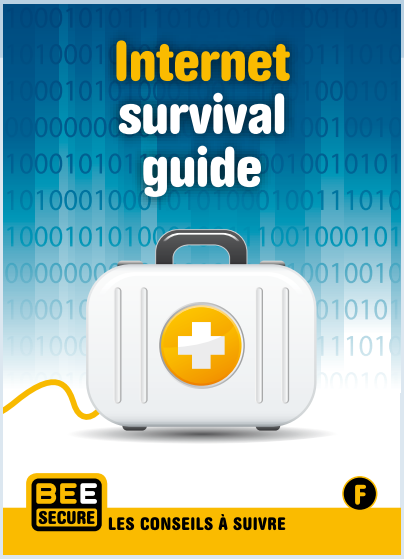
Internet survival guide

BEE SECURE

F

LES CONSEILS À SUIVRE



Ce guide est destiné aux étudiants et lycéens. Il leur fournit conseils, astuces et bonnes pratiques afin de protéger leur matériel informatique et leurs données numériques.

Il peut également servir à toute personne désirant protéger ses données et sa vie privée.

Un ordinateur ou une tablette peuvent se remplacer. Par contre, la perte d'un travail d'étude peut avoir de lourdes conséquences.

L'attention de l'utilisateur est attirée sur le fait que toutes les données contenues dans cette brochure sont fournies sans garantie, malgré le soin qui y est apporté. La responsabilité des auteurs ne peut être mise en cause.

Editeur : SNJ
Annexe Forum Geesseknäppchen
40, bld. Pierre Dupong
L-1430 Luxemburg
B.P. 707 · L-2017 Luxemburg

info@bee-secure.lu
www.bee-secure.lu

Service National de la Jeunesse
kanner jugend telefon
SECURITY MADEIN.LU
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Co-financed by the European Union
Connecting Europe Facility

Notice légale

Cette brochure a été rédigée dans le cadre du projet BEE SECURE.
Le projet est mis en œuvre par le Service National de la Jeunesse (SNJ), le KannerJugendTelefon (KJT) et securitymadein.lu.

Tirage 5000 exemplaires
ISG · v.3 - 09.2018

Le contenu de cette brochure se base sur la publication « Internet survival guide », publié par CASES.

1) La Sécurité physique

Pour protéger tes données, tu dois d'abord protéger tes appareils : tablettes, PC, disques durs, clés usb…

- Ne laisse pas ton appareil sans surveillance. Les ordinateurs portables utilisés dans des endroits publics doivent être attachés avec un câble antivol.
- Si tu es quand même forcé de laisser ton appareil sans surveillance, assure-toi que le verouillage d'écran est activé. Vérifie que ton appareil est bien protégé par un mot de passe, par un code PIN, par reconnaissance faciale, ou par empreinte digitale.
- Chiffre ton disque dur ainsi que les sauvegardes et stocke-les hors de vue.
- Ne laisse pas traîner tes clés usb ou cartes SD si tu y stockes des documents. N'utilise pas de clés usb inconnues : elles peuvent contenir des logiciels malveillants.

Chiffrement des données :

Tous les systèmes d'exploitation récents offrent la possibilité de chiffrer des données : **« Bitlocker »** sous Microsoft Windows et **« FileVault »** sous Apple OS X.

Il existe également des outils de chiffrement indépendants de votre système d'exploitation, comme Boxcryptor, DiskCryptor, VeraCrypt… Ils permettent par exemple de chiffrer les données sur le cloud et d'y accéder à travers n'importe quel appareil.

Téléchargement sous :

bee-secure.lu/fr/cryp

2) La configuration de l'ordinateur

- **Les comptes utilisateurs :** n'utilise pas le mode « administrateur » en permanence mais plutôt un compte utilisateur « restreint » et protégé par mot de passe pour surfer sur Internet, travailler et jouer. Active l'économiseur d'écran ou un mode veille automatique qui ne se débloqueront qu'à l'aide d'un mot de passe.

- **Root et jailbreak** te permettent à faire des ajustements avancés (supprimer des applications installées par défaut, libérer de la mémoire). Par contre, ceci permet aussi à des application malicieuses de contourner toutes les mesures de sécurité, et ainsi de prendre contrôle de ton téléphone entier. Ainsi elles peuvent voler des données confidentielles (comme des mots de passe ou des données bancaires). Il faut donc éviter root et jailbreak en toutes circonstance.

- **Mises à jour :** Assure-toi que toutes les applications sur tes appareils seront mises à jour automatiquement. Si tu possèdes des appareils où il n'existe pas une telle fonction de mises à jour automatique (comme p.ex. les télévisions, ou d'autres appareils «intelligents»), consulte régulièrement le site internet du fabricant pour déterminer s'il y a une nouvelle version du logiciel.

- **Anti-virus :** installe un logiciel antivirus automatiquement mis à jour - si possible quotidiennement. Pour les solutions gratuites consulte :

N'oublie pas de faire un scan régulier de ton ordinateur. Ne te fie qu'aux alertes de ton antivirus et ignore les messages via web ou mail qui prétendent que ton ordinateur serait infecté.

- **Sauvegardes (Backup) :** utilise les fonctions de sauvegarde que propose ton système d'exploitation. Stocke tes données

(chiffrées si possible) sur des disques durs externes et/ou sur le cloud.

- **Permissions:** Dès que tu as téléchargé une nouvelle application, vérifie si elle peut accéder ta caméra, ton microphone, ta position, tes contacts ou d'autres données, et si elle peut faire des appels payants. Si applicable, retire ces permissions dans les paramètres du système, ou désinstalle l'application complètement.

Le navigateur web :

Comme les extensions sont souvent la raison de publicité involontaire, essaie d'éviter toute extension de fonction nalité non-indispensable. Vérifie régulièrement si des extensions ont été installées à ton insu. Toutefois, l'utili sation des plugins suivants est conseillée :

- **NoScript,** qui prévient l'exécution de scripts poten tiellement malicieux, mais qui est rend l'utilisation du navigateur nettement moins confortable :

bee-secure.lu/fr/nosc

- **https everywhere,** pour que la communication avec le serveur soit réalisée en mode chiffré :

eff.org/HTTPS-everywhere

- **Flashblock,** (inutile si tu utilises NoScript), qui bloque le module adobe flash, souvent source d'attaques

bee-secure.lu/fr/flbl

- **Les adblocker** bloquent la publicité, des faux messages et les pop-ups sur les sites internet.

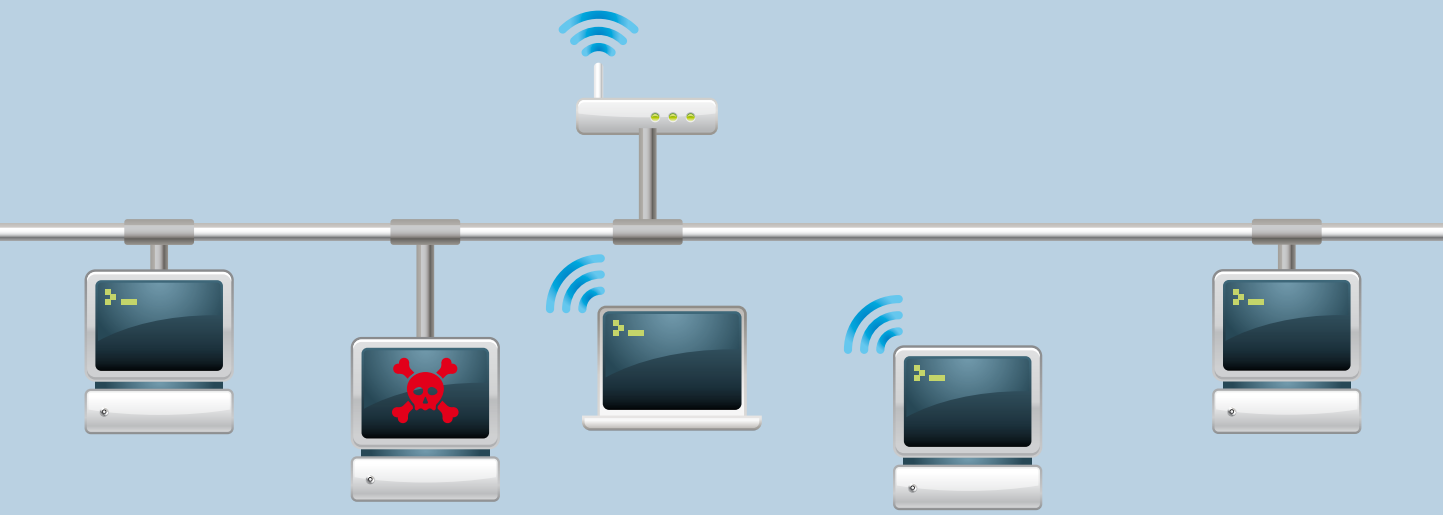
- **Les réseaux sans fil (WiFi) :** Si tu utilises le WiFi à la maison, pense à sécuriser le point d'accès sans fil (router). Il est fortement conseillé de mettre en place le mode de chiffrement WPA2 et de changer de mot de passe régulièrement. Désactive les fonctionnalités de contrôle à distance du routeur WiFi, si tu ne les utilise pas.

A l'école ou l'univ', utilise les accès réservés à l'enseignement (WiFi de l'école, EduROAM) lorsqu'il est disponible. Il offre un accès Internet sécurisé et un service helpdesk si nécessaire.

- **Réseaux publics :** N'utilise les réseaux inconnus et non-sécurisés qu'en dernier recours, comme ils donnent la possibilité aux hackers d'écouter tout ce que tu fais sur internet. Dans de tels réseaux, n'utilise que des connexions sécurisées si tu surfes sur internet (fait attention à l'usage de HTTPS) ou si tu récupères tes mails (fait attention à l'usage de TLS/SSL dans les paramètres). Les applications comme Messenger, WhatsApp, Snapchat et autres sont bien sécurisées en général, tel que tu peux les utiliser sans soucis. Évite par contre toute action douteuse comme les log-ins, l'entrée de données sensibles, ou les achats en ligne.

- **Bluetooth :** pense à désactiver Bluetooth lorsqu'il n'est pas utilisé.

- **Partage de fichiers, Localisation et NFC :** désactive le partage de fichiers et de ressources (accès Internet, disques durs, imprimante, etc.) lorsqu'il n'est pas nécessaire.



3) Les mots de passe

Les mots de passe représentent la fondation de ta sécurité numérique.

Utilise des mots de passe assez longs (plus de 12 caractères) ou, mieux encore, des « phrases de passe », contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.

Le mot de passe ne doit pas :

- faire partie d'un dictionnaire ;
- correspondre à des données personnelles (noms, date de naissance, etc) ;
- être une suite logique de chiffres ou de lettres (123456, abcdef…).

Utilise un mot de passe différent pour chaque service en ligne pour éviter que la divulgation accidentelle ou mal intentionnée d'un mot de passe ne donne accès à tous vos comptes d'un coup.

Active la double authentification chaque fois que c'est possible.

Remplace tes mots de passe par défaut, et ne les communique à personne.

**Le mot de passe,
c'est comme une brosse à dents.
Cela ne se partage pas.**

Choisir ses mots de passe :

Choisis une phrase facilement mémorisable, comme par exemple « **L**a **m**er **e**st **u**n **e**space **d**e **r**igueur **e**t **d**e **l**iberté **!** » (Victor Hugo). En prenant la première lettre de chaque mot, on obtient :
« Lmeuedredl! ». En remplaçant certains caractères par des chiffres, cela donne **« Lme1edr+dl! »**.

Alternativement tu peux également utiliser la phrase entière comme ton mot de passe. Essaie par contre d'éviter des phrases trop connues (comme des proverbes) ou trop évidentes («je m'appelle ...»).

En général, plus ton mot de passe est créatif, plus il est sûr.

Teste ton mot de passe :  **pwdtest.bee-secure.lu**

Gérer ses mots de passe

Utiliser des mots de passe distincts et de qualité pour chaque service en ligne s'avère difficile, surtout lorsqu'on utilise de nombreux services. On peut s'en sortir en choisissant un mot de passe très solide qui sera décliné en plusieurs variantes (p. ex. ajouter le service en ligne comme préfixe ou suffixe : **« FB:Lme1edr+dl! »** avec FB pour Facebook) ou bien utilisant un gestionnaire de mots de passe comme LastPass ou KeePass.

 **bee-secure.lu/fr/keep**

Ces outils permettent de mémoriser autant de mots de passe que nécessaire, de générer des mots de passe solides et nous alertent sur les problèmes de sécurité qui affectent les différents services utilisés.

En plus, le gestionnaire de mots de passe te protègera des tentatives de phishing puisqu'il distinguera une page de connexion légitime d'un leurre qui vise uniquement à extorquer des identifiants. À noter que pour cette fonctionnalité tu dois généralement installer une extension pour ton navigateur.

Attention toutefois : un gestionnaire de mots de passe est comparable à un coffre-fort. Si tu y stocke tous tes mots de passe, la clé de ce coffre-fort doit être très solide et ne doit en aucun cas être divulguée, ni perdue. Active la double authentification sur ton gestionnaire de mots de passe.

4) Les règles de comportement

Sois vigilant !

Méfie-toi des arnaques sur Internet. Ton comportement en ligne a un impact direct sur la sécurité de tes données.

La navigation sur le web :

- Évite absolument d'entrer des mots de passe ou autres informations personnelles sur un ordinateur qui ne t'appartient pas (évite en particulier l'e-banking et le commerce électronique).
- Si tu dois vraiment entrer un mot de passe sur un ordinateur qui ne t'appartient pas, utilise au moins le mode « private browsing » (CTRL-MAJ-P sous Firefox ou Internet Explorer, CTRL-MAJ-N sous Chrome) - les données personnelles et les mots de passe ne seront alors pas stockés. Un clavier virtuel sera également avantageux.
- En général, vérifie si « https » constitue le début de la barre d'adresse de ton navigateur lors de l'introduction de données sensibles comme les mots de passe. Si ton navigateur web te prévient que le certificat d'un site utilisant SSL (https comme préfixe) n'est pas valide, quitte le site sans effectuer de transaction.

- Certains sites peuvent provoquer l'infection de ton système par une simple visite (drive-by download). Évite donc les sites dans lesquels tu n'as pas une confiance absolue. Évite de cliquer sur les publicités ainsi que sur les liens contenus dans un courrier électronique.

Un logiciel comme Sandboxie ou Adblocker peut t'aider à protéger ton ordinateur.

bee-secure.lu/fr/sand

ou réduis au moins tes droits si tu es administrateur.

Le courrier électronique et les messages :

- Ne réponds pas aux mails et messages qui demandent la saisie d'informations confidentielles ou personnelles (comme les mots de passe, numéros de comptes, cartes de crédits, etc).
- Ne clique pas sur les liens ou pièces jointes si tu n'en connais pas la provenance de façon certaine.
- Aie un esprit critique et analyse chaque message avant d'agir, même si le message provient d'une connaissance :

  - ☐ Son message est-il étrange ? Inattendu ?
  - ☐ Utilise-t-il un langage inhabituel ?
  - ☐ S'agit-il d'un message de détresse ?
  - ☐ Propose-t-il de participer à un concours ? De profiter d'une aubaine ?
  - ☐ Le message contient-il un lien ou une pièce jointe ?

Si tu réponds positivement à une de ces questions, sois prudent et tente de contacter ton interlocuteur par un autre canal.

- Sois conscient qu'une adresse e-mail peut très facilement être falsifiée.

Le spam :

• Pour éviter le spam (courrier indésirable), utilise 2 adresses e-mail :

  • 1 adresse principale pour les relations de confiance ;
  • 1 adresse secondaire (ou un alias) pour les contacts publics.

Pense aussi aux services d'e-mails jetables pour les informations non-personnelles :

bee-secure.lu/fr/spm1

- Ne communique pas ton adresse e-mail principale à tout le monde et évite de l'afficher ouvertement à des endroits publiquement accessibles (Blog, Facebook, flyer, etc.).

- Ne réponds jamais aux spams.

Les hoax :

Evite de faire circuler les canulars et fausses nouvelles ou désinformations. Souviens-toi que :

- les virus ne sont pas annoncés par courrier électronique ;
- les correctifs de sécurité ne sont pas distribués par e-mail ;
- les e-mails et messages qui t'invitent à les diffuser à tous tes contacts (lettres en chaîne) sont presque toujours des canulars ou des arnaques.

En cas de doute, vérifie les informations reçues :

www.hoaxbuster.com
www.mimikama.at

Bref, apprends à reconnaître les e-mails et messages suspects :

bee-secure.lu/fr/spm2

Pour cliquer malin dans toutes les situations, suis les conseils de BEE SECURE :

www.bee-secure.lu/fr/clever-klicken

Réseaux sociaux et protection des données :

- Limite autant que possible la dissémination d'informations personnelles. Pense à revoir les paramètres de confidentialité de ton service favori.
- Évite de publier des données ou photos à caractère privé sur les réseaux sociaux (Facebook, Snapchat, Instagram, etc.). Tu perds le contrôle de tes données dès qu'elles sont publiées sur Internet ; ne les mets en ligne que si tu es prêt à les rendre publiques.
- Demande la permission des personnes représentées sur des photos avant de les publier. Les lois sur le droit à l'image, au Luxembourg comme dans d'autres pays, s'appliquent.

Petit rappel sur le droit à l'image :

bee-secure.lu/fr/cprt

- Pose-toi les questions suivantes avant de partager du contenu sur les réseaux sociaux :

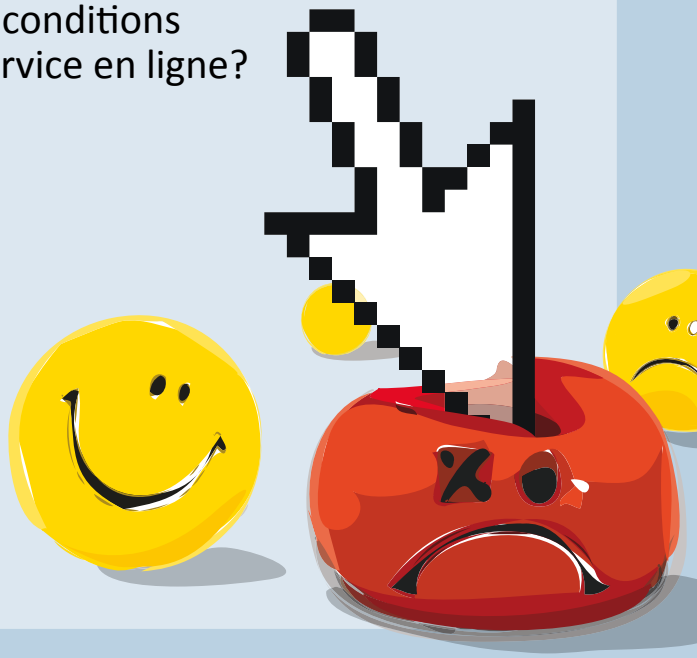
  - ☐ Le texte ou les images sont-ils libres de droit ?
  - ☐ Les personnes figurant sur les images ont elles donné leur accord pour que leurs photos soient publiées?
  - ☐ Le message n'est-il pas diffamatoire, calomnieux, discriminatoire ou haineux ?
  - ☐ Le message respecte-t-il les conditions générales d'utilisation du service en ligne?

Conseils et astuces sur Facebook :

bee-secure.lu/fr/fcbk

Quelle que soit ton humeur,
reste fair-play.
Le harcèlement n'est pas un jeu :

bee-secure.lu/fr/beefair



5) Les aspects juridiques

Sois responsable !

Tu n'es pas anonyme en ligne… et la loi s'applique également sur Internet :

bee-secure.lu/fr/lois

Sois prudent en rédigeant des textes ou commentaires et en publiant des photos ou vidéos en ligne - la législation usuelle en matière de diffamation, calomnie et droit à l'image s'applique.

Si tu es témoin d'un harcèlement, il faut réagir, sinon, tu es co-responsable. Tu peux par exemple utiliser les procédures de reporting sur Facebook (ou autres réseaux sociaux) pour dénoncer du contenu diffamatoire ou inapproprié. Souvent, le harcèlement cesse lorsque l'auteur se rend compte que la victime n'est pas seule…

Si tu es victime de harcèlement, voici quelques bons réflexes à adopter :

1. Ne réponds jamais à des messages harcelants ou menaçants
2. Bloque tes agresseurs
3. Garde des preuves (p. ex. capture d'écran)
4. Dénonce-le en contactant les responsables du site ou du réseau social
5. Modifie tes informations en ligne

Pour plus d'information, consulte le dossier « Not funny - Bee fair » de BEE SECURE.

NOT FUNNY
BEE FAIR

bee-secure.lu/fr/beefair

Ce que dit la loi…

Injure : l'injure constitue une atteinte à l'honneur. Il s'agit d'une infraction prévue par le Code pénal qui est punissable d'une peine d'emprisonnement de 8 jours à deux mois et d'une amende pouvant atteindre 5.000 euros ou d'une de ces deux peines seulement.

Atteinte au droit à la vie privée : ce droit est consacré par la loi du 11/08/1982 mais également par l'article 8 de la Convention européenne des droits de l'homme. On n'a donc pas le droit de révéler, sans l'accord de l'intéressé des informations relatives à sa vie privée et familiale.

Downloads : tout n'est pas permis…

Installe les logiciels légaux et utilise les services légaux (musique, films,…)

En tant qu'étudiant au Luxembourg, tu as accès à de nombreuses ressources gratuitement (Office 365 pour l'Education, EduCloud,…) ou à des tarifs avantageux (non-profit, tarifs « educational »).

bee-secure.lu/fr/legal

Ne fais pas un usage illégal de plates-formes de téléchargement (Peer-to-Peer ou directes).

Non seulement, les téléchargements illégaux sont sanctionnés par la loi, mais en plus ces plates-formes sont connues pour contenir un pourcentage élevé de fichiers infectés (virus, troyans).

Il existe entretemps un large éventail de **solutions de streaming légales**, gratuites car financées par de la publicité ou payantes (alors souvent sans pub).

ß

6) Les tablettes et les smartphones

Les tablettes et les smartphones sont des ordinateurs (presque) comme les « grands ». Mais leur taille réduite et leur usage nomade leur confèrent des risques supplémentaires… Quelques bons réflexes s'imposent :

- Sécurise l'appareil. Utilisez un mot de passe fort pour verrouiller le smartphone ou la tablette. Ne te contente pas d'un code PIN à 4 chiffres! En cas de vol, cela te laissera le temps d'effacer ton smartphone ou tablette à distance en te connectant à ton compte.
- Réfléchis avant d'installer une application. Vérifie bien à quelles informations l'application aura accès, avant de l'installer. Certaines applications accèdent par exemple à ta localisation, tes contacts, ton profil sur les réseaux sociaux… N'installe que des applications dont tu as vraiment besoin et qui viennent de sources de confiance.
- Reste prudent avec les hotspots Wi-Fi. Lorsque tu utilises des points d'accès publics ou non sécurisés, évite d'utiliser des sites et des applications qui requièrent des informations personnelles ou une identification.
- Désactive la connectivité WiFi, Bluetooth et NFC si tu ne les utilises pas.
- Le petit plus : mets en place un code supplémentaire pour accéder au paramétrage de ta tablette ou smartphone. Cela évitera qu'un « ami » modifie vos paramètres à votre insu.
- Si tu partages ta tablette, crée des comptes différents pour chaque utilisateur.

Pour en savoir plus sur les risques liés aux smartphones :

bee-secure.lu/fr/phon

7) Le cloud

Le cloud permet de pouvoir accéder à ses documents, photos, vidéos ou tout type de fichier où que l'on soit, sur n'importe quel ordinateur ou terminal. Cela nous évite de devoir copier nos documents sur différents appareils pour pouvoir y accéder. Le Cloud facilite le travail à distance et permet par exemple de travailler à plusieurs sur le même document sans être au même endroit.

Le cloud peut nous rendre plus efficaces dans notre travail et nous aider à sauvegarder nos documents… Mais il comporte également des risques. Pour limiter ces risques, quelques règles élémentaires s'imposent :

1. Utilise un mot de passe solide pour te connecter à ton Cloud *(voir § Mots de passe page 7).*
2. Utilise la double authentification si cela est possible.
3. Chiffre tes documents ou données sensibles stockées sur le Cloud *(voir §1, « Chiffrement des données » page 3)*.
4. Protège tous les appareils qui ont accès à ton Cloud *(cf. § Tablettes et Smartphones page 15).*

Il convient toutefois d'être attentif aux conditions d'utilisation et aux garanties offertes par les différents services de cloud. Quelques points à vérifier :

- ☐ Qui a accès à tes données ?
- ☐ Quelle utilisation le prestataire de cloud peut-il en faire?
- ☐ Quelles sont les garanties offertes quant à la protection des données ?
- ☐ Qu'en est-il en cas d'interruption ou de cessation du service ?
- ☐ La destruction de tes données est-elle garantie lorsque tu les effaces ?

Plus d'information sur le cloud peuvent être trouvées sous :

bee-secure.lu/fr/cloud