Une idée largement répandue, tant dans la vie quotidienne que dans le milieu professionnel, est que les cybermenaces ne concernent pas les utilisateurs. Si initialement, le seul risque informatique était le dysfonctionnement d'un ordinateur dû à un virus, les attaques actuelles peuvent avoir des conséquences bien plus graves.

Au lieu de se décourager face aux risques liés à Internet, il est crucial de démystifier les attaques informatiques, présentant des moyens simples et efficaces pour les éviter. La sécurité dépend avant tout de la connaissance et de la compréhension des risques.

Dans les sections suivantes, nous explorerons comment utiliser Internet de manière plus sécurisée pour prévenir les actes de malveillance.

Commençons par différencier le format et l'extension d'un fichier. Un fichier se réduit fondamentalement à une séquence de 0 et de 1 compréhensible par l'ordinateur. Chaque fichier a un format, une convention d'écriture, qui lui confère des propriétés interprétables par des logiciels.

L'extension, quant à elle, représente le suffixe du nom de fichier renseigné par le créateur (ex. : logo-anssi.jpg pour une image de l'ANSSI).

En résumé, soyez prudent lors des téléchargements et de l'ouverture de fichiers provenant d'Internet, de clés USB ou de disques durs externes. Les cyberattaques souvent débutent par un clic innocent. Installez un antivirus provenant d'une source fiable, effectuez des scans réguliers du disque, et en milieu professionnel, laissez ces manipulations aux équipes informatiques.

Le prochain module abordera la sécurisation du poste de travail. En attendant, examinons de plus près les bonnes pratiques lors de la navigation sur Internet ou de l'utilisation de la messagerie électronique.

Dans le contexte du navigateur, deux protocoles dominent : "http" non sécurisé et "https" sécurisé. Il est recommandé de privilégier les sites affichant le HTTPS.

Qu'est-ce qu'un cookie ? Bien plus qu'une friandise ! C'est un objet lié à un site web, stocké sur l'ordinateur, permettant au site de conserver des informations sur le client.

Il n'existe pas de navigateur idéal, chacun ayant ses avantages et inconvénients. Choisissez en fonction de vos besoins.

Même si l'échange d'e-mails semble anodin, nos boîtes aux lettres électroniques sont exposées à diverses menaces. Soyez vigilant quotidiennement et adoptez les bonnes pratiques pour utiliser votre messagerie en toute sécurité.

En résumé, comprenez les menaces liées à la messagerie et adoptez les bonnes pratiques pour protéger votre organisation.

Avant d'afficher une page web, le navigateur utilise un serveur DNS pour obtenir l'adresse IP du site. L'utilisation d'un serveur mandataire peut optimiser la sécurité et prévenir les infections.

En conclusion, respectez les paramètres de base pour assurer la sécurité de vos appareils. Les équipements modernes offrent diverses interfaces de communication, mais soyez conscient des risques potentiels liés à ces fonctionnalités.

définition des la mission 10

1. Cyber Malveillances : Actions malveillantes opérées sur le cyberespace, englobant des activités comme les attaques informatiques, la diffusion de virus et les menaces électroniques visant à causer des dommages aux systèmes informatiques.

2. Débuts de l'informatique : La période initiale du développement des technologies de l'information, marquée par les premiers ordinateurs et les débuts de l'utilisation de la technologie numérique.

3. Fichiers : Des ensembles de données organisées, représentés en langage binaire (suite de 0 et de 1) et compréhensibles par les ordinateurs. Ils peuvent contenir divers types d'informations, tels que du texte, des images ou des programmes.

4. Format (d'un fichier) : La structure spécifique d'un fichier, définie par une convention d'écriture particulière. Il permet aux logiciels de reconnaître et interpréter le contenu du fichier.

5. **Extension (d'un fichier) :** Un suffixe ajouté au nom d'un fichier pour indiquer son type ou sa nature, souvent utilisé pour identifier le programme associé à son ouverture (par exemple, .jpg pour une image).

6. Sécurité : Ensemble de mesures visant à protéger les systèmes informatiques, les données et les utilisateurs contre les menaces potentielles telles que les cyberattaques, les virus et les accès non autorisés.

7. Téléchargements : L'acte de récupérer des fichiers ou des données depuis Internet vers un dispositif local, comme un ordinateur, un smartphone ou une tablette.

8. Antivirus : Un logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants, y compris les virus, les vers et les chevaux de Troie, afin de protéger un système informatique.

9. **Messagerie électronique :** Un système de communication électronique permettant l'échange d'e-mails entre utilisateurs via Internet.

10. Protocoles (http, https) :** Des règles et des conventions définissant la manière dont les données sont transmises sur Internet. "http" (Hypertext Transfer Protocol) est non sécurisé, tandis que "https" (Hypertext Transfer Protocol Secure) est sécurisé grâce au chiffrement.

11. Cookies : De petits fichiers texte stockés sur l'ordinateur d'un utilisateur par un site web, contenant des informations sur les préférences et les interactions passées, facilitant ainsi une expérience utilisateur personnalisée.

12. Navigateur :Un logiciel permettant aux utilisateurs d'accéder et de visualiser des pages web sur Internet. Exemples : Chrome, Firefox, Safari.

13. Serveur DNS : Un serveur qui traduit les noms de domaine en adresses IP, facilitant ainsi l'acheminement des données sur Internet.