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.