COURRIELS D'HAMEÇONNAGE BANCAIRE

Les courriels d'hameçonnage bancaire sont des courriels d'escrocs qui incitent les destinataires à partager leurs données personnelles, financières ou de sécurité.

COMMENT CELA SE PASSE-T-IL ?

Ces courriels :

peuvent ressembler aux correspondances envoyées par les banques (ex. logo, trame et discours identiques à de vrais courriels).

vous invitent à télécharger un document attaché ou à cliquer sur un lien.

Les cybercriminels comptent sur le fait que les gens sont pressés ; au premier abord, ces faux courriels peuvent sembler vrais.

Les cybercriminels investissent de plus en plus les terminaux mobiles tablette et smartphone. Veillez à la mise à jour de leurs logiciels notamment de sécurité.

QUE FAIRE ?

- **Gardez vos logiciels et votre antivirus à jour.**
- Malgré l'urgence décrite, **prenez le temps d'examiner attentivement** la demande.
- Soyez très **vigilant/e** si un courriel «bancaire» vous invite à communiquer une information sensible (ex. votre mot de passe de compte en ligne).
- **Vérifiez attentivement le courriel** : comparez l'adresse avec de précédents messages authentiques de votre banque. Contrôlez les fautes d'orthographe/de grammaire.
- **Ne répondez pas à un courriel suspect,** renvoyez-le plutôt à votre banque en tapant l'adresse vous-même.
- **Ne cliquez pas sur le lien « télécharger le document attaché ».**
- En cas de doute, **connectez-vous à votre site bancaire ou appelez votre banque**.
- N'agissez jamais dans la précipitation.

#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICE NATIONALE | FÉDÉRATION BANCAIRE FRANÇAISE