LA CYBERSÉCURITÉ EST
L'AFFAIRE DE CHACUN

LA SÉCURITÉ EN LIGNE & MOI

EDITION 2025

EDITEUR RESPONSABLE : DENIS MATHEN, GOUVERNEUR DE LA PROVINCE DE NAMUR,
PLACE SAINT-AUBAIN 2, 5000 NAMUR – EDITION 2025

EDITO

LA CYBERCRIMINALITÉ : UN DANGER BIEN RÉEL, SOUVENT SOUS-ESTIMÉ

À l'ère du tout numérique, nos vies personnelles comme professionnelles dépendent plus que jamais des technologies connectées : smartphones, ordinateurs, objets intelligents, services en ligne. Autant de portes ouvertes sur un monde d'opportunités… mais aussi de menaces invisibles.

La cybercriminalité n'est plus un problème qui touche uniquement les institutions ou les grandes entreprises, elle peut affecter chacun d'entre nous. Les cyberattaques se multiplient et se sophistiquent, profitant de nos failles techniques, mais aussi – et surtout – de nos failles humaines. Parce que la première cible des cybercriminels, ce n'est pas la machine… c'est l'utilisateur. Et, tout le monde peut être concerné, souvent sans le savoir.

Face à ce constat, il m'apparaît primordial de s'informer mais surtout d'insister sur la prévention face à ce type de risque, pour que chacun puisse se prémunir au mieux contre la cybercriminalité.

Cet outil de prévention est le fruit de plusieurs réflexions mise en avant, notamment, au travers de la cellule de sécurité et de la commission provinciale sur la prévention de la criminalité, ainsi que le résultat d'une collaboration productive entre différents acteurs et institutions.

Ce document vous permettra, je l'espère, de mieux comprendre les menaces qui nous entourent mais également d'identifier les risques concrets, d'adopter les bons réflexes pour se protéger et pour prévenir les risques ou pour réagir efficacement en cas d'incident.

En cybersécurité, l'information est notre premier rempart car une personne bien informée est déjà beaucoup plus difficile à piéger !

DENIS MATHEN – GOUVERNEUR DE LA PROVINCE DE NAMUR

INTRODUCTION

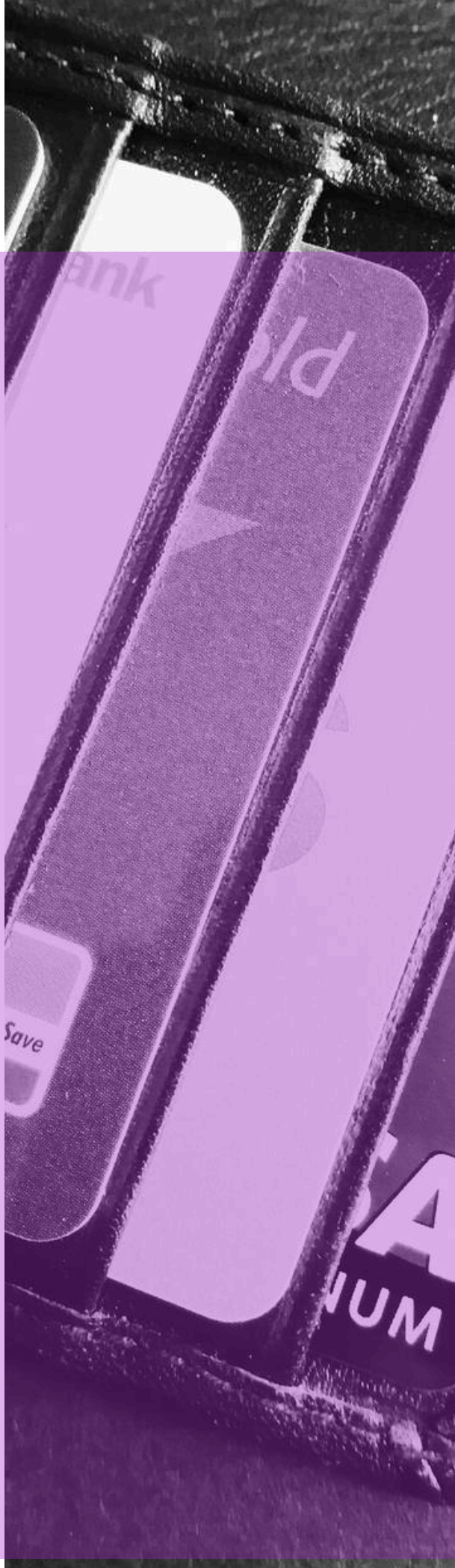
POURQUOI SE PRÉOCCUPER DE LA CYBERCRIMINALITÉ ?

Avez-vous déjà reçu de faux appels d'assistance technique ? Des e-mails ou des SMS alarmants concernant une fraude bancaire ? Ou encore une demande d'argent d'un proche sur les réseaux sociaux ?
Malheureusement, la réponse à ces questions est probablement positive. En effet, tout le monde est concerné un jour ou l'autre par la cybercriminalité, même si vous utilisez peu Internet.

LA CYBERCRIMINALITÉ, C'EST QUOI ?

La cybercriminalité désigne l'ensemble des infractions commises via des réseaux informatiques ou des appareils connectés à Internet. Elle englobe les actions malveillantes qui visent à exploiter des systèmes, des réseaux, ou des données pour voler des informations, causer des perturbations, ou obtenir de l'argent.

La cybercriminalité est l'affaire de chacun !



COMMENT RECONNAÎTRE LES ARNAQUES ?

Il existe quelques signes faciles pour repérer les arnaques.

INFORMATIONS SENSIBLES

Les entreprises et les organismes publics ne vous demanderont jamais vos informations personnelles ou sensibles par e-mail, SMS ou téléphone. Ne communiquez JAMAIS les informations de votre **Digipass** ou de l'application **Itsme**, vos **informations bancaires** ou vos **mots de passe** par quelque moyen que ce soit.

Vous avez droit à une prime de la Région wallonne, puis-je avoir vos coordonnées bancaires ?

OFFRES TROP AVANTAGEUSES

Soyez également attentif aux messages trop beaux pour être vrais ou aux promesses irréalistes :

Félicitations, vous avez gagné un prix !

Concours inédit pour gagner le nouvel iPhone. Remplissez le formulaire et tentez votre chance !

Si l'offre semble **trop avantageuse**, c'est bien souvent **une arnaque**. Soyez aussi vigilant par rapport aux offres d'abonnement avec une période d'essais gratuite. Cet abonnement risque de devenir payant par la suite.

URGENCE ET PEUR

Agissez maintenant ou votre compte sera bloqué définitivement !

Les messages peuvent aussi jouer sur l'urgence et la peur. Vous serez confronté à des **menaces**, des **ultimatums** ou des demandes de **paiements immédiats**.
Découvrez des messages types sur la page suivante.

COMMENT RECONNAÎTRE LES ARNAQUES ?

Bonjour, nous avons constaté un dysfonctionnement sur votre appareil. Contactez le helpdesk au numéro suivant pour solutionner votre problème.

Vous avez des paiements en retard. Réglez-les immédiatement, en cliquant sur ce lien et complétez vos informations personnelles pour éviter une coupure.

FAUSSES FACTURES

Des escrocs peuvent envoyer des factures frauduleuses par e-mail en modifiant simplement le numéro de compte bancaire. Le reste du document semble crédible, mais **l'argent est redirigé vers un compte appartenant aux criminels**. Vérifiez toujours les coordonnées bancaires auprès de la personne ou de l'organisme concerné, surtout en cas de changement inhabituel.

DEMANDES DE TRANSFERT D'ARGENT ET CRYPTOMONNAIE

Ne donnez jamais suite aux demandes d'utilisation de **sociétés de transfert de fond** comme par exemple Western Union, Ria Money Transfert, Money Trans, Money Gram... Ces sociétés ne sont à utiliser que si vous connaissez personnellement le destinataire. Restez vigilant aussi face aux demandes venant de personnes que vous connaissez.
Prudence également avec la **cryptomonnaie** ! Cette dernière est souvent utilisée par les criminels comme moyen de paiement car elle est difficile à tracer.

USURPATION D'IDENTITÉ

Vous êtes contacté par e-mail, par sms ou via les réseaux sociaux, par un proche, un parent ou un ami, qui a besoin d'une aide financière urgente. Souvent, votre contact s'est fait **voler son profil** ou son adresse **e-mail**.
Les personnes malveillantes font aussi **appel à l'émotionnel** pour vous inciter à agir dans leur sens :

Bonjour papa/maman, mon portefeuille a été volé. Je n'ai plus de sous sur moi. Peux-tu m'envoyer de l'argent ? Je suis vraiment dans la galère...

COMMENT RECONNAÎTRE LES ARNAQUES ?

Salut, un proche est gravement malade et je dois payer des frais médicaux pour son traitement. Je suis à court d'argent. Peux-tu m'envoyer 400 € via ce lien ? Je te rembourserai rapidement.

"MONEY MULE"

Les money mules, ou "mules financières", sont des personnes utilisées par des escrocs pour faire transiter de l'argent volé. Cela peut sembler anodin : on vous propose de recevoir de l'argent sur votre compte, puis de le renvoyer à quelqu'un d'autre, parfois en gardant une commission. Mais en réalité, il s'agit d'un délit grave. Même si vous ne savez pas que l'argent vient d'une fraude, vous risquez des poursuites judiciaires pour blanchiment d'argent. Cela peut entraîner de lourdes amendes, voire une peine d'emprisonnement.
Ces demandes peuvent venir d'inconnus, mais aussi de proches qui, parfois sans s'en rendre compte, participent à ce type d'arnaque. Ne laissez jamais quelqu'un utiliser votre compte bancaire, même une personne de confiance. Si vous avez un doute, signalez-le aux autorités.

SPOOFING

Le numéro affiché sur votre téléphone semble provenir d'une institution officielle (banque, administration…), mais c'est une imitation. C'est ce qu'on appelle le spoofing. Des applications **permettent de falsifier ces numéros officiels**. Soyez prudent, même si le numéro paraît légitime. En cas de doute, raccrochez et rappelez via un numéro officiel trouvé sur le site web de l'institution.

COMMENT RECONNAÎTRE LES ARNAQUES ?

FARNAQUE AUX SENTIMENTS

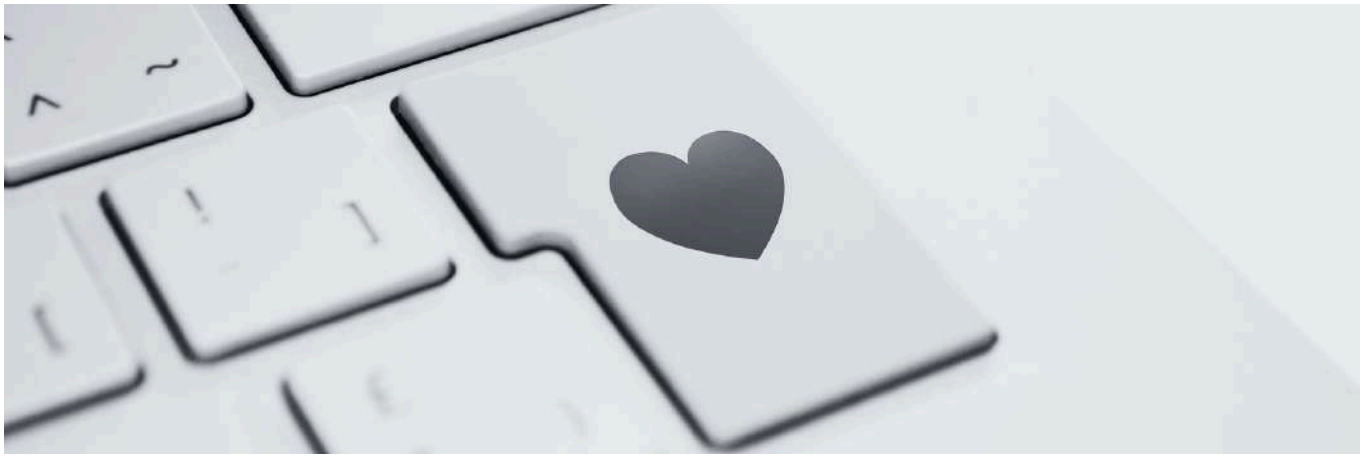
Avec l'essor des réseaux sociaux (Facebook, Instagram, TikTok, Whatsapp…) et des sites de rencontres, les cyberarnaques aux sentiments, comme le catfishing, deviennent de plus en plus fréquentes. Le catfishing est une pratique qui consiste à créer un **faux profil en ligne** pour tromper des victimes. Les arnaqueurs se servent souvent de photos volées et de fausses informations pour gagner votre **confiance** et établir une **relation émotionnelle.**

Leur objectif ? Manipuler vos sentiments pour obtenir des faveurs, des informations personnelles ou de l'argent. Ils peuvent prétendre être dans une situation désespérée ou feindre des intentions romantiques parfois **durant des années**.

COMMENT SE PROTÉGER ?

D'abord, vérifiez l'identité de votre interlocuteur. Faites des recherches sur les photos ou les informations partagées.
Méfiez-vous des histoires trop parfaites, des incohérences ou des excuses pour éviter les appels vidéo ou les rencontres en personne.
Ne partagez jamais d'informations sensibles (données bancaires, mots de passe, informations privées…)
Refusez toute demande d'argent. C'est l'un des signes les plus courants d'arnaque.

En cas de doute, arrêtez toute communication et signalez le profil suspect sur la plateforme concernée.



COMMENT RECONNAÎTRE LES ARNAQUES ?

ORTHOGRAPHE ET NOM DE DOMAINE

Les fautes d'orthographe ou de grammaire dans les messages (e-mails, sms...) doivent attirer votre attention. Soyez aussi attentif aux erreurs de traduction, aux tournures de phrase bizarres et aux **noms de domaine ou de site web inhabituels** comme "www.amazonn.be" par exemple.
Les **logos utilisés** peuvent être déformés ou flous : c'est un indicateur à prendre en compte.

EXPÉDITEURS INCONNUS

Méfiez-vous particulièrement des expéditeurs inconnus et des **messages non sollicités**. Parfois, bien que l'expéditeur semble officiel, un survol de son adresse e-mail peut révéler une origine suspecte. Découvrez comment survoler un lien ou une adresse e-mail en page 9.
Exemple d'une origine **suspecte** :

Ici, le lien renvoie vers un site internet et non une adresse e-mail. Le lien n'est donc pas conforme.

Exemple d'une origine **conforme** :

Ici, le lien renvoie effectivement vers l'adresse e-mail indiquée. Le lien est donc conforme.

LIENS ET FICHIERS JOINTS SUSPECTS

Les adresses qui ne commencent pas par "https://" ou des **liens raccourcis** (bit.ly, tinyurl...) masquent souvent une destination suspecte.
Les fichiers non sollicités, surtout s'ils se terminent en **.exe, .zip ou .scr**, peuvent contenir des virus ou des logiciels malveillants.

FAUX QR CODES

Les escrocs remplacent parfois des QR codes par des faux qui vous redirigent vers des sites malveillants.
Vérifiez toujours la source d'un QR code, méfiez-vous des QR collés sur des affiches ou bornes de paiement, et privilégiez les applications officielles pour vos transactions.
En cas de doute, ne scannez pas et signalez l'anomalie.

COMMENT RECONNAÎTRE LES ARNAQUES ?

COMMENT DÉCOUVRIR SI UNE ORIGINE SUSPECTE SE CACHE DERRIÈRE UNE ADRESSE E-MAIL OU UN LIEN ?

Sans cliquez, passez votre curseur sur l'expéditeur (l'adresse e-mail) ou le lien URL.

Vérifiez si l'adresse qui s'affiche correspond à ce qui est attendu ou indiqué dans le message.
Pour savoir comment faire, consultez la vidéo réalisée par Safe on Web : https://youtu.be/dNfrBD2e5Ss (ou via le QR code ci-contre).

QUE FAIRE EN CAS D'INCIDENT ?

QUE FAIRE EN CAS D'INCIDENT ?

Surtout, **ne paniquez pas !** Cela peut arriver à tout le monde. Heureusement, des solutions et des aides existent. Suivez les étapes suivantes et récoltez un maximum de preuves pour porter plainte à la police :

Déconnectez tous les supports (smartphone, tablette, TV, PC...) d'Internet

→

Changez immédiatement vos mots de passe en passant par un autre appareil

↓

Contactez votre banque et signalez-lui les faits en urgence pour bloquer les transactions frauduleuses

←

Si vous n'arrivez pas à contacter votre banque, bloquez vos cartes ou applications bancaires via Card Stop au 078 170 170

↓

Déposez plainte le plus rapidement possible au poste de police (www.police.be)

Pour déposer une plainte, soyez le plus précis possible !

- Faites des **captures d'écran** des messages, des sites frauduleux, profils sur les réseaux sociaux, offres frauduleuses...
- **Copiez** l'adresse du site frauduleux ou l'adresse e-mail suspecte.
- **Imprimez** les e-mail ou les extraits de comptes avec les heures de retrait.

EN PARALLÈLE...

- Vérifiez que les comptes ou applications ne contiennent pas de **données étrangères** pouvant permettre un piratage via la fonction "mot de passe oublié".
- Analysez l'ordinateur avec un **antivirus**, voire réinstallez-le s'il est compromis, pour supprimer toute trace des attaquants. Selon la situation, une copie de l'appareil pourrait être nécessaire pour une enquête policière avant toute réinstallation.

COMMENT PROTÉGER SES COMPTES ET SES APPAREILS ?

Pour éviter de faciliter la tâche aux personnes mal intentionnées, mettez en pratique ces conseils de sécurité.

UN MOT DE PASSE FORT

Un mot de passe fort signifie :

- Une **longueur** de 14 à 15 caractères ;
- **Combiner** majuscules, minuscules, chiffres et caractères spéciaux (!@#$%^&*) ;
- Eviter les mots courants, les dates d'anniversaire ou les informations personnelles faciles à deviner ;
- Eviter d'utiliser le même mot de passe pour tous vos comptes ;
- **Changer régulièrement** votre mot de passe (tous les 6 à 12 mois maximum).

N'enregistrez jamais vos mots de passe de manière automatique sur vos navigateurs.

Vous pouvez plutôt utiliser des **logiciels coffre-fort de mots de passe** comme Bitwarden, 1Password, LastPass ou Dashlane… Ils stockent en toute sécurité vos identifiants et génèrent des mots de passe robustes pour chaque service. Vous n'avez qu'à retenir un seul mot de passe maître pour y accéder.

NE PAS PARTAGER VOS CODES ET VOS MOTS DE PASSE

Même si cela semble évident, **ne partagez JAMAIS vos codes d'accès**. Pour rappel, les codes de votre **Digipass**, les données de l'application **Itsme** et vos **informations bancaires** ne doivent jamais être communiquées par quelque moyen que ce soit à qui que ce soit.

LA DOUBLE AUTHENTIFICATION

La double authentification est un moyen de sécuriser vos comptes en ajoutant **une étape supplémentaire** après l'entrée de votre mot de passe.

COMMENT PROTÉGER SES COMPTES ET SES APPAREILS ?

La double authentification peut inclure :

- Un code envoyé par SMS ou e-mail ;
- Une notification ou un code dans une application (comme Google Authenticator ou Microsoft Authenticator) ;
- Une empreinte digitale ou une reconnaissance faciale.

Cela rend le piratage beaucoup plus compliqué.

Retrouvez sur Safe on Web, une vidéo qui vous explique le processus de la double authentification, étape par étape : https://surfersanssoucis.safeonweb.be/fr/modules/3

L'INSTALLATION DES MISES À JOUR ET D'UN ANTIVIRUS

Faites régulièrement les **mises à jour** de vos téléphones, ordinateurs et applications. Installez un **antivirus** pour protéger vos données.

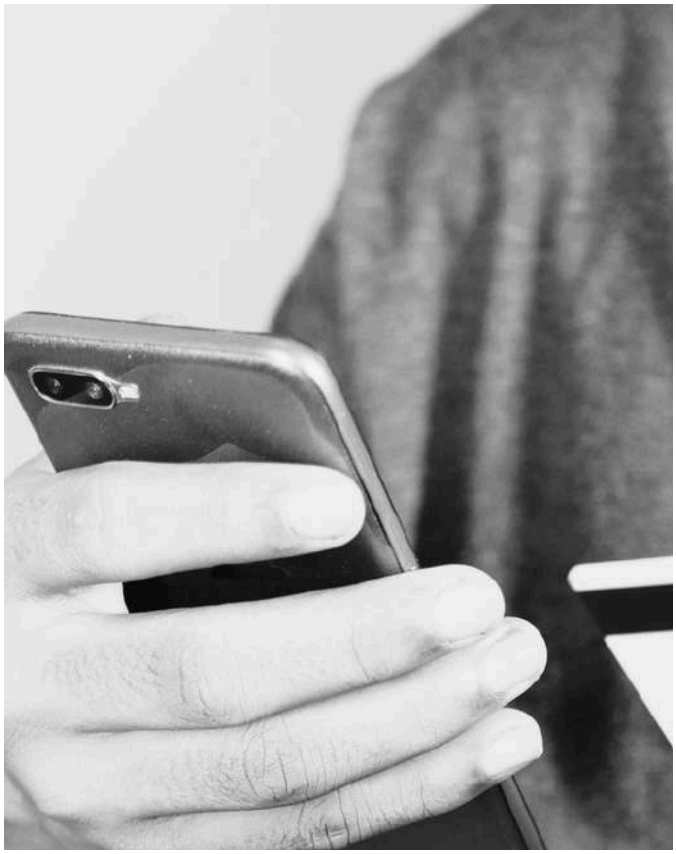
RESSOURCES ET CONTACTS UTILES

LES SERVICES DE POLICE

Les coordonnées des services de police sont accessibles sur notre site web.

https://www.om-mp.be/fr/votre-mp/parquets-procureur-roi/namur/votre-zone-police

Vous pouvez également les joindre en appelant le : **101**



DES RESSOURCES UTILES

Pour plus d'informations sur la cybersécurité, consultez les ressources ci-dessous.

Safe on Web
www.safeonweb.be

Be Safe
www.besafe.be

Cyber Simple
www.cybersimple.be

Centre pour la Cybersécurité de Belgique
https://ccb.belgium.be

L'IMPACT DE L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) fait partie de notre quotidien pour nous faciliter la vie : elle recommande des vidéos, corrige nos fautes… Mais elle est aussi capable de générer de **faux contenus réalistes** comme des deepfakes. Ce sont des vidéos ou des images ultra-réalistes qui montrent des personnes disant ou faisant des choses qu'elles n'ont jamais faites.
Cela fonctionne aussi avec des **imitations vocales**. Un malfaiteur pourrait, par exemple, reproduire la voix d'un proche, d'un supérieur ou d'une célébrité, pour demander de l'argent ou des informations sensibles.

Les IA analysent des tonnes de données pour fonctionner. Cela peut poser un problème si ces données personnelles sont mal protégées ou utilisées à des fins frauduleuses.

Les IA peuvent **créer et diffuser de fausses informations** rapidement, rendant difficile de distinguer le vrai du faux.

Les pirates utilisent aussi l'IA pour **automatiser et personnaliser les cyberattaques**. L'objectif est de rendre les e-mails de phishing plus convaincants et ciblés.

POUR SE PROTÉGER

Ne croyez pas tout ce que vous voyez ou entendez sur Internet, surtout si cela semble choquant ou inhabituel. Il est important de toujours vérifier les sources des vidéos, images ou articles. Renforcez aussi vos comptes en ligne.

UN FAUX PROFIL CRÉÉ PAR L'IA, VOUS N'Y CROYEZ PAS ? FAITES LE TEST…

Rendez-vous sur ce site :
www.thispersondoesnotexist.com
Vous y rencontrerez des personnes qui n'existent pas. Leur photo a été créée de toutes pièces par l'IA. Bluffant non ?

SOYEZ ACTIFS DANS LA PRÉVENTION

N'oubliez pas que quelques gestes simples permettent de se protéger de la majorité des menaces et arnaques. Les messages frauduleux ne sont limités que par l'imagination des malfaiteurs. Prenez toujours le temps de lire attentivement le message pour éviter les éventuelles arnaques.
En cas de besoin, des solutions existent si vous êtes victime de la cybercriminalité.

N'hésitez pas à partager les conseils de ce guide et vos propres bonnes pratiques à vos proches.

Pour protégez les autres utilisateurs, n'hésitez pas à signaler les messages suspects à **Safe on Web** (suspect@safeonweb.be).

L'application est également disponible sur le Google Play Store ou sur l'Apple Store.

La sécurité en ligne est l'affaire de chacun !

VOCABULAIRE

IL EXISTE PLUSIEURS TYPES DE CYBERCRIME. RETROUVEZ ICI LE VOCABULAIRE SPÉCIFIQUE EXPLIQUÉ EN QUELQUES MOTS. CETTE LISTE N'EST PAS EXHAUSTIVE.

- **Phishing (Hameçonnage)** : E-mails ou SMS qui ressemblent à des messages officiels mais visent à voler des informations personnelles.
- **Escroqueries financières** : Faux investissements, demandes d'argent, ou messages trompeurs sur des gains de loterie.
- **Vol d'identité** : Usage des informations personnelles pour des fraudes bancaires ou administratives.
- **Spywares et malwares** : Logiciels qui, une fois installés, collectent des données sans le consentement de l'utilisateur.
- **Catfishing :** Création de faux profils en ligne pour tromper quelqu'un, souvent sur des sites de rencontres ou réseaux sociaux, dans le but de manipuler, escroquer ou obtenir des informations personnelles.
- **Deepfake :** Vidéos ou sons modifiés par l'IA pour imiter une personne et tromper les autres.
- **Spoofing** : technique de fraude qui consiste à usurper l'identité d'une personne, d'un site ou d'un appareil pour tromper quelqu'un.