norton™

Phictionnaire

Le dictionnaire du phishing (indispensable pour chaque Cybercitoyen)

Table des Matières

Avant-Propos 03

Qu’est-ce que le phishing? 04

Le Phictionnaire

- L’alerte aux informations de compte 05
- La suspension de compte 05
- La vérification de compte 06
- L’arnaque au crédit 06
- La fausse Livraison 07
- La tentative de connexion 07
- L’arnaque à l’arnaque 08
- Les fausses offres 08
- L’arnaque au retard 09
- L’arnaque au colis 09
- L’activité suspecte 10
- L’arnaque aux remboursements 10
- L’arnaque aux impôts 11
- L’arnaQR Code 11

Nos recommandations 12

Avant-Propos

Siggi Stefnisson
CTO at Gen™

Les consommateurs sont les cibles privilégiées de la cybercriminalité moderne. En 2023, les escroqueries et les attaques de phishing visant les consommateurs ont représenté deux tiers de toutes les cyberattaques mondiales, selon les données sur les menaces de Gen. Il est en effet plus avantageux d'exploiter les failles liées aux êtres humains plutôt que celles des logiciels et des systèmes des entreprises.

Ce virage dans la cybercriminalité s'accompagne d'une sophistication des attaques de phishing. Les générations plus anciennes se souviendront des débuts des escroqueries, souvent truffées d'erreurs linguistiques et contextuelles qui les rendaient faciles à repérer. Aujourd'hui, les cybercriminels utilisent l'intelligence artificielle (IA) et des outils tels que ChatGPT pour créer des communications très ciblées, sans erreurs. Par conséquent, le taux de réussite du phishing augmente.

Pour enrayer ce phénomène, l'approche de la cybersécurité doit également évoluer. Il ne suffit plus de protéger la vulnérabilité des appareils avec des logiciels, nous devons protéger l'individu, ce que j'appelle la sécurité centrée sur l'humain. Malgré les mauvaises intentions des cybercriminels qui utilisent l'IA pour mener des attaques, celle-ci joue un rôle essentiel dans la détection des escroqueries, et depuis plus d'une décennie, Norton intègre l'IA dans ses produits pour aider à rendre Internet plus sûr. Parallèlement, nous mettons l'accent sur le facteur humain de la sécurité en ligne grâce à l'éducation, qui, nous en sommes convaincus, contribuera à réduire le risque d'erreur humaine.

Comme son nom l'indique, le Phictionnaire est un dictionnaire des attaques de phishing récemment détectées et bloquées par Norton. Nous les exposons ici pour vous aider à repérer les signes révélateurs de communications suspectes conçues pour voler vos informations personnelles. En tant que défenseurs de la liberté numérique pour tous, et partout, le Phictionnaire inclut également une liste de conseils pour vous aider à déceler ce qui constitue ou non une attaque de phishing si vous en rencontrez une.

Le Phictionnaire se devait d'exister pour aider à régler un problème devenu fréquent. J'espère que vous le trouverez utile.

Restez en sécurité.

Qu'est-ce que le Phishing ?

Le phishing est une forme d'escroquerie qui vise à inciter les victimes à divulguer volontairement des informations sensibles en se faisant passer pour une entité de confiance, comme une institution bancaire ou un proche.

Bien que l'e-mail soit le vecteur le plus fréquemment utilisé, d'autres moyens de communication, tels que les messages textes, les vidéos, les sites web et les images, peuvent également servir à orchestrer ce type d'attaque.

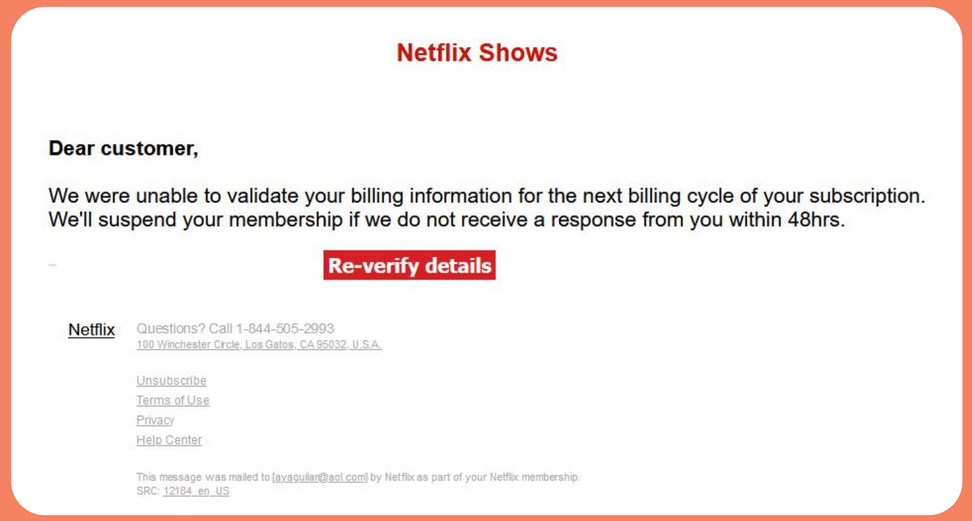
L'objectif d'une attaque de phishing est généralement de voler des mots de passe de comptes sensibles, de récupérer des numéros de carte de crédit ou de pousser la victime à télécharger des logiciels malveillants. Ces programmes peuvent alors être exploités pour surveiller l'activité de l'utilisateur ou bloquer l'accès à des fichiers jusqu'au paiement d'une rançon.

Le phishing reste l'une des méthodes de fraude les plus redoutablement efficaces. C'est pourquoi nous avons choisi de mettre en lumière certains des exemples les plus courants...

L’alerte aux informations de compte

01. **Un e-mail ou un SMS envoyé à un individu par un fournisseur de services auquel vous êtes abonné.**
Netflix : Le renouvellement automatique de votre abonnement a échoué. Veuillez régulariser le paiement avant le [date]. Rendez-vous sur <|url|>

02. **Une arnaque qui consiste à faire croire au destinataire de la nécessité de mettre à jour ses informations de compte, généralement les détails de paiement.**



Netflix Shows

Dear customer,

We were unable to validate your billing information for the next billing cycle of your subscription.
We'll suspend your membership if we do not receive a response from you within 48hrs.

Re-verify details

Netflix Questions? Call 1-844-505-2993
100 Winchester Circle, Los Gatos, CA 95032, U.S.A.

Unsubscribe
Terms of Use
Privacy
Help Center

This message was mailed to [ayaguilar@aol.com] by Netflix as part of your Netflix membership.
SRC: 12184_en_US

La suspension de compte

01. **Un message reçu demandant au destinataire de rétablir son compte suspendu.**
Votre compte Apple Pay a été suspendu, veuillez mettre à jour vos coordonnées.

02. **Un faux message adressé à un individu lui demandant de récupérer son compte dans un délai spécifique, faute de quoi cela entraînera une suspension permanente.**
Nous avons temporairement suspendu votre compte PayPal. Pour le rétablir, suivez les instructions ci-dessous. Veuillez effectuer la récupération dans les 2 jours, sinon votre compte PayPal sera fermé de façon permanente. Nous sommes désolés pour la gêne occasionnée. Merci de votre attention.

La vérification de compte

01. **Un e-mail frauduleux envoyé par des escrocs et ressemblant à un message d'un contact d'une entité bien connue dans le but d'extraire les identifiants de connexion du compte.**
Nouvelle connexion détectée depuis : [Nom du pays] Windows 10. Suivez le lien ci-dessous pour débloquer votre compte : [Lien pour vérifier votre compte] Veuillez vérifier votre compte dans les 24 heures, sinon votre compte PayPal sera résilié de manière permanente. Cordialement, PayPal.

L’arnaque au crédit

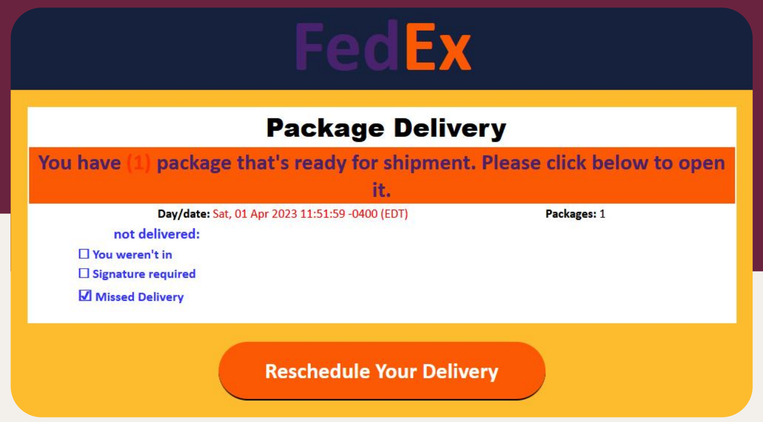
01. **Un rappel financier frauduleux dans le but de voler des informations personnelles et financières.**
Rappel : Si les dossiers en retard ne sont pas traités, cela affectera votre crédit.

02. **Un prêt proposé à des conditions très (trop) avantageuses et limitées dans le temps : Un premier versement est généralement rapidement sollicité par les escrocs (frais de dossiers, d’assurance etc.).**
Obtenez un crédit à taux 0 sans conditions et en moins de 48h.

La fausse livraison

01. **Un message frauduleux simulant une tentative de livraison conçu pour extraire des informations personnelles de la cible.**
Notre chauffeur a tenté de livrer votre colis aujourd'hui mais personne n'était là pour le réceptionner. Pour reprogrammer une nouvelle date de livraison, allez sur <|url|> :

02. **Un SMS ou un e-mail envoyé par une entreprise de livraison légitime, conçu pour tromper quelqu'un afin de partager des informations sans le savoir.**
Votre colis ne peut pas être livré en raison d'un numéro de maison incorrect.



La tentative de connexion

01. **Un message informant le destinataire qu'un utilisateur inconnu a tenté d'accéder à leur compte.**
Alerte BNP Paribas : Une connexion a été effectuée depuis une localisation inconnue : Melbourne, VIC. Ce n'était pas vous ? Veuillez vérifier maintenant en cliquant sur <|url|>

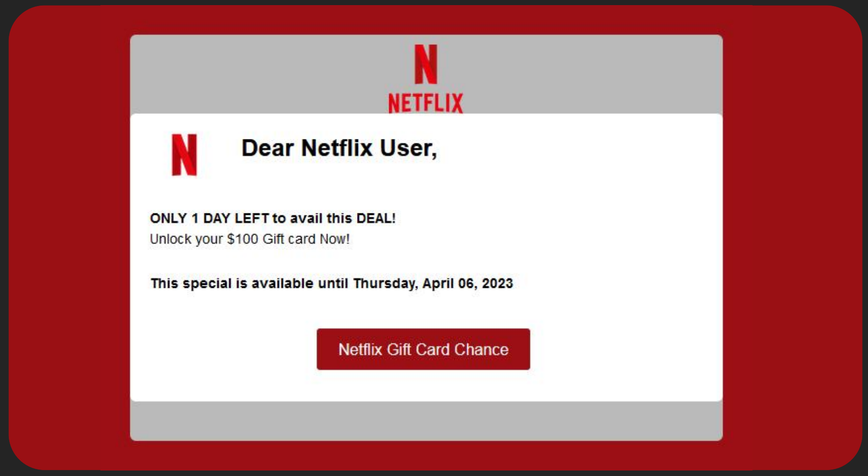
02. **Une tentative de tromper quelqu'un en lui faisant croire que son compte a été piraté, afin de le convaincre de partager des informations personnelles.**
Alerte RBC : Votre compte en ligne est temporairement verrouillé en raison d'une tentative de connexion inhabituelle. Veuillez-vous connecter et confirmer vos informations.

L’arnaque à l’arnaque

01. **Une technique utilisée par les cybercriminels pour tromper les gens en leur faisant croire que leur appareil a été infecté par des logiciels malveillants.**
DANGER : Une menace a infecté votre ordinateur ! Agissez maintenant pour protéger vos fichiers confidentiels en cliquant <|url|>.

Les fausses offres

01. **Une arnaque conçue pour propager des logiciels malveillants ou obtenir des informations personnelles en affichant une offre attractive accompagnée d'un lien vers un site Web malveillant pour la réclamer.**
Gagnez 100€ en 2 minutes en répondant à ce sondage!

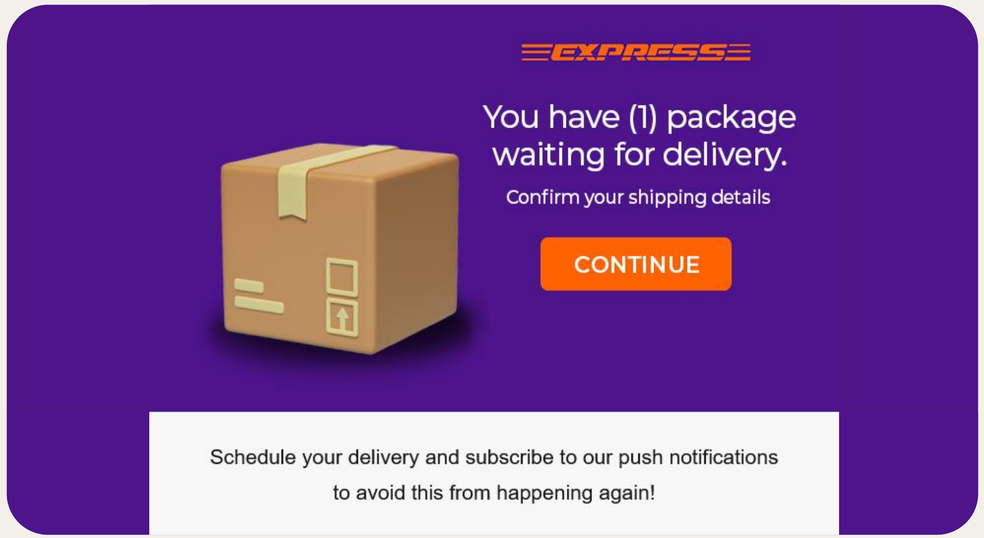


L’arnaque au retard

01. **Une tactique qui joue sur les leviers de la peur et de l'urgence pour voler des informations personnelles ou financières.**
Votre paiement est en retard. Pour éviter les frais de retard, veuillez consulter (URL)

L’arnaque au colis

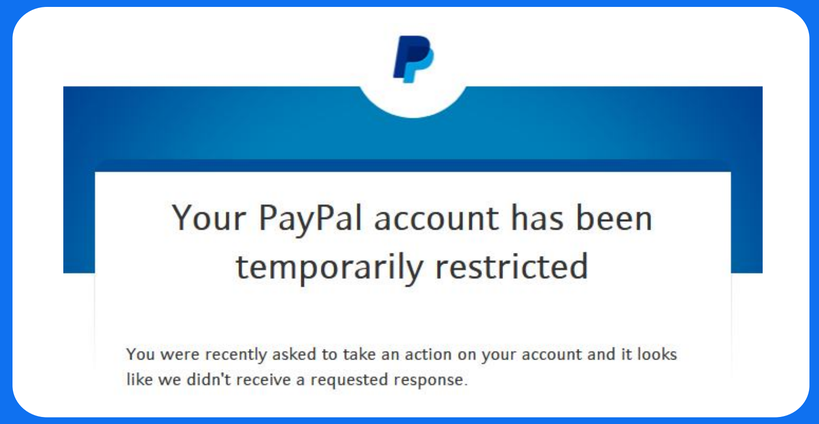
01. **Un message reçu détaillant les informations de livraison et demandant les préférences de livraison ou de paiement.**
Bonjour Votre colis CHRONOPOST avec suivi <|numéro|> attend que vous définissiez vos préférences de livraison : <|url|>



L’activité suspecte

01. **Un message reçu sur de fausses activités suspectes sur un de vos comptes.**
Amazon : votre compte a été verrouillé en raison d'une activité suspecte : Cliquez sur le lien ci-dessous pour déverrouiller votre compte. <|url|>

02. **Une notification reçue qui copie point par point celle d’une marque existante informant le client que son compte personnel a été verrouillé.**
PayPal : votre compte a été verrouillé en raison d'une activité suspecte. Cliquez sur le lien ci-dessous pour déverrouiller votre compte : <|url|>



L’arnaque aux remboursements

01. **Un message provenant d'une organisation ou d'un individu semblable à une vraie administration, tentant d’avoir accès aux données bancaires et personnelles en proposant de faux remboursements.**
[Ameli] Vous avez un remboursement en attente. Cliquez ici

L’arnaque aux impôts

01. **Un message frauduleux déguisé en provenance d'une entreprise de l’administration Française.**
Impot.Gouv : Votre déclaration de revenus de [montant] n'a pas pu être traitée en raison d'informations insuffisantes fournies. Veuillez les mettre à jour immédiatement sur <|url|>

L’arnaQR Code ?

01. **Une invitation à scanner un QR code, sur une affiche, un flyer ou autre, qui s’avère être finalement un moyen d’accéder à votre téléphone et d’y installer des malwares ou logiciels espions.**
Flashez ce QR pour en savoir plus

Nos Recommandations

Vous devriez maintenant bien connaitre les différents types de phishing les plus courants et le langage qu'ils utilisent. Même si certaines semblent évidentes, les tentatives de phishing deviennent de plus en plus difficiles à identifier. Les cybercriminels synchronisent leurs attaques, personnalisent leurs messages et utilisent des technologies avancées pour augmenter leurs chances de réussite. Voici ce à quoi vous devez faire attention :

Trop beau pour être vrai
Méfiez-vous des e-mails vous promettant de l'argent facile, des cadeaux, ou des sites web douteux vendant des produits incroyables à des prix alléchants. Si cela semble trop beau pour être vrai, c'est probablement le cas.

Erreur de la banque en votre (dé)faveur
Aucune banque ne vous demandera jamais d'informations sensibles par e-mail ou téléphone. Ne fournissez jamais ces informations en réponse à un e-mail.

Le syndrome du Bescherelle
Si un e-mail est truffé de fautes d'orthographe ou de tournures étranges, cela doit toujours être un signal d'alarme.

Veuillez agréer l'expression de mes salutations distinguées
Si un e-mail commence par des salutations génériques comme « Monsieur ou Madame », cela peut être un signe qu'il s'agit d'un modèle de phishing envoyé à plusieurs cibles.

Signé un inconnu qui ne vous veut pas du bien
Si vous recevez des e-mails non sollicités de la part de parfaits inconnus ou de fournisseurs inhabituels, il est préférable de les supprimer. Si vous les ouvrez, évitez de cliquer sur les liens ou les pièces jointes.

Demande d’action immédiate
Suppression de votre compte imminente, ou piratage détecté : Une astuce courante pour vous faire agir est de créer un faux sentiment d'urgence. Un moyen de vous faire agir vite et sans réfléchir.

Les faux amis
Si un e-mail semble suspect, prenez toujours le temps de vérifier l'adresse de l'expéditeur ou le nom de domaine et autres indices indiquant qu'il pourrait être frauduleux.

« Vous avez gagné un iPhone 17 »
Si vous recevez un e-mail affirmant que vous avez gagné un jeu concours auquel vous n'avez jamais participé, alors quelque chose ne va évidemment pas.

Gardez cette liste à portée de main et consultez-la chaque fois que vous recevez une communication suspecte. En cas de doute, faites preuve de prudence et examinez attentivement le message pour votre sécurité en ligne et protéger vos informations personnelles des cybercriminels. **Pour une meilleure protection, installez un antivirus réputé doté de technologies anti-phishing, comme Norton 360.**

Obtenir une protection

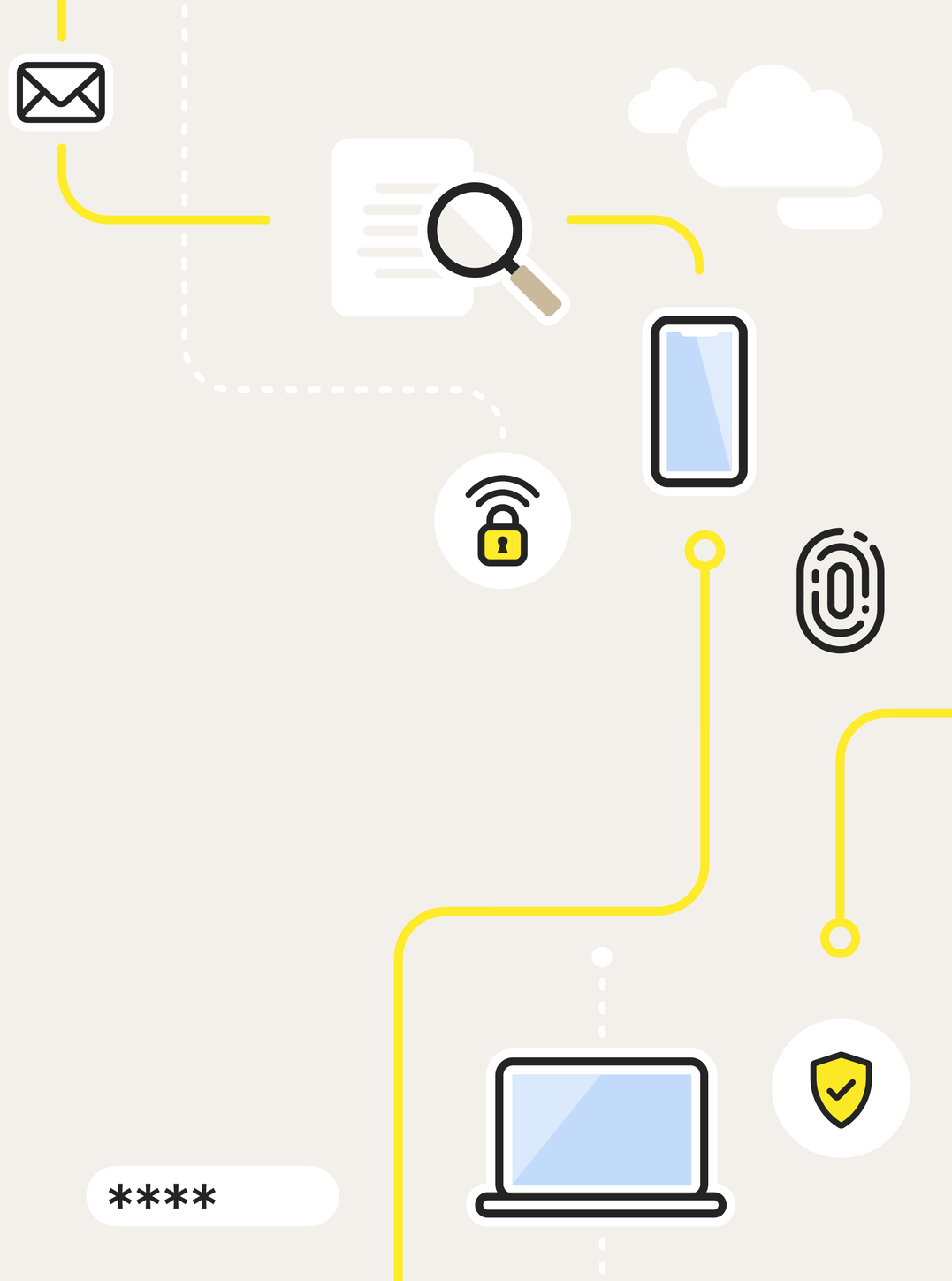
Avertissement

Tous les exemples fournis sont de véritables tentatives de phishing, actuelles ou récentes, et ne sont pas générés par Norton.

Tous les logos ou marques déposées affichés sont la propriété des marques respectives.

À propos de Norton

Norton est une marque leader en matière de cybersécurité et fait partie de Gen™, une entreprise mondiale dédiée à la liberté numérique grâce à une famille de marques grand public de référence. Norton permet à des millions de personnes et de familles de bénéficier d'une protection primée pour leurs appareils, leur vie privée en ligne et leur identité.



Copyright © 2024 Gen Digital Inc. All rights reserved