Fiche résumé

La cybersécurité au travail

Quels sont les objectifs de la **cybersécurité** ?

- **Protéger les données sensibles de l'entreprise et l'employé**
- **Prévenir les attaques informatiques**
- **Maintenir la disponibilité des systèmes et des services**
- **Informer les employés sur les pratiques de sécurité informatique**

Quels sont les principaux types de cyberattaques

Les cybercriminels utilisent différents moyens pour tenter d'attaquer :

Le Phishing

Le but du phishing est d'usurper votre identité numérique et de dérober vos identifiants pour les utiliser dans un but criminel.

Attaque DDoS

Le but est d'envoyer une énorme quantité de demandes à un site web en une fois pour le rendre volontairement inaccessible aux autres utilisateurs.

Ingénierie sociale

Le but est de tromper les gens pour obtenir des informations confidentielles ou accéder à des systèmes en se faisant passer pour quelqu'un d'autre

Chaque employé fait partie d'un environnement informatique

Au travail, chaque action que vous entreprenez peut avoir un impact sur la sécurité de toute l'institution

Votre matériel informatique *(PC, portable, smartphone, montre connecté, tablette, ...)* **est relié à une infrastructure commune à toutes l'entreprise ...**

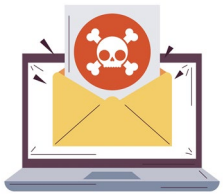
... chaque employé devient donc une porte d'entrée potentielle pour une cyber attaque si on est pas assez attentif aux risques existants

Quelques bons réflexes de **cybersécurité**

1 Choisir un mot de passe fort et unique

Créez des mots de passe complexes comprenant une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Évitez d'utiliser des mots de passe évidents comme "123456" ou "motdepasse". Utilisez un gestionnaire de mots de passe pour générer et stocker des mots de passe uniques pour chaque compte. Des mots de passe forts rendent plus difficile l'accès non autorisé à vos comptes par des attaquants.

2 Être vigilant face aux e-mails et aux liens suspects :



Méfiez-vous des e-mails inattendus, surtout avec des pièces jointes ou des liens. Vérifiez l'adresse de l'expéditeur et recherchez des signes de tromperie (comme des fautes d'orthographe ou des demandes urgentes d'informations personnelles). Si un e-mail semble suspect, contactez l'expéditeur par un autre moyen pour vérifier sa légitimité. Les attaques de phishing sont courantes et peuvent compromettre vos informations personnelles ou installer des logiciels malveillants sur votre appareil.

3 Mettre à jour régulièrement les logiciels et les systèmes

Installez les mises à jour de votre système d'exploitation, de vos applications et de vos logiciels de sécurité dès qu'elles sont disponibles. Activez les mises à jour automatiques lorsque c'est possible. Les mises à jour corrigent souvent des vulnérabilités de sécurité que les attaquants pourraient exploiter.

4 Utiliser une authentification à deux facteurs (2FA)

En plus de votre mot de passe, utilisez une deuxième forme de vérification, comme un code envoyé par SMS, une application d'authentification ou une clé de sécurité physique. Configurez vos comptes importants, tels que les e-mails et votre banque. Cette authentification ajoute une couche supplémentaire de protection, rendant plus difficile pour les attaquants d'accéder à vos comptes même s'ils connaissent votre mot de passe.

5 Sauvegarder régulièrement les données

Effectuez des sauvegardes fréquentes de vos fichiers importants, soit sur un disque dur externe, soit sur un service de stockage cloud sécurisé. Automatisez les sauvegardes si possible et vérifiez régulièrement que les sauvegardes sont complètes et fonctionnelles.

Les sauvegardes permettent de restaurer vos données en cas de perte due à une cyberattaque, une panne matérielle ou une suppression accidentelle.

Cybersécurité et travail à distance, soyez vigilants !

Protégez vos données lors de vos déplacements professionnels ou de votre télétravail grâce à ces conseils pratiques de cybersécurité.

Le VPN, un super-héros de la sécurité

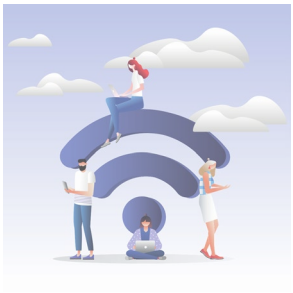
Pourquoi ? Un VPN chiffre votre connexion internet, rendant vos communications sécurisées.

Comment ? Assurez-vous que votre entreprise fournit un VPN. Activez-le chaque fois que vous utilisez une connexion internet publique ou non sécurisée.

Maintenez vos logiciels à jour

Pourquoi ? Les mises à jour corrigent les vulnérabilités de sécurité.

Comment ? Activez les mises à jour automatiques sur tous vos appareils et logiciels. Vérifiez régulièrement la disponibilité des mises à jour.



Évitez les connexions Wi-Fi publiques non sécurisées

Pourquoi ? Les réseaux Wi-Fi publics non sécurisés peuvent être facilement compromis.

Comment ? Évitez d'utiliser les réseaux Wi-Fi publics pour accéder à des informations sensibles. Si vous devez utiliser un Wi-Fi public, connectez-vous toujours via un VPN pour chiffrer votre connexion. Utilisez de préférence un hotspot personnel sécurisé.

Soyez vigilant face aux e-mails et liens suspects

Pourquoi ? Les attaques de phishing sont courantes et peuvent compromettre vos informations.

Comment ? Ne cliquez pas sur les liens ou les pièces jointes provenant de sources inconnues. Vérifiez toujours l'adresse de l'expéditeur avant de répondre ou d'agir.

Continuez à apprendre sur 123 digit !