Fiches réflexes :

SUSPICION DE HAMEÇONNAGE



Qu’est-ce que le hameçonnage ?

Il s'agit d'une tentative de fraude visant à vous inciter à cliquer sur un lien malveillant, ouvrir une pièce jointe infectée ou encore transmettre vos identifiants ou des données personnelles. Ces messages prennent souvent l’apparence d’institutions connues : banques, administrations, prestataires, direction, collègues, etc.

Signes d’un message suspect :

- Expéditeur inconnu ou adresse étrange.
- Fautes d’orthographe ou de syntaxe.
- Ton alarmiste ou pressant : "Urgent", "Votre compte sera bloqué", etc.
- Demande de cliquer sur un lien ou de saisir des identifiants.
- Pièce jointe inattendue (même d’un contact connu).

Que faire en cas de doute ?

- Ne cliquez sur rien (ni lien, ni pièce jointe).
- Ne répondez pas au message.
- Signalez immédiatement au référent cybersécurité ou responsable informatique ou/et à votre supérieur hiérarchique si besoin.
- Conservez le message suspect sans l’effacer.
- Déconnectez-vous du réseau si vous avez cliqué ou ouvert une pièce jointe

Que doit faire l’établissement ?

- Analyse de l’email et de son origine.
- Vérification de l’intégrité du poste.
- Information du personnel si besoin.
- Déclaration à l’ANS / CERT Santé et, si nécessaire, à la CNIL.

Comment se protéger à l’avenir ?

- Vérifiez toujours l’adresse de l’expéditeur.
- Passez la souris sur les liens pour voir l’adresse réelle.
- Ne communiquez jamais vos identifiants par email.
- Soyez prudent, même avec des messages internes.
- Signalez systématiquement les messages suspects.

Collectif SI Médico-Social Hauts-de-France