COURRIELS D'HAMEÇONNAGE

L'hameçonnage renvoie à des courriels de fraudeurs incitant 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.

reproduisent les logos, lay-outs et tons de vrais courriels.

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

utilisent un langage qui évoque l'urgence.

QUE FAIRE ?

- **Gardez vos logiciels à jour,** tout comme vos browser, antivirus et système d'exploitation.
- Soyez très **vigilant/e** si un courriel « bancaire » vous invite à communiquer une information sensible (ex. vos codes pour les services bancaires 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/téléchargez pas le document attaché**.
- En cas de doute, **double-cliquez** sur votre site bancaire ou appelez votre banque.

Les cybercriminels escomptent que les gens sont occupés ; au premier abord, ces faux courriels peuvent passer pour vrais.

#CyberScams

Attention quand vous utilisez un dispositif mobile : un téléphone ou une tablette peuvent avoir plus de mal à détecter une tentative d'hameçonnage.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · Politie Police · febelfin · Cyber Security Coalition