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.