Pourquoi proposer l’authentification multifacteur en ligne

En créant des comptes personnels sur internet, pour l’usage par exemple de sites de e-commerce, de banque, de messagerie… les particuliers fournissent des données personnelles dont certaines sont sensibles. L’accès à ces comptes se fait grâce à la mise en place d’un mécanisme d’authentification pour vérifier que la personne qui se connecte est bien la personne autorisée à y accéder. Ce mécanisme d’authentification peut être simple avec seulement un mot de passe par exemple, ou multifacteur c’est-à-dire exigeant un mot de passe et un autre dispositif.

Un second facteur d’authentification plus compliqué à obtenir

Comme le rappelle la Cnil dans sa fiche pratique, une authentification multifacteur empêche le cyberpirate qui aurait réussi à se procurer les identifiants et le mot de passe de l’usager d’accéder au compte, faute de disposer du second facteur d’authentification généralement plus compliqué à obtenir. Concrètement, ce second facteur peut consister en un code reçu par mail ou par SMS, par téléphone ou bien généré

via une application installée sur le matériel. Ce code confidentiel n’est généralement valable que quelques minutes. À noter, depuis fin 2019, les banques et les prestataires de services de paiement sont obligés de proposer une authentification multifacteur pour les paiements à distance, l’accès au compte ainsi que pour les opérations sensibles.

Pour consulter la fiche de la Cnil : www.cnil.fr