5 JE RESTE VIGILANT AU QUOTIDIEN

Les cybercriminels ne prennent pas de vacances, alors le risque est permanent.

- Je respecte les consignes informatiques et les bonnes pratiques apprises dans mon entreprise.
- En cas de doute, j'informe l'équipe **Informatique :**

➔ Email suspect
➔ Comportement anormal du pc ou applications...
➔ Personne inconnue dans les locaux.

QUE FAIRE EN CAS D'ATTAQUE ?

La cellule de crise cyber sécurité

- Une cellule de crise cyber sécurité est en place au sein de l'entreprise pour m'informer et me guider sur la conduite à tenir.

Message que je peux recevoir :

CELLULE 3C - DSI : Attaque informatique en cours.
Déconnecter WIFI et câble réseau des PC.
Ne les éteignez pas. Ne contactez pas la DSI.
Informations par SMS.

- Je débranche le câble réseau.
- Je désactive le WIFI selon la procédure ci-dessous.

Je fais un clic droit sur le logo **WIFI**
Ensuite, je fais un clic sur le mode avion
Lorsque je vois le globe ou le mode avion
mon pc n'est plus connecté au réseau.

- J'attends les consignes et informations de la DSI et de mes responsables hiérarchiques.

DE SANGOSSE
Siège social : «Bonnel» CS 10005
47480 PONT DU CASSE
05 53 69 36 30

En savoir plus :

GUIDE PRATIQUE POUR RESTER VIGILANT AU QUOTIDIEN

LES 5 BONS RÉFLEXES POUR LA SÉCURITÉ DE L'INFORMATION

1 JE PROTÈGE L'INFORMATION

- Sous forme papier ou numérique, lors de toutes mes conversations Teams, WhatsApp ou autre, l'échange d'informations est permanent.
- Les protéger est un devoir.

Ex : Lors d'un démarchage téléphonique : ne pas parler des logiciels, des outils Cyber que j'utilise.

2 JE PROTÈGE MES IDENTIFIANTS

- En plus de la solution de double authentification **« DUO »** et de politique de changement de mot de passe, je choisis un mot de passe robuste :
  - ➔ Difficile à deviner,
  - ➔ Long, complexe,
  - ➔ Différent pour chaque application.
- J'utilise un gestionnaire de mots de passe (coffre-fort) Bitwarden (préconisé), Keepass etc.

Celui-ci permettra de ne plus avoir à retenir les mots de passe et appliquer les recommandations ci-dessus facilement.

- Je ne partage pas mes logins/identifiants et mots de passe.

3 JE SÉCURISE MES APPAREILS

Protéger mes appareils est primordial.
Je prends les précautions nécessaires :

Mon compte

Des personnes malveillantes peuvent récolter mes informations à mon insu, afin d'accéder à mon système informatique et / ou usurper mon identité.

- Je verrouille mes appareils lorsque je m'absente, même quelques minutes.

Messagerie mail

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des cyberattaques.

RAPPEL : Un clic suffit pour être hacké

- Dans les emails, j'applique ce que j'ai appris lors des tests phishing.
- J'ignore les pièces jointes et liens inconnus ou suspects.

Logiciels et mises à jour

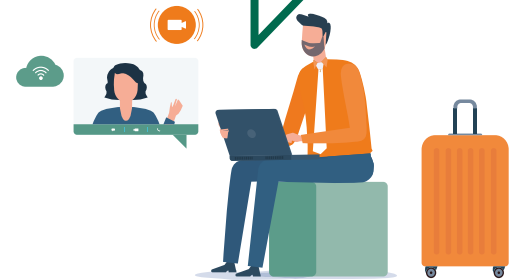
Mettre à jour régulièrement les logiciels de mes appareils numériques est essentiel.

- Avant de télécharger un logiciel, je vérifie sa légitimité avec l'équipe **Informatique.**

Si les mises à jour ne sont pas effectuées régulièrement, les attaquants peuvent plus facilement mener à bien leurs opérations.

- Je les fais même si cela est souvent contraignant.
- Je reste vigilant lors de ma navigation sur internet.

4 JE RESTE PRUDENT EN DÉPLACEMENT



- Je ne laisse jamais mes appareils sans surveillance *(ex : même quand je vais aux toilettes dans un train).*
- Je verrouille mon pc et mon téléphone dès que je m'absente du bureau, d'une salle de réunion, etc.
- Je reste vigilant dans les zones à risques (train, taxi et hôtel).
- J'évite les réseaux WIFI publics ou inconnus, j'utilise plutôt le partage de connexion 4G de mon smartphone.
- J'utilise **systématiquement** mon VPN.
- Je ne laisse personne brancher un objet sur mon pc.
- Je ne branche pas mes appareils sur des ports USB publics.
- Je n'emprunte pas de câbles d'alimentation.
- Je n'accepte aucun goodies de type connecté.
- Quand je suis nomade je ne prends que l'essentiel, j'utilise un filtre de confidentialité.
- Je fais attention à ce que je dis dans les lieux publics.