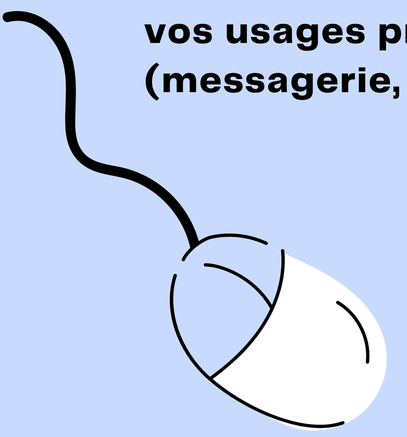
Bonnes pratiques et mesures préventives afin de limiter les risques cyber

Échange téléphonique

_ Soyez vigilants concernant les appels d'origine inconnue ou inattendue
– Méfiez-vous des appels de personnes inconnues exigeant de vous une réponse
ou une action immédiate et vous intimant de ne pas en informer votre hiérarchie
ou vos collaborateurs.
–Ne transmettez jamais d'informations personnelles (mot de passe, code de cartes bancaires…) par téléphone. Aucune administration ou société commerciale sérieuse ni même votre service informatique ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone

Visite d'un site web ou Lancement d'une application

Vérifier la fiabilité et la réputation des sites que vous visitez
– Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs.
– Restez attentifs aux liens renvoyés par les moteurs de recherche avant de cliquer
–Soyez vigilants aux fausses informations
–N'en dites pas trop sur les réseaux sociaux, vos données peuvent être exploitées
par des personnes malveillantes
–Pour limiter l'effet boule de neige d'une action malveillante, séparez
vos usages professionnels et personnels (messagerie, équipements, identifiants..)



Réception d'un Courriel

–Soyez vigilants concernant les documents transmis en pièce jointe de courriels
–Vérifier la cohérence entre l'expéditeur présumé et le contenu du message
et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement
l'émetteur du mail
–Ne pas ouvrir les pièces jointes provenant d'expéditeurs inconnus ou d'un
expéditeur connu mais dont la structure du message est inhabituelle ou vide
– Si des liens figurent dans un courriel, soyez très vigilants, passer la souris dessus
sans cliquer. l'adresse complète du site s'affichera dans la barre d'état.
–Ne jamais répondre par courriel à une demande d'informations personnelles
ou confidentielles
–Méfiez-vous des messages (mail, SMS, chat…) dont la provenance ou la forme
est douteuse.
–Attention aux appels aux dons frauduleux

Utilisation d'une clé USB ou d'un dispositif connectable

–N'insérez aucun support USB dont vous ignorez la provenance dans votre ordinateur. Il pourrait être porteur d'un virus et infecter votre machine.
–Soyez vigilants lorsque vous insérez votre clé USB sur un équipement que vous
ne connaissez pas.
–Vérifier la présence d'un antivirus fonctionnel et à jour sur le poste sur lequel
vous vous apprêtez à insérer une clé USB.