À l'approche des vacances d'été, un petit rappel des bonnes pratiques de sécurité s'impose. Ces pratiques ne s'appliquent pas uniquement à l'intérieur de l'université, mais également lorsque vous êtes en déplacement professionnel ou en voyage.

Avant votre départ

Interrogez-vous et vérifiez la législation en vigueur dans le pays de destination

Certains pays disposent de lois en vigueur sur le matériel informatique, le stockage de donnée, les applications etc… et pourraient vous contraindre à des vérifications une fois sur leurs sols.

Assurez-vous de n'emporter que le stricte nécessaire des outils/données

Indispensables à la réalisation de vos tâches ou missions. Évitez le plus possible d'emporter des données sensibles.

Assurez-vous de stocker les données de manière sécurisée

et ne pas les rendre facilement accessibles en cas de contrôle inopiné.

Faites la mise à jour de vos appareils avant de partir

et assurez-vous que les données que vous emportez en voyage ont été sauvegardées sur un autre support que vous laisserez dans un endroit sécurisé.

Pendant votre déplacement

Protégez vos écrans des regards indiscrets
en vous plaçant de manière à ce que les personnes autour ne puisse pas les voir (dos contre un mur par exemple) et utilisez des filtres de confidentialité (à placer devant l'écran).

Faites attention à vos conversations, soyez discret
et ne partagez pas à haute voix des données de votre organisation qui pourraient être confidentielles.

Ne laissez jamais vos équipements sans surveillance
y compris dans les chambres d'hôtel ou dans les coffres de voiture. Si vous ne pouvez pas faire autrement, une idée pourrait être d'enfermer votre PC dans votre valise, elle sera plus difficile à dissimuler par le personnel de ménage par exemple.

Ne vous connectez jamais à des réseaux publics
il est très facile d'avoir accès directement à vos téléphones ou vos ordinateurs via ces réseaux non sécurisés. Les attaquants pourraient voir tout ce que vous faites et ce que vous tapez, comme des codes confidentiels ou des informations bancaires. Si vous n'avez pas accès à un réseau sécurisé, utilisez le partage de connexion de votre téléphone et configurez un mot de passe fort, ou encore une connexion via client VPN si vous en possédez un.

Ne vous branchez pas sur des stations de recharge publiques ou des ports USB inconnus.
Les pirates y placent parfois des logiciels malveillants destinés à infecter vos équipements ou à récupérer vos données. Utilisez plutôt une batterie externe et n'autorisez jamais l'accès à votre téléphone.

BON ÉTÉ!

Le Service des Ressources Informationnelles