TEXTO D'HAMEÇONNAGE BANCAIRE

L'hameçonnage par texto (smishing: SMS + phishing) est une tentative par des escrocs de s'approprier des données personnelles, financières ou de sécurité par texto.

COMMENT CELA SE PASSE-T-IL ?

Le texto vous demandera typiquement de cliquer sur un lien/d'appeler un numéro pour "vérifier", "actualiser" ou "réactiver" votre compte. Mais… le lien aboutit à un faux site et l'appel vous mène chez l'escroc prétendant être la vraie société.

QUE FAIRE ?

- **Ne cliquez pas sur des liens, documents attachés ou images** que vous recevez dans des textos non sollicités sans en 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.**

#CyberScams

EUROPOL EC3 European Cybercrime Centre
EBF European Banking Federation
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy
ABBL
SECURITY MADE IN.LU
BEE SECURE