



DIRECTION
INTERDÉPARTEMENTALE
DE LA POLICE NATIONALE
MOSELLE

COMMUNIQUÉ DE PRESSE

Metz, le 26 février 2026

FRAUDES AU FAUX CONSEILLER BANCAIRE / FAUX COURSIER

La police nationale de la Moselle invite la population à la plus grande méfiance suite à une recrudescence des fraudes au faux conseiller bancaire / faux coursier.

C'est un type d'escroquerie qui consiste à tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes bancaires.

Mode opératoire :

En général, l'escroc appelle la victime et se présente comme conseiller ou agent du service anti-fraude de sa propre banque.

Il dispose souvent de nombreuses informations concernant la victime pour crédibiliser son arnaque : identité, adresse, coordonnées de sa carte bancaire... Dans certains cas, il usurpe même le numéro de téléphone de la banque, qui s'affiche sur le téléphone de la victime.

L'escroc prétend avoir identifié des actions suspectes (opération frauduleuses) en cours sur le compte bancaire de la victime et lui propose de les bloquer en urgence.

Il demande ensuite à la victime de lui communiquer des codes qu'elle reçoit par SMS ou lui fait confirmer des actions sur son application bancaire. Ces codes ou confirmations permettent en réalité à l'escroc de valider des opérations frauduleuses sur les comptes de la victime : achats par carte bancaire, ajout de bénéficiaire et virements...

Dans certains cas, le faux conseiller demande à la victime le code secret de sa carte bancaire et lui envoie un faux coursier ou un prétendu employé de la banque pour récupérer la carte à son domicile, au prétexte de la sécuriser ou bien de la détruire. Les escrocs utiliseront alors la carte de la victime pour des retraits d'argent ou des achats.

Les informations utilisées par l'escroc pour cibler la victime et crédibiliser son escroquerie ont pu être obtenues de différentes manières : [hameçonnage](#) (phishing), [piratage de compte](#), [virus](#) voleur de mots de passe sur un des appareils de la victime (ordinateur, téléphone...), [fuite de données personnelles](#) détenues par une organisation, etc.

Conseils :

- Ne cédez jamais à la pression. Au contraire, elle doit vous alerter.
- Jamais un conseiller de votre banque ne vous appelle pour vous demander votre code de carte bancaire.
- Votre banque ne vous demandera jamais de remettre votre carte et votre code à un coursier .
- En cas de doute, ne cliquez jamais sur un lien reçu par courriel ou SMS. Connectez-vous sur votre espace client depuis votre application mobile ou à partir de votre moteur de recherche.

Et si une personne vous appelle : Raccrochez et contactez vous-même l'établissement pour lequel elle prétend travailler après avoir trouvé ses coordonnées sur son site officiel, afin de vous assurer de son identité. Ne validez aucune opération sur votre application bancaire si vous n'en êtes pas à l'origine. Aucune validation de votre part n'est nécessaire pour annuler ou bloquer un paiement frauduleux. Ne communiquez pas vos mots de passe et vos codes de sécurité. Jamais votre conseiller ne vous demandera ces informations : elles sont confidentielles.

Si vous êtes victime :

Faites opposition sur votre carte bancaire.

Déposez une plainte au commissariat ou rendez-vous sur le site MaSécurité pour une plainte en ligne.