La sécurité informatique est un sujet crucial : sur nos PC, nos smartphones ou tout autre appareil connecté à Internet. Pour protéger nos données, il est essentiel d'adopter de bonnes habitudes.

1. Qu'est-ce que la sécurité informatique ?

La sécurité informatique inclut la protection du matériel, des données et de la vie privée contre des menaces telles que les virus, les pirates informatiques, le vol de données ou toute forme d'attaques malveillantes.

Les fiches de cette thématique présentent des moyens techniques, juridiques, pratiques et humains pour renforcer sa sécurité informatique, et plus particulièrement sa sécurité en ligne, aussi appelée cybersécurité. Pour être efficaces, tous ces moyens doivent être associés à une analyse et à une réduction des risques.

Il sera également question de :

- protéger et de préserver sa santé, aussi bien physique que mentale avec le numérique (voir fiche 9.11.).
- protéger l'environnement avec une utilisation raisonnée et raisonnable du numérique (voir fiche 9.12.).

2. 10 règles essentielles pour assurer sa cybersécurité

1. **Créez des mots de passe forts** (voir fiche 9.4. ; 9.7. et 9.8.)
   - Utilisez des MAJUSCULES, minuscules, chiffres, caractères spéciaux : @ ! - _ &
   - Utilisez des mots de passe différents pour chaque service.
   - Changez régulièrement vos mots de passe, plusieurs fois par an.
   - Mémorisez vos mots de passe ou utilisez des moyens pour vous en souvenir facilement.

2. **Sauvegardez régulièrement**
   Faites des sauvegardes régulières de vos données (voir fiche 9.5. et 9.9.) sur différents supports : disques durs externes, sauvegardes en ligne…

3. **Mettez à jour**
   Veillez à la mise à jour de vos appareils et logiciels (voir fiche 9.5. et 9.8.).
   Les mises à jour corrigent souvent des failles de sécurité ou renforcent la sécurité.

4. **Connaissez vos ennemis**
   Comprendre les différents types de menaces et s'en protéger (voir fiche 9.2. et 9.8.).
   - Posez un regard critique sur les informations que vous recevez
   - Utilisez des outils d'analyse comme l'antivirus

5. **Méfiez-vous des réseaux Wi-Fi publics**
   Évitez les réseaux Wifi publics ou inconnus (voir fiche 9.9. et 2.5.). Très faciles d'accès, ces réseaux peuvent être contrôlés par des personnes malintentionnées pour intercepter vos informations personnelles. Evitez autant que possible de réaliser des opérations à caractère sensible comme des paiements bancaires.

6. Contrôlez les paramètres
Contrôlez les permissions, l'accessibilité et les options de confidentialité de vos appareils (voir fiche 9.6.). Savoir qui a accès à quoi permet de limiter les risques de fuites d'informations et les pertes de données. Faites attention aux autorisations demandées par les applications et les sites web que vous visitez.

7. Séparez usages privés et professionnels
Séparez bien vos usages privés et professionnels (voir fiche 9.10. et 9.11.).
Évitez de partager des informations professionnelles sur vos réseaux sociaux personnels, et inversément. Le partage et l'interprétation d'informations peuvent très vite nuire à votre réputation dans la vie physique ou en ligne, ainsi qu'à celle de la structure pour laquelle vous travaillez.

8. Evitez les sites douteux ou illicites (voir fiche 9.6. et 9.8.).
N'utilisez pas de plateformes non-officielles et ne téléchargez pas de fichiers provenant d'un site de téléchargement illégal. Sur ces sites, de nombreux fichiers sont infectés et peuvent contenir des virus et autres logiciels malveillants.

9. Communiquez en conscience
Réfléchissez à toutes les informations que vous communiquez, partagez sur les réseaux sociaux ou les plateformes collaboratives (voir fiche 9.6. et 9.10.). De nombreuses informations personnelles peuvent tomber entre de mauvaises mains et être utilisées pour vous nuire. De même, ne relayez pas d'informations non vérifiées.

10. Restez vigilant·e
Dans le doute, demandez de l'aide à une personne de confiance ou à un·e professionnel·le. Les usages et pratiques évoluent sans cesse, il est donc important de se mettre régulièrement à jour et de demander conseils.

3. La sécurité à tout âge : CYBERSIMPLE.be

L'initiative **cybersimple.be** est le fruit d'une étroite collaboration entre Google et Test-Achats.
Elle vise à promouvoir un Internet plus sûr et à sensibiliser les consommateur·rices à mieux se protéger face aux risques possibles sur le net.

L'objectif est de fournir des connaissances utiles pour optimiser et maintenir sa sécurité sur le Web.

Le site aborde les problématiques principales auxquelles doit faire face chaque utilisateur·rice.

C'est simple et ludique, grâce à différents outils de sécurité et de nombreux conseils concrets.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin