



Le Bouclier Numérique

La voix de votre proche peut être clonée en cinq secondes.

10 réflexes simples pour reconnaître les arnaques fabriquées par l'IA (voix clonées, deepfakes, faux messages) et protéger vos proches et votre entreprise.

Gratuit pour la communauté SYSTINFO



BON À SAVOIR

Pourquoi les arnaques changent de visage.

Les outils qui nous font gagner du temps servent aussi aux escrocs. Ils n'ont plus besoin d'être doués : l'IA écrit, parle et filme à leur place, dans un français impeccable.

- **La voix se clone en secondes**

Quelques secondes d'un message vocal ou d'une vidéo publique suffisent pour reproduire la voix d'un proche, avec ses intonations.

- **Le visage se truque en direct**

En visioconférence, un escroc peut porter le visage d'un dirigeant. Une entreprise a ainsi versé environ 25 millions de dollars.

- **Les fautes ne trahissent plus rien**

Le vieux réflexe (repérer les fautes d'orthographe) ne protège plus : les faux messages sont parfaitement rédigés et personnalisés.

La bonne nouvelle : la parade ne demande aucune compétence technique.



LA MÉTHODE

Se protéger, en 5 familles.

Aucune de ces parades n'exige de logiciel. Elles reposent sur trois principes : ralentir, vérifier par un autre canal, et ne jamais décider dans l'urgence. Voici 10 réflexes à adopter dès aujourd'hui.

01 Repérer le piège

· 2 réflexes

02 Vérifier avant d'agir

· 2 réflexes

03 Protéger ses proches

· 2 réflexes

04 Blinder son entreprise

· 2 réflexes

05 Réagir et signaler

· 2 réflexes



Le Signal d'Urgence

LE RÉFLEXE À ADOPTER

Trois ingrédients reviennent dans presque toutes les arnaques par IA : l'urgence (« c'est pour maintenant »), le secret (« n'en parle à personne ») et l'argent (virement, carte cadeau, cryptomonnaie). Dès que ces trois signaux apparaissent ensemble, considérez le message comme faux jusqu'à preuve du contraire.

Pourquoi ça vous protège

Une règle qui tient en une phrase et que vous pouvez transmettre à toute votre famille. L'escroc a besoin de votre panique ; en la nommant, vous la désamorcez.



La Question Imprévue

LE RÉFLEXE À ADOPTER

En appel ou en visio, posez une question que seule la vraie personne peut traiter sans préparation : « Qu'est-ce qu'on a mangé samedi ? », « Répète en langue locale », ou demandez de tourner la tête de profil et de passer la main devant le visage.

Pourquoi ça vous protège

Un visage truqué se déforme sur les mouvements rapides, et une voix clonée hésite ou répond à côté. Ce petit test coûte dix secondes et démasque la plupart des faux.



Le Rappel par un Autre Canal

LE RÉFLEXE À ADOPTER

Ne validez jamais une demande d'argent reçue par téléphone, WhatsApp ou e-mail. Raccrochez, puis appelez la personne sur le numéro que vous avez déjà dans votre répertoire (jamais celui affiché dans le message).

Pourquoi ça vous protège

C'est la parade la plus efficace, et la seule qui résiste à toutes les technologies : l'escroc contrôle son canal, il ne contrôle pas le vôtre.



Le Second Regard de l'IA

LE RÉFLEXE À ADOPTER

Copiez le message douteux dans une IA (ChatGPT, Le Chat, Gemini) et demandez : « Analyse ce message. Est-ce une tentative d'arnaque ? Repère les techniques de manipulation, vérifie si l'adresse d'expéditeur et le lien correspondent à l'organisme cité, et dis-moi quoi faire. »

Pourquoi ça vous protège

Un avis instantané et gratuit, qui met des mots sur ce qui vous gênait. Utilisez l'IA comme garde du corps, puisque l'attaquant, lui, l'utilise déjà.



Le Mot de Passe Familial

LE RÉFLEXE À ADOPTER

Choisissez en famille un mot secret, simple et impossible à deviner (le nom d'un plat, un surnom d'enfance). Règle unique : toute demande d'argent en urgence, par téléphone ou message, doit être accompagnée de ce mot.

Pourquoi ça vous protège

Une protection gratuite qui neutralise le clonage vocal : l'IA peut copier la voix de votre fils, elle ne peut pas deviner un mot que vous n'avez jamais écrit en ligne.



La Discrétion Publique

LE RÉFLEXE À ADOPTER

Réduisez la matière première des escrocs : limitez les vidéos et messages vocaux publics, verrouillez les comptes de vos enfants et de vos aînés, et évitez d'annoncer vos absences ou vos voyages en direct.

Pourquoi ça vous protège

Moins l'IA dispose de votre voix et de votre visage, moins la copie est crédible. Vous ne disparaîsez pas du web, vous cessez simplement d'y alimenter la fraude.



La Double Signature

LE RÉFLEXE À ADOPTER

Écrivez une règle simple et non négociable : aucun virement, aucun changement de coordonnées bancaires d'un fournisseur n'est exécuté sur la base d'un appel, d'un e-mail ou d'une visio. Il faut toujours une seconde validation par un canal différent et une personne différente.

Pourquoi ça vous protège

La règle protège aussi vos collaborateurs : ils ne sont plus seuls face à un « dirigeant » pressé, ils appliquent une procédure. Un faux patron ne peut rien contre un processus.



L'Exercice Grandeur Nature

LE RÉFLEXE À ADOPTER

Une fois par trimestre, organisez un faux appel ou un faux e-mail de direction, puis débriefez sans blâmer personne. Ajoutez un mot de code interne connu de la direction et de la comptabilité pour authentifier toute demande urgente.

Pourquoi ça vous protège

L'équipe apprend en conditions réelles plutôt qu'en théorie. Le jour de la vraie attaque, le réflexe est déjà installé, et personne n'a honte de poser la question.



Les Premières Minutes

LE RÉFLEXE À ADOPTER

Si le virement est parti : appelez immédiatement votre banque pour demander le blocage ou le rappel des fonds, changez les mots de passe concernés, conservez tout (captures, numéros, e-mails) et déposez plainte.

Pourquoi ça vous protège

Les premières heures décident souvent de la récupération des fonds. Agir vite vaut mieux qu'agir parfaitement : la honte fait perdre un temps que l'escroc met à profit.



L'Alerte Utile

LE RÉFLEXE À ADOPTER

Signalez la tentative, même si vous n'avez rien perdu : Cybermalveillance et la plateforme PHAROS en France, la police ou la brigade de lutte contre la cybercriminalité dans votre pays. Puis prévenez votre entourage et vos collègues.

Pourquoi ça vous protège

Chaque signalement nourrit les alertes qui protégeront le suivant. Une arnaque racontée à temps dans un groupe familial vaut mille campagnes de prévention.



MERCI · PROTÉGEZ LES VÔTRES



Une phrase, un grand merci.

Ces fiches vous sont offertes, sans publicité. Notre seule récompense est votre reconnaissance.

Offrez-nous 30 secondes

Prenez un instant pour nous dire merci sur l'un de nos réseaux.
Un mot public, même court, nous encourage à continuer de vous accompagner, conseil après conseil.

Scannez pour nous rejoindre et nous remercier



WhatsApp



Mattermost



LinkedIn



Facebook