Hameçonnage

Comprendre les **menaces**

L'hameçonnage ou *phishing* en anglais est une technique frauduleuse destinée à leurrer une personne pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe ...) en se faisant passer pour un tiers de confiance. Le leurre peut être un faux message, un SMS ou un appel téléphonique semblant venir d'une banque, d'un réseau social, d'un fournisseur d'énergie, d'un site de commerce en ligne, d'une administration ou autre.

Le but recherché par les pirates :
Voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires ...) pour en faire un usage frauduleux.

Les bonnes **pratiques**

- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone.
- Avant de cliquer sur un lien douteux, positionnez le curseur sans cliquer pour vérifier l'adresse réelle.
- Vérifiez l'adresse du site dans votre navigateur pour détecter tout site frauduleux.
- En cas de doute, contactez directement l'organisme concerné.

Comment se **protéger** ?

Reconnaître un mail de phishing :
Soyez vigilant envers des signes d'alerte comme une offre alléchante, une apparence suspecte, une pièce jointe inattendue, etc.

Exemples de mails suspects :

- Demande de mise à jour ou confirmation de données sous menace de sanction.
- Problème de paiement ou facturation, incitant à régler un impayé.
- Demande d'informations contre un cadeau ou pour participer à un jeu-concours.
- Appel à l'aide d'un prétendu proche nécessitant une aide financière.

Si vous êtes **victime**

Dans le cadre professionnel :

- Prévenez immédiatement le support informatique.

Dans le cadre privé :

- En cas de doute, contactez directement l'organisme concerné.
- Changez immédiatement le mot de passe divulgué sur tous les sites.
- Conservez les preuves, surtout le message d'hameçonnage, pour déposer plainte.

Groupe CAL
Des agriculteurs engagés !