Fiche de sensibilisation au phishing (hameçonnage)

BIOTECH DENTAL GROUP

Date : 27 mai 2025
Objectif : savoir identifier, éviter et signaler une tentative de phishing

1 . Qu'est-ce que le phishing ?

Le phishing est une tentative frauduleuse visant à tromper un utilisateur pour lui soutirer des informations sensibles (identifiants, mots de passe, données bancaires, etc.) ou lui faire installer un logiciel malveillant.

Ces attaques se font souvent par courriel, mais aussi via SMS, appels téléphoniques ou réseaux sociaux.

2 . Reconnaître un courriel phishing

- Expéditeur douteux (adresse courriel suspecte, nom d'expéditeur incohérent avec l'adresse, ...),
- Message alarmiste ou urgent,
- Fautes de grammaire ou d'orthographe,
- Demande d'information sensible,
- Pièces jointes et liens suspects,
- Signature de courriel générique ou manquante.

3 . Que faire en cas de doute ?

- Ne pas cliquer sur les liens ou pièces jointes,
- Ne pas répondre au message,
- Transférer le mail au service informatique,
- Déplacer le message dans les « Eléments indésirables » ou dans un dossier « Phishing »,
- Après analyse de l'équipe informatique, supprimer le message si confirmé comme étant du phishing,
- Changer de mot de passe.

4 . À intégrer dans sa routine

- Toujours vérifier l'adresse de l'expéditeur,
- Réfléchir avant de cliquer sur des liens ou pièces jointes,
- Ne pas transmettre d'identifiants par courriel,
- Signaler systématiquement les messages suspects,
- Avoir un mot de passe robuste,
- Mettre à jour régulièrement l'antivirus,
- Être attentif aux formations et messages de sécurité dispensés par l'entreprise.

5 . Que faire si l'on se fait piéger ?

- Signaler l'incident à l'équipe informatique,
- Attendre les instructions de l'équipe informatique (Changer de mot de passe, réinstaller le PC, ...).

6 . Ce que vous risquez en cas de fuite des données

Le phishing présente plusieurs types de risque pour les entreprises : Pertes financières, vol de données sensibles, pouvant entraîner la perte de confiance des clients, et affecter la réputation de l'entreprise.

Le phishing présente également des risques pour VOUS : usurpation d'identité, harcèlement, piratage de compte, ...

7 . Coordonnées du DPO

Si vous avez des questions n'hésitez pas à contacter votre DPO, qui vous accompagne dans vos démarches de sécurisation des données à l'adresse : **dpo.bd@biotech-dental.com**

Aurélia DUBOIS
Senior Vice-President Legal
DPO
Groupe Biotech Dental

BIOTECH DENTAL GROUP