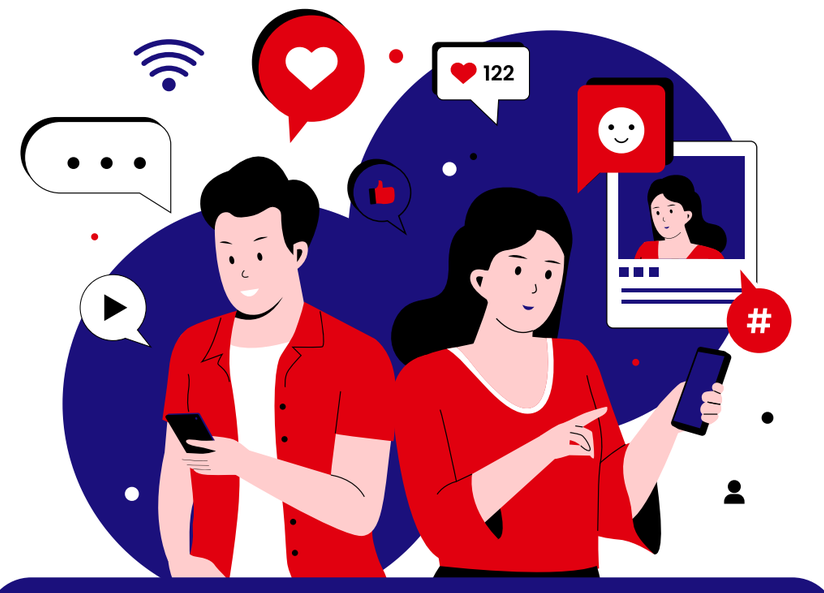
SOMMES-NOUS SURVEILLÉS ?

Like et je te dirai qui tu es

Quand on publie un message ou une photo sur les réseaux sociaux, on partage non seulement le contenu visible, mais aussi des **métadonnées** : qui communique avec qui, à quel moment, depuis quel endroit, avec quel appareil, etc.

En acceptant les **cookies et les Conditions Générales d'Utilisation,** on autorise les plateformes à collecter et stocker ces **traces numériques** : likes, commentaires, photos, recherches, déplacements... Grâce à elles, les réseaux sociaux construisent un **profil détaillé de chaque utilisateur** : habitudes, centres d'intérêts et opinions, aussi bien politiques, sexuelles, religieuses que culturelles.



Avec 10 likes, un réseau en sait plus sur vous que votre collègue de bureau ; 70 likes que vos amis ; 125 likes qu'un membre de votre famille et 225 likes que votre conjoint.

Légal... mais questionnable !

Le **suivi publicitaire** (ou "pistage publicitaire") permet d'envoyer des publicités adaptées à votre profil.

Les **"traqueurs"** et cookies sont utilisés sur une grande majorité de sites : ils vous pistent sur internet pour enrichir votre profil.

La **géolocalisation** permet de savoir ou vous êtes... et où vous n'êtes pas. En 2018, des traces des courses sur Strava de soldats ont permis de géolocaliser des bases militaires secrètes.

Pendant les guerres, ces données ont été utilisées pour repérer des personnalités politiques ou des soldats.

Du profil au profit

Beaucoup d'**entreprises privées et d'administrations publiques** traitent et stockent les données personnelles. Certaines entreprises ont fondé leur modèle d'affaire sur la **collecte et l'agrégation de données publiques et semi-publiques** dans le but de construire des profils de réputation de personnes et d'entreprises et de monétiser l'accès à ces informations.

Parfois, ces données sont **volées** soit par des employés, soit par des cybercriminels. Ces données sont ensuite **mises en vente ou publiées** gratuitement sur le Darknet. Au delà du spam publicitaire, les utilisateurs peuvent être victimes d'attaques ou d'arnaques.

Le phishing ou hameçonnage

Ces attaques utilisent les **coordonnées** laissées sur des sites de commerce en ligne, de livraison ou même des sites de banques ou d'organismes de santé, et qui ont été vendues ou piratées, pour envoyer des messages qui jouent sur les émotions pour faire **cliquer sur un lien, un bouton ou une pièce jointe** pour implanter des virus informatiques dans les appareils.

La fraude au président

Escroquerie où un cybercriminel **se fait passer pour un dirigeant d'entreprise** (souvent le PDG) afin de tromper un employé et lui faire effectuer un virement urgent vers un compte frauduleux. L'arnaque repose sur **l'usurpation d'identité**, la pression psychologique et le caractère soi-disant confidentiel de la demande. Elle vise principalement les entreprises et peut causer des pertes financières importantes.

Le doxxing

Il s'agit de la **divulgation publique d'informations intimes**. Issu d'une vengeance personnelle, d'activisme politique, de jalousie ou d'une volonté de nuire à l'image sans réel fondement, le doxxing peut avoir des conséquences graves, comme du harcèlement, et plus spécifiquement du cyberharcèlement, la perte d'un emploi ou des difficultés familiales.

Pour aller plus loin :

- *Cybersécurité et hygiène numérique au quotidien : 129 bonnes pratiques à adopter pour se protéger*, de Gildas Avoine, Pascal Junod, Dunod, 2024.
- *Guide de survie des aventures sur Internet*, par les associations Ritimo, CECIL, et LDH, 2023
- degooglisons-internet.org et outils de protection de la vie privée sur privacyguides.org

Les Maths en Scène
Les Maths où on ne les attend pas !
ESCRIME
ESprit CRitique & Mathématique
Un chemin vers la citoyenneté
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
Liberté
Égalité
Fraternité