→**Dangers liés à l'utilisation de systèmes d'information non protégés:**

1. Intrusion ou piratage - gagner l'accès à un système informatique à l'insu de son propriétaire

2. Virus et vers--- programmes qui empêchent les systèmes informatiques de fonctionner correctement

3. Cheval de Troie--- Ces programmes ont deux composants ; l'un fonctionne comme un serveur et l'autre comme un client pour attaquer l'intégrité des données, voler des informations privées sur le système cible, stocker les frappes de touches et les rendre visibles pour les pirates, en envoyant des fichiers locaux privés en pièce jointe à un courriel.
4. Spoofing : tromper les autres utilisateurs d'ordinateur pour qu'ils pensent que la source de leurs informations provient d'un utilisateur légitime.
5. Sniffing -- utilisé par les pirates pour scanner les identifiants de connexion et les mots de passe sur les fils.

6. Déni de service---Le but principal de cette attaque est de faire tomber le réseau ciblé et de lui faire refuser le service aux utilisateurs légitimes.

→Avantages du contrôle parental sur les appareils:

1. Filtrez et bloquez le contenu que vous ne voulez pas que vos enfants voient, comme la violence et la pornographie.

2. Restreindre les informations qui sont partagées.

3. Fixez des limites de temps pour la durée pendant laquelle les enfants sont en ligne.

4. - • 4. Contrôlez l'heure à laquelle les enfants peuvent accéder à Internet.

5. • 5. Définissez des profils différents pour que chaque membre de la famille ait un niveau d'accès qui lui convient.

→Risques d'atteinte à la sécurité:

1. Perturbation des activités

2. Pertes financières

3. Perte d'intimité

4. Atteinte à la réputation

5. Perte de confiance

6. Sanctions légales

7. Ralentissement de la croissance

8. Perte de vie

→Il existe des moyens techniques pour restreindre l'accès à certains services à partir de vos appareils. Il est possible de les obtenir à partir de vos appareils ou en parlant à un agent sur l'un de nos différents canaux.

→Il est interdit d'utiliser les réseaux de communications électroniques pour la publication de contenus illicites ou tout autre acte susceptible d'affecter la sécurité des réseaux ou des systèmes d'information.

→Il est interdit de concevoir des virus trompeurs, des logiciels espions, des logiciels potentiellement indésirables ou tout autre dispositif entraînant des pratiques frauduleuses.