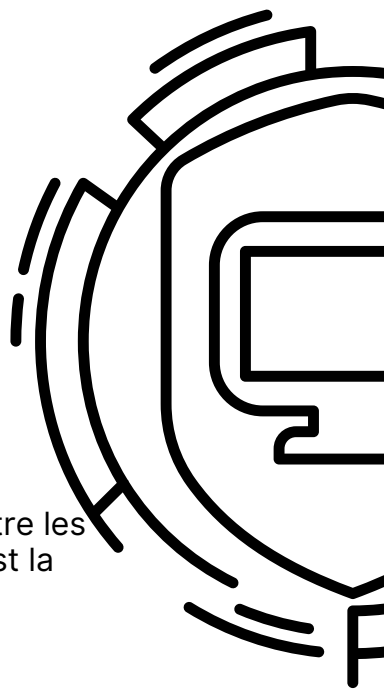
MARZ 2023

3+ Report

ANALYSE DE LA SÉCURITÉ PRIVÉE

CIBERSÉCURITÉ



QU'EST-CE QUE C'EST ?

Également connue sous le nom de sécurité numérique, cette pratique consiste à protéger vos informations, vos appareils et vos biens numériques. Cela comprend les informations personnelles, les comptes, les fichiers, les photos et l'argent.
Les menaces de sécurité sont devenues un problème pour tous les utilisateurs qui manipulent des appareils électroniques. Le vol de données et l'atteinte à la vie privée ont contraint les utilisateurs à adopter des mesures de sécurité plus complexes.

La cybersécurité protège les systèmes, les réseaux et les programmes contre les attaques en ligne et les cybermenaces. C'est pourquoi elle est cruciale. C'est la ligne de défense dont disposent les particuliers et les entreprises pour se protéger contre les accès non autorisés aux centres de données et autres systèmes informatiques.

TYPES OF ELECTRONIC SECURITY

Hardware:
Il protège l'intégrité de l'équipement physique d'un système informatique.

Software:
C'est qui protège l'intégrité du support opérationnel d'un système informatique.

Réseau :
L'opération consistant à protéger les données, les applications, les appareils et les systèmes connectés au réseau.

Personnel :
Fichiers, comptes, photos et argent.

Physique :
Il s'agit de l'identification et de l'analyse des dangers et des risques auxquels sont confrontés ou susceptibles d'être confrontés les installations, les biens et les processus.

Logique :
Se réfère à la manière de mettre en œuvre des procédures pour garantir que seules les personnes ou les systèmes d'information autorisés peuvent accéder aux données.

LES CYBERATTAQUES LES PLUS COURANTES

Attaque par déni de service ou DDoS :

Il consiste à provoquer le crash d'un serveur en surchargeant sa bande passante. Ces actions forcent l'interruption d'un site web.

Malware ransomware

Il se caractérise par la restriction de l'accès à un système informatique et la demande d'une rançon pour lever le blocage. Il entraîne une perte massive de données et des dommages économiques importants.

Troyens bancaires

Un logiciel malveillant est installé sur n'importe quel appareil en visitant un site web infecté, en téléchargeant une pièce jointe à un courriel ou même en téléchargeant une application. Une fois ce virus installé sur le téléphone portable, il détecte l'utilisation des services en ligne d'une banque afin de capturer des données personnelles et bancaires.

RECOMMENDATIONS

- Activez toujours la vérification en deux étapes sur tous vos appareils.
- Assurez-vous que vos données personnelles sont cachées.
- Effectuez des contrôles de sécurité sur votre réseau.
- Ne téléchargez des fichiers que si la source est fiable et vérifiée.
- Installez toujours un antivirus et mettez-le à jour fréquemment.
- Créez des mots de passe forts et sécurisés.
- Méfiez-vous de l'affichage d'informations personnelles sur les réseaux sociaux.
- Ne donnez pas d'informations bancaires, d'adresses, de localisation, etc à des personnes inconnues qui s'identifient comme des employés.