

La double authentification

la protection indispensable pour sécuriser vos accès.

Aujourd'hui, un simple mot de passe pour s'authentifier en tant qu'utilisateur n'apporte plus un niveau de sécurité satisfaisant et ne protège pas suffisamment vos données sensibles.

Les occasions de se faire dérober son mot de passe sont fréquentes.

Même en appliquant les règles suivantes :

- mot de passe différent pour chaque compte ;
- modification régulière des mots de passe ;
- utilisation de phrases secrètes difficile à deviner ;
- pas d'informations personnelles faciles à trouver (date de naissance, numéro de téléphone etc.).

De nombreuses techniques cybermalveillantes permettent de trouver vos mots de passe (cheval de Troie, phishing, écoute du clavier informatique etc.).

En cas de piratage, vos informations personnelles comme professionnelles seront perdues, exploités, revendus avec des conséquences souvent dramatiques.

La solution la plus efficace : la double authentification



Dans le domaine de la sécurité informatique, le principe de la double authentification, complémentaire à d'autres mesures de sécurité est efficace et simple.



Saisie du login et du mot de passe.



Le système envoie un code chiffré sur le smartphone personnel.



La saisie du code ouvre l'accès après la double authentification.