



# MODE OPERATOIRE



## 1. APPEL

L'escroc contacte la victime par téléphone en se faisant passer pour un conseiller bancaire. Il indique à la victime qu'elle a été victime d'une fraude à la carte bancaire.



## 2. MISE EN CONFIANCE

L'escroc indique à la victime qu'il va annuler les opérations frauduleuses. Pour gagner en crédibilité, il lui demande de vérifier ses informations personnelles.



## 3. COMPROMISSION

L'escroc demande à la victime de lui communiquer les codes de confirmation qu'elle reçoit par SMS et de valider les opérations sur l'application bancaire.

## 5. ENVOI D'UN COURSIER

L'escroc invite la victime à faire opposition sur ses cartes bancaires et à les remettre à un coursier qui se présentera à son domicile.

## 4. OPÉRATIONS FRAUDULEUSES

Grace à ces opérations, l'escroc réalise des paiements en ligne et/ou des virements bancaires sur des comptes frauduleux.



# ACTES PREPARATOIRES



## RECUPERATION DE DONNEES

Les escrocs récupèrent ou acquièrent des données personnelles de leurs victimes notamment sur le *darkweb* pour mener à bien leurs attaques et gagner en crédibilité lors de l'échange avec la victime.



## ANONYMAT

Les escrocs peuvent s'appuyer sur des technologies modernes pour modifier leurs voix, usurper un numéro de téléphone (*spoofing*) et se rendre quasiment anonymes.



## SCRIPT DE COMMUNICATION

Les escrocs préparent un discours de nature à créer un effet de surprise et exercent une pression psychologique insistant notamment sur l'urgence à agir, pour induire les victimes en erreur.

## COMMENT S'EN PREMUNIR ?

- ✗ Votre banque ne vous demandera jamais de réaliser des opérations bancaires *via* les outils d'authentification mis à votre disposition sur votre application bancaire.
- ✗ Ne communiquez jamais vos codes de confirmation.
- ✗ Si vous avez un doute, raccrochez et contactez immédiatement votre banque pour vérifier que vous avez le bon interlocuteur.
- ✗ Si vous avez été victime de ce type de fraude, modifiez vos codes d'accès à votre espace bancaire, contactez votre banque et déposez plainte sans délai dans une brigade de gendarmerie ou un commissariat de police.

SOURCES

[https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000006417968/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417968/)

[https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000006418192/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418192/)

[https://www.legifrance.gouv.fr/codes/article\\_lc/LEGIARTI000030939438/](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/)

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/fraude-faux-conseiller-bancaire#protection-fraude-faux-conseiller-bancaire>