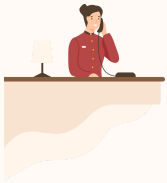

RÉCEPTIONNISTES, SOYEZ VIGILANTS !

1. ATTENTION À VOS PROPOS !

Ne donnez aucune informations par message ou téléphone ; elles pourraient être utilisées plus tard pour piéger l'établissement.
Ex : Aucun contact Booking.com ne vous appellera pour discuter avec vous de votre facture, d'un avoir ou autre...

2. VÉRIFIER LES LIENS

Vérifiez sur 3 sites (**à mettre en favoris**) **avant de cliquer sur un lien.**
Ex. URL Void, ShouldIClick, Virus Total

3. NE PAS OUVRIR DE PJ INCONNUES

N'ouvrez aucune pièce jointe si vous ne connaissez pas l'expéditeur.
Ex : N'ouvrez pas de PJ de la part d'un client qui n'a pas encore fait son check-in.
Pour les impressions, demandez le N° de chambre et vérifiez qu'il s'agit du bon client !

4. SE MÉFIER DES MAILS QUI SEMBLENT AUTOMATIQUES

Ne cliquez pas sur une demande de changement de mot de passe si vous n'êtes pas à l'origine de la demande.
Changez en revanche régulièrement les mots de passe des extranets et logiciels clés, surtout en cas de doute d'infection.

5. LANCER UNE ANALYSE PAR SEMAINE

Analysez vos PC de réception chaque semaine par un logiciel puissant qui détecte et désactive les logiciels malveillants.
Ex: RogueKiller

6. APPLIQUER LES BONNES PRATIQUES CYBER !

- **Pas de mot de passe sur un post-it** à côté du PC ;
- **Pas d'envoi de mot de passe** par mail ;
- **Pas de copie/scan de données sensibles** (pièce d'identité, CB...)
- **N'insérez aucune clé USB** (trouvée ou remise par une personne) dans les PC de l'hôtel.

GHR
GROUPEMENT DES HOTELLERIES & RESTAURATIONS DE FRANCE