CYBERSÉCURITÉ

Que dois-je faire ?

MON ENVIRONNEMENT DE TRAVAIL

- Utiliser un bon antivirus ! Un prix minime à payer pour garantir la sécurité de ses données.
- Ne pas télécharger de logiciels "crackés". Un pirate a pu y installer un virus !
- Ne pas aller sur les sites de streaming illégaux. Ces sites peuvent exécuter des scripts à votre insu encore ouvrir des fenêtres pouvant exploiter des failles de sécurité de votre navigateur.
- Segmenter l'utilisation personnel et professionnel. Par exemple, d'un point de vue personnel et professionnel, utilisez deux adresses de messagerie différentes.

NE PAS SE SENTIR INVULNÉRABLE

- ·Ne pas croire que nous n'avons rien à perdre même si nous sommes piratés. En réseau, tout le monde peut s'infecter et tout comme le coronavirus, vous pouvez infecter d'autres personnes.
- Rien n'est infaillible. La cybersécurité touche tout le monde et toutes les plateformes (Windows, MacOS, Linux, Android...). D'ailleurs, les pirates développent de plus en plus de virus pour Apple.
- Ne pas croire qu'un antivirus vous protège de tout! Le meilleur mécanisme de protection c'est vous! A vous d'appliquer les règles de bon usage pour ne pas vous faire piéger.

LA RÉCUPÉRATION DE DONNÉES

- Faire attention aux fausses pages dites d'hameçonnage (phishing). Les hackers répliquent de fausses pages vers lesquelles ils vous redirigent dans un mail bien confectionné. Ils volent alors vos identifiants que vous avez cru entrer sur un site légitime alors qu'il s'agit d'un site pirate.
- Lorsqu'un lien est présent (dans un mail par exemple), sans cliquer, passez votre souris sur ce lien. Le véritable lien de redirection caché est inscrit sur la bulle qui apparaît.
- Toujours regarder scrupuleusement l'adresse d'un site consulté car "faceboook.fr" n'est pas la même chose que "facebook.fr"
- Avoir au minimum un cadenas sur chaque site consulté (surtout en cas de paiement en ligne ou envoi de données sensibles telles qu'une connexion à un site). L'utilisation du protocole HTTPS est obligatoire depuis le RGPD afin de garantir la sécurité des données personnelles de chaque usager.
- Ne pas se connecter sur des réseaux inconnus. Un pirate pourrait créer un faux réseau Wifi nommé "WIFI-GRATUIT" par exemple et intercepter toutes les données sortant de votre smartphone.

LES MOTS DE PASSE

- Utilisez un mot de passe unique pour chaque service.
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'une date de naissance etc.)
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours, est un bon compromis pour les systèmes contenant des données sensibles.
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé aux risques (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ; utilisez plutôt un conteneur de mot de passe sécurisé tel que "Keepass" préconisé par l'ANSSI.
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
- Pour générer les mots de passe, voici une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).
- Deux méthodes pour choisir vos mots de passe :
  - La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi deviendra ght8CD%E7am ;
  - La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.