

L'IA REND LES ARNAQUES PLUS CONVAINCANTES

Les escrocs rendent les faux messages, appels téléphoniques et vidéos plus convaincants grâce à l'intelligence artificielle (IA). **Vérifiez via une source fiable.**

UN LIEN, UN NUMÉRO OU UN COMPTE SUSPECT ?
PARTAGEZ-LE SUR SAFEONWEB.BE ET AIDEZ-NOUS À METTRE FIN À LA FRAUDE.

Safeonweb.be

CENTRE FOR CYBERSECURITY BELGIUM

.be

L'IA REND LES ARNAQUES PLUS CONVAINCANTES

Grâce à l'intelligence artificielle (IA), les escrocs peuvent rendre leurs arnaques plus réalistes et plus difficiles à reconnaître. Même en étant vigilant, il devient compliqué de distinguer le vrai du faux. **Ne vous fiez pas uniquement à ce que vous lisez, entendez ou voyez.**

GARDEZ VOTRE SANG-FROID
STOP. VÉRIFIEZ. PARTAGEZ.

MESSAGE

VOUS RECEVEZ UN MAIL OU UN MESSAGE WHATSAPP DE VOTRE BANQUE OU DE VOTRE FOURNISSEUR D'ÉNERGIE ?

Logo, présentation, formulation… Tout semble officiel. Pourtant, grâce à l'IA, les escrocs peuvent imiter ces messages jusque dans les moindres détails.

APPEL

UN PROCHE VOUS TÉLÉPHONE POUR VOUS DEMANDER DE L'AIDE EN URGENCE ?

Même une voix familière peut être imitée grâce à l'IA. Vous pourriez croire parler à un membre de votre famille alors qu'il s'agit d'un escroc.

VIDÉO

VOUS VOYEZ UNE VIDÉO DANS LAQUELLE UNE CÉLÉBRITÉ OU UNE PERSONNALITÉ POLITIQUE RECOMMANDE UN INVESTISSEMENT TRÈS RENTABLE ?

Méfiez-vous ! Grâce à l'IA, les escrocs peuvent créer de fausses vidéos dans lesquelles une personne semble dire ou faire des choses qu'elle n'a jamais dites ou faites.

COMMENT SE PROTÉGER ?

1 Prenez votre temps

Les escrocs cherchent souvent à vous faire agir dans l'urgence. Ne cédez pas à la pression. Prenez le temps de réfléchir et de vérifier avant d'agir.

2 Vérifiez via une source fiable

Ne vous fiez pas uniquement aux apparences.

→ **UN MESSAGE SUSPECT ?** Ne cliquez pas sur les liens suspects et n'ouvrez pas les pièces jointes douteuses. Rendez-vous directement sur le site officiel ou l'application de l'organisme concerné.

→ **UN APPEL D'UN PROCHE ?** Rappelez-le sur son numéro habituel. Vous pouvez aussi convenir à l'avance d'un code secret avec vos proches pour confirmer leur identité.

→ **UNE VIDÉO ÉTONNANTE ?** Vérifiez si vous retrouvez cette information dans d'autres sources fiables.

3 Gardez vos codes secrets

Ne communiquez jamais vos mots de passe, votre code PIN ou vos codes bancaires et itsme®, même si la demande semble provenir d'une personne ou d'un organisme de confiance.

VOICI COMMENT PROCÈDENT LES ARNAQUEURS

› Ils se renseignent sur vous

Les escrocs récupèrent des informations sur les réseaux sociaux : nom, famille, profession, centres d'intérêt… L'IA leur permet d'automatiser cette collecte d'informations et rend ainsi leurs arnaques plus personnelles et crédibles.

› Ils gagnent votre confiance

Ils se font passer pour une banque, une administration, une entreprise ou une personne que vous connaissez.

› Ils jouent sur vos émotions

Peur, urgence, compassion… Ils cherchent à vous faire réagir rapidement, sans vous laisser le temps de réfléchir.

› Ils vous poussent à agir

Cliquer sur un lien, donner un code, transférer de l'argent ou installer une application…

LEUR OBJECTIF : VOLER VOTRE ARGENT OU VOS DONNÉES PERSONNELLES.

VOUS ÊTES VICTIME ?

Coupez tout contact

Ne répondez plus aux escrocs. Bloquez le numéro, le profil ou l'adresse e-mail.

Protégez votre argent

Si vous avez communiqué des données bancaires, transféré de l'argent ou constaté des retraits suspects, contactez immédiatement votre banque via Fraudstop au

078 170 170

Conservez des preuves et déposez une plainte

Gardez les messages, les adresses web et les coordonnées bancaires de l'escroc. Faites des captures d'écran et déposez plainte auprès de la police locale.

Prévenez votre entourage

Si les escrocs ont usurpé l'identité d'un proche ou d'une organisation, informez-les.

Signalez l'arnaque

- Partagez les infos concernant la fraude via notre formulaire en ligne sur safeonweb.be ou en scannant le code QR.
- Transférez les messages suspects à **SUSPECT@SAFEONWEB.BE**

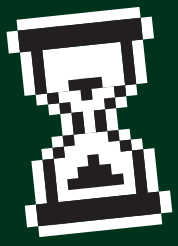
FACE AUX ARNAQUES, GARDEZ LES BONS RÉFLEXES

→ UN MESSAGE, UN APPEL OU UNE VIDÉO VOUS SEMBLE AUTHENTIQUE ?
Vérifiez via une source fiable.

→ ON VOUS MET SOUS PRESSION ?
Prenez votre temps.

→ ON VOUS DEMANDE DE L'ARGENT, DES CODES OU DES DONNÉES ?
Arrêtez et vérifiez.

→ VOUS AVEZ UN DOUTE ?
Parlez-en à une personne de confiance et demandez-lui conseil.



L'IA REND LES ARNAQUES PLUS CONVAINCANTES. MAIS LE BON RÉFLEXE RESTE LE MÊME :

VÉRIFIEZ VIA UNE SOURCE FIABLE.

Plus d'infos sur **safeonweb.be**

Safeonweb.be