN
economie
SPF Economie, P.M.E., Classes moyennes et Energie
sni syndicat neutre pour indépendants
Financé par l'Union européenne
NextGenerationEU

Webinaires Cyber Challenge

Dans le cadre du projet Cyber Challenge, plusieurs webinaires ont été organisés afin de sensibiliser les indépendants, PME et professions libérales aux principaux enjeux de la cybersécurité.

Ces sessions en ligne ont permis de présenter les risques les plus fréquents auxquels les entreprises sont confrontées aujourd'hui (phishing, piratage de comptes, pertes de données, etc.), mais aussi de partager des conseils pratiques et accessibles pour améliorer la protection de son activité au quotidien.

Les webinaires abordent notamment :

- les menaces cyber les plus courantes pour les petites structures,
- les bonnes pratiques de sécurité numérique,
- les outils et mesures simples à mettre en place pour renforcer la protection de ses données,
- ainsi que les solutions d'accompagnement proposées dans le cadre du projet Cyber Challenge.

Les replays des webinaires sont disponibles via les liens ci-dessous.

- Replay du webinaire Cyber Challenge pour les **indépendants et PME** : https://youtu.be/miL2k1-n5Tk
- Replay du webinaire Cyber Challenge pour les **professions libérales** : https://youtu.be/56Eo2Egb3bE

Retrouvez toute notre actualité dans L'Indépendant

Le SNI publie chaque mois son magazine L'Indépendant, une publication dédiée à l'information et à l'accompagnement des indépendants et des PME en Belgique. À travers ses différentes rubriques, le magazine décrypte les enjeux économiques, politiques et réglementaires qui influencent directement l'activité des entrepreneurs.

Chaque numéro propose des analyses, dossiers thématiques et articles de fond sur les sujets clés pour les indépendants : évolution de la législation, actualité socio-économique, digitalisation des entreprises, cybersécurité, intelligence artificielle, gestion d'entreprise ou encore transformation du commerce et des métiers. L'objectif est d'apporter aux entrepreneurs une information claire, concrète et directement utile dans leur quotidien professionnel.

Le magazine met également en avant des conseils pratiques, des fiches didactiques, des questions-réponses juridiques ainsi que des témoignages d'entrepreneurs et d'experts. Ces contenus permettent d'illustrer les bonnes pratiques, de partager des expériences de terrain et d'aider les indépendants à mieux anticiper les défis auxquels ils peuvent être confrontés.

À travers L'Indépendant, le SNI informe, sensibilise et accompagne les entrepreneurs afin de les aider à développer et sécuriser durablement leur activité.

Le magazine est accessible gratuitement à tous les membres du SNI.

Pour en savoir plus sur les services du SNI et les modalités d'adhésion, consultez : www.sninet.be

MOT DU SECRÉTAIRE GÉNÉRAL

Protéger les indépendants face aux cybermenaces : notre engagement est total

La cybersécurité est aujourd'hui un enjeu stratégique pour les indépendants et les PME. À mesure que la digitalisation s'accélère — outils cloud, intelligence artificielle, réseaux sociaux, facturation électronique, commerce en ligne — les opportunités de développement s'accompagnent également de risques accrus.

Le projet Cyber Challenge s'inscrit dans cette réalité. Il s'intègre plus largement dans la dynamique européenne de renforcement de la résilience numérique, soutenue par le plan de relance européen (NextGenerationEU), notamment à travers des initiatives telles que Cyber4SME, mises en œuvre par le SPF Économie. L'objectif est clair : accompagner concrètement les petites structures face aux cybermenaces croissantes et les préparer aux nouvelles exigences réglementaires européennes.

À travers ce projet, le SNI a voulu proposer une approche accessible, pragmatique et adaptée au terrain. Il ne s'agit pas de complexifier la gestion quotidienne des entrepreneurs, mais de leur permettre d'identifier les priorités, de renforcer leurs pratiques et de sécuriser leur activité de manière proportionnée.

Ce livret blanc synthétise les constats, les enseignements et les bonnes pratiques issus du Cyber Challenge. Il démontre qu'une cybersécurité efficace repose avant tout sur des mesures simples, structurées et adaptées à chaque réalité professionnelle.

Renforcer la sécurité numérique, c'est protéger son entreprise, ses clients et sa continuité d'activité. Le SNI poursuivra son engagement pour soutenir durablement la résilience des indépendants.

Christophe Wambersie
Secrétaire général du Syndicat neutre pour indépendants

Sommaire

Éditeur responsable :
Le Syndicat Neutre pour Indépendants

Conception graphique et coordination :
V&Com SRL

Les enjeux de la cybersécurité dans les dix prochaines années

L'accélération technologique transforme radicalement notre rapport au risque. Dans un monde où la connectivité devient l'oxygène de l'économie, la cybersécurité ne peut plus être une simple fonction technique reléguée au second plan. Elle s'impose désormais comme le pivot stratégique de la gouvernance moderne. Voici une analyse des mutations profondes qui attendent les organisations au cours de la prochaine décennie.

Le paysage numérique de la prochaine décennie ne sera pas une simple extension du nôtre ; il s'annonce comme un terrain de mutations profondes où la sécurité deviendra la condition sine qua non de toute activité pérenne. Demain, la question ne sera plus de savoir si une entreprise peut se protéger ponctuellement, mais comment elle intègre la résilience numérique au cœur de son modèle de développement. Le premier grand défi réside dans l'évolution de l'intelligence artificielle. Si l'IA offre des gains de productivité inédits, elle oblige aussi à repenser la défense pour la rendre plus réactive. La sécurité de demain sera proactive, capable d'identifier les signaux faibles et de neutraliser les anomalies de manière automatisée pour préserver la continuité du travail. Cette automatisation ne sera pas un luxe, mais une nécessité pour contrer des attaques elles-mêmes pilotées par des algorithmes capables de tester des milliers de failles en quelques secondes.

Sécurisez vos données **partout et pour toujours**

Cette évolution s'accompagne d'une dispersion totale des données. Avec la généralisation du travail hybride et l'omniprésence des objets connectés, le périmètre traditionnel de l'entreprise s'efface. Dans dix ans, protéger son activité signifiera sécuriser chaque point d'interaction, du capteur industriel au terminal mobile, imposant une approche où la confiance se vérifie à chaque étape. Parallèlement, l'émergence de nouvelles capacités de calcul, notamment quantiques, forcera une mise à jour progressive de nos standards de chiffrement pour garantir, sur le long terme, l'inviolabilité du secret des affaires et de la propriété intellectuelle. Ce basculement vers une cryptographie post-quantique sera l'un des chantiers les plus stratégiques de la décennie pour éviter que les archives numériques d'aujourd'hui ne deviennent lisibles par les processeurs de demain.

La **dépendance au cloud** aura de conséquences

L'enjeu de la souveraineté et de la dépendance numérique prendra également une dimension nouvelle. Les entreprises s'appuient de plus en plus sur des infrastructures cloud mondialisées, ce qui concentre les risques. Une défaillance chez un fournisseur majeur pourrait paralyser des milliers de PME simultanément. La prochaine décennie obligera donc les dirigeants à repenser leur «chaîne d'approvisionnement numérique» avec la même rigueur que leurs flux logistiques physiques. La cybersécurité ne s'arrêtera plus aux murs de l'organisation, mais englobera l'ensemble de son écosystème de partenaires et de sous-traitants. La responsabilité de l'entreprise sera engagée sur toute la ligne, imposant des audits de sécurité croisés et une transparence totale sur les méthodes de stockage et de traitement des flux.

Votre sécurité numérique comme **preuve de votre sérieux**

L'enjeu de la décennie sera également humain et stratégique. La cybersécurité ne sera plus perçue comme une barrière technique, mais comme un pilier de la gouvernance et un gage de professionnalisme. La réputation numérique deviendra l'actif le plus précieux d'une marque : une entreprise incapable de protéger les données de ses clients perdra instantanément sa place sur le marché. Face à un cadre réglementaire qui se précise, à l'image de la directive européenne NIS2, la maturité numérique deviendra un critère de sélection majeur pour les partenaires. Les organisations qui réussiront seront celles qui auront su transformer la sécurité en une culture partagée, où chaque collaborateur, bien informé et soutenu par des outils robustes, devient un acteur de la stabilité globale et de la pérennité de l'organisation dans un monde hyper-connecté.

La cybersécurité sort définitivement du cadre informatique pour devenir une condition de survie économique. Face à la menace quantique et à l'automatisation des attaques, les entreprises devront non seulement investir dans la technologie, mais surtout dans la confiance et la culture de la vigilance. La capacité à protéger ses flux et ses données ne sera plus un avantage compétitif, mais le socle même de toute existence sur le marché de demain.

Deux indépendants partagent leur expérience du Cyber Challenge

Dans le cadre du Cyber Challenge, deux indépendants ont accepté de se prêter au jeu d'un audit numérique afin d'évaluer et renforcer la protection de leurs activités en ligne. Nous leur avons demandé de retracer leur expérience. Comment ont-ils découvert le dispositif ? Qu'ont-ils appris ? Et surtout, qu'est-ce que cela a changé concrètement dans leur quotidien d'indépendant ?

Premier témoignage avec **Jad Riahi**, *fondateur d'une toute jeune entreprise 100 % digitale.*

>>Jad Riahi, très satisfait par sa participation au Cyber Challenge

Pouvez-vous vous présenter et nous parler de votre commerce ?

Je m'appelle Jad Riahi et je suis le fondateur de BE STRIDE, une toute jeune entreprise lancée en juin 2025. BE STRIDE est un commerce exclusivement en ligne, où toutes les activités sont informatisées : la boutique, la gestion des commandes, le mailing, la publicité, les paiements. Je m'adresse principalement aux sportifs. Je vends des articles de sport, et plus particulièrement des chaussettes techniques : des modèles traditionnels, mais aussi des versions plus spécifiques qui favorisent, par exemple, la circulation sanguine. Il faut savoir que je suis basketteur à la base et cette passion m'a permis d'acquérir une vraie expertise et de comprendre les besoins concrets des sportifs sur le terrain.

Comment avez-vous entendu parler du Cyber Challenge ?

C'est lors d'une discussion avec Dimitri De Poorter, impliqué dans le projet, que j'ai découvert l'initiative. Je me suis dit : « Pourquoi pas ? » Très vite, j'ai compris l'intérêt. Mon activité repose entièrement sur le numérique : ma boutique est en ligne, je gère un volume important d'emails, mes publicités sont digitales, mes comptes bancaires aussi. Si je me fais pirater, les conséquences peuvent être énormes. Participer au Cyber Challenge était l'occasion d'obtenir des conseils pratiques et de sécuriser l'ensemble de mon écosystème digital.

Combien de temps cet audit vous a-t-il pris ?

Honnêtement, très peu de temps. L'inscription, l'audit et la mise en place des premières recommandations ont été rapides et fluides. En une dizaine de minutes, l'essentiel était fait. Les échanges avec les auditeurs étaient accessibles et compréhensibles. On ne vous parle pas en jargon technique incompréhensible. Cela rend l'expérience rassurante et motivante.

Étiez-vous déjà sensibilisé aux enjeux de cybersécurité avant de participer au Cyber Challenge ?

Pas vraiment. Avant cet audit, je dois reconnaître que je n'y accordais pas beaucoup d'importance. Mais les choses ont évolué. Je recevais de plus en plus de spams très crédibles, notamment des faux messages semblant provenir d'OVH. Les tentatives de phishing, autrefois imparfaites, deviennent aujourd'hui extrêmement subtiles. On peut cliquer par erreur très facilement. Et quand on entend autour de soi des histoires de comptes piratés ou de données volées, cela devient inquiétant.

Avez-vous mis en pratique les conseils reçus ?

Oui, immédiatement. J'ai sécurisé tous mes mots de passe et j'ai activé la double authentification sur mes outils. Je savais qu'il fallait le faire, mais comme beaucoup d'indépendants, je repoussais par manque de temps. Le Cyber Challenge m'a donné le déclic. Aujourd'hui, je peux dire que mon environnement numérique est bien mieux protégé.

Quels bénéfices concrets en tirez-vous ?

Au-delà de la sécurité personnelle, c'est aussi un argument commercial. Je peux rassurer mes clients en leur garantissant que leurs données sont protégées et que je respecte les règles du RGPD. Pour moi, c'est essentiel. Non seulement par éthique, mais aussi pour éviter tout risque juridique. Une fuite de données pourrait entraîner des poursuites. Je ne veux pas prendre ce risque.

Deuxième témoignage avec **Maxime Fenez**, *indépendant dans le domaine du sport.*

Pouvez-vous vous présenter et nous parler de votre commerce ?

Je suis coach sportif diplômé d'un bachelier en coaching sportif et je travaille comme préparateur physique indépendant à Bruxelles, notamment chez The Motion Factory. J'y accompagne des sportifs en suivi individuel, en réathlétisation et en cours collectifs. Je suis aussi coach de basket, spécialisé dans le développement des skills (dribble, déplacements, lecture du jeu). Ma spécificité est de combiner préparation physique et travail technique spécifique à ce sport pour proposer un encadrement structuré et adapté au niveau de chaque athlète.

Comment avez-vous entendu parler du Cyber Challenge ?

J'ai vu une publicité sur les réseaux sociaux. Ça tombait bien parce que je voulais faire le point sur mes outils informatiques et leur sécurité. J'en utilise beaucoup au quotidien sans toujours savoir s'ils sont bien protégés. Le Cyber Challenge m'a semblé être une bonne occasion d'y voir plus clair.

Avant cet audit, comment décririez-vous votre présence en ligne ?

Je suis surtout présent sur Instagram et Facebook pour développer ma visibilité et je commence à investir davantage YouTube. Dans mon métier, la crédibilité est essentielle et construire une communauté prend du temps. Si je perdais l'accès à mes comptes, l'impact serait direct, car c'est mon principal canal de communication avec mes clients.

Concrètement, en quoi a consisté le Cyber Challenge pour vous ?

Après l'inscription, j'ai été contacté rapidement pour fixer un entretien téléphonique. On a fait le point sur mes habitudes numériques, mes outils, la gestion de mes données et de mes accès. Certains sujets comme le cloud, la sécurité des appareils ou le phishing m'ont fait prendre conscience de risques que je minimisais. J'ai aussi réalisé un scan en ligne recommandé pour évaluer ma situation plus de façon plus concrète.

Combien de temps cela vous a-t-il pris et était-ce compatible avec votre activité quotidienne d'indépendant ?

Le processus a été rapide et l'équipe flexible pour fixer le rendez-vous. L'attente du rapport était normale. C'est totalement compatible avec mon activité, et même plus essentiel que je ne le pensais. Les conseils sont clairs et pratiques. Il faut prendre un peu de temps pour appliquer certaines recommandations mais rien n'est trop technique et tout est bien expliqué.

>>Maxime Fenez a grâce à cet audit le sentiment d'avoir vraiment protégé ses données clients.

La question de la protection des données et de la cybersécurité a-t-elle été abordée ?

Oui, c'était le sujet principal. J'étais déjà sensibilisé à la protection des données notamment parce que je traite des informations personnelles liées à la santé. L'audit a surtout confirmé que j'étais sur la bonne voie et il m'a permis de renforcer certains points.

Quelles ont été les principales recommandations qui vous ont marqué ?

La séparation entre l'usage privé et professionnel m'a marqué parce que j'utilise le même téléphone pour les deux. La question des mots de passe et des sauvegardes m'a aussi fait réfléchir à l'importance de mieux protéger mes comptes professionnels.

Pensez-vous mettre en pratique ces conseils rapidement ?

Oui, j'ai déjà installé un gestionnaire de mots de passe et j'ai revu tous mes accès. Les autres améliorations seront mises en place progressivement.

Quels bénéfices concrets votre commerce peut-il tirer de cet audit ?

Cela permet d'éviter des problèmes comme la perte d'accès à mes réseaux sociaux ou à mes données clients. Être mieux protégé, c'est protéger son image et sa relation client, et pouvoir se concentrer sur son métier sans inquiétude.

Web, VPN et IA : adoptez les bons réflexes pour sécuriser vos données

La transformation digitale des activités professionnelles offre des opportunités de croissance inédites, mais elle demande une constante vigilance : protéger son environnement de travail est aujourd'hui une priorité absolue face à des menaces toujours plus sophistiquées. Une protection efficace ne repose pas sur un outil miracle, mais sur une approche globale qui mêle logiciels robustes, hygiène technique et discernement. Voici nos conseils pour y parvenir.

La protection de vos données ne s'improvise pas : elle commence par le choix de vos outils et se prolonge dans vos habitudes quotidiennes. Voici comment bâtir un environnement numérique robuste en 4 étapes clés.

1 PRÉPAREZ votre environnement de travail

Votre navigateur est votre première ligne de défense. Ne le laissez pas sans protection.

- **Privilégiez un navigateur axé sur la sécurité** (Ex. Brave ou Firefox configuré) : Privilégiez les options axées sur la vie privée qui bloquent les menaces avant même qu'elles n'apparaissent.
- **Ajoutez des filtres :** Installez des extensions spécialisées pour stopper les publicités malveillantes et les traceurs.
  Attention : Téléchargez toujours vos extensions sur des plateformes reconnues (Google Play Store, etc.) tout en vérifiant le nombre d'utilisateurs, la date de la dernière mise à jour et les avis.
- **La règle d'or :** Ne cliquez jamais sur « Plus tard » pour une mise à jour. Elles sont là pour boucher les failles de sécurité que les pirates adorent exploiter.

2 Adoptez les BONS RÉFLEXES sur le Web

La technique fait beaucoup, mais votre bon sens fait le reste.

- **Vérifiez la présence du petit « cadenas »** : Avant de taper le moindre mot de passe, assurez-vous que le protocole HTTPS est présent dans la barre d'adresse.
- **Restez vigilant :** Le phishing (hameçonnage) est de plus en plus sophistiqué. Au moindre doute sur un mail ou un lien, abstenez-vous de cliquer.
- **Nettoyez vos traces :** Limitez l'usage des cookies en choisissant vos préférences spécifiquement ou en refusant systématiquement les cookies pour garder le contrôle sur vos informations personnelles.

3 LE VPN : un allié à ne pas sous-estimer

Le VPN ou **Virtual Private Network ou réseau privé virtuel** sécurise le transfert de données. Il change votre géolocalisation, ne protège ni contre le phishing ni contre les virus.

- **L'utilité :** Si vous utilisez un Wi-Fi public, il vous protégera en remplaçant votre adresse IP par la sienne ;
- **Attention aux idées reçues :** Un VPN n'est pas une « cape d'invisibilité ». Si vous vous connectez à votre compte pro ou Facebook, la plateforme sait toujours qui vous êtes ;
- **La confiance avant tout :** Puisque tout votre trafic passe par ce fournisseur, choisissez-en un dont la réputation est irréprochable (Ex. Proton VPN).

4 Apprivoisez l'IA sans prendre de risques

L'Intelligence Artificielle est un assistant brillant, mais elle peut devenir une source de fuites massives si elle est mal utilisée.

- **Discipline des données :** Ne partagez jamais d'informations confidentielles (nom, prénom, adresse, mails, informations médicales, téléphone, etc.) ou de secrets de fabrication sur une IA publique. Une fois saisies, ces données ne vous appartiennent plus ;
- **Méfiez-vous des « hallucinations » :** L'IA peut affirmer des contre-vérités avec une assurance déconcertante. La vérification des informations données par l'Intelligence artificielle est primordiale ;
- **Le mot de la fin :** Considérez l'IA comme un stagiaire très rapide mais parfois étourdi : il faut **systématiquement le relire** avant de valider son travail.

Comment repérer un mail de **phishing** ?

1. Ne pas se fier à l'expéditeur :
Ne vous fiez pas au nom affiché (ex: « Support Microsoft »). Regardez l'adresse courriel réelle derrière le nom. Alerte : support@microsoft-security-fix.net au lieu de @microsoft.com.

2. Survolez les liens sans cliquer dessus :
C'est le test le plus efficace. Avant de cliquer sur un bouton ou un lien bleu, posez votre souris sur le lien (sans cliquer !). Observez, l'adresse de destination s'affiche en bas à gauche de votre écran.

3. L'urgence est une ennemie :
Les pirates jouent sur vos émotions pour vous faire perdre votre discernement. Certains mots sont suspects : « Action immédiate requise », « Compte suspendu », « Facture impayée », « Dernier avertissement ». Si un courriel vous demande de faire quelque chose de critique tout de suite, c'est probablement une tentative de manipulation.

La gestion des accès et des mots de passe doit être votre priorité

Ne pensez pas que ce sont les plus grands hackers au monde qui parviennent à pirater les mails et les profils des réseaux sociaux. Nombreux sont ceux qui profitent de VOS failles pour entrer dans votre vie numérique et voler vos données et quelle est la première de ces failles ? Elle commence souvent par un raccourci que nous prenons tous : choisir un mot de passe facile à retenir… et donc facile à pirater. Et avec l'aide de l'Intelligence artificielle, il ne faut plus 3 minutes pour pirater vos mots de passe mais 3 secondes. Découvrez comment leur rendre la vie plus compliquée.

Votre mot de passe n'est pas un simple code : c'est le premier rempart de votre identité numérique. Voici comment transformer vos accès en forteresse en 4 étapes clés.

1 La règle d'or : un mot de passe doit-être LONG ET COMPLEXE

Oubliez les prénoms ou les dates de naissance de vos proches. Oubliez le traditionnel « 1 2 3 4 ». Un logiciel de « force brute »peut craquer un code simple en quelques minutes.

- **L'objectif :** 12 caractères minimum. N'hésitez pas à le finir par un espace après le dernier caractère. Les machines ne le reconnaissent pas encore.

- **La recette :** Choisissez un proverbe, une phrase fétiche, la première phrase de votre livre ou de votre chanson préférés et prenez comme mot de passe la première phrase en y incluant des chiffres et des caractères spéciaux.
- **Le résultat :** Vous passez d'un temps de piratage de quelques secondes à... plusieurs siècles. C'est mathématique : plus c'est long, plus c'est décourageant pour le pirate.

2 EVITEZ de mettre le même mot de passe partout

Choisir le même mot de passe partout, c'est plus simple. C'est vrai mais c'est dangereux pour la protection de vos activités en ligne.

- **Le principe :** Un service = Un mot de passe unique.
- **Le bénéfice :** Si un site est piraté, vos autres comptes (banque, courriels, réseaux sociaux) restent totalement isolés et sécurisés.

Comment savoir si le mot de passe de ma messagerie a été piraté ? Encodez-le sur le site https://haveibeenpwned.com/ Si c'est le cas, même si la tentative remonte à plusieurs mois ou semaines, il est fortement recommandé de changer TOUS vos mots de passe. En effet, les informations volées circulent entre pirates sur le dark web, et d'autres cybercriminels peuvent tenter de réutiliser vos anciens identifiants sur différentes plateformes.

3 Allégez votre mémoire avec un GESTIONNAIRE de mots de passe

On ne va pas se mentir : personne ne peut retenir 50 codes complexes. C'est là qu'intervient le gestionnaire (ou coffre-fort numérique). Il permet de stocker tous vos mots de passe au même endroit, protégé par un mot de passe fort qu'il gère lui-même.

- **Il mémorise pour vous :** Plus besoin de retenir quoi que ce soit, sauf le mot de passe maître du coffre, et génère un mot de passe fort pour CHAQUE plateforme.
- **Il audite :** Il vous alerte si un de vos codes est trop faible ou a été compromis.
- **Anti-phishing :** Si vous êtes sur un faux site, le gestionnaire refusera de remplir les champs. C'est une sécurité instantanée contre les arnaques.
- **Quelques noms de gestionnaires de mots de passe :** 1Password, NordPass, Dashlane, Bitwarden, KeePass, etc.

L'authentification par double facteur : comment ça marche ?

Voici comment l'activer sur les deux plateformes les plus populaires : Facebook et Gmail. En général, toutes les plateformes ont le même fonctionnement qu'elles.

FACEBOOK : Clic sur la petite photo de profil / Paramètres et confidentialité / Paramètres / Mot de passe et sécurité / Activez l'authentification à deux facteurs et entrez votre numéro de téléphone – SMS gratuit (ou mail ou code de sauvegarde à copier ou imprimer)

GMAIL : Clic sur la photo de votre compte Google / Gérer votre compte Google / Sécurité / Dans la section comment vous connecter à Google, cliquez sur authentification à double facteur et entrez votre numéro de téléphone. Sms ou appel gratuit.

4 La DOUBLE AUTHENTIFICATION : une deuxième sécurité de taille

Même avec une serrure blindée, un deuxième verrou est toujours plus sûr. La 2FA demande une validation supplémentaire (souvent sur votre téléphone) pour se connecter.

- **À privilégier :** Les applications d'authentification (Google Authenticator, Microsoft Authenticator) ou les clés physiques.
- **À éviter si possible :** Le SMS, qui peut être détourné par des pirates expérimentés (technique du *SIM swapping*). L'idéal est de bien conserver les codes de sécurité transmis par les différentes plateformes.

La sauvegarde est l'assurance-vie de vos données

Même avec la meilleure protection, le risque zéro n'existe pas. Panne matérielle, erreur humaine ou cyberattaque… Face à l'imprévu, la survie d'une activité repose sur une stratégie de sauvegarde rigoureuse. En s'affranchissant du facteur humain, l'automatisation assure une régularité sans faille et garantit la disponibilité constante de vos informations les plus récentes. Nous allons vous guider pour que la sauvegarde devienne une simple routine.

Voici comment construire une stratégie de sauvegarde robuste en 4 piliers.

1 L'AUTOMATISATION pour ne pas oublier

L'erreur humaine est la première cause de perte de données. En automatisant vos sauvegardes, vous garantissez une régularité sans faille.

- **Connaissez-vous le versionnage ?** Il permet de remonter dans le temps pour récupérer un document sain avant une erreur de manipulation ou une corruption par un virus.
- **Programmez des sauvegardes régulièrement :** et pourquoi ne pas le faire en dehors de vos heures d'utilisation ?
- **N'oubliez pas de déconnecter les back-ups externes** dès que la sauvegarde est finie.

2 Adopter la RÈGLE D'OR du « 3-2-1 »

Cette méthode est mondialement connue :

- **Faites 3 versions de vos données** (l'original + deux sauvegardes).
- **Sur 2 supports différents** (par exemple : un serveur local et un disque dur – Attention : un disque dur a aussi une durée de vie limitée).
- **& 1 copie hors site** (dans un Cloud sécurisé) pour parer aux sinistres physiques comme les incendies.

La méthode GFS (« Grandfather-Father-Son » ou « Grand-père – Père – Fils ») est une stratégie de rotation des sauvegardes qui organise les copies de données selon trois cycles : quotidien (fils), hebdomadaire (père) et mensuel (grand-père). Cette approche permet de conserver un historique des sauvegardes sur une longue période tout en limitant l'espace de stockage nécessaire.

3 Verrouiller la CONFIDENTIALITÉ

Une sauvegarde volée ne doit pas devenir une fuite de données.

- **Chiffrement :** Activez systématiquement le chiffrement de vos sauvegardes. Vos fichiers deviennent illisibles sans la clé.
- **La clé de récupération :** C'est votre filet de sécurité. Stockez-la précieusement dans un gestionnaire de mots de passe ou un coffre-fort physique. Sans elle, même vous ne pourrez plus accéder à vos données.

4 TESTER avant d'avoir des problèmes

Une sauvegarde n'a de valeur que si elle fonctionne réellement. C'est le principal conseil que vous devez garder en tête.

- **Chaque trimestre :** Testez la restauration de quelques fichiers au hasard.
- **Chaque année :** Simulez une restauration complète de votre système.

L'œil de l'expert : Faites auditer votre stratégie par un prestataire externe. Un regard neutre permet d'identifier les failles invisibles de l'intérieur.

Comment choisir un bon antivirus ?

Le site **https://www.av-test.org/fr/** a été créé par un institut de recherche allemand indépendant dédié à la sécurité informatique, actif depuis plus de 20 ans. Ses experts réalisent des tests de qualité sur divers produits de sécurité informatique au niveau international. Le site propose un comparatif détaillé des logiciels, basé sur des protocoles de test rigoureux, sans influence de sponsors. Les utilisateurs peuvent choisir entre des solutions gratuites ou payantes en fonction de leurs besoins, telle que la protection d'un ou plusieurs appareils.

Ne sous-estimez pas le poids de l'humain dans les problèmes de Cybersécurité

L'humain est votre meilleur bouclier contre les cybermenaces.
En cybersécurité, le calme plat n'est pas une garantie d'immunité. Si les outils techniques sont indispensables, c'est votre sensibilisation ainsi que celle proposée à vos collaborateurs qui constituent la première ligne de défense de l'entreprise.

Voici comment transformer la vigilance en 4 étapes.

1 Déjouer les ERREURS HUMAINES

L'humain est souvent la cible préférée des pirates. Pour ne pas se laisser surprendre, l'information est votre meilleure arme :

- **Restez aux aguets :** Consultez régulièrement le site Safeonweb pour connaître les campagnes de phishing en cours et parlez-en autour de vous ;
- **Formez-vous :** Utilisez les guides pratiques du CCB pour apprendre à détecter les fraudes ;

Avez-vous pensé au **super administrateur** ?

Lorsque vous téléchargez des applications ou des logiciels, il est essentiel de maîtriser qui a le pouvoir de les installer. La création d'un compte super administrateur sur chaque ordinateur de la maison peut vous offrir un contrôle total du système. Ce rôle permet de gérer les fichiers critiques, d'installer ou de désinstaller des programmes sans restriction, et de configurer les droits des autres utilisateurs.

En environnement partagé, au travail comme à la maison, ce compte garantit que les utilisateurs non autorisés ne peuvent pas effectuer des modifications risquées, renforçant ainsi la sécurité comme l'installation de n'importe quelle application. Il est aussi crucial en cas de problème technique, car il permet de réparer des fichiers corrompus ou de désinstaller des logiciels malveillants. Avec des paramètres de sécurité renforcés, un mot de passe robuste, et une gestion centralisée des accès, le super administrateur protège le système contre des intrusions. Toutefois, prudence : un tel accès doit être bien sécurisé pour éviter tout risque de mauvaise manipulation ou d'intrusion non désirée.

- **Automatisez votre veille :** Abonnez-vous aux newsletters spécialisées pour passer d'une posture subie à une posture proactive.

2 Harmoniser les RÉFLEXES en interne

La sécurité ne doit pas être une question d'interprétation personnelle. Pour éviter les failles évitables, structurez vos usages :

- **La charte informatique :** Établissez des règles claires, partagées et acceptées par tous.
- **Le guide des bonnes pratiques :** Un document simple qui récapitule les gestes quotidiens (mots de passe, verrouillage de session, usage des clés USB).

3 Créer un PLAN DE RÉPONSE aux Incidents (PRI)

Ne subissez pas l'incident, gérez-le. Un « Plan de Réponse aux Incidents » (PRI) permet de réagir rapidement et méthodiquement pour minimiser l'impact d'une cyberattaque. C'est l'équivalent d'un plan d'évacuation en cas d'incendie. Un bon PRI inclut :

- **Détection et analyse :** Identification rapide de l'incident, évaluation de l'ampleur, des systèmes touchés et des personnes concernées.
- **Confinement et éradication :** Isolation des systèmes compromis pour limiter la propagation et suppression des éléments malveillants.
- **Restauration :** Récupération des données à partir de sauvegardes sécurisées, achats de nouvelles machines ou systèmes et reprise des activités.
- **Apprentissage et amélioration :** Analyse post-incident pour comprendre l'attaque et renforcer les défenses.

4 L'ASSURANCE contre les cyber-risques peut être un filet de sécurité

Même avec la meilleure défense, le risque zéro n'existe pas. L'assurance cyber-risques est votre dernier rempart pour :

- Couvrir les pertes d'exploitation et les frais de restauration.
- Accéder immédiatement à des **experts en gestion de crise** et des conseils juridiques.

Votre premier réflexe doit être régional : ce sont les aides les plus accessibles pour vous.

Le guide complet des aides publiques en cybersécurité en Wallonie, à Bruxelles et au niveau européen

Face à la recrudescence des cyberattaques, les pouvoirs publics ont mis en place des dispositifs de soutien pour accompagner les entreprises. Ces aides s'articulent autour de trois besoins clés : le conseil et le diagnostic (audit de vulnérabilité), la formation (montée en compétences des équipes) et le soutien financier (primes, prêts et incitants fiscaux).

En Belgique, le soutien aux entreprises est réparti entre plusieurs niveaux de pouvoir. Comprendre leur rôle respectif vous aidera à savoir où chercher en premier :

- **Les aides au niveau régional** prennent la forme d'aides directes, de subsides, de formations et d'accompagnement (ex.: Chèques-Entreprises, VLAIO, Hub.Brussels).
- **Les aides au niveau national** prennent la forme de sensibilisation et d'incitants fiscaux (ex. : Safeonweb, déduction fiscale majorée).
- **Les aides européennes** prennent la forme de projets plus larges, innovants ou collaboratifs souvent à destination de PME déjà plus matures (ex. : CYSSME, Digital Europe Programme)

Votre premier réflexe doit être régional : ce sont les aides les plus accessibles pour vous.

Les aides en Wallonie

La Wallonie a fait des « chèques entreprises » la colonne vertébrale de sa stratégie de promotion de la cybersécurité. Elle se concentre sur le subventionnement de conseils d'experts labellisés. L'approche est très fluide : vous commencez par un audit ciblé avec le chèque « Cybersécurité » (qui couvre 75 % des coûts avec un maximum de 10.000 €) ou par un diagnostic plus large avec le chèque « Maturité numérique ». Une fois ce plan d'action établi, vous avez à votre disposition le prêt (avantageux) « Digit Online » (de Wallonie Entreprendre) qui permettra de financer l'achat de matériel ou de logiciels spécifiques. Ce prêt subordonné est à taux préférentiel avec un maximum de 75.000 €.

Vous pouvez également former vos employés à la cybersécurité : le Forem propose des aides pour des formations certifiantes.

Les aides en Région de Bruxelles – Capitale

Le modèle bruxellois est simple et logique : commencez par un « Digital First Coaching » (proposé par hub.brussels) pour obtenir un diagnostic gratuit, puis utilisez la « Prime à la digitalisation » pour financer directement les solutions recommandées.

La « Prime à la digitalisation » de la Région de Bruxelles-Capitale soutient l'acquisition d'équipements informatiques, de logiciels (CRM, Cloud) et d'outils de cybersécurité (pare-feu, antivirus). L'intervention varie entre 25 % et 70 % selon la taille de l'entreprise.

A Bruxelles, vous pouvez aussi bénéficier de prêts alternatifs si vous ne souhaitez pas passer par votre organisme bancaire. Le « Prêt Proxi » permet ainsi à des particuliers (proches, clients) de prêter à une entreprise bruxelloise en bénéficiant d'un avantage fiscal (crédit d'impôt).

Comment savoir de quelle région, je dépends ?

Ces aides sont attribuées en fonction du siège d'exploitation ou du siège social de votre activité. Pour cela, elle doit être enregistrée à la Banque Carrefour des entreprises (BCE) et être active dans la région concernée (Wallonie, Bruxelles et Flandre) pour bénéficier des aides.

vous souhaitez former vos employés, sachez qu'Actiris peut prendre en charge jusqu'à 100 % des frais de formation en technologies de l'information et de la communication (TIC). Digitalcity.brussels est un autre pôle formation-emploi des métiers du numérique mis à votre disposition.

Les aides au niveau fédéral

Ses deux actions principales sont :

La sensibilisation au travers des plateformes Safeonweb et du Centre pour la Cybersécurité Belgique (CCB) pour obtenir des conseils pratiques, des alertes de sécurité et des outils de prévention accessibles à tous les citoyens et entreprises.

L'incitant fiscal : Indépendamment des primes régionales, le gouvernement fédéral propose une déduction fiscale majorée pour les investissements numériques, ce qui inclut spécifiquement la sécurité des données et des réseaux via le SPF Finances.

Les aides au niveau européen

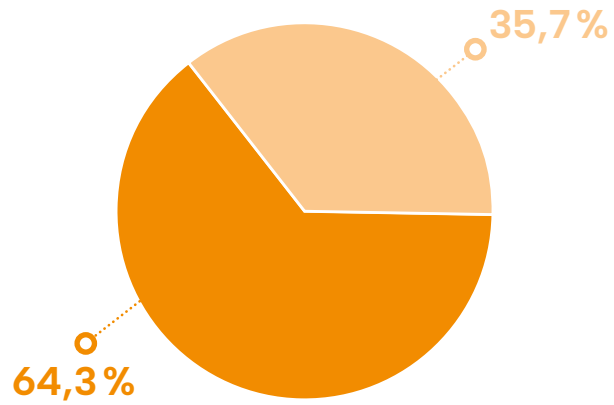
Ces aides complètent les autres offres en se concentrant sur la sensibilisation générale et sur des projets de plus grande envergure. Parmi elles, la CYSSME (Cybersecurity for SMEs). Ce parcours entièrement pris en charge pour les PME de moins de 250 employés, inclut un audit, un plan d'action et un accompagnement par des experts. C'est une solution idéale pour une entreprise qui souhaite structurer sa stratégie de cybersécurité de A à Z avec un encadrement de qualité. Il offre un accompagnement structuré (audit et outils) pouvant aller jusqu'à 20.000 € financés sans coût direct pour l'entreprise sélectionnée. Pour des projets de recherche plus ambitieux, il existe les programmes Digital Europe et Horizon Europe.

Votre avis compte

Afin d'évaluer l'expérience des participants et l'impact du projet, une enquête de satisfaction est proposée aux indépendants et aux PME ayant pris part au Cyber Challenge. Cette démarche permet de recueillir le retour des indépendants et des PME ayant pris part au programme afin d'évaluer la qualité de l'accompagnement proposé, la pertinence des recommandations en cybersécurité et l'utilité des outils mis à disposition. Les réponses collectées contribuent également à identifier les points d'amélioration et à adapter le projet afin de répondre au mieux aux besoins réels des entrepreneurs face aux défis numériques et aux risques cyber.

Les premiers résultats de cette enquête mettent en évidence un niveau de satisfaction très positif parmi les participants. **Plus de 60 % des répondants déclarent recommander le programme sans hésitation à d'autres indépendants**, ce qui témoigne de l'intérêt et de la pertinence de l'accompagnement proposé dans le cadre du Cyber Challenge.

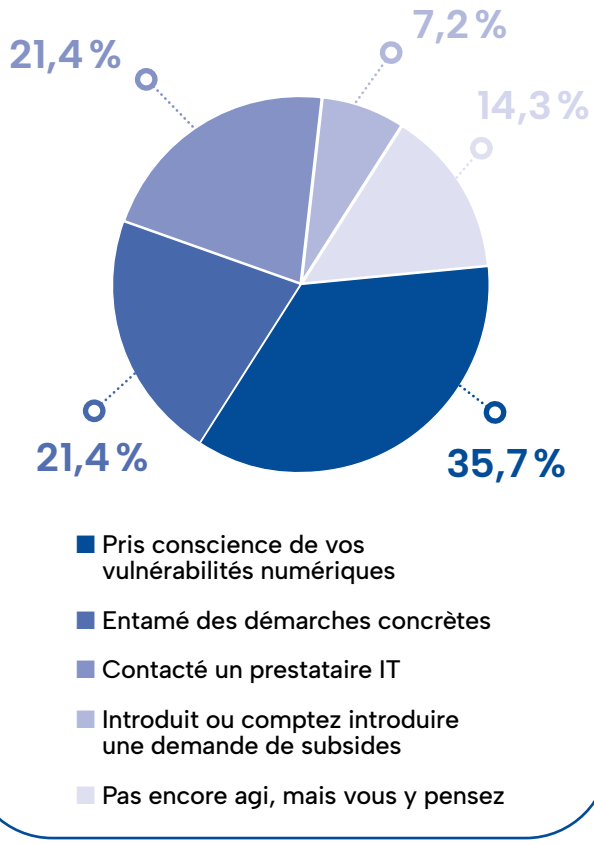
Recommanderiez vous ce programme à d'autres indépendants ?



Ces retours confirment l'un des objectifs principaux du projet : permettre aux indépendants et aux PME de mieux comprendre les risques numériques auxquels ils sont exposés et les encourager à adopter des mesures concrètes pour sécuriser leur environnement numérique.

L'enquête met également en évidence l'impact du programme sur la sensibilisation des entrepreneurs aux enjeux de cybersécurité. **Plusieurs participants indiquent avoir pris conscience de leurs vulnérabilités numériques et avoir engagé ou envisagé des démarches afin de renforcer la protection de leur activité et de leurs données.**

À la suite du programme, vous avez



Nous remercions l'ensemble des participants qui ont pris le temps de partager leur expérience. Leurs retours constituent un élément essentiel pour améliorer en continu le projet et renforcer l'accompagnement proposé aux entrepreneurs dans la protection de leur activité.

Le cyberscan

Les cyberattaques sont de plus en plus répandues dans notre monde numérisé. Et aucune PME ni indépendant n'est à l'abri. Plus d'une PME belge sur cinq a déjà été victime d'un incident de sécurité informatique !

C'est pourquoi le SPF Economie a lancé depuis 2022 le Cyberscan.

Spécialement conçu pour les petites entreprises et les indépendants dans un langage accessible, cet outil permet de faire le point sur votre niveau de cybersécurité au travers de huit modules :

1. INVENTORIER et ANALYSER : faites le point sur votre situation ;
2. Disposer des PROCÉDURES adéquates : faites un plan ;
3. SENSIBILISER : votre plan en pratique ;
4. Attribuer les RÔLES-CLÉS : répartissez les responsabilités ;
5. Système de DÉFENSE : déployez les bons outils ;
6. SAUVEGARDER : faites des copies de secours ;
7. Mettre À JOUR : restez préparé ;
8. ÉVALUER : utilisez au mieux vos ressources disponibles.

Pour chacun des modules, vous recevrez des conseils adaptés à votre situation, une check-list et un guide téléchargeable pour les mettre en œuvre.

Ne vous faites pas avoir par les hackers, faites le Cyberscan sur https://economie.fgov.be/fr/cyberscan !

STARTER | INDÉPENDANT | COMMERÇANT | PME | ARTISAN | PROFESSION LIBÉRALE

Le SNI accompagne TOUS les indépendants dans tous leurs choix

DÉFENSE INDIVIDUELLE & **DÉFENSE COLLECTIVE**

NOUS PRENONS À COEUR LES DROITS ET INTÉRÊTS DE CHAQUE INDÉPENDANT ET CHEF D'ENTREPRISE

- CONSEIL JURIDIQUE, SOCIAL ET FISCAL
- ASSISTANCE JURIDIQUE
- RÉCUPÉRATION DE CRÉANCES
- PROBLÈMES DE PERSONNEL
- CONTRATS SUR MESURE
- AIDE AUX STARTERS
- SUBSIDES
- OUTILS RGPD
- MAGAZINE
- INFOSESSIONS ET WEBINAIRES
- NETWORKING
- RÉDUCTIONS ET AVANTAGES
- PROGRAMME DIGITAL COMMERCE
- PROGRAMME BECYBERSAFE
- PROGRAMME PROCOMMERCE

Et bien plus encore !

CONTACT ?

Nous sommes accessibles au **02 308 21 08** ou **info@sninet.be.**
Un de nos collaborateurs vous rencontrera afin de répondre à toutes vos questions.
Faisons connaissance en visitant notre site grâce au QR code suivant.

www.sninet.be @SNIwallobrux @ SNI_be @ SNI_communication
SNI - Syndicat neutre pour indépendants @ SNI_be