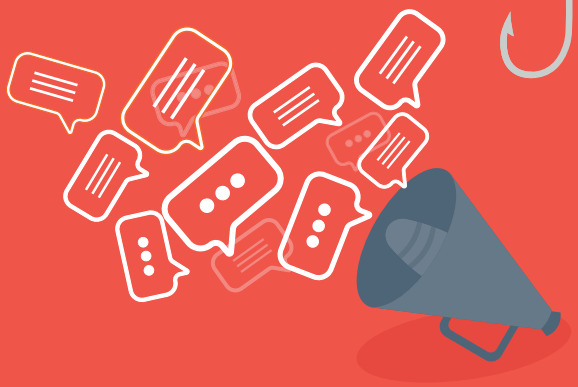
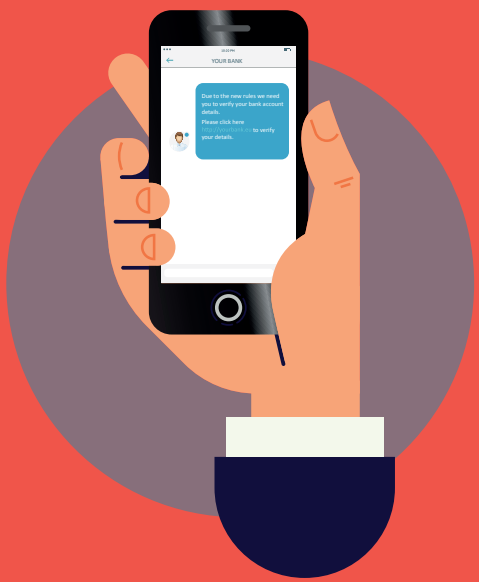
TENTATIVE DE VOL DE DONNÉES PERSONNELLES (« PHISHING » / « HAMEÇONNAGE »)

L'hameçonnage par texto est une tentative d'appropriation de données personnelles (financières ou de sécurité) par des escrocs.





COMMENT CELA SE PASSE-T-IL ?

Le texto vous demandera de cliquer sur un lien ou d'appeler un numéro pour « vérifier », ou « actualiser » ou « réactiver » votre compte bancaire… mais le lien aboutit à un faux site bancaire ou l'appel vous met en relation avec l'escroc prétendant être une banque qui captera vos données confidentielles ou tentera de vous faire réaliser des opérations à son profit.

COMMENT SE PRÉMUNIR D'UN TEXTO FRAUDULEUX?

- **Ne cliquez pas sur des liens, documents attachés ou images** que vous recevez dans des textos non sollicités sans avoir d'abord vérifié l'expéditeur.
- **Ne vous pressez pas.** Prenez votre temps et faites les vérifications appropriées avant de répondre.
- **Ne répondez jamais à un texto** vous demandant votre code PIN ou votre mot de passe de banque en ligne ou toutes autres données de sécurité.
- Si vous pensez avoir répondu à un texto d'hameçonnage et avoir fourni vos données bancaires, **contactez votre banque immédiatement.**

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

#CyberScams