

NOS PRÉCONISATIONS ET CONSEILS

face à la cyberattaque
Viamedis



Nos préconisations

- **Ne pas répondre à des prises de contact de VIAMEDIS, ITELIS, KALIXIA ou HÉLIUM**, par téléphone ou par mail pour obtenir vos coordonnées bancaires et/ou personnelles.
- **Ne jamais communiquer vos identifiants et vos mots de passe**, cela même à votre banque.
- **Redoubler de vigilance dans les prochaines semaines** concernant toutes les communications que vous pourriez recevoir et de ne jamais utiliser les liens directement fournis dans ces communications reçues afin d'**éviter toute tentative de phishing**.
- **Ne jamais régler un reste à charge par téléphone avec votre carte bancaire**.

Nos conseils

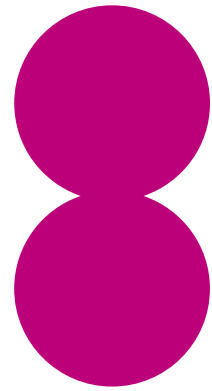
▪ Comment agir face à un appel ou un mail suspicieux ?

1. Nous vous recommandons de **conserver toutes les preuves** (messages, adresse du site web, captures d'écran...) de cette démarche suspicieuse.
2. **Ne cliquez sur aucun lien et ne communiquez jamais par téléphone ou mail vos données personnelles et/ou bancaires ainsi que vos mots de passe.**
3. **Faites une déclaration** sur le site du gouvernement dédié à ce sujet : internet-signalement.gouv.fr

▪ Que faire si vous constatez une anomalie avérée sur vos données personnelles et/ou bancaires ?

Alertez immédiatement votre banque et déposez plainte. Vous pouvez être accompagné(e) gratuitement dans cette démarche par l'association **France Victimes au 116 006** (appel et service gratuits) : numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.





Hélium

Partenaire santé & prévoyance