

L'HAMEÇONNAGE (phishing)



CYBERCRIMINEL



VOL DE DONNÉES PERSONNELLES

Technique :

Leurre envoyé via un faux message, SMS ou appel téléphonique de banques, de réseaux sociaux, d'opérateurs, de fournisseurs d'énergie, d'e-commerce...

But :

Voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux

Comment éviter de se faire hameçonner ?



CONTACTS UTILES

- Signal-spam.fr
 - Phishing-initiative.fr
 - Info_Escroqueries
- 0 805 805 817 (gratuit)

VICTIME



Ne communiquez jamais d'informations sensibles par messagerie ou téléphone



Confirmez avec l'organisme concerné



Vérifiez votre dernière connexion



Utilisez des mots de passe différents et complexes



Ne cliquez jamais sur un lien douteux



Vérifiez l'adresse du site dans votre navigateur



Activez la double authentification

SI VOUS AVEZ MALENCONTREUSEMENT COMMUNIQUÉ VOS DONNÉES PERSONNELLES, VOUS DEVEZ :

- Faire opposition immédiatement (en cas d'arnaque bancaire)
- Déposer plainte
- Changer vos mots de passe

POUR EN SAVOIR PLUS, RETROUVEZ LA FICHE RÉFLEXE DÉTAILLÉE SUR :

www.cybermalveillance.gouv.fr