



**CODE
CONFIANCE**
COMPRENDRE • ANTICIPER • SÉCURISER

SÉCURITÉ | PRÉVENTION | BONNES PRATIQUES

FICHE PRATIQUE

Plus informés,
plus protégés !

SIM Swapping

Comprendre, repérer, réagir

Des repères fiables
pour un monde plus serein

Votre
identité numérique
vaut mieux
qu'une simple carte SIM !

1 Le mécanisme en 4 étapes

Une fraude bien rodée, qui peut aller très vite.

1



**Des données personnelles
fuitent ou sont récupérées**
(fuites de données, phishing,
réseaux sociaux, etc.).

2



**Le fraudeur se fait passer
pour vous auprès de l'opérateur**
(avec vos informations
personnelles).

3



**Votre numéro est transféré
vers une autre SIM ou eSIM.**

4



**Il intercepte vos SMS/codes
et tente de prendre le contrôle
de vos comptes.**

2

Pourquoi c'est grave ?

Le SIM swapping peut avoir des conséquences importantes.



**Réinitialisation
de mots de passe**
et accès à
vos comptes.



**Détournement
de codes bancaires**
et risques de
fraude financière.



**Prise de contrôle
de l'email**
et accès à vos
informations sensibles.



**Accès aux réseaux
sociaux ou services
sensibles**
(cloud, administration,
entreprise, etc.).

3

Les signaux d'alerte

Soyez attentif à ces signes qui doivent vous alerter.



Votre téléphone perd soudainement le réseau.



Vous recevez des alertes ou codes non demandés.



Des mots de passe semblent modifiés.



Des connexions inhabituelles apparaissent
sur vos comptes.

4

eSIM : ce qu'il faut comprendre



L'eSIM n'est pas la cause du problème.

Elle remplace la carte physique, mais si un fraudeur parvient à faire valider un transfert de ligne, votre numéro peut aussi être activé à distance sur une eSIM.

Le vrai enjeu est donc la vérification d'identité et la sécurité des procédures opérateur.

5

A Ce que les opérateurs doivent faire

Des mesures indispensables pour mieux protéger les clients.



Traiter tout changement de SIM/eSIM comme une opération sensible.



Renforcer l'authentification et les contrôles anti-usurpation.



Alerter le client avant et après toute activation.



Bloquer ou vérifier en cas de doute.



Surveiller les demandes anormales et former les conseillers.

B

Les bons réflexes côté utilisateur

Des gestes simples qui font une grande différence.



Protéger votre compte opérateur.



Ne pas dépendre du SMS comme seul 2e facteur.



Préférer une appli d'authentification, des passkeys
ou une clé de sécurité.



Sécuriser en priorité votre adresse email.



Réagir immédiatement si votre mobile perd le réseau
sans raison.



À RETENIR

**Le SIM swapping n'est pas une simple fraude télécom.
C'est une attaque contre votre identité numérique.**

Votre sécurité
commence par la connaissance.