Bonnes pratiques sécurité informatique

Un poste de travail mal protégé peut mettre en péril non seulement les informations traitées sur le poste lui-même, mais également les systèmes auxquels il se connecte. Une fois piraté, il peut devenir une porte d'entrée vers des systèmes plus sensibles dès lors qu'un logiciel espion a pu être installé à l'insu de l'utilisateur.

Le comportement de l'utilisateur de ce poste de travail est essentiel, s'il applique les règles élémentaires de sécurité, il va renforcer la sécurité de ce poste et de l'ensemble des systèmes auxquels il se connecte.

Des règles comportementales à respecter

- **Le mot de passe est la clé d'accès à l'information, cette clé doit être personnelle et suffisamment complexe pour ne pas pouvoir être trop facilement découverte (*https://securite-informatique.dsi.universite-paris-saclay.fr/docs/motdepasse.pdf*).**
- **Ne pas laisser visibles ses mots de passe (post-it sur l'écran, sous le clavier, …).**
- **Verrouiller sa session dès que l'on s'éloigne de son ordinateur.**
- **Ne pas ouvrir les courriers électroniques douteux ou d'expéditeurs inconnus.**
- **Ne jamais répondre aux courriels demandant des informations personnelles (mot de passe, code d'accès, …).**
- **Sauvegarde systématique et quotidienne des données sensibles (Suivre les consignes fournies par le service informatique dont dépend l'utilisateur).**
- **Fermer à clé la porte de son bureau en cas d'absence.**
- **Rendre compte sans délai de tout incident (*securite.di@universite-paris-saclay.fr*).**