FICHE RÉFLEXE CYBERSÉCURITÉ

ANATOMIE D'UN FAUX SMS

GUIDE VISUEL

Apprenez à repérer les arnaques par SMS (smishing) — exemples annotés, indices qui trahissent le faux

Faux SMS — Chronopost / Colis

ARNAQUE

> Chronopost: Votre colis **n°FR928471** est retenu en douane. Frais de 1,90€ requis avant livraison. Réglez maintenant : **chronopost-livraison.xyz/payer**

INDICES QUI TRAHISSENT L'ARNAQUE

- **URL suspecte :** le vrai domaine est chronopost.fr, pas "chronopost-livraison.xyz"
- **Urgence artificielle :** pression pour payer sans vérifier
- **Frais de douane par SMS :** les vrais opérateurs n'envoient jamais ce type de demande
- **Numéro de colis invalide :** vérifiable sur le vrai site

Faux SMS — Ameli / Assurance Maladie

ARNAQUE

> AMELI: Votre **remboursement de 43,20€** est disponible. Mettez à jour vos coordonnées bancaires pour recevoir votre virement : **ameli-remb.fr/mise-a-jour**

INDICES QUI TRAHISSENT L'ARNAQUE

- **Demande de CB / IBAN par SMS :** Ameli ne demande jamais ça par SMS
- **Domaine non officiel :** le vrai est ameli.fr uniquement
- **Montant précis pour crédibilité :** technique classique d'ingénierie sociale
- **Lien raccourci ou domaine proche :** "ameli-remb.fr" ≠ "ameli.fr"

Faux SMS — Impôts / DGFiP

ARNAQUE

> DGFiP: **Remboursement fiscal de 178€** vous est du. Cliquez sur le lien pour recevoir votre virement sous 24h : **impots-gouv.remboursement.net**

INDICES QUI TRAHISSENT L'ARNAQUE

- **La DGFiP ne rembourse jamais par SMS :** tout passe par impots.gouv.fr
- **Domaine piégé :** "impots-gouv.remboursement.net" ≠ "impots.gouv.fr"
- **Délai de 24h :** pression temporelle pour court-circuiter votre vigilance
- **Faute sur "dû" :** "vous est du" sans accent — indice de masse automatisée

Faux SMS — CPF / Mon Compte Formation

ARNAQUE

> MonCompteFormation: **1 750€ de droits CPF** vont expirer le 31/12. Utilisez-les maintenant en 2 minutes : **cpf-formation-rapide.com/activer**. Gratuit, sans engagement.

INDICES QUI TRAHISSENT L'ARNAQUE

- **Les droits CPF n'expirent pas par SMS :** gérés sur moncompteformation.gouv.fr
- **Domaine non officiel :** jamais "cpf-formation-rapide.com"
- **"Gratuit, sans engagement" :** signal d'alerte commercial agressif
- **Arnaque aux formations fictives :** déjà condamnée par la CNIL

QUE FAIRE FACE À UN SMS SUSPECT ?

1. **Ne pas cliquer** sur le lien, ne pas rappeler le numéro indiqué
2. Signaler le SMS au **33700** (service gratuit de signalement smishing) — transférez le SMS
3. Signaler l'URL sur **phishing-initiative.fr** pour la faire bloquer
4. Si vous avez cliqué : changez vos mots de passe, faites opposition si vous avez saisi vos données bancaires

Astuce : En cas de doute sur un SMS d'un organisme officiel, allez directement sur le site officiel en tapant l'URL à la main dans votre navigateur — jamais via le lien du SMS.

Besoin d'une sensibilisation de vos équipes aux arnaques par SMS et email ?
ayinedjimi-consultants.fr/contact