SAÉ 14 Se présenter sur internet

L'identité numérique

L'identité numérique est une empreinte numérique, c'est-à-dire les données que les personnes laissent sur le réseau, mais uniquement les données directement liées à un individu spécifique, telles que les données de fichiers, les données sociales ou les numéros de carte bancaire, les antécédents médicaux, les comptes de différents services.

Les systèmes informatiques modernes peuvent analyser efficacement de grandes quantités d'informations sur les utilisateurs. Il existe de nombreux outils pour suivre l'empreinte en ligne des utilisateurs, et les réseaux sociaux et les pages Web peuvent également stocker de grandes quantités de données. Si une personne n'a laissé son nom, sa photo ou ses documents numérisés nulle part, mais est toujours active sur Internet, il n'est pas difficile de déterminer son identité.

Mais l'absence de lois et de réglementations dans le monde numérique a amené les personnes qui envoient des documents, des identifiants et d'autres informations importantes à perdre le contrôle de leur identité. Le récepteur de données rencontre également un problème, qui est de s'assurer de l'authenticité des données, et la personne qui transmet les données est bien celle qu'elle prétend être.

Une bonne identité numérique nécessite quatre choses :

1. L'un est une grande fiabilité. Établi par le gouvernement pour répondre aux exigences standard du gouvernement et des entreprises pour l'enregistrement initial et une série d'utilisations ultérieures, et pour garantir que la norme de haute fiabilité reste inchangée chaque fois que l'identité numérique est utilisée pour la vérification.

2. La seconde est l'unicité. Chaque personne n'a qu'une seule identité numérique dans un système, et chaque identité système correspond à une seule personne.

3. La troisième consiste à créer après le consentement de l'individu. Veiller à ce que les individus sachent à quoi les agences de données personnelles accéderont et comment elles seront utilisées lorsqu'ils s'enregistreront et utiliseront leurs identités numériques.

4. Le quatrième est de protéger la vie privée des utilisateurs. Prenez des mesures de sécurité intégrées pour garantir la confidentialité et la sécurité, tout en permettant aux utilisateurs d'accéder à leurs données personnelles et en leur permettant de décider qui a accès à ces données.

La plupart de mes traces Internet sont des réseaux sociaux personnels et une partie de ma participation à des activités sociales, de la publication de rapports et d'activités communautaires.

Afin de contrôler mes traces :

La première étape consiste à fermer les comptes de médias sociaux qui ne sont plus utilisés pour supprimer des photos et des vidéos.

La deuxième étape consiste à vérifier les médias sociaux existants pour les informations sensibles telles que les adresses, les informations bancaires, etc.

La troisième étape consiste à vérifier s'il reste des informations de carte bancaire sur le site Web d'achat en ligne et à supprimer l'application indésirable dans le téléphone mobile.

En Chine, une application appelée "National Anti-Fraud Center" est largement diffusée. Elle est créée par le gouvernement. Sa fonction est d'identifier et de bloquer les logiciels malveillants et le vol en ligne, et elle montre et éduque les utilisateurs sur la manière de les prévenir et de les éviter.