# Fiche Pratique N°47 : Reconnaître et déjouer les arnaques en ligne V1.1

7 nov, 2026 · @Gabriel

***Objectif :*** *apprendre à repérer les tentatives d'hameçonnage par courriel (phishing) et par SMS (smishing), adopter les bons réflexes et savoir où les signaler.*

- ***Public visé :*** *débutant à intermédiaire*
- ***Temps estimé :*** *15 minutes*
- ***Difficulté :*** *★☆☆☆☆ (Très facile)*
- ***Prérequis :*** *aucun*
- ***Fiches associées :*** *N°46 (gestes de base), N°48 (outils de cybersécurité dans le navigateur), N°53 (IA et vie privée)*

## 1. Pourquoi cette fiche ? (Le problème)

| Problème | Solution |
|---|---|
| Vous recevez des SMS ou des courriels suspects | Apprendre à reconnaître les indices |
| Vous ne savez pas si un lien est fiable | Méthode de vérification en 3 étapes |
| Vous avez peur de vous faire piéger | Entraînement « Vrai ou piège » |

**Le bénéfice :** quelques réflexes simples suffisent à déjouer la grande majorité des messages frauduleux, sans aucun logiciel.

## 2. Les 5 indices qui ne trompent pas

| Indice | Exemple | Pourquoi c'est suspect |
|---|---|---|
| **Urgence** | « Régularisez sous 48 h » | La pression empêche de réfléchir : c'est le but |
| **Fautes ou tournures bizarres** | « Votre colis est en attante » | Fréquent dans les messages frauduleux, mais de moins en moins : un message bien écrit n'est pas forcément sûr |
| **Lien bizarre** | `colissimo-suivi-fr.info` | Le suivi Colissimo se fait sur le site de La Poste, `laposte.fr` |
| **Demande d'informations** | « Confirmez votre mot de passe » | Un organisme sérieux ne demande jamais un mot de passe, un code reçu par SMS ou un numéro de carte par message |
| **Expéditeur inconnu** | +33 7 55 90 12 08 | Ne rappelez pas ce numéro : contactez l'organisme par ses coordonnées habituelles |


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°47 : Reconnaître et déjouer les arnaques en ligne V1.1

## 3. La méthode de vérification en 3 étapes

### Étape 1 : ne cliquez pas

Ne cliquez jamais sur un lien reçu par SMS ou par courriel si vous avez un doute. Ne répondez pas non plus au message.

- **Vous devez voir :** le message toujours non ouvert, ou ouvert sans avoir touché au lien.

### Étape 2 : vérifiez par vous-même

- **Pour un colis :** tapez vous-même l'adresse du transporteur dans le navigateur, puis saisissez le numéro de suivi.
- **Pour une banque :** connectez-vous avec son application officielle, ou appelez le numéro inscrit au dos de votre carte.
- **Pour un organisme :** passez par l'adresse que vous connaissez déjà (favori, courrier papier), pas par le lien du message.
- **Vous devez voir :** sur le site officiel, aucune alerte ni somme à payer correspondant au message reçu.

### Étape 3 : signalez

- **SMS ou appel suspect :** transférez le SMS au **33700**, puis envoyez par SMS le numéro de l'expéditeur quand le service vous le demande.
- **Courriel suspect :** signalez-le sur **Signal Spam** (`signal-spam.fr`), puis supprimez-le.
- **Site d'hameçonnage :** soumettez son adresse à **Phishing Initiative** (`phishing-initiative.fr`) pour le faire vérifier et bloquer.
- **Victime ou doute sérieux :** rendez-vous sur **17Cyber** (`17cyber.gouv.fr`), qui évalue votre situation et vous oriente. Pour un conseil par téléphone : **Info Escroqueries** au 0 805 805 817 (gratuit, du lundi au vendredi, de 9 h à 18 h 30).
- **Vous devez voir :** un accusé de réception du 33700, ou la confirmation de votre signalement sur le site.

⚠️ Si vous avez déjà saisi des informations bancaires, appelez immédiatement votre banque pour faire opposition, puis changez les mots de passe concernés. En cas de perte d'argent, déposez plainte.

## 4. Entraînement « Vrai ou piège »

### Exemple 1

**SMS :** « Votre colis n° FR8891204 est en attente. Des frais de douane de 2,30 € restent dus. Régularisez sous 48 h : `colissimo-suivi-fr.info/regul` »

**Votre réponse :** vrai ou piège ?

**Réponse :** 🚨 **Piège.** Indices : urgence (48 h), petite somme pour endormir la méfiance (2,30 €), lien qui n'est pas celui de La Poste (`laposte.fr`), numéro inconnu.


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°47 : Reconnaître et déjouer les arnaques en ligne V1.1

### Exemple 2

**Courriel :** « Votre compte Netflix sera suspendu. Mettez à jour votre paiement : `netflix-facturation.com` »

**Réponse :** 🚨 **Piège.** Indices : menace de suspension, adresse qui n'est pas celle de Netflix, demande de paiement. Vérifiez en ouvrant vous-même l'application Netflix.

### Exemple 3

**SMS :** « Votre code de vérification est 482913. Ne le partagez avec personne. »

**Réponse :** ✅ **Vrai, si vous venez de vous connecter.** C'est un code de double authentification. Si vous n'avez rien demandé, quelqu'un essaie d'entrer dans votre compte : ne communiquez jamais ce code, même à une personne qui se présente comme votre banque, et changez votre mot de passe.

⚠️ Les adresses des exemples sont fictives et volontairement non cliquables : ne les tapez pas.

## 5. Challenge 7 jours

**Challenge :** pendant 7 jours, chaque fois que vous recevez un SMS ou un courriel suspect, appliquez la méthode en 3 étapes et notez les indices repérés.

Vous allez constater :

- que les mêmes ficelles reviennent sans cesse (colis, impôts, amende, compte suspendu) ;
- qu'un signalement prend moins d'une minute.

## 6. En résumé (ce que vous gagnez)

| Action | Gagné |
|---|---|
| Reconnaître les 5 indices | La plupart des pièges repérés avant de cliquer |
| Appliquer la méthode en 3 étapes | Vérification systématique, sans stress |
| Signaler (33700, Signal Spam, Phishing Initiative, 17Cyber) | Protection collective : les numéros et sites sont bloqués plus vite |

## 7. À retenir absolument

- **Dans le doute, ne cliquez pas :** passez par le site ou l'application que vous connaissez.
- **Personne de sérieux** ne vous demande un mot de passe, un code reçu par SMS ou un numéro de carte.
- **SMS suspect :** 33700 ; **courriel :** Signal Spam ; **site :** Phishing Initiative ; **victime :** 17Cyber.
- **Argent en jeu :** banque d'abord, plainte ensuite.

**Test final :**


gabriel.ananda@mailo.com
CC BY SA

# Fiche Pratique N°47 : Reconnaître et déjouer les arnaques en ligne V1.1

1. Retrouvez un SMS suspect dans votre téléphone et listez ses indices.
2. Transférez-le au 33700.
3. Si vous avez reçu l'accusé de réception : vous savez déjouer et signaler ✅

## 8. Liens avec le Petit Guide

| Indice ou méthode | Notion du Petit Guide |
|---|---|
| Lien bizarre | §5 – Navigateur web, §20 – Protocole |
| Demande d'informations | §23 – Mot de passe / authentification |
| Double authentification | §23 – Mot de passe / authentification |
| Signalement | §26 – Antivirus / malware |

## Références


- INC (Institut national de la consommation) – Que faire en cas de phishing ou d'hameçonnage ?
- Futura – Signaler un SMS frauduleux au 33700 (procédure)
- Cybermalveillance.gouv.fr – Fiche réflexe Hameçonnage (2026)
- INC – 17Cyber, l'assistance pour les victimes de cybermalveillance



gabriel.ananda@mailo.com
CC BY SA