

# COURRIELS D'HAMEÇONNAGE BANCAIRE

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.



**utilisent** un langage qui évoque l'urgence.

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

## QUE FAIRE ?

- **Gardez vos logiciels à jour**, et e.a. vos browser, antivirus et système d'exploitation.
- 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/téléchargez pas le document attaché**, retapez plutôt l'adresse correcte de votre banque dans votre browser.
- 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.



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

#CyberScams

