À l'ère de l'IA, ne croyez pas tout ce que vous voyez. Doutez.

Le mini-guide pour reconnaître les manipulations par l'image et la voix, et adopter les bons réflexes.



NOUVEY
CYBERSÉCURITÉ SANTÉ
MAYOTTE RÉUNION

Le vrai danger n'est pas l'IA. C'est ce qu'elle vous fait croire.

✚ *De quoi parle-t-on ?*

Aujourd'hui, l'IA est devenue si performante qu'elle peut recréer le visage d'un proche, la voix d'un collègue ou les traits d'une personne connue, de façon presque indétectable à l'œil ou à l'oreille.

C'est ça, un deepfake : une image, une vidéo ou une voix fabriquée par intelligence artificielle pour imiter une personne réelle.

Le plus inquiétant : cloner une voix ne demande que quelques secondes d'enregistrement. Un message vocal, une vidéo publiée en ligne, un extrait d'appel peuvent suffire.

✚ *Pourquoi faut-il être vigilant ?*

Un deepfake peut nous faire croire qu'une demande vient d'une personne de confiance, et donc nous pousser à agir sans vérifier.

Il ne cherche pas à pirater votre ordinateur. Il cherche à vous faire agir : transférer de l'argent, communiquer un mot de passe, ouvrir un accès, valider une opération… parce que vous croyez parler à quelqu'un que vous connaissez.

Cela peut arriver dans la vie privée comme au travail :

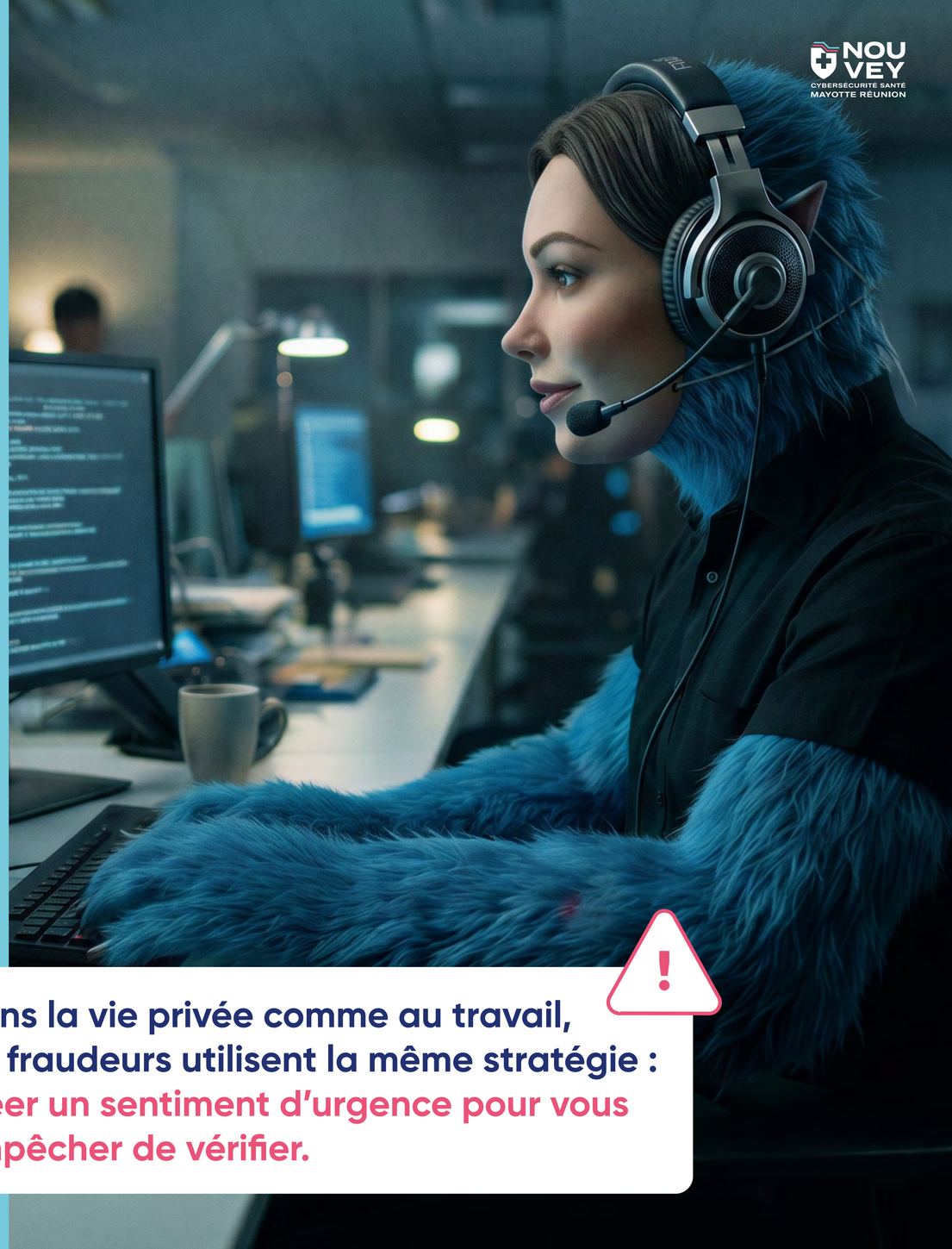
Sphère personnelle : un faux appel d'un proche en difficulté, qui réclame de l'aide en urgence.

Sphère professionnelle : un faux message d'un supérieur ou d'un confrère, qui demande un virement, un accès ou des données sensibles.

✚ *Et concrètement ?*

Dans la vie privée, vous recevez un appel. C'est la voix de votre mère. Elle est paniquée : un accident, un problème, elle a besoin d'argent tout de suite. La voix est juste, l'émotion aussi. Mais ce n'est peut-être pas elle.

Au travail, vous recevez un message vocal de votre responsable. Il vous demande de régler une facture urgente avant la fin de journée, « pendant qu'il est en réunion ». Le ton est habituel, la demande crédible. Sauf qu'il n'a jamais passé ce message.



Dans la vie privée comme au travail, les fraudeurs utilisent la même stratégie : créer un sentiment d'urgence pour vous empêcher de vérifier.



NOUVEY
CYBERSÉCURITÉ SANTÉ
MAYOTTE RÉUNION

Les bons réflèxes

Face à une demande inhabituelle, même d'une voix ou d'un visage familier :

01

Ne jamais transférer d'argent

ou de données sur la base d'un seul appel ou message. Une demande légitime supportera toujours une vérification.

02

Vérifiez par un autre canal

Rappelez la personne sur son vrai numéro, ou contactez-la autrement. Ne répondez jamais directement à la demande reçue.

03

En cas de doute, signalez

Prévenez votre entourage, votre service ou votre établissement. Votre vigilance protège aussi les autres.

04

Méfiez-vous de l'urgence

Plus on vous presse, plus vous devez ralentir. L'urgence est l'outil préféré des fraudeurs.

05

Posez une question piège

Demandez une information que l'on ne peut pas deviner ou trouver en ligne, que seule la vraie personne pourrait connaître. Une IA ne saura pas répondre.

Les bonnes pratiques

Attention aux informations que vous donnez à certaines IA !

Sur des outils d'IA ou sur les réseaux sociaux :

01 Evitez de donner trop d'informations vous concernant car les pirates peuvent s'en servir contre vous

02 Anonymiser au maximum les données que vous envoyez

03 N'y partagez aucun document qui comportent des noms, prénoms de patients ou même les vôtres !

Les IA ne sont pas conçus pour héberger des données médicales et ne disposent pas de la certification HDS exigée en France. Vous perdez le contrôle sur ce qui est fait des informations transmises : certaines peuvent être analysées pour améliorer le service.





NOUVEY
CYBERSÉCURITÉ SANTÉ
MAYOTTE RÉUNION

En cas de fuite ou de mauvaise utilisation des données, votre responsabilité professionnelle peut être engagée.

Vrai / faux

"On peut toujours reconnaître un deepfake à l'œil nu."

Faux

Les meilleurs deepfakes sont aujourd'hui indétectables sans outil spécialisé. Ne comptez pas sur votre seul jugement : comptez sur la méthode (vérifier par un autre canal).

"Les deepfakes ne visent que les célébrités et les grandes entreprises."

Faux

N'importe qui peut être imité, ou recevoir un faux appel d'un proche. La cible, c'est la confiance, pas la notoriété.

"Une voix connue n'est plus une preuve d'identité."

Faux

Un numéro affiché peut être falsifié. Le numéro n'est jamais une preuve d'identité.

"20 secondes d'enregistrement suffisent à cloner une voix."

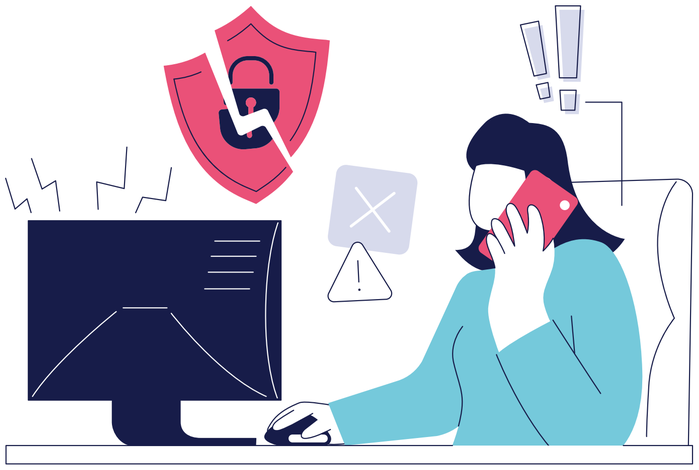
Vrai

Un message vocal, une vidéo publiée en ligne, un extrait d'appel : la matière première est souvent déjà disponible.

"Même un expert peut se faire piéger par un deepfake."

Vrai

La qualité des faux ne dépend plus du regard de celui qui les reçoit. Personne n'est immunisé, d'où l'importance de la vérification systématique.



COFFRE-FORT DE MOTS DE PASSE

Le bon réflexe pour protéger vos accès

Un coffre-fort de mots de passe vous aide à créer, stocker et retrouver des mots de passe différents pour chaque compte, sans avoir à tous les mémoriser.



Un coffre-fort ne remplace pas la vigilance, mais il aide à adopter une bonne habitude : ***1 compte = 1 mot de passe différent***

01 Pourquoi c'est utile ?

- 1 compte = 1 mot de passe différent
- Des mots de passe plus longs et plus robustes
- Moins de risques en cas de fuites de données
- Moins besoin de tout retenir

02 Comment ça fonctionne ?

- Vous retenez 1 seul mot de passe maître
- Le coffre-fort chiffre vos identifiants
- Il peut générer des mots de passe robustes
- Certaines solutions facilitent le partage d'accès en équipe

03 Les bons réflexes

- ✔ Choisir un mot de passe maître long, unique, et difficile à deviner
- ✔ Activer la double authentification si possible
- ✔ Garder ses appareils et logiciels à jour
- ✔ Vérifier l'adresse du site avant de se connecter
- ✔ Suivre les conseils de sa structure si vous travaillez en équipe

04 Les erreurs à éviter

- ✖ Réutiliser le même mot de passe partout
- ✖ Noter ses accès sur un post-it ou dans un fichier non protégé
- ✖ Envoyer un mot de passe par mail ou par messagerie
- ✖ Oublier que la sécurité dépend du mot de passe maître
- ✖ Confondre coffre-fort sécurisé et enregistrement des mots de passe directement dans le navigateur

DISPONIBLE SUR

Application mobile · Logiciel ordinateur · Extension navigateur

Pour aller plus loin

Scannez le QR code
pour accéder à toutes nos ressources.

Plus d'infos sur nouvey.re

Fiches pratiques, vidéos et conseils mis à jour régulièrement
Un doute, une question ? Retrouvez nos points de contact sur le site

NOUVEY
CYBERSÉCURITÉ SANTÉ
MAYOTTE RÉUNION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé La Réunion

ars Agence Régionale de Santé Mayotte

CHU CENTRE HOSPITALIER UNIVERSITAIRE LA RÉUNION

GHER Groupe Hospitalier Est Réunion

CHR CENTRE HOSPITALIER OUEST REUNION

EPSM RÉUNION

TESIS E-SANTÉ