MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

CYBERGEND 80
Gendarmerie départementale de la Somme

FACE AUX
CYBERMENACES
ADOPTEZ LES BONS RÉFLEXES !

ARNAQUE SENTIMENTALE

MODE OPÉRATOIRE
Une fausse relation amoureuse sur Internet. Après parfois plusieurs mois, l'escroc prétexte une urgence médicale ou un voyage pour vous soutirer de l'argent. Il ne viendra jamais.

LE BON RÉFLEXE
N'envoyez jamais d'argent à une personne rencontrée exclusivement sur Internet. Coupez immédiatement le contact au moindre doute.

FAUX CONSEILLER BANCAIRE

MODE OPÉRATOIRE
Un faux conseiller bancaire vous appelle en connaissant déjà vos données personnelles et simule une urgence pour obtenir vos codes ou vos validations.

LE BON RÉFLEXE
Raccrochez immédiatement. Votre banque ne vous demandera jamais vos codes. En cas de validation, la banque ne vous remboursera pas.

FAUX RIB / FACTURE

MODE OPÉRATOIRE
Après avoir demandé un devis légitime, vous recevez un e-mail dont l'adresse d'envoi et le RIB ont été modifiés par des pirates pour détourner votre paiement.

LE BON RÉFLEXE
Vérifiez scrupuleusement l'adresse mail de l'expéditeur.
Téléphonez impérativement à l'entreprise pour confirmer le RIB avant tout virement.

FAUX GAIN / LOTERIE

MODE OPÉRATOIRE
Un message inattendu annonce que vous avez gagné le premier prix d'un concours. Pour percevoir votre gain, vous devez cliquer sur un lien piège conçu pour voler vos coordonnées bancaires ou vos données.

LE BON RÉFLEXE
Ne cliquez jamais sur ces liens.
Si vous n'avez pas participé à un concours, vous ne pouvez pas avoir gagné.

FAUX SMS D'AMENDE ANTAI

MODE OPÉRATOIRE
Vous recevez un SMS d'alerte pour une amende impayée. Le message vous invite à cliquer d'urgence sur un lien imitant le site officiel de l'ANTAI pour régulariser la situation sous peine de majoration.

LE BON RÉFLEXE
L'administration n'envoie jamais de SMS pour notifier ou réclamer le paiement d'une contravention : ignorez-les.
Vérifiez sur l'application ou le site officiel.

FRAUDE AUX PETITES ANNONCES

MODE OPÉRATOIRE
Pour une location ou un achat, le vendeur vous met en confiance avec une fausse pièce d'identité. Il refuse le paiement sécurisé de la plateforme pour contourner les règles. Le bien n'existe pas ou n'est jamais livré.

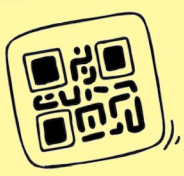
LE BON RÉFLEXE
Exigez uniquement le système de paiement sécurisé de la plateforme. Refusez catégoriquement les virements immédiats ou mandats cash.

L'ARNAQUE À L'URGENCE FAMILIALE

MODE OPÉRATOIRE
Vous recevez un message WhatsApp ou par SMS d'un numéro inconnu : "Coucou maman, j'ai cassé mon téléphone, c'est mon nouveau numéro. J'ai une facture urgente à payer, tu peux me faire un virement ?"

LE BON RÉFLEXE
Ne jamais envoyer d'argent sans avoir contacté l'enfant sur son ancien numéro de téléphone ou de vive voix.

FAUX QR CODE (QUISHING)



MODE OPÉRATOIRE
De faux QR codes sont collés sur des horodateurs, bornes, terrasses ou envoyés par courrier. En les scannant, la victime est renvoyée vers un site frauduleux pour voler ses coordonnées bancaires.

LE BON RÉFLEXE
Toujours se méfier des QR codes isolés dans l'espace public et préférer l'utilisation des applications officielles.

FAUX SUPPORT TECHNIQUE

MODE OPÉRATOIRE
Un écran bloqué simule une panne grave. Un message vous presse d'appeler d'urgence un numéro payant où un faux technicien prend le contrôle de votre PC pour vous extorquer de l'argent.

LE BON RÉFLEXE
Pas de panique ! Redémarrez le PC, n'appelez aucun numéro et ne payez rien. À la réouverture du navigateur, refusez de restaurer la session précédente.

SIGNALEMENT ET ASSISTANCE

Si vous êtes victime ou témoin d'une tentative d'escroquerie, déposez plainte auprès de votre brigade de gendarmerie locale ou signalez les contenus suspects sur la plateforme officielle `Internet-signalement.gouv.fr` (Pharos) ou via `Cybermalveillance.gouv.fr`.

Pour les alertes sur mobile, utilisez le 33700, la plateforme de signalement des SMS et appels indésirables / frauduleux (il suffit de transférer le SMS suspect au 33700).