Etes-vous Cybervigilant ?

Cybersecurity, la responsabilité de chacun

En route.
Vers mieux.

Contenu

Introduction

1. Pourquoi la cybersécurité est importante pour la SNCB ?

Le succès et la continuité des services de la SNCB dépendent en grande partie du **bon fonctionnement des systèmes d'information**. Ces systèmes constituent le cœur de notre organisation : ils collectent, stockent, traitent et diffusent des informations essentielles à notre fonctionnement quotidien. Cependant, ce pouvoir s'accompagne également de responsabilités. Si ces systèmes sont utilisés de manière abusive ou sont **insuffisamment protégés, les conséquences peuvent être graves** :

- Des informations confidentielles peuvent être divulguées ;
- Des données peuvent être modifiées ou détruites par inadvertance ;
- Des systèmes peuvent devenir temporairement ou même durablement inutilisables.

De tels incidents entraînent non seulement des risques financiers et juridiques, mais peuvent également nuire gravement à la confiance envers la SNCB et à notre image.

2. Vous êtes notre pare-feu humain !

A la SNCB, nos spécialistes IT mettent tout en œuvre pour protéger nos systèmes d'information. Ils construisent des murs numériques, installent des logiciels de protection et surveillent les activités suspectes. Mais même la meilleure technologie ne suffit pas sans un maillon essentiel : **vous.**

Chaque collègue est un maillon indispensable de notre cybersécurité. Vous êtes notre pare-feu humain, la première ligne de défense contre les fuites de données, les abus et les cyberattaques. Car même si nos systèmes sont parfaitement sécurisés, un seul moment d'inattention peut avoir de graves conséquences. Pensez à votre nom d'utilisateur et à votre mot de passe : ils vous donnent accès à des informations sensibles telles que les données clients, les systèmes techniques ou les documents internes.

Si vous laissez traîner ces données, si vous laissez votre appareil sans surveillance ou si vous ne respectez pas les directives, vous risquez, souvent sans le vouloir, de compromettre le fonctionnement de la SNCB.
C'est pourquoi il est important de rester vigilant, de suivre **les règles de sécurité** et de signaler immédiatement toute situation suspecte. Ensemble, nous veillons à la sécurité de nos informations, à la fiabilité de nos systèmes et au maintien de la confiance dans la SNCB.

La cybersécurité ne commence pas avec le service informatique, mais à chaque clic que vous effectuez.

Grâce à votre vigilance, vos connaissances et votre bon sens, vous empêchez les cyberattaques avant qu'elles ne causent des dégâts.

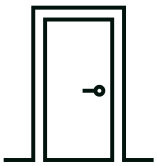
Vous êtes un maillon indispensable, notre ‘pare-feu humain’.

Etes-vous cybervigilant ?

Suivez le guide !

Thème 1 :
Un lieu de travail sécurisé

> Empêchez tout accès non autorisé



La sécurité de nos systèmes d'information commence par l'**accès physique** à nos bâtiments et lieux de travail. Les personnes non autorisées ne peuvent pas obtenir l'accès aux bâtiments, aux zones de travail et au matériel de travail de la SNCB. Un seul moment d'inattention peut conduire à la consultation d'informations sensibles qui traînent sur les bureaux, au vol, à la modification ou à la perte de données sensibles.

C'est pourquoi il est crucial que seules les **personnes autorisées** aient accès à nos locaux. Vous jouez un rôle clé à cet égard. En adoptant quelques habitudes simples, vous contribuerez à protéger nos informations, nos collègues et notre infrastructure

Qu'attendons-nous de vous ?

- **Ne laissez personne entrer en même temps que vous dans une zone sécurisée.** Le tailgating, c'est lorsqu'une personne sans autorisation vous suit dans une zone sécurisée sans utiliser son propre badge — même si elle semble familière ou amicale.
  - Les collègues doivent également utiliser leur propre badge.
  - Fermez la porte derrière vous, même si quelqu'un vous suit de près.
- **Accompagnez toujours personnellement les visiteurs.**
  - Ne laissez jamais les visiteurs se promener seuls.
  - Signalez les visiteurs à l'accueil ou à la sécurité.
- **Fermez les portes et les portails derrière vous.**
  - Ne laissez aucune porte ouverte, même 'pour un instant'.
  - Vérifiez que les portes automatiques se ferment effectivement.
- **Utilisez correctement votre badge.**
  - Ayez toujours votre badge à portée de main.
  - Ne prêtez jamais votre badge et ne le laissez pas sans surveillance.
- **Adressez-vous aimablement aux personnes sans badge.**
  - Demandez-leur si vous pouvez les aider et orientez-les vers l'accueil.
- **Signalez immédiatement les incidents ou les situations suspectes.**

Thème 1 :
Un lieu de travail sécurisé

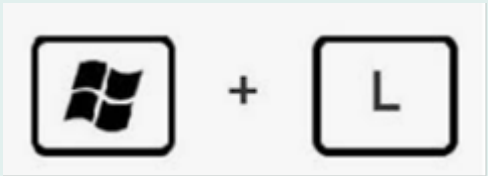
> Un lieu de travail bien rangé est un lieu de travail sûr

Un lieu de travail bien rangé ne se limite pas à une impression de propreté, c'est **un élément essentiel de la sécurité de l'information**. Les documents confidentiels laissés sur les bureaux, les imprimantes ou dans les corbeilles à papier peuvent facilement être vus ou pris par des personnes non autorisées. Les données numériques stockées sur des appareils non surveillés ou des clés USB présentent également un risque.

En adoptant une attitude responsable sur votre lieu de travail, vous contribuez à **protéger les informations sensibles et à prévenir les fuites de données**.

Qu'attendons-nous de vous ?

- **Ne laissez traîner aucun document confidentiel.**
  Rangez-les dans une armoire, un tiroir ou un casier fermant à clé.
- **Récupérez directement les documents imprimés à l'imprimante**. Ne laissez rien à la vue d'autrui.
- **Détruisez correctement les documents sensibles.**
- **Ne laissez jamais un appareil (ordinateur, ordinateur portable, etc.) sans surveillance.**. Verrouillez votre appareil chaque fois que vous vous absentez. Utilisez les touches "**Windows + L**" sur votre clavier.



- **Ne laissez pas de clés USB ou de disques durs externes sans surveillance**. Conservez-les en lieu sûr, sous clé, ou emportez-les avec vous.

Thème 2 :
Sécurisez vos appareils (mobiles)

> Sécurisez le matériel informatique

A la SNCB, vous disposez d'un matériel informatique professionnel tel qu'un **ordinateur portable**, un **smartphone** ou une **tablette**. Ces appareils sont préconfigurés correctement par nos équipes informatiques afin que vous puissiez **travailler en toute sécurité et efficacement**.

Mais la sécurité ne s'arrête pas à l'installation. Vous jouez également un rôle crucial dans la protection de votre appareil et des données de l'entreprise. Une utilisation négligente ou des modifications personnelles peuvent entraîner des dysfonctionnements, des pertes de données, voire des incidents de sécurité.

Qu'attendons-nous de vous ?

- **Téléchargez les applications uniquement à partir des app stores officiels.** N'installez jamais de logiciel ou de matériel de votre propre initiative. Demandez toujours l'approbation au service IT.
- **Ne modifiez pas votre appareil** : Le débridage (jailbreak), qui consiste à modifier, contourner ou supprimer les restrictions de sécurité, rend votre appareil très vulnérable.
- **N'ignorez pas les avertissements,** veillez à ce que votre appareil et vos applications soient toujours à jour. Connectez votre ordinateur portable au réseau de la SNCB au moins une fois par mois pour les mises à jour, les sauvegardes et la synchronisation.
- **Verrouillez toujours votre appareil**, même si vous ne vous absentez qu'un instant. Sur votre PC : utilisez la combinaison de touches icône Windows + L. Sur votre smartphone ou tablette : définissez un verrouillage de l'écran dans les paramètres.
- **Prévoyez des données de contact en cas de perte** : indiquez un numéro de téléphone sur votre appareil afin que l'on puisse vous contacter en cas de perte (ne faites pas référence à la SNCB).
- **N'utilisez pas d'ordinateur ou d'ordinateur portable personnel pour un usage professionnel** : vous ne pouvez pas utiliser votre propre appareil pour accéder aux applications M365 de la SNCB ou aux données de l'entreprise. Travaillez exclusivement avec le matériel qui vous a été fourni par la SNCB.
- **Signalez immédiatement toute perte ou vol :** contactez directement IT Service Desk > **02/607 33 00.**

Thème 2 :
Sécurisez vos appareils (mobiles)

> Utilisez des mots de passe forts et longs que vous changez régulièrement

Votre **mot de passe** est plus qu'un code : c'est la **clé de tout**. Il donne accès à votre appareil, au réseau et aux systèmes de la SNCB. Un mot de passe faible, c'est comme une clé laissée sous un paillasson : facile à trouver et rapidement utilisé à mauvais escient. Les mots de passe basés sur des informations personnelles telles que votre nom, votre date de naissance ou ce que vous partagez sur les réseaux sociaux sont particulièrement vulnérables. Parfois, un mot de passe seul ne suffit pas. C'est pourquoi nous utilisons **l'authentification à deux facteurs (2FA)** : un contrôle supplémentaire par SMS, itsme ou B-Key. La 2FA complique considérablement la tâche des hackers, même si votre mot de passe est volé.

Qu'attendons-nous de vous ?

- **Utilisez des mots de passe forts et longs** que vous changez régulièrement.
  Un mot de passe doit remplir au moins trois des conditions suivantes :
  - contenir au moins 1 lettre majuscule ;
  - contenir au moins 1 lettre minuscule ;
  - contenir au moins 1 chiffre ;
  - contenir au moins un caractère spécial (~!@#$%^&*_-+=`|(){}[]:'";<>,.\/). Un espace est également un caractère spécial.
- **Utilisez un mot de passe différent pour chaque application ou site internet**. Cela permet de limiter les dégâts si un mot de passe venait à être piraté.
- **Protégez correctement votre mot de passe.** Ne l'écrivez pas et ne le conservez pas à proximité de votre appareil. Ne le communiquez jamais à d'autres personnes, pas même à votre famille, à vos collègues ou à IT-support. Votre mot de passe est strictement personnel !
- **Activez l'authentification à deux étapes**. A la SNCB, cela se fait via B-Key, Itsme ou un certificat.
- **Vous pensez que votre mot de passe a été volé ? Modifiez immédiatement tous vos mots de passe !**

Conseil : **Choisissez une phrase complète facile à retenir,** par exemple:

'"Ma 1ère voiture était une Opel Corsa rouge." Grâce à la combinaison de différents caractères et l'utilisation d'espaces, il s'agit d'un mot de passe long et fort. Facile à retenir pour vous et plus difficile à pirater.

Thème 2 :
Sécurisez vos appareils (mobiles)

> En déplacement ? Soyez vigilant !

Lorsque vous travaillez en dehors du bureau ou à domicile, vous êtes moins bien protégé. Vous utilisez plus souvent des réseaux non sécurisés et vous avez moins de contrôle sur votre environnement. Cela vous rend plus vulnérable aux **risques numériques** tels que :

- le vol ou la perte de votre appareil – sans une bonne sécurité, des informations sensibles peuvent tomber entre de mauvaises mains ;
- la mise sur écoute de votre connexion – les hackers peuvent intercepter vos communications à votre insu via le Wi-Fi public ;
- le social engineering – il s'agit de faux appels téléphoniques ou de questions trompeuses visant à obtenir des informations confidentielles.

Nos équipes techniques assurent une connexion sécurisée, mais il est important que vous suiviez également les règles de sécurité appropriées lorsque vous êtes en déplacement afin de protéger les données de la SNCB.

Qu'attendons-nous de vous ?

- **Assurez-vous que votre appareil est à jour avant de partir.**
- **Ne laissez jamais votre appareil sans surveillance.**
- **Gardez votre appareil hors de vue dans la voiture et près de vous dans les transports en commun.**
- **Utilisez toujours le VPN de la SNCB.** Votre trafic Internet est ainsi chiffré – sécurisé, même en déplacement.
- **Évitez les réseaux Wi-Fi publics ou non sécurisés.**
- **Désactivez les connexions inutilisées** (telles que le Wi-Fi ou le Bluetooth)**.**
- **Ne laissez personne regarder votre écran ou pendant que vous tapez votre mot de passe.**
- **Soyez discret lors de vos appels téléphoniques** – les informations confidentielles n'ont pas leur place dans la rue.
- **Si vous voyagez en dehors de l'UE, que vous avez utilisé votre ordinateur portable ou votre appareil portable et que vous soupçonnez que votre appareil a été piraté**, veuillez demander au IT Service Desk d'inspecter votre appareil avant de vous reconnecter au réseau SNCB.
- **Signalez immédiatement la perte ou le vol de votre appareil au IT Service Desk.** > **02/607 33 00.**

Thème 3 :
Sécurisez vos informations

> Droits d'accès : seuls ceux qui en ont besoin y ont accès

Tout le monde ne peut pas avoir accès à toutes les informations, applications ou systèmes de la SNCB. Et ce, pour une bonne raison : un accès non autorisé peut entraîner la fuite, la modification ou même la destruction de données sensibles. Qu'il s'agisse d'informations sur les clients, de systèmes techniques ou de documents internes : une erreur peut avoir des conséquences importantes.

C'est pourquoi l'accès est strictement réservé aux **collaborateurs autorisés** et uniquement lorsque cela est nécessaire à l'exercice de leurs fonctions.

Les droits d'accès doivent être clairement **justifiés** et officiellement **approuvés** par le chef immédiat de l'utilisateur.

Qu'attendons-nous de vous ?

- **N'utilisez jamais le login de quelqu'un d'autre**, même avec son autorisation. Votre compte est strictement personnel.
- **Ne partagez aucune information confidentielle avec des personnes non autorisées**, y compris votre famille, vos amis ou des collègues qui n'y ont pas accès.
- Vous êtes responsable ou gestionnaire ? **Ne donnez accès qu'aux personnes qui en ont vraiment besoin pour exercer leurs fonctions. Vérifiez régulièrement vos accès**.
- **Vous remarquez quelque chose de suspect ? Signalez-le immédiatement auprès de l'IT Service Desk et changez votre mot de passe.**

Thème 3 :
Sécurisez vos informations

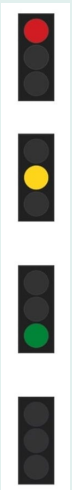
> Classification des données : savoir ce que l'on partage

À la SNCB, nous traitons chaque jour **des informations précieuses**. Qu'il s'agisse de plans techniques ou de données sur les clients, ces données sont essentielles à notre fonctionnement et à notre réputation. Mais toutes les informations ne peuvent pas être partagées librement. Il est donc important de savoir quelles sont les données sensibles et comment les traiter en toute sécurité.

Grâce à **la classification des données**, nous nous assurons que les informations soient traitées de manière appropriée. C'est une façon intelligente de réduire les risques, de respecter la législation et de collaborer de manière professionnelle. Et vous jouez un rôle important à cet égard.

Qu'attendons-nous de vous ?

- **Classifiez et traitez correctement les informations :** Classez correctement les informations lors de la création, du stockage ou du partage de documents. **Utilisez les étiquettes suivantes, conformément au protocole TLP** (Traffic Light Protocol, également appelé « protocole du feu tricolore ») **:**



TLP:RED (Secret) : Le contenu est très sensible, destiné à un groupe très restreint et ne peut être partagé avec d'autres sans l'approbation du propriétaire du contenu.

TLP:AMBER (Confidentiel) : Le contenu est réservé à un groupe désigné et ne peut être partagé avec d'autres sans l'approbation du propriétaire du contenu, et uniquement selon le principe du besoin de savoir. Pour un usage interne uniquement, l'étiquette **TLP:AMBER+STRICT** peut être appliquée, ce qui implique que l'information ne peut pas être partagée avec des clients externes.

TLP:GREEN (Interne) : Le contenu est destiné à un groupe au sein de la SNCB et de ses filiales, mais peut être partagé avec d'autres personnes au sein de la SNCB et de ses filiales ou – avec l'approbation de la direction – avec un groupe externe limité.

TLP:CLEAR (Public) : Le contenu peut être divulgué à toute personne, y compris en dehors de la SNCB et de ses filiales.

- **Sauvegardez les informations en toute sécurité :** utilisez uniquement des emplacements de stockage approuvés tels que M365 (SharePoint, Teams). L'utilisation de clés USB ou de services de stockage cloud personnels n'est pas autorisée, car aucune sauvegarde des données locales n'est possible.
- **Soyez vigilant lorsque vous partagez des informations :** vérifiez toujours que le destinataire est autorisé à recevoir les informations.

> Utilisez les e-mails de manière sûre et professionnelle

L'e-mail est **un moyen de communication incontournable au sein de la SNCB**. Nous l'utilisons quotidiennement pour partager des informations, collaborer et améliorer nos services. Cependant, l'e-mail comporte également des risques. Afin de protéger nos réseaux et nos données, la SNCB se réserve le droit de filtrer et de contrôler les e-mails pour s'assurer de leur utilisation **correcte et légale**.

Les e-mails ne sont pas toujours sécurisés. Ils peuvent contenir des virus, être accompagnés de pièces jointes dangereuses ou être utilisés à des fins d'hameçonnage. Les spams et les messages frauduleux peuvent également surcharger le système et le rendre temporairement inutilisable. Il est donc crucial que nous soyons tous **vigilants** et **responsables dans nos échanges d'e-mail**.

Qu'attendons-nous de vous ?

- **Signalez immédiatement les e-mails suspects** ou les tentatives d'hameçonnage via le bouton "Signaler le message" dans Outlook ou via l'IT Service Desk.
- **Utilisez votre compte belgiantrain exclusivement à des fins professionnelles.**
- **Utilisez toujours le système d'e-mail officiel de la SNCB.**
- **Soyez prudent lorsque vous transférez des informations confidentielles.**
- **N'ouvrez pas les messages ou les pièces jointes suspects,** en particulier ceux provenant d'expéditeurs inconnus.
- **N'envoyez pas d'e-mails inappropriés** (par exemple, contenant du contenu discriminatoire, pornographique ou illégal).
- **N'envoyez pas de chaînes de mails** – elles ne proviennent pas de la SNCB et n'ont pas leur place dans nos boîtes mail.

Thème 3 :
Sécurisez vos informations

> Surfez sur internet en toute sécurité

À la SNCB, **l'utilisation sécurisée d'internet** n'est pas un luxe, mais une nécessité absolue. Chaque clic compte. Afin de garantir la fiabilité et la sécurité de notre réseau, la SNCB se réserve le droit de filtrer et de contrôler le trafic internet pour vérifier qu'il est utilisé de manière légale et correcte.

Une navigation imprudente peut avoir de graves conséquences :

- En publiant des messages sur des forums ou dans des chats, vous risquez d'être inondé de spams.
- Le téléchargement de logiciels provenant de sites internet non fiables peut entraîner l'installation de virus ou de spywares sur votre appareil.
- Les logiciels malveillants peuvent divulguer des informations confidentielles et entraîner des fuites de données.
- Un seul appareil infecté peut mettre en danger l'ensemble du réseau SNCB.
- Une navigation inappropriée peut entraîner des coûts élevés, une perte de temps et une atteinte à la réputation.

Une utilisation sûre d'internet protège non seulement votre appareil, mais aussi les données, les systèmes et l'image de la SNCB.

Qu'attendons-nous de vous ?

- **Utilisez Internet uniquement à des fins professionnelles avec votre appareil de la SNCB.**
- **Ne visitez que des sites internes fiables.**
- **Soyez attentif au hameçonnage : les sites internet frauduleux peuvent être très réalistes.**
- **Ne partagez pas d'informations confidentielles ou professionnelles sur des forums ou dans des chats publics.**
- **Ne téléchargez pas ou ne partagez pas de fichiers illégaux (tels que des films, de la musique ou des logiciels).**
- **N'effectuez aucune action susceptible d'endommager les systèmes de la SNCB.**
- **Ne jouez pas à des jeux sur votre appareil de travail.**
- **N'installez pas de logiciels ou d'applications sans autorisation.**
- **Ne visitez pas de sites internet inappropriés ou illégaux.**

Thème 3 :
Sécurisez vos informations

> Clé USB, disque dur ou carte mémoire ? Ne les branchez jamais !

Les clés USB, les disques durs externes et les cartes mémoire – également connus sous le nom de supports amovibles – semblent pratiques, mais constituent un risque sérieux pour la sécurité. Ils peuvent être perdus, volés ou contenir des logiciels malveillants qui peuvent compromettre votre appareil et nos systèmes.

Pour éviter les fuites de données et des virus informatiques, **vous n'êtes pas autorisé à utiliser des supports amovibles**, à moins d'avoir reçu l'autorisation explicite du service informatique.

Qu'attendons-nous de vous ?

- **Vous avez trouvé une clé USB ?** Ne la branchez jamais. Apportez-la directement à votre service informatique local.
- **Ne sauvegardez pas de données confidentielles sans sécurité** (mot de passe ou cryptage).
- **N'utilisez pas de supports non sécurisés pour partager des informations sensibles.**

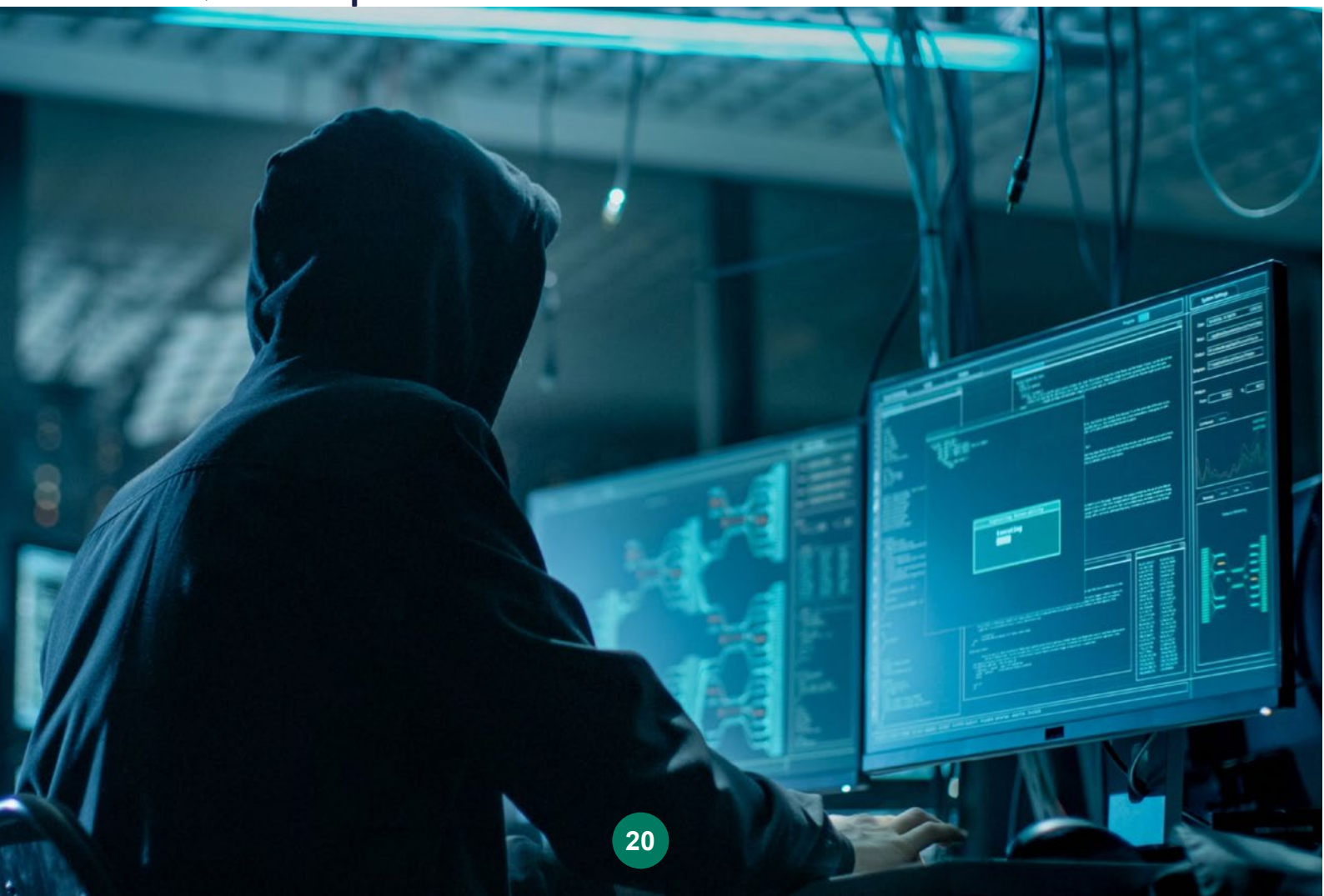
Thème 4 :
Signalez immédiatement tous les (cyber)incidents éventuels

> Signalez immédiatement tous les (cyber)incidents éventuels

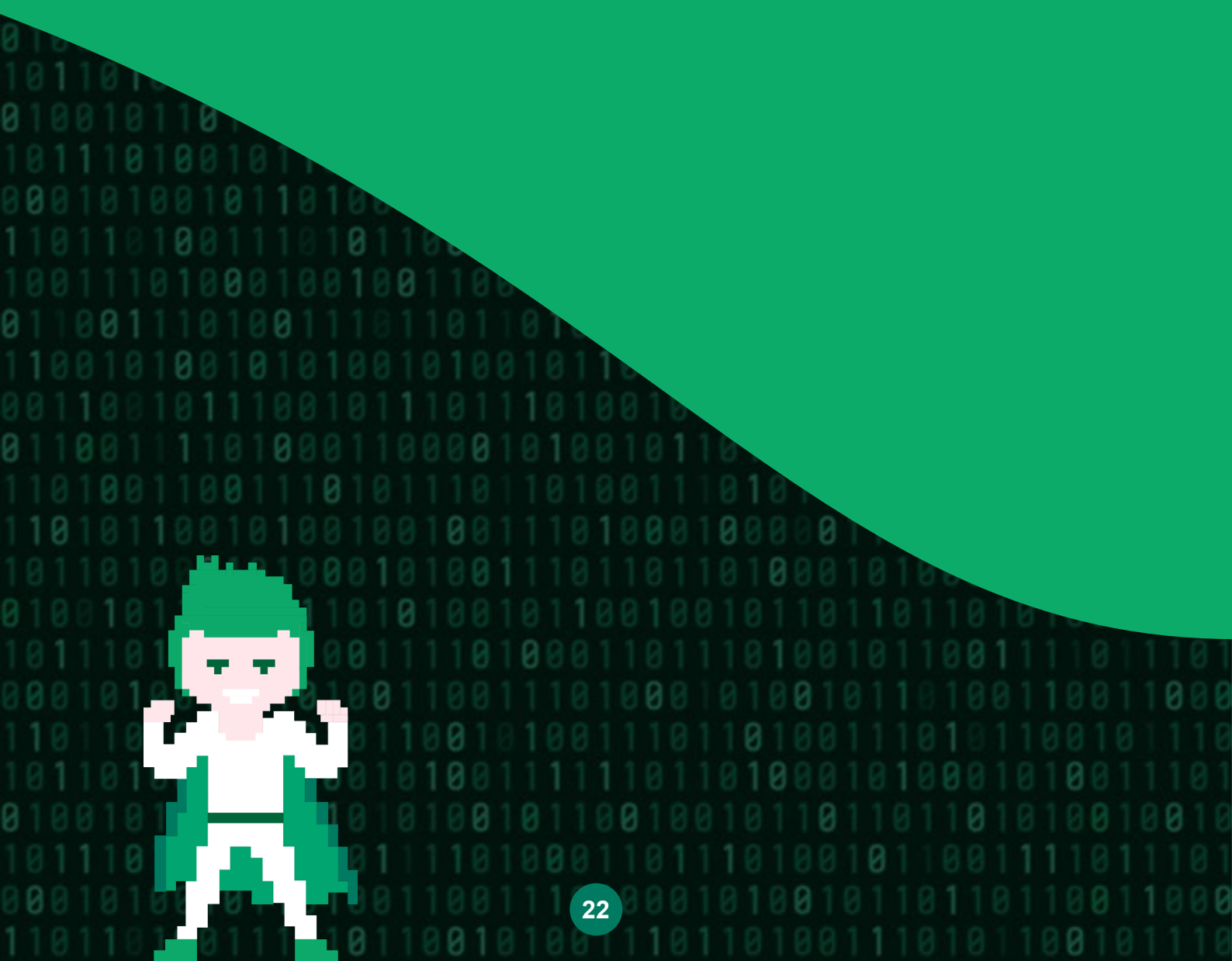
Signalez immédiatement tous les incidents au **IT Service Desk**.
Qu'il s'agisse de problèmes de logiciel, de pannes de réseau, de matériel endommagé, de ralentissements du système, de paramètres incorrects, d'hameçonnage, de virus ou d'accès non autorisés : **une notification rapide est essentielle.** C'est la seule façon pour nous d'intervenir rapidement, de limiter les dégâts et d'éviter que cela ne se reproduise. Ne pas signaler un incident peut avoir de graves conséquences.

IT SERVICE DESK:
Disponible 24h/24 et 7j/7
au numéro de téléphone : 02/607 33 00

Conseil : Enregistrez ce numéro de téléphone dans votre smartphone !



Quiz



Quiz

Répondez à ce petit quiz pour tester vos connaissances sur la protection de l'information. Les solutions se trouvent à la fin de cette brochure.

Question	Vrai	Faux
1. Vous pouvez prêter votre badge sans problème à un collègue s'il a oublié le sien. Vrai ou faux ?		
2. Afin d'assurer la continuité du service, on m'a demandé mon mot de passe. Je peux refuser de le donner. Vrai ou faux ?		
3. Mon mot de passe est très compliqué et difficile à retenir, je n'ai donc pas besoin de le renouveler régulièrement. Vrai ou faux ?		
4. J'ai perdu mon ordinateur portable, mais ce n'est pas grave car c'était déjà une vieille machine qui ne valait pas grand-chose. J'attendrai mon retour de congé pour le signaler. Vrai ou faux ?		
5. L'accès aux systèmes et aux informations de la SNCB n'est autorisé qu'aux collaborateurs qui en ont besoin dans le cadre de leurs fonctions. Vrai ou faux ?		
6. Il ne faut jamais brancher une clé USB trouvée, même pour savoir à qui elle appartient. Vrai ou faux ?		
7. Vous pouvez simplement supprimer les e-mails suspects sans les signaler, à condition de ne pas les ouvrir. Vrai ou faux ?		
8. Il est important de désactiver les connexions inutilisées telles que le Wi-Fi et le Bluetooth lorsque vous êtes en déplacement. Vrai ou faux ?		

Réponses

1. **Faux : Votre badge est personnel et ne peut jamais être prêté. Cela permet d'éviter que des personnes non autorisées aient accès à des zones sensibles. Chacun doit utiliser son propre badge.**

2. **Vrai : Un mot de passe est strictement personnel et ne doit jamais être partagé. Il existe d'autres solutions pour assurer la continuité du service sans compromettre la sécurité du système d'information de la SNCB (par exemple : s'assurer que la personne qui reprend mes tâches en mon absence dispose des accès nécessaires via son propre compte).**

3. **Faux : Aucun mot de passe n'est inviolable, aussi complexe soit-il. Ce n'est qu'une question de temps avant qu'il ne soit découvert. Il est donc nécessaire de le renouveler régulièrement afin de réduire le risque qu'il soit découvert, au moins tous les 90 jours.**

4. **Faux : L'ordinateur portable est peut-être ancien et n'a plus beaucoup de valeur, mais les données qu'il contient sont très importantes ! La perte de données sur un appareil peut avoir de graves conséquences juridiques et financières pour la SNCB.**

5. **Vrai : Les droits d'accès ne sont accordés qu'aux collaborateurs autorisés et doivent être officiellement approuvés. Cela permet d'éviter que des données sensibles ne tombent entre de mauvaises mains ou ne soient modifiées ou supprimées par inadvertance.**

6. **Vrai : Une clé USB inconnue peut contenir des virus ou des logiciels malveillants (malwares). Ne les branchez jamais, mais apportez-les directement à votre service informatique local. Vous éviterez ainsi d'endommager votre appareil et le réseau.**

7. **Faux : Les e-mails suspects ou les tentatives d'hameçonnage doivent toujours être signalés via le bouton "Signaler le message" dans Outlook ou via l'IT Service Desk. Vous contribuez ainsi à protéger le réseau de la SNCB contre des attaques plus larges.**

8. **Vrai : En désactivant les connexions inutilisées, vous réduisez le risque que des hackers accèdent à votre appareil via des réseaux non sécurisés ou des appareils à proximité.**

Cyber- & Information Security Office:

ciso@sncb.be

IT SERVICE DESK:

Disponible 24h/24 et 7j/7 : 02/607 33 00

Lay-out : B-CP.01

SNCB – octobre 2025