01 — Faux messages officiels

Vérifier un message sans utiliser son lien ni son numéro.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Élise attend un colis. Un SMS annonce un supplément de 1,90 € à régler dans l'heure pour éviter son retour. Le lien ressemble au nom du transporteur et une page demande sa carte bancaire. Le lendemain, un autre message promet un remboursement de santé et réclame les mêmes informations. Élise se demande si le petit montant rend la demande acceptable.

Comprendre le piège

Le fraudeur emprunte une identité connue pour obtenir un paiement, un mot de passe ou des données. Un logo, un cadenas HTTPS ou un français correct ne prouvent pas qui contrôle la page. Le fait d'attendre réellement un colis rend le prétexte crédible, sans authentifier le SMS.

Les signes d'alerte

• Une échéance très courte pousse à agir avant de vérifier.

• Le message demande carte bancaire, mot de passe ou code de connexion.

• Le lien conduit vers une adresse différente du service attendu.

• La vérification proposée reste dans le message reçu : lien, QR code ou numéro.

01 — Vérifier et réagir

Le réflexe à retenir

Fermer le message et ouvrir l’application habituelle du transporteur ou le site connu, saisi soi-même. Vérifier le suivi ou contacter le service par ses coordonnées déjà connues.

Que faire si j’ai été victime ?

J’ai seulement ouvert la page

La fermer et ne rien saisir. Un clic seul ne prouve pas une infection ; si un téléchargement ou une installation a suivi, demander une assistance technique.

J’ai donné un mot de passe

Depuis un appareil de confiance, le remplacer sur le vrai service et sur les comptes qui le réutilisent. Activer la double authentification et vérifier les sessions.

J’ai donné ma carte ou constaté un débit

Contacter immédiatement la banque par ses coordonnées habituelles pour faire opposition et signaler les opérations.

Je conserve puis je signale

Garder le message et son adresse. Signaler le SMS au 33700 ou le courriel à Signal Spam. En cas de préjudice, préparer un dépôt de plainte.

À vous de jouer

Sur papier, entourer les demandes du SMS fictif, puis écrire le chemin de vérification indépendant. Ne pas ouvrir de site suspect pour faire l’exercice.

Réponses personnelles : .....

.....

01 — Petit quiz

Une seule réponse par question. Choisir puis expliquer sa décision. Les corrections figurent dans le document séparé « Quiz corrigés » et sur la page de la situation.

1. Élise attend bien un colis. Le SMS est-il authentifié ?

A. Oui, puisqu'un colis existe.

B. Non, il faut une vérification indépendante.

C. Oui, si le montant est faible.

2. Quelle vérification est la plus sûre ?

A. Ouvrir l'application habituelle du transporteur.

B. Répondre au SMS.

C. Appeler le numéro du SMS.

3. La carte a été saisie. Quelle priorité ?

A. Effacer le SMS.

B. Attendre le prochain relevé.

C. Contacter la banque immédiatement.

4. Où orienter le signalement d'un SMS suspect ?

A. Vers le vendeur de l'ordinateur.

B. Vers le 33700.

C. Vers le correspondant du SMS.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Hameçonnage

Service-Public — Spam vocal et SMS

Cybermalveillance.gouv.fr — Signaler un courriel frauduleux

Sources vérifiées le 12 novembre 2026. Conditions des services à vérifier lors des démarches.