10 arnaques en ligne

Livret apprenant illustré — édition du 12 novembre 2026

À qui s’adresse ce module ?

Aux adultes, seniors, familles et débutants qui utilisent une messagerie, un smartphone ou Internet. Aucun compte bancaire, document d’identité ou secret réel n’est nécessaire. Les exemples et personnages sont fictifs. Ces dix sujets forment un choix pédagogique, sans classement par fréquence ou gravité.

Ce que l’on apprend

Reconnaître une demande à risque, suspendre une action sous pression, vérifier l’identité par un autre canal et choisir une première démarche adaptée. Une victime peut être trompée même si elle connaît les règles ; l’objectif est de lui rendre la possibilité d’agir, sans jugement.

Comment travailler

Suivre les dix séquences à son rythme ou les répartir en ateliers. Chaque séquence associe une illustration, un cas à discuter, les alertes, un réflexe, les démarches et quatre questions corrigées. La correction affiche aussi une explication ; le score n’est pas une certification de sécurité.

Vérifier hors du message

Utiliser une application déjà connue, un favori créé auparavant ou des coordonnées conservées indépendamment. Ne pas demander à l’expéditeur suspect de prouver lui-même son identité. Un message bien écrit, un logo, un cadenas ou une photo ne suffisent pas.

Les exercices restent fictifs

Ne jamais cliquer sur un vrai lien suspect pendant l’atelier, envoyer de paiement d’essai, contacter un escroc ou partager ses propres identifiants. Un participant peut passer une activité sensible sans avoir à se justifier. Pour un incident réel, utiliser la page « Aide et démarches » en privé.

Les dix situations

01 — Faux messages officiels

02 — Faux conseiller bancaire

03 — Faux investissements et plateformes crypto

04 — Arnaque sentimentale

05 — Faux support technique

06 — Fausses ventes et faux paiements

07 — Faux RIB et facture détournée

08 — Faux proche en difficulté

09 — Fausses offres d’emploi

10 — Chantage intime et fausse webcam piratée

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.

02 — Faux conseiller bancaire

Interrompre une demande bancaire pressante et rappeler par un canal connu.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Un homme appelle Samira et se présente comme le service antifraude. Il connaît son nom et évoque un achat de 780 €. Le numéro affiché ressemble à celui de sa banque. Pour annuler l'achat, il lui demande de valider une notification et de transférer son épargne sur un « compte sécurisé ». Il propose ensuite qu'un coursier récupère sa carte.

Comprendre le piège

L'escroc utilise la peur de perdre son argent pour faire autoriser un paiement ou un virement. Des informations exactes et un numéro affiché peuvent être usurpés. Une validation dans l'application peut exécuter l'opération dont l'appelant prétend empêcher la réalisation.

Les signes d'alerte

• Une personne demande un code secret ou un code reçu par SMS.

• Elle dicte des validations censées annuler une fraude.

• Elle réclame un virement de sécurité ou la remise de la carte.

• Elle interdit de raccrocher ou de parler à l'agence.

02 — Vérifier et réagir

Le réflexe à retenir

Raccrocher. Rappeler la banque avec le numéro figurant sur la carte, un document habituel ou l'application déjà installée. Ne valider aucune opération dictée par l'appelant.

Que faire si j'ai été victime ?

Des codes ou une validation ont été donnés

Alerter sans attendre la vraie banque et expliquer précisément ce qui a été communiqué ou confirmé.

La carte est compromise

Demander l'opposition immédiatement. Ne remettre ni carte ni code à un coursier.

Un virement est parti

Demander à la banque si elle peut tenter son rappel et contester les opérations concernées. Une récupération ou un remboursement ne sont pas garantis par cette démarche.

Préparer la suite

Garder horaires, numéros, messages et références d'opérations. Changer l'accès bancaire si compromis avec l'aide de la banque ; déposer plainte.

À vous de jouer

À deux, un participant lit le scénario et l'autre formule sa phrase pour mettre fin à l'appel. Il montre ensuite où retrouver le vrai numéro, sans afficher de donnée bancaire personnelle.

Réponses personnelles : .....

.....

02 — 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. Le numéro affiché suffit-il à reconnaître la banque ?

A. Oui, toujours.

B. Oui, si l'appelant connaît mon nom.

C. Non, il peut être usurpé.

2. On demande de valider pour annuler un achat. Que faire ?

A. Raccrocher puis joindre la banque indépendamment.

B. Valider rapidement.

C. Transmettre le code à un proche de l'appelant.

3. Un coursier vient prendre la carte. Quelle réponse ?

A. La couper puis la lui donner.

B. Refuser et alerter la banque.

C. Lui laisser le code séparément.

4. Une demande de rappel de virement garantit-elle de récupérer l'argent ?

A. Oui, si elle est immédiate.

B. Oui, après une plainte.

C. Non, il faut agir vite sans promesse de résultat.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Faux conseiller bancaire

Service-Public — Arnaque sur Internet et THESEE

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

03 — Faux investissements et plateformes crypto

Repérer une promesse financière trompeuse et vérifier l’identité d’un intermédiaire.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Une publicité montre une personnalité connue recommandant une plateforme. Marc verse 250 € et voit ses gains augmenter sur un tableau de bord. Son interlocuteur lui propose un rendement de 12 % par mois « sans risque ». Quand Marc veut retirer, il doit d’abord payer une taxe de 600 €. Un autre contact promet de récupérer tout son argent moyennant une avance.

Comprendre le piège

Le tableau de bord peut afficher des chiffres inventés. Une publicité, une vidéo ou un premier petit retrait peuvent servir à gagner la confiance. L’identité d’une entreprise réellement autorisée peut aussi être copiée. La demande de nouveaux frais pour libérer des fonds et la promesse de récupération payante doivent provoquer l’arrêt.

Les signes d’alerte

• Des gains élevés sont présentés comme garantis ou sans risque.

• Un inconnu presse de verser plus ou guide chaque opération.

• Le retrait exige des taxes ou frais supplémentaires inattendus.

• Le contact renvoie uniquement vers ses propres preuves et liens.

03 — Vérifier et réagir

Le réflexe à retenir

Suspendre tout versement. Accéder soi-même au site de l’AMF pour vérifier les autorisations applicables et les alertes, puis confronter le domaine et les coordonnées. L’absence d’une liste noire ne certifie pas la fiabilité.

Que faire si j’ai été victime ?

Arrêter l’escalade

Ne pas payer la taxe de déblocage ni un prétendu récupérateur de fonds. Ne pas donner d’accès à distance.

Alerter les services de paiement

Joindre rapidement la banque ou le prestataire utilisé. Transmettre dates, montants et destinataires pour examiner les possibilités d’action.

Conserver le dossier

Garder annonces, échanges, adresses de sites, justificatifs et, pour les crypto-actifs, adresses de portefeuille et identifiants de transaction.

Demander une orientation

Consulter les informations de l’AMF et déposer plainte. Une autorisation vérifiée n’élimine pas le risque de perte ; aucun retour des fonds n’est promis.

À vous de jouer

Classer « courbe de gains », « identité vérifiée par une source indépendante » et « demande de taxe avant retrait » en preuve insuffisante, vérification utile ou alerte.

Réponses personnelles : .....

.....

03 — 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. Une belle courbe de gains prouve-t-elle que les fonds sont disponibles ?

A. Non, l’affichage peut être fabriqué.

B. Oui, si elle monte régulièrement.

C. Oui, avec un logo connu.

2. La plateforme réclame une taxe pour retirer. Quelle décision ?

A. Payer une dernière fois.

B. Arrêter les versements et demander de l’aide.

C. Emprunter pour débloquer.

3. Le nom est absent des listes noires. Que conclure ?

A. Le placement est garanti.

B. Le capital est assuré.

C. Cela ne suffit pas à établir sa fiabilité.

4. Un contact promet le remboursement contre une avance. Que faire ?

A. Refuser et vérifier indépendamment.

B. Lui transmettre ses accès.

C. Lui verser une petite avance.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Escroquerie au placement

AMF — Crypto-actifs : attention aux arnaques

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

04 — Arnaque sentimentale

Reconnaître une pression affective et soutenir une victime sans la culpabiliser.

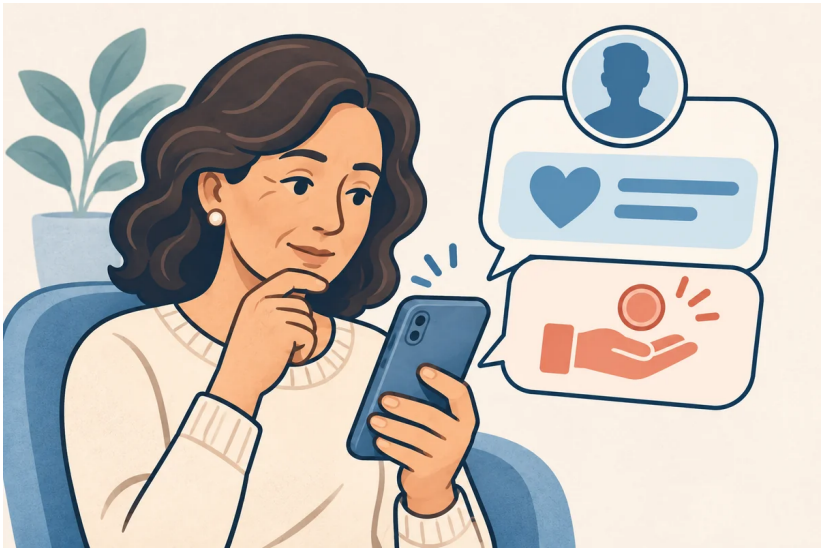

Illustration de formation créée par IA — exemple fictif.

Mise en situation

Depuis six semaines, Claire échange chaque soir avec un homme rencontré en ligne. Il reporte toujours leur rencontre. Il affirme maintenant être bloqué à l'étranger et demande 900 € pour une urgence, en insistant pour que Claire n'en parle à personne. Une amie doute ; Claire hésite, car elle a l'impression de bien le connaître.

Comprendre le piège

Le lien affectif peut rendre une demande d'argent difficile à refuser. Des photos et des conversations prolongées ne vérifient pas l'identité. L'escroquerie peut aussi prendre la forme d'une proposition d'investissement. Une visio ou une recherche d'image ne constituent pas à elles seules une garantie.

Les signes d'alerte

• L'attachement devient très rapide et les demandes financières progressent.

• Les rencontres réelles échouent toujours pour un nouveau motif.

• Une urgence impose un paiement discret ou difficile à récupérer.

• La personne tente d'éloigner la victime de ses proches.

04 — Vérifier et réagir

Le réflexe à retenir

Ne pas envoyer d'argent à une personne connue uniquement à distance. Prendre du recul avec une personne de confiance, sans devoir prouver seul que tout le récit est faux.

Que faire si j'ai été victime ?

Interrompre les demandes

Cesser les versements et les échanges avec l'escroc. Préserver les messages déjà reçus avant de bloquer le profil si cela peut se faire sans prolonger le contact.

Chercher du soutien

Parler à un proche bienveillant ou à France Victimes au 116 006. La responsabilité de la tromperie appartient à l'escroc.

Limiter les conséquences

Prévenir rapidement la banque si de l'argent ou des informations bancaires ont été transmis. Sécuriser les comptes compromis.

Signaler et porter plainte

Signaler le profil à la plateforme et réunir échanges, paiements et identifiants pour la plainte. Utiliser le parcours officiel THESEE si ses conditions sont remplies, ou la police/gendarmerie.

À vous de jouer

Rédiger une réponse de soutien à Claire en trois phrases, puis proposer un premier geste concret. Aucun participant n'a à raconter une histoire personnelle.

Réponses personnelles : .....

.....

04 — 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. Un premier appel vidéo certifie-t-il l’identité ?

A. Oui, définitivement.

B. Non, il faut rester prudent.

C. Oui, si le visage paraît sympathique.

2. Quelle phrase aide Claire ?

A. Tu aurais dû comprendre.

B. Paie pour être fixée.

C. On peut regarder cela ensemble et chercher de l’aide.

3. Quel geste est prioritaire si les demandes continuent ?

A. Arrêter les paiements et les contacts.

B. Négocier un dernier paiement.

C. Proposer un autre moyen de paiement.

4. Que conserver pour les démarches ?

A. Seulement la photo du profil.

B. Les échanges, identifiants et justificatifs de paiement.

C. Rien, tout effacer immédiatement.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Escroquerie sentimentale

Service-Public — Arnaque sur Internet et THESEE

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

05 — Faux support technique

Faire la différence entre une alerte de page web et un dépannage demandé volontairement.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

En lisant un article, André voit une page rouge avec une sirène : « Votre ordinateur est infecté, appelez immédiatement. » Un prétendu technicien lui demande d'installer un outil pour prendre la main et de payer 180 €. Pour vérifier le remboursement annoncé, il exige ensuite qu'André ouvre son compte bancaire pendant la connexion.

Comprendre le piège

Une page web peut afficher une fausse alerte et donner l'impression que tout l'ordinateur est bloqué. Le fraudeur cherche à obtenir paiement ou accès à distance. Un outil de téléassistance peut être légitime ; son utilisation imposée par un inconnu reste dangereuse.

Les signes d'alerte

• Un numéro de dépannage apparaît dans une fenêtre alarmante non sollicitée.

• Le correspondant exige une prise de contrôle immédiate.

• Il réclame une carte, des codes ou l'ouverture de la banque.

• Il menace de supprimer les fichiers si la victime refuse.

05 — Vérifier et réagir

Le réflexe à retenir

Ne pas appeler le numéro affiché. Fermer l’onglet ou le navigateur ; si nécessaire, demander à un proche de confiance de le fermer. Choisir soi-même l’assistance depuis un contact connu.

Que faire si j’ai été victime ?

Une prise de contrôle est en cours

Couper la connexion Internet de l’appareil pour interrompre l’accès et cesser le contact. Utiliser un autre appareil de confiance pour les démarches urgentes.

Un paiement ou des accès bancaires ont été exposés

Prévenir immédiatement la banque, faire opposition si la carte est compromise et signaler les opérations.

Contrôler l’ordinateur

Demander une assistance fiable pour rechercher les accès et logiciels ajoutés, les désactiver et vérifier le système. Ne pas considérer la seule fermeture de la fenêtre comme une remise en sécurité après téléassistance.

Sécuriser et documenter

Depuis un appareil de confiance, changer les mots de passe exposés. Garder reçus, nom de l’outil et échanges ; déposer plainte si escroquerie.

À vous de jouer

Trier deux situations : une aide demandée à son réparateur habituel, et un numéro imposé par une page alarmante. Expliquer comment interrompre une téléassistance non autorisée.

Réponses personnelles : .....

.....

05 — 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. Une sirène dans une page prouve-t-elle une infection ?

A. Oui, toujours.

B. Oui, si le logo est connu.

C. Non, une page peut fabriquer cette alerte.

2. Un inconnu contrôle déjà l’ordinateur. Premier geste ?

A. Couper sa connexion Internet.

B. Ouvrir la banque devant lui.

C. Payer pour qu’il parte.

3. L’outil porte un nom connu. L’intervention est-elle fiable ?

A. Oui, le logiciel suffit.

B. Non, il faut vérifier qui intervient et pourquoi.

C. Oui, si l’intervention dure longtemps.

4. Après une prise de contrôle, fermer la page suffit-il ?

A. Oui, tout est réparé.

B. Oui, après paiement.

C. Non, faire vérifier les accès et logiciels ajoutés.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Faux support technique

17Cyber — Diagnostic et assistance

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

06 — Fausses ventes et faux paiements

Vérifier un paiement dans le service habituel et rester dans le cadre de la plateforme.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Nadia vend un appareil photo 240 €. Un acheteur lui envoie une capture indiquant « paiement effectué » et un lien pour récupérer la somme. La page réclame sa carte et 35 € d'assurance. Dans une autre annonce, un vendeur propose le même appareil à moitié prix mais exige un acompte hors plateforme et refuse les questions.

Comprendre le piège

Un faux vendeur peut encaisser sans livrer. Un faux acheteur peut inventer un paiement pour voler le bien, des données ou des frais. Une capture et un courriel ne confirment pas l'encaissement. Sortir de la plateforme peut faire perdre les protections prévues par ses conditions.

Les signes d'alerte

• Une offre très attractive s'accompagne d'un refus de vérification.

• L'interlocuteur impose une messagerie ou un lien de paiement extérieur.

• Le vendeur doit payer des frais pour recevoir la vente.

• Une preuve de paiement est montrée sans opération vérifiable dans le compte.

06 — Vérifier et réagir

Le réflexe à retenir

Ouvrir soi-même l’application habituelle et vérifier la transaction. Lire les règles de paiement de la plateforme et différer l’envoi du bien tant que le paiement n’est pas confirmé.

Que faire si j’ai été victime ?

Prévenir les acteurs concernés

Signaler rapidement le profil et la transaction à la plateforme. Alerter la banque ou le prestataire de paiement si une somme ou des données ont été transmises.

Protéger les moyens exposés

Faire opposition si la carte est compromise. Remplacer les mots de passe saisis sur un faux site, depuis le vrai service.

Constituer les preuves

Garder annonce, pseudo, conversations, lien, justificatifs et suivi de livraison. Ne pas envoyer de nouveaux frais pour tenter de récupérer les précédents.

Engager les démarches

Selon les conditions de la plateforme, demander l’ouverture d’un litige. Pour la plainte, suivre le parcours officiel approprié, notamment THESEE si éligible, ou se rendre à la police/gendarmerie.

À vous de jouer

Décider si Nadia peut expédier à partir de la capture seule, puis écrire le chemin de vérification du paiement. Identifier le geste à refuser dans la seconde annonce.

Réponses personnelles : .....

.....

06 — 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. Quelle vérification compte avant d’envoyer le bien ?

A. La transaction dans le service ouvert soi-même.

B. La capture de l’acheteur.

C. Son message très poli.

2. Il faut payer 35 € pour recevoir le prix de vente. Que faire ?

A. Payer sans vérifier.

B. Transmettre sa carte à l’acheteur.

C. Suspendre et vérifier les règles de la plateforme.

3. Quitter la plateforme peut-il modifier les recours ?

A. Non, jamais.

B. Oui, selon les conditions de la plateforme.

C. Oui, mais cela garantit un meilleur prix.

4. Après une fraude, faut-il payer des frais de récupération proposés par le même contact ?

A. Non, alerter les services concernés.

B. Oui, pour fermer le dossier.

C. Oui, si le montant est faible.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Vente entre particuliers

Justice.fr — Faux acheteur sur Internet

Service-Public — Arnaque sur Internet et THESEE

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

07 — Faux RIB et facture détournée

Confirmer un changement bancaire hors de l’échange qui l’annonce.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Paul doit régler 1 250 € à son artisan. Dans la conversation de devis, un nouveau courriel annonce un changement de compte et joint un RIB. La signature et le montant sont exacts. Le message insiste pour payer avant midi. Quand Paul appelle le numéro présent dans ce nouveau courriel, la personne confirme le changement.

Comprendre le piège

Une messagerie peut être compromise et la facture remplacée. Les détails exacts du chantier renforcent l’apparence d’authenticité. Le contact contenu dans le message douteux peut conduire au fraudeur ; une confirmation obtenue par ce même canal ne lève donc pas le doute.

Les signes d’alerte

• Les coordonnées bancaires changent juste avant le règlement.

• Le message exige une exécution urgente.

• Le nom du bénéficiaire ou un avertissement bancaire paraît incohérent.

• Le seul moyen de confirmer figure dans le nouveau message.

07 — Vérifier et réagir

Le réflexe à retenir

Suspendre le virement et joindre l’artisan à son numéro habituel, conservé avant ce courriel. Confirmer l’identité du bénéficiaire et ses coordonnées par ce canal indépendant.

Que faire si j’ai été victime ?

Contacter la banque immédiatement

Indiquer qu’un virement a été fait vers un bénéficiaire frauduleux et demander une tentative de rappel. Le retour des fonds reste incertain.

Prévenir le vrai créancier

Le joindre par ses coordonnées connues pour qu’il vérifie aussi sa messagerie et prévienne d’autres destinataires si nécessaire.

Vérifier les comptes concernés

Si sa propre messagerie a pu être piratée, depuis un appareil de confiance changer le mot de passe, activer la double authentification et faire contrôler les accès et renvois de courrier.

Conserver et déposer plainte

Garder factures, RIB reçu, courriels et référence du virement. Demander une orientation aux services officiels ; ne pas négocier avec l’auteur.

À vous de jouer

Comparer un ancien devis et le nouveau message fictif, sans vrai IBAN. Choisir le numéro à utiliser et rédiger la question de confirmation.

Réponses personnelles : .....

.....

07 — 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. Un message dans un fil existant est-il forcément fiable ?

A. Oui, le fil l’authentifie.

B. Non, un compte peut être compromis.

C. Oui, avec la signature habituelle.

2. Quel numéro utiliser pour confirmer le nouveau RIB ?

A. Celui du nouveau message.

B. Celui d’un lien de ce message.

C. Le numéro de l’artisan déjà connu.

3. Le virement est déjà exécuté. Que faire en premier ?

A. Alerter la banque et demander un rappel.

B. Attendre la livraison du chantier.

C. Envoyer un second virement.

4. Un avertissement sur le bénéficiaire apparaît. Quelle attitude ?

A. L’ignorer si le courriel est poli.

B. Suspendre pour vérifier indépendamment.

C. Modifier au hasard le nom.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Fraude au virement et faux RIB

17Cyber — Diagnostic et assistance

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

08 — Faux proche en difficulté

Vérifier une demande familiale avant d’envoyer de l’argent.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Gérard reçoit : « Coucou papa, mon téléphone est cassé, voici mon nouveau numéro. » Son supposé fils demande 680 € pour une facture, à virer sur le compte d’un ami. Il ne peut pas parler et répète que c’est urgent. Les messages sont affectueux. Gérard pense reconnaître son ton.

Comprendre le piège

Le fraudeur crée une urgence familiale et justifie le changement de numéro pour empêcher la vérification. Un compte connu peut aussi être piraté. Une voix ou une photo peuvent être imitées ; la familiarité ressentie ne remplace pas le rappel au contact habituel.

Les signes d’alerte

• Un nouveau numéro s’accompagne immédiatement d’un problème urgent.

• La conversation vocale ou le contact habituel sont évités.

• L’argent doit aller à un tiers ou par un moyen inhabituel.

• La demande exige la discrétion et s’impatiente si l’on vérifie.

08 — Vérifier et réagir

Le réflexe à retenir

Appeler le proche à son ancien numéro ou joindre une autre personne de confiance qui peut confirmer la situation. Si personne ne répond, attendre cette confirmation avant de payer.

Que faire si j’ai été victime ?

Cesser les échanges

Ne plus envoyer d’argent ni de données. Garder les messages, puis bloquer le contact frauduleux.

Alerter la banque

Si un virement ou un paiement a été fait, joindre rapidement la banque pour examiner les possibilités de blocage, rappel et contestation.

Prévenir le vrai proche

Le contacter par un canal connu et avertir les autres proches susceptibles de recevoir la même demande.

Conserver et signaler

Garder numéros, échanges et justificatifs. Signaler le SMS au 33700 et le compte à la messagerie. En cas d’escroquerie, préparer une plainte.

À vous de jouer

Jouer une conversation où Gérard répond qu’il rappellera par son moyen habituel. Proposer une autre vérification si son fils ne répond pas.

Réponses personnelles : .....

.....

08 — 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. Le style affectueux prouve-t-il que c’est son fils ?

A. Oui, un escroc ne le ferait pas.

B. Oui, avec une photo.

C. Non, il faut vérifier par un autre canal.

2. Le fils ne répond pas au numéro habituel. Que faire ?

A. Attendre ou joindre un autre proche fiable.

B. Payer par prudence.

C. Envoyer sa carte au nouveau numéro.

3. Le compte destinataire appartient à un ami inconnu. Que signifie ce détail ?

A. Une garantie supplémentaire.

B. Un signal d’alerte à vérifier.

C. La preuve d’un dépannage normal.

4. Gérard a payé. Faut-il attendre que le faux proche réponde ?

A. Oui, jusqu’au lendemain.

B. Oui, pour récupérer le reçu.

C. Non, prévenir rapidement la banque.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Faux enfant en difficulté

Service-Public — Spam vocal et SMS

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

09 — Fausses offres d’emploi

Vérifier un recrutement et refuser d’avancer des fonds.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Yanis reçoit une proposition de travail à domicile très bien payée, sans entretien. Le recruteur lui réclame une pièce d’identité et 95 € pour un kit de départ. Une variante lui envoie un chèque pour acheter du matériel et demande de reverser rapidement le surplus. Une autre offre rémunère quelques tâches, puis impose un dépôt pour débloquer la suite.

Comprendre le piège

Le fraudeur peut chercher de l’argent, des documents d’identité ou un intermédiaire pour déplacer des fonds. Un contrat ou un numéro SIRET peuvent être copiés. Un chèque crédité provisoirement peut ensuite être rejeté ; le reversement demandé reste alors à la charge de la personne trompée.

Les signes d’alerte

• Le salaire est disproportionné et le recrutement évite les vérifications normales.

• Il faut payer pour obtenir le poste ou accéder aux tâches.

• On demande d’encaisser puis de reverser de l’argent.

• Des documents sensibles sont réclamés avant toute identification indépendante.

09 — Vérifier et réagir

Le réflexe à retenir

Ne pas avancer d'argent ni reverser un chèque. Retrouver soi-même l'entreprise et confirmer l'offre auprès de son service recrutement, par des coordonnées indépendantes.

Que faire si j'ai été victime ?

Stopper le circuit financier

Ne plus verser ni transférer d'argent. Prévenir immédiatement la banque si un chèque, un virement ou la carte sont concernés.

Protéger les informations transmises

Si une pièce d'identité ou d'autres données ont été données, demander conseil sur les risques d'usurpation et prévenir les organismes concernés. Ne pas envoyer de nouvelles pièces au même contact.

Alerter la plateforme et l'entreprise

Signaler l'offre au site d'emploi et à l'entreprise dont l'identité est utilisée, par leurs vrais contacts. France Travail peut accompagner la vérification d'une offre.

Conserver les preuves et porter plainte

Garder annonce, contrat, échanges et justificatifs. En cas d'utilisation de l'identité, documenter aussi ces faits pour les démarches auprès de la police/gendarmerie.

À vous de jouer

Repérer les trois demandes financières différentes du scénario. Écrire ce qui doit être vérifié avant d'envoyer des documents à un recruteur.

Réponses personnelles : .....

.....

09 — 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. Le SIRET sur le contrat suffit-il ?

A. Non, l’identité peut être copiée.

B. Oui, il garantit le recruteur.

C. Oui, sans entretien.

2. Un chèque apparaît crédité. Peut-on reverser le surplus sans vérification ?

A. Oui, immédiatement.

B. Oui, si le recruteur insiste.

C. Non, demander confirmation à la banque.

3. Un dépôt permettrait de débloquer des tâches rémunérées. Que faire ?

A. Payer une petite somme.

B. Refuser et arrêter les versements.

C. Emprunter le dépôt.

4. Des données d’identité ont été transmises. Quelle attitude ?

A. Demander conseil et surveiller les usages frauduleux.

B. Envoyer davantage de documents.

C. Ignorer, puisqu’aucun paiement n’a eu lieu.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Fausses offres d’emploi

Cybermalveillance.gouv.fr — Arnaque à la tâche

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

10 — Chantage intime et fausse webcam piratée

Réagir à une menace sans payer ni rester isolé.



Illustration de formation créée par IA — exemple fictif.

Mise en situation

Camille reçoit un courriel prétendant avoir filmé sa webcam et citant un ancien mot de passe. Il exige une rançon sous 24 heures. Dans un autre cas fictif, une personne menace réellement de diffuser un contenu intime obtenu lors d'un échange. Camille hésite à payer et n'ose en parler à personne. Aucun contenu intime n'est montré dans cet atelier.

Comprendre le piège

Deux situations doivent être distinguées : un message de masse prétendant avoir piraté une webcam, et une menace de diffusion reposant sur un contenu réel ou fabriqué. Un ancien mot de passe peut venir d'une fuite ; sa présence ne démontre pas l'existence d'un enregistrement. Dans les deux cas, payer ne garantit pas la fin du chantage.

Les signes d'alerte

• Une menace de diffusion sert à imposer argent ou nouveaux contenus.

• Une échéance courte et la honte empêchent de demander de l'aide.

• Un ancien secret est utilisé comme prétendue preuve d'un piratage récent.

• Le contact veut isoler la personne ou obtenir toujours davantage.

10 — Vérifier et réagir

Le réflexe à retenir

Ne pas payer ni envoyer d’autres contenus. Cesser le contact, préserver les menaces accessibles sans les relayer et demander de l’aide à une personne de confiance.

Que faire si j’ai été victime ?

Se faire accompagner

La personne visée n’est pas responsable du chantage. Parler à un proche et contacter France Victimes au 116 006 ; pour un mineur ou des cyberviolences concernant un jeune, solliciter le 3018.

Limiter la diffusion

Signaler le compte et les contenus à la plateforme, demander leur retrait et restreindre la visibilité des contacts. Ne pas republier les images pour dénoncer les faits.

Sécuriser les comptes

Changer les mots de passe exposés ou réutilisés depuis un appareil de confiance et activer la double authentification. L’ancien mot de passe ne prouve pas un accès actuel.

Conserver et déposer plainte

Garder menaces, pseudos, adresses et demandes de paiement. Pour un mineur, ne pas télécharger ni faire circuler de contenu intime ; demander aux enquêteurs ou au 3018 comment préserver les éléments. Porter plainte via le parcours adapté ou la police/gendarmerie.

À vous de jouer

Comparer les deux cas sans regarder ni produire de contenu intime. Écrire une phrase de soutien et une démarche immédiate qui ne dépend pas d’un paiement.

Réponses personnelles : .....

.....

10 — 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. Un ancien mot de passe prouve-t-il une vidéo récente ?

A. Oui, toujours.

B. Non, il peut provenir d'une fuite antérieure.

C. Oui, si le message est urgent.

2. Payer garantit-il l'arrêt du chantage ?

A. Oui, avec un reçu.

B. Oui, une seule fois.

C. Non, de nouvelles demandes peuvent suivre.

3. Comment aider un jeune concerné ?

A. Écouter, solliciter un adulte de confiance et le 3018.

B. Lui demander de tout raconter devant le groupe.

C. Diffuser la menace avec les images.

4. Quelle preuve conserver en priorité sans relayer d'image intime ?

A. Une publication publique des images.

B. Les messages de menace, pseudos et demandes d'argent.

C. Aucune trace des échanges.

Pour vérifier les repères

Cybermalveillance.gouv.fr — Sextorsion

Cybermalveillance.gouv.fr — Webcam prétendue piratée

e-Enfance — Le 3018

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

Aide et démarches pour les victimes

Choisir les gestes adaptés à ce qui s’est passé. Ne pas attendre une plainte pour alerter la banque si un paiement est concerné.

Si de l’argent ou une carte sont concernés

Contacter immédiatement la banque ou le prestataire de paiement par son moyen habituel. Expliquer si l’on a transmis une carte, communiqué un code, validé une opération ou envoyé un virement. Demander les mesures possibles : opposition, contestation et, pour un virement, tentative de rappel. Ne pas attendre un signalement ou une plainte pour alerter la banque. Aucun remboursement ni retour des fonds n’est assuré par ce module.

Si un compte ou un appareil est compromis

Depuis un appareil de confiance, modifier les mots de passe exposés ou réutilisés et activer la double authentification. Si quelqu’un contrôle l’ordinateur, couper sa connexion Internet et organiser une vérification technique. Le service officiel 17Cyber peut aider à identifier l’incident et orienter les démarches.

Garder des éléments utiles

Conserver les messages, dates, adresses de sites, pseudos, références de transactions et justificatifs déjà disponibles. Écrire une chronologie factuelle. Ne pas prolonger la conversation pour obtenir une preuve et ne pas diffuser publiquement des données personnelles ou images intimes.

Signaler au bon endroit

Le 33700 reçoit les signalements de SMS et d’appels indésirables ; Signal Spam traite les courriels indésirables. Signaler aussi le profil ou la transaction à la plateforme concernée. PHAROS sert au signalement de contenus illicites sur Internet, selon son périmètre. Un signalement ne remplace ni l’urgence bancaire ni un dépôt de plainte.

Démarches et accompagnement

Déposer plainte

Consulter le parcours officiel « Arnaque sur Internet / THESEE » sur Service-Public pour vérifier l'éligibilité au téléservice. Toutes les situations ne relèvent pas de THESEE. La police ou la gendarmerie peuvent recevoir la plainte et orienter la personne ; apporter les preuves disponibles. Ne pas utiliser les liens d'un prétendu enquêteur qui vous contacte spontanément.

Être soutenu

France Victimes, au 116 006, accompagne les victimes. Le 3018 aide face aux violences numériques concernant les jeunes. Demander l'aide d'une personne de confiance et garder les démarches personnelles en dehors du groupe de formation. Le chantage et la manipulation relèvent de la responsabilité de leurs auteurs.

Éviter une seconde escroquerie

Refuser de payer un prétendu spécialiste qui garantit de récupérer des fonds, de supprimer une vidéo ou de débloquer un compte. Vérifier soi-même l'identité de tout intervenant. Les fraudeurs peuvent revenir sous une nouvelle identité, y compris celle d'un service public.

Accès officiels utiles

17Cyber — Diagnostic et assistance

Service-Public — Arnaque sur Internet et THESEE

Service-Public — Spam vocal et SMS

Cybermalveillance.gouv.fr — Signaler un courriel frauduleux

PHAROS — Signaler un contenu illicite

e-Enfance — Le 3018

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

Ma fiche réflexe contre les arnaques

À conserver près de son téléphone ou de son ordinateur.

Suspendre la demande

Prendre le temps de vérifier. Ne transmettre ni secret ni paiement sous la pression d’un correspondant.

Vérifier hors du message

Rappeler au numéro déjà connu ou ouvrir soi-même l’application habituelle. Le logo, le numéro apparent et le petit montant ne suffisent pas.

Si j’ai déjà agi

Banque : alerte immédiate si argent ou moyen de paiement exposé. Comptes : changer les secrets divulgués depuis un appareil de confiance. Appareil contrôlé : couper Internet et demander une aide fiable.

Conserver puis demander de l’aide

Garder messages et justificatifs déjà accessibles. 17Cyber : orientation technique. 116 006 : aide aux victimes. 3018 : cyberviolences concernant les jeunes. Les liens officiels figurent dans le document « Aide et démarches ».

Refuser de payer une seconde fois

Une taxe de déblocage, une rançon ou une promesse de récupération contre avance peut prolonger l’escroquerie. Aucun remboursement n’est garanti.

Mon contact de confiance

Nom ou rôle : .....
Coordonnées que j’ai vérifiées : .....

17Cyber — Diagnostic et assistance

Service-Public — Arnaque sur Internet et THESEE

e-Enfance — Le 3018

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