MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND 80
Gendarmerie départementale de la Somme

13 mars 2026

Ce mode opératoire, bien que connu, s'enracine **durablement** sur notre territoire. Les fraudeurs ne se contentent plus de piratages **virtuels** : ils s'invitent désormais jusqu'à votre **boîte aux lettres**.
La **vigilance** n'est plus une option, c'est une **nécessité**.

DÉCRYPTAGE : LE MODE OPÉRATOIRE EN 4 ÉTAPES !

1. L'APPÂT (L'urgence administrative)

Tout commence par un SMS, un mail, ou un appel prétextant une **fraude majeure** sur votre compte, souvent localisée à l'étranger. L'objectif est de déclencher un **état de panique** pour court-circuiter votre **esprit critique**.

2. LA MANIPULATION (L'ingénierie sociale)

Vous êtes mis en relation avec un **faux conseiller** très convaincant. Sous couvert de "sécuriser" votre compte, il vous soutire vos **identifiants**, votre **numéro de carte** et, étape cruciale, votre **code secret (PIN)**. Jamais une banque ne vous demandera ce code.

3. LE PIÈGE PHYSIQUE (La boîte aux lettres)

L'escroc prétend que votre carte est **compromise** et doit être « **expertisée** ». Il vous demande de la placer dans une **enveloppe** dans votre boîte aux lettres. Un **complice**, le « coursier », passe la récupérer en quelques **minutes**, sans aucun contact physique avec vous.

4. LA SPOLIATION (L'usage frauduleux)

Munis de votre carte physique et du code PIN **que vous leur avez fourni**, les malfaiteurs procèdent à des **retraits massifs** aux automates les plus proches, épuisant vos **plafonds bancaires**, avant même que l'**alerte** ne puisse être donnée.

CONSEILS PRÉVENTIFS : COMMENT SE PROTÉGER ?

✔ **Raccrochez systématiquement** : Si vous recevez un appel suspect, ne poursuivez pas la conversation. Rappelez votre banque via le numéro OFFICIEL enregistré dans votre répertoire ou au dos de votre carte.

✔ **Le code PIN est sacré** : Votre banque connaît votre numéro de carte, mais elle n'aura JAMAIS besoin de votre code secret pour bloquer une transaction. Ne le donnez sous aucun prétexte.

✔ **Pas de coursier pour une carte** : Aucun service officiel n'envoie de personnel récupérer un moyen de paiement à domicile. Une carte compromise doit être découpée par vos soins.

✔ **Méfiez-vous du « Spoofing »** : Les escrocs peuvent faire apparaître le vrai numéro de votre agence sur votre écran. Ne vous fiez pas au nom ou au numéro qui s'affiche sur votre écran.

VICTIME ? *FAITES OPPOSITION IMMÉDIATEMENT AUPRÈS DE VOTRE BANQUE, SIGNALEZ LES FAITS SUR CYBERMALVEILLANCE.GOUV.FR, ET DÉPOSEZ PLAINTE.*