

L'arnaque au faux support technique

Un écran qui hurle « virus détecté », un numéro à appeler, un faux technicien très serviable : l'escroquerie qui vide les comptes en une heure.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/faux-support-technique

Le scénario est rodé : une alerte alarmante bloque l'écran — « virus détecté, appelez Microsoft au 01... » — ou un appel spontané annonce un problème sur « votre ordinateur ». Au bout du fil, un « technicien » patient et professionnel propose de tout réparer : il suffit d'installer un petit logiciel d'accès à distance... L'arnaque au faux support technique fait des dizaines de milliers de victimes par an en France, particuliers ET entreprises — et elle se déjoue à 100 % quand on connaît le script.

1. Le script de l'arnaque, étape par étape

- L'accroche : fausse alerte plein écran (avec sons et compte à rebours) sur un site piégé, faux appel « de Microsoft / du fournisseur d'accès / de la banque », ou email alarmant
- La prise de contrôle : la victime installe l'outil d'accès à distance « pour le diagnostic » (AnyDesk, TeamViewer...) — l'escroc voit et pilote tout
- La mise en scène : défilement d'écrans techniques, « détection » de problèmes graves inventés — tout est théâtre
- L'extorsion : paiement d'une « réparation » ou d'un « abonnement de protection », voire connexion à la banque « pour vérifier » — et les virements partent
- La persistance : les victimes qui ont payé sont rappelées des mois après (« remboursement », « renouvellement ») — le fichier des victimes se revend

ATTENTION

Le fait de base qui démonte toute l'arnaque : NI Microsoft, NI Apple, NI votre banque, NI votre fournisseur d'accès ne vous appellent spontanément pour un problème sur votre ordinateur. Jamais. Un appel entrant de ce type est une arnaque, à 100 %, sans exception. On raccroche.

2. Face à la fausse alerte qui bloque l'écran

- Ne pas appeler le numéro, ne rien installer, ne rien payer
- Fermer l'onglet ou le navigateur : Ctrl+W, ou gestionnaire des tâches (Ctrl+Maj+Échap) si tout semble bloqué — l'alerte n'est qu'une page web en plein écran
- Au redémarrage du navigateur, ne pas restaurer les onglets
- Rien n'était infecté avant l'alerte ; il n'y a rien à réparer — c'est le principe même du piège
- Signaler le site sur signal-spam ou au référent informatique

3. Si le mal est fait

- L'escroc a pris la main : déconnecter Internet, désinstaller l'outil d'accès à distance, faire analyser le poste avant de le réutiliser — l'escroc a pu laisser des accès
- Changer les mots de passe saisis pendant ou après l'incident, depuis un autre appareil
- Paiement effectué : opposition immédiate auprès de la banque, demande de rappel des virements
- Déposer plainte (le service en ligne THESEE traite précisément ces escroqueries) et signaler sur cybermalveillance.gouv.fr
- En entreprise : traiter comme un incident (voir notre guide) — le poste a été manipulé par un tiers hostile

4. Protéger l'entreprise et les proches

- En parler explicitement en sensibilisation : le scénario raconté une fois est déjoué à vie — c'est l'arnaque la plus « vaccinable » qui soit
- Établir la règle interne : tout support informatique passe par le prestataire ou le référent connu — personne d'autre ne prend jamais la main sur un poste
- Verrouiller les outils d'accès à distance légitimes (voir notre guide) : mots de passe forts, MFA, pas d'accès permanent inutile
- Penser aux publics fragiles autour de vous : cette arnaque cible massivement les seniors — le réflexe « on raccroche et on rappelle le vrai numéro » se partage en famille

L'essentiel à retenir

- 01 Ancrer la règle : aucun éditeur ni opérateur n'appelle spontanément
- 02 Savoir fermer une fausse alerte (Ctrl+W, gestionnaire des tâches)
- 03 Définir qui est LE support légitime de l'entreprise
- 04 Ne jamais installer un accès à distance à la demande d'un inconnu
- 05 En cas de doute après incident : analyse du poste et changement des mots de passe
- 06 Déposer plainte et signaler — même pour une tentative

Questions fréquentes

L'alerte semblait vraiment venir de Windows, avec les logos officiels...

C'est une page web qui imite les alertes système — logos, sons et plein écran compris. Le test simple : une vraie alerte Windows ne demande jamais d'appeler un numéro de téléphone. Toute « alerte » avec un numéro à appeler est une arnaque, quelle que soit sa qualité graphique.

J'ai laissé l'accès à distance mais rien payé. Suis-je tranquille ?

Pas encore : pendant la session, l'escroc a pu copier des fichiers, installer un accès persistant ou récupérer des mots de passe enregistrés. Le poste doit être analysé (voire réinstallé au moindre doute), les mots de passe sensibles changés, et les comptes surveillés. Ne rien avoir payé vous a épargné le pire, pas tout.

La banque peut-elle rembourser les sommes versées ?

C'est difficile quand la victime a elle-même validé les paiements — mais pas toujours impossible, selon les circonstances et la rapidité de réaction. Opposition et signalement immédiats, dépôt de plainte, et contestation écrite auprès de la banque : chaque heure compte, et le dossier de plainte est indispensable.

Pour aller plus loin

Cybermalveillance.gouv.fr — fiche faux support technique — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/arnaque-au-faux-support-technique

THESEE — déposer plainte en ligne — www.service-public.fr/particuliers/vosdroits/N31138

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr