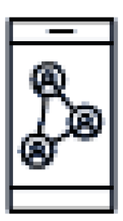
LES 10 REGLES D'OR

DE LA CYBERSECURTIE

PROTEGEZ VOS COMPTES AU MOYEN D'UNE AUTHENTIFICATION FORTE

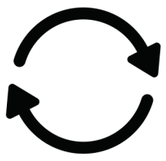
La longueur, un gage de sécurité. Les mots de passe longs sont plus efficaces car ils sont plus difficiles à cracker pour les cybercriminels étant donné les nombreuses combinaisons de caractères possibles. Les mots de passe forts comportent **au moins 12 caractères**, **ne sont pas faciles à deviner et doivent contenir : des majuscules, des minuscules, des caractères numériques et des caractères spéciaux (&,$,%, !,=,+..). Utilisez l'authentification multifacteurs dès que possible.**

MOTS DE PASSE DIFFERENTS



Utilisez des mots de passe différents pour les comptes professionnels et les comptes privés

STOCKAGE DES DONNEES CENTRALISE

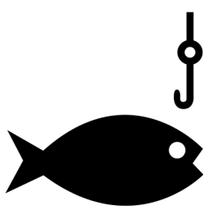


Stockez toutes vos données dans un système où les données sont régulièrement sauvegardées de manière centralisée

MISES A JOUR DE SECURITE

Effectuez les mises à jour de sécurité sur tous vos appareils dès qu'elles sont disponibles

MEFIEZ-VOUS DES MESSAGES INATTENDUS



Protégez-vous contre le phishing en vous posant les questions suivantes :

- Est-ce que je connais l'expéditeur ?
- Est-ce que j'attendais un message à ce sujet ?
- Le message évoque-t-il un éventuel partage d'informations telles qu'un nom d'utilisateur, un mot de passe ou des coordonnées bancaires ?
- Est-ce urgent ?
- Où le lien mène-t-il ? (passez simplement votre souris dessus, sans cliquer)
- Le message contient-il un code QR ?
- Le message s'adresse-t-il à moi personnellement ?
- Le message contient-il des erreurs linguistiques ?
- Le message se trouve-t-il dans le dossier « Courrier indésirable » ?
- Quelqu'un essaie-t-il de susciter ma curiosité ?
- Un paiement est-il demandé ?

Comment réagir face à un e-mail de phishing :

- N'y répondez pas, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.
- Ne communiquez jamais les informations bancaires demandées par SMS ou par mail
- Signalez la tentative de phishing à [] et supprimez l'e-mail ou le SMS.

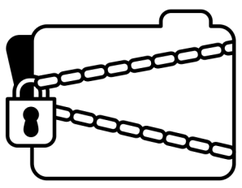
LES 10 REGLES D’OR
DE LA CYBERSECURTIE

EVITEZ LES WI-FI PUBLICS

Évitez les Wi-Fi publics et utilisez le réseau privé virtuel (VPN) de l'organisation

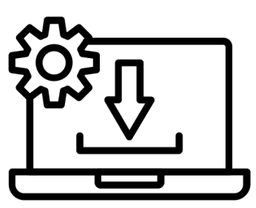
NE PAS LAISSEZ D’INFORMATIONS PHYSIQUES

Ne laissez jamais d'informations physiques (papiers, etc.) ou d'appareils sur votre bureau sans surveillance



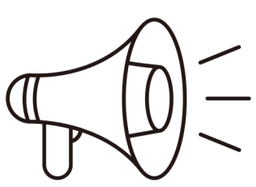
RESPECTEZ LES MESURES SUIVANTES LORSQUE VOUS TRAITEZ DES INFORMATIONS INTERNES OU CONFIDENTIELLES

- Verrouillez votre ordinateur lorsque vous le laissez sans surveillance.
- Ne laissez pas d'ordinateurs ou de documents sans surveillance sur votre bureau en dehors des heures de travail.
- Ne laissez pas de papier sans surveillance dans les imprimantes.
- Faites toujours attention à votre environnement lorsque vous accédez à des informations confidentielles ou que vous en discutez dans des lieux publics. Dans la mesure du possible, essayez de vous isoler pour éviter que quelqu'un n'entende une conversation.



TELECHARGER DES APPLICATIONS OU LOGICIELS

N'utilisez que des sites et des plateformes officiels pour télécharger des applications et des logiciels



SIGNALEZ TOUS LES INCIDENTS LIÉS À LA SÉCURITÉ DE L'INFORMATION À VOTRE FOURNISSEUR IT

N’hésitez jamais à prendre contact avec [Fournisseur IT] si :

- vous avez des questions ou des remarques sur ce document ;
- vous constatez une violation de ce document ;
- vous soupçonnez la présence d'incidents ou en avez la confirmation