éclaire
le phare numérique

CyberPeace Institute

Hygiène numérique

L'hygiène numérique est un ensemble de bonnes pratiques qui permettent de protéger vos informations personnelles et vos appareils contre les cybermenaces. En adoptant ces gestes simples, vous pouvez réduire les risques liés à la cybersécurité comme la perte de données, l'utilisation de logiciels dépassés, l'absence de protection antivirus ou encore le piratage de vos comptes.

Problèmes courants liés à un manque d'hygiène numérique:

Perte de données: L'absence de sauvegardes régulières peut entraîner une perte irréversible de vos informations en cas de panne ou de cyberattaque.

Logiciels obsolètes: Ne pas mettre à jour vos logiciels expose les systèmes à des failles de sécurité connues.

Protection antivirus insuffisante: Un antivirus inactif ou dépassé peut laisser passer des menaces.

Violations de sécurité: Des mots de passe faibles et un contrôle d'accès insuffisant facilitent les intrusions non autorisées.

éclaire
le phare numérique

CyberPeace Institute

Bonnes pratiques:

Gestion des mots de passe:

- Ne partagez jamais vos mots de passe, y compris avec votre entourage et vos collègues.
- Utilisez un mot de passe unique pour chaque compte, en utilisant un gestionnaire de mots de passe pour les générer et les stocker en toute sécurité.
- Privilégiez des mots de passe d'au moins 16 caractères avec une combinaison de majuscules, minuscules, chiffres et symboles.

Surveillance des activités suspectes:

- Si vous suspectez une intrusion, assurez-vous que votre authentification multifacteur (MFA) soit activée, changez de mot de passe et déconnectez tous les autres appareils connectés au compte.

Sauvegardes régulières:

- Effectuez des sauvegardes fréquentes pour éviter la perte de vos données.
- Testez régulièrement vos sauvegardes pour vous assurer qu'elles fonctionnent correctement.

Sécurité de la messagerie:

- Ne cliquez pas sur les liens ou pièces jointes de courriels non sollicités.

Protection antivirus:

- Maintenez votre antivirus actif et à jour.

Verrouillage de l'écran:

- Activez un économiseur d'écran protégé par un mot de passe lorsque vous quittez votre poste, quel que soit l'endroit où vous vous trouvez.

Sécurité physique:

- Ne laissez pas de documents sensibles visibles et verrouillez les bureaux et armoires.

Formation:

- S'informer régulièrement au sujet des actualités liées aux cybermenaces.

Élimination sécurisée des données:

- S'assurer de la destruction définitive des documents confidentiels (sous forme papier et numérique) avec un outil dédié ou une déchiqueteuse.

Protection des appareils portables:

- Ne laissez pas vos appareils sans surveillance et utilisez des technologies de reconnaissance faciale ou d'empreinte digitale (Face ID, Touch ID, etc.).

Vigilance et discrétion dans les espaces publics:

- Soyez vigilant et faites preuve de discrétion lorsque vous vous connectez à vos comptes, consultez vos données personnelles ou que vous avez des discussions sur des sujets sensibles en public.

Pour aller plus loin et tester vos connaissances en matière de cybersécurité, réalisez les exercices interactifs proposés par Take9.

éclaire
le phare numérique

CyberPeace Institute

Exercice sur la robustesse des mots de passe:

Évaluez les mots de passe suivants :

- Passw0rd
- 123456
- kitty1995
- 1l0v3t0d0aquap0n3y0nfr1day
- Le mot de passe "1l0v3t0d0aquap0n3y0nfr1day" est le plus fort grâce à sa longueur et sa complexité, ainsi que par l'utilisation de chiffres à la place de lettres.

Conseils pour protéger votre sécurité et votre vie privée en ligne

- Évitez de publier des informations sensibles (adresse, photos à caractère trop personnel, numéro de téléphone, carte bancaire) sur les réseaux sociaux.
- Ajustez les paramètres de confidentialité de vos comptes, par exemple en mettant en place une vérification en deux étapes, une adresse de récupération du compte et des questions de sécurité.
- Vérifiez les permissions d'accès aux données que vous accordez à vos applications (GPS, contacts, etc.).
- Assurez-vous que vos transactions en ligne se font sur des sites sécurisés avec la mention: « https:// » avec un cadenas.

En adoptant ces bonnes pratiques, vous renforcez votre cybersécurité et minimisez les risques liés aux cybermenaces.