Guide de l'informatique de base

Offert par Obsiden à tous les participants d'Obsiden Boost

Ce guide s'adresse aux indépendants, ASBL, commerces et petites structures qui utilisent l'informatique tous les jours sans avoir de service informatique interne. Il ne demande aucune connaissance technique. Chaque chapitre contient des conseils concrets, applicables en quelques minutes, et une courte liste de vérification.

Obsiden SRL — Rue du Pays-du-Roi 29, 5377 Somme-Leuze — contact@obsiden.be — +32 (0)86 66 53 00

---

1. Les mots de passe : votre première serrure

Un mot de passe réutilisé sur plusieurs sites est la porte d'entrée la plus fréquente des incidents. Quand un site se fait pirater, les adresses e-mail et mots de passe volés sont testés automatiquement sur les boîtes mail, les banques en ligne et les outils professionnels.

À faire :

- Utilisez une phrase de passe plutôt qu'un mot : « CafeChaud!Lundi7h » est plus solide et plus facile à retenir que « Az3rty! ».
- Un mot de passe différent pour chaque service, en commençant par les trois qui comptent le plus : la boîte mail professionnelle, la banque, et l'accès à votre site ou à votre comptabilité.
- Installez un gestionnaire de mots de passe (Bitwarden, 1Password, ou celui intégré à votre navigateur). Vous ne retenez plus qu'un seul mot de passe : celui du coffre.
- Ne notez jamais de mot de passe dans un fichier Word, un carnet près de l'écran, ou un e-mail envoyé à vous-même.
- Changez immédiatement un mot de passe si vous l'avez communiqué par téléphone ou tapé sur une page suspecte.

Vérification : mes trois comptes les plus sensibles ont-ils chacun un mot de passe unique, connu de moi seul ?

---

2. La double authentification (MFA) : la mesure la plus rentable

La double authentification demande, en plus du mot de passe, une confirmation sur votre téléphone. Même si votre mot de passe est volé, le voleur reste dehors. C'est la mesure qui évite le plus d'incidents pour le moins d'effort.

À faire :

- Activez-la d'abord sur la boîte mail professionnelle : c'est elle qui permet de réinitialiser tous les autres comptes.

- Ensuite sur la banque, la comptabilité, le site web, les réseaux sociaux de l'organisation.
- Préférez une application (Microsoft Authenticator, Google Authenticator) au SMS, plus facile à détourner.
- Conservez les codes de secours fournis lors de l'activation, imprimés et rangés hors du bureau.
- Ne validez jamais une notification d'authentification que vous n'avez pas déclenchée vous-même : c'est le signe que quelqu'un possède votre mot de passe. Refusez, puis changez-le.

Vérification : si je perds mon téléphone aujourd'hui, ai-je un moyen de me reconnecter à ma boîte mail ?

---

3. Les sauvegardes : ce qui vous sauve vraiment

Une panne de disque, un vol d'ordinateur, une erreur de manipulation ou un rançongiciel ont le même effet : les données disparaissent. La seule protection qui fonctionne toujours est une sauvegarde récente, testée, et hors de portée.

La règle 3-2-1 : trois copies de vos données, sur deux supports différents, dont une copie hors site (cloud ou disque conservé ailleurs).

À faire :

- Identifiez ce qui ne peut pas être reconstitué : comptabilité, contrats, photos de chantier, fichiers clients, modèles de documents.
- Une sauvegarde automatique vaut mieux qu'une sauvegarde manuelle : on oublie toujours de faire la manuelle.
- Un disque dur branché en permanence n'est pas une sauvegarde : un rançongiciel le chiffre aussi. Débranchez-le ou utilisez une solution cloud avec historique des versions.
- Attention : la synchronisation (OneDrive, Google Drive, Dropbox) n'est pas une sauvegarde. Si vous supprimez ou chiffrez un fichier, la modification se propage. Vérifiez que l'historique des versions et la corbeille longue durée sont activés.
- Testez une restauration deux fois par an : prenez un fichier au hasard et restaurez-le. Une sauvegarde jamais testée n'est qu'une hypothèse.

Vérification : si mon ordinateur principal disparaît ce soir, que perds-je exactement, et en combien de temps puis-je reprendre mon activité ?

---

4. Reconnaître un e-mail frauduleux (phishing)

La grande majorité des attaques commence par un e-mail. Les faux messages imitent une banque, un transporteur, l'administration, un fournisseur, ou même un collègue.

Les signaux d'alerte :

- Une urgence inhabituelle : « votre compte sera bloqué dans 24 heures ».

- Une demande de paiement, de changement de numéro de compte, ou de communication d'un code reçu par SMS.
- Une adresse d'expéditeur presque correcte : contact@obsiden-be.com au lieu de contact@obsiden.be.
- Un lien dont l'adresse réelle (visible en survolant sans cliquer) ne correspond pas au texte affiché.
- Une pièce jointe inattendue : facture, bon de commande, fichier HTML ou ZIP.

La règle d'or de la facture : tout changement de numéro de compte bancaire annoncé par e-mail se vérifie par téléphone, au numéro que vous connaissez déjà, jamais à celui indiqué dans le message. Cette seule habitude évite l'essentiel des fraudes au virement.

Si vous avez cliqué : ne vous cachez pas. Déconnectez l'ordinateur du réseau, changez le mot de passe du compte concerné depuis un autre appareil, vérifiez qu'aucune règle de transfert automatique n'a été ajoutée dans votre boîte mail, et prévenez votre prestataire.

---

5. Garder ses appareils à jour

Les mises à jour ne sont pas des caprices d'éditeur : elles bouchent les failles utilisées par les attaquants, souvent quelques jours après leur publication.

À faire :

- Activez les mises à jour automatiques de Windows, macOS, iOS et Android.
- Mettez aussi à jour les navigateurs, la suite bureautique, et les logiciels métier.
- Remplacez les systèmes qui ne reçoivent plus de mises à jour (Windows 10 après sa fin de support, vieux téléphones) : ils restent vulnérables pour toujours.
- N'oubliez pas les équipements réseau : box internet, routeur, NAS, caméras, imprimante connectée. Changez systématiquement leur mot de passe d'usine.
- Redémarrez les postes au moins une fois par semaine : beaucoup de mises à jour ne s'appliquent qu'au redémarrage.

---

6. Antivirus et protection du poste

L'antivirus intégré à Windows (Microsoft Defender) est correct s'il est actif et à jour. Pour une organisation, une solution gérée centralement apporte en plus l'alerte et la visibilité : vous savez qu'un poste est infecté avant que le client ne vous appelle.

À faire :

- Vérifiez qu'un antivirus est actif sur chaque poste, et qu'aucun n'est resté désactivé « le temps d'installer un logiciel ».
- N'installez que des logiciels téléchargés depuis le site officiel de l'éditeur.
- Travaillez avec un compte utilisateur standard plutôt qu'administrateur pour les tâches quotidiennes.

- Verrouillez l'écran dès que vous quittez votre poste (touche Windows + L).
- Activez le chiffrement du disque (BitLocker sur Windows Pro, FileVault sur Mac) : un portable volé devient illisible.

---

7. Wi-Fi, réseau et travail à distance

- Changez le mot de passe administrateur de votre box ou routeur : celui d'usine est public.
- Utilisez le chiffrement WPA2 ou WPA3, jamais WEP.
- Créez un réseau « invités » séparé pour les visiteurs, les clients et les objets connectés. Ils n'ont pas à voir vos ordinateurs de travail.
- Sur un Wi-Fi public (hôtel, gare, café), évitez les accès sensibles ou utilisez un VPN.
- Pour le télétravail, passez par les outils prévus (VPN, bureau à distance sécurisé) plutôt que par un partage de fichiers ouvert sur internet.

---

8. Messagerie et outils collaboratifs

- Utilisez une adresse au nom de votre domaine (prenom@votre-organisation.be) plutôt qu'une adresse gratuite : c'est plus crédible et plus facile à récupérer en cas de départ d'un collaborateur.
- Configurez les protections du domaine (SPF, DKIM, DMARC) pour empêcher qu'on usurpe votre adresse pour arnaquer vos clients. Votre prestataire peut le faire en une intervention.
- Créez un compte par personne : jamais de compte partagé. Sans cela, impossible de savoir qui a fait quoi, ni de couper un accès proprement.
- Rangez les documents de travail dans un espace partagé (SharePoint, Google Drive, serveur) plutôt que sur le bureau d'un poste : le départ d'une personne ne doit pas emporter les fichiers.
- Passez en revue une fois par an la liste des personnes ayant accès à vos outils, et supprimez les comptes inutilisés.

---

9. Vos données et vos obligations (RGPD, en pratique)

Toute organisation qui traite des données de clients, de membres ou de patients est concernée, même seule et sans site web.

Le minimum sérieux :

- Sachez quelles données vous détenez, où elles se trouvent, et qui y accède.
- Ne collectez que ce qui est nécessaire, et ne conservez pas indéfiniment : fixez une durée.
- Tenez un registre simple des traitements (un tableau suffit pour une petite structure).

- Vérifiez que vos prestataires (comptable, hébergeur, logiciel métier) présentent des garanties et hébergent de préférence en Europe.
- En cas de fuite de données présentant un risque, une notification à l'Autorité de protection des données est prévue dans les 72 heures. Préparer le réflexe évite la panique.

---

10. Que faire en cas d'incident

Les trente premières minutes comptent plus que tout le reste.

1. **Isoler** : débranchez le câble réseau ou coupez le Wi-Fi de la machine concernée. N'éteignez pas brutalement : des traces utiles disparaîtraient.
2. **Alerter** : prévenez la personne responsable et votre prestataire informatique. Ne gérez pas seul.
3. **Ne pas payer** : en cas de rançongiciel, payer ne garantit rien et encourage la récidive.
4. **Changer les accès** depuis un appareil sain : boîte mail d'abord, puis banque et outils métier.
5. **Prévenir** votre banque en cas de fraude au virement, et déposer plainte à la police locale.
6. **Restaurer** depuis une sauvegarde saine, puis vérifier avant de rebrancher.
7. **Noter** ce qui s'est passé et quand : cela sert à l'assurance, à la plainte, et à éviter que cela recommence.

À préparer dès aujourd'hui, sur papier : le numéro de votre prestataire, celui de votre banque, la liste de vos comptes critiques, et l'endroit où se trouvent vos sauvegardes. Ce document doit être lisible sans ordinateur.

Votre plan en 10 points

1. Activer la double authentification sur la boîte mail professionnelle.
2. Mettre un mot de passe unique sur les trois comptes les plus sensibles.
3. Installer un gestionnaire de mots de passe.
4. Mettre en place une sauvegarde automatique hors site.
5. Tester une restauration de fichier.
6. Activer les mises à jour automatiques partout.
7. Changer les mots de passe d'usine de la box, du NAS et de l'imprimante.
8. Créer un réseau Wi-Fi invités séparé.
9. Supprimer les comptes des personnes parties.
10. Écrire sur papier la fiche réflexe « en cas d'incident ».

Si vous cochez ces dix points, vous êtes déjà au-dessus de la moyenne des petites structures belges.

Aller plus loin avec Obsiden

Obsiden accompagne les indépendants, ASBL et petites entreprises en Belgique : audit informatique et cybersécurité, infogérance, sauvegarde, sensibilisation des équipes et feuille de route à budget maîtrisé.

- Audit IT gratuit en ligne : https://obsiden.be/audit-it
- Centre de ressources : https://obsiden.be/ressources
- Nous contacter : https://obsiden.be/contact — contact@obsiden.be — +32 (0)86 66 53 00

Ce guide est fourni à titre informatif et ne remplace pas une analyse adaptée à votre situation.