

Proposition de corrigé – mail/phishing

De :	Jules-martine@ecovibe.com
À :	liste-clients-2024
Cc :	
Cci :	
Objet :	Mail frauduleux ? que faire ?

NON OFFICIEL

Chers clients,

Nous souhaitons vous informer sur un sujet crucial : le **phishing**. Cette pratique consiste à tromper une personne en se faisant passer pour une entité de confiance dans le but de récupérer des informations sensibles, telles que des mots de passe ou des coordonnées bancaires. Les attaques de phishing peuvent prendre plusieurs formes, notamment des courriels, des messages texte ou des sites web frauduleux.

Si vous pensez avoir été victime de phishing, comme récemment l'un de nos clients, voici quelques pratiques recommandées :

1. **Ne cliquez pas sur les liens** : Ne répondez pas et évitez de cliquer sur les liens suspects contenus dans le message.
2. **Changez vos mots de passe** : Si vous avez donné des informations personnelles, modifiez immédiatement vos mots de passe sur les sites concernés.
3. **Contactez votre banque ou votre fournisseur** : Informez-les immédiatement pour qu'ils puissent prendre des mesures nécessaires.
4. **Signalez l'incident** : Prévenez votre service informatique ou les autorités compétentes pour qu'ils puissent enquêter.

Pour vous protéger, restez vigilant et vérifiez toujours l'expéditeur des courriels avant d'agir. En cas de doute, n'hésitez pas à nous contacter.

Prenez soin de votre sécurité en ligne !

Cordialement,

Jules MARTIN
D.A.F