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.