stat

RÉSEAUX SOCIAUX

Comment protéger votre vie privée et sécuriser votre compte X

resolock

Sommaire

Aujourd'hui, les réseaux sociaux font partie intégrante de notre vie quotidienne. Nous y partageons des moments de notre vie, des photos, des opinions et des informations personnelles. Mais savons-nous vraiment comment protéger notre vie privée sur ces plateformes ? Sommes-nous conscients des risques liés à la sécurité de nos comptes ?

Pour répondre à ces problématiques, je vous présente une série de six guides numériques. Chaque guide se concentre sur un réseau social spécifique, vous fournissant une présentation détaillée des divers paramètres de confidentialité disponibles. En outre, il vous apprend à sécuriser votre compte et ainsi prévenir différents risques tels que les piratages et les violations de données.

Cette série de six guides numériques couvre les réseaux sociaux les plus populaires : Facebook, X, Instagram, LinkedIn, TikTok et Snapchat. Chacun de ces guides est écrit de manière claire et concise, avec des instructions détaillées et des exemples pratiques pour vous aider à comprendre les paramètres de confidentialité et de sécurité de chaque réseau social. Ce guide-ci se consacre au réseau social **X (Twitter)**.

J’espère que cette série vous sera utile pour protéger votre vie privée et sécuriser vos comptes sur les réseaux sociaux. Que vous soyez un utilisateur occasionnel ou un utilisateur avancé, ces guides vous donneront les connaissances nécessaires pour naviguer en toute sécurité sur les réseaux sociaux les plus populaires.

Pour consulter les autres guides de la série, rendez-vous sur mon site
https://www.resolock.com/guides

Bonne lecture ✨
Julien Teste-Harnois, fondateur de Resolock

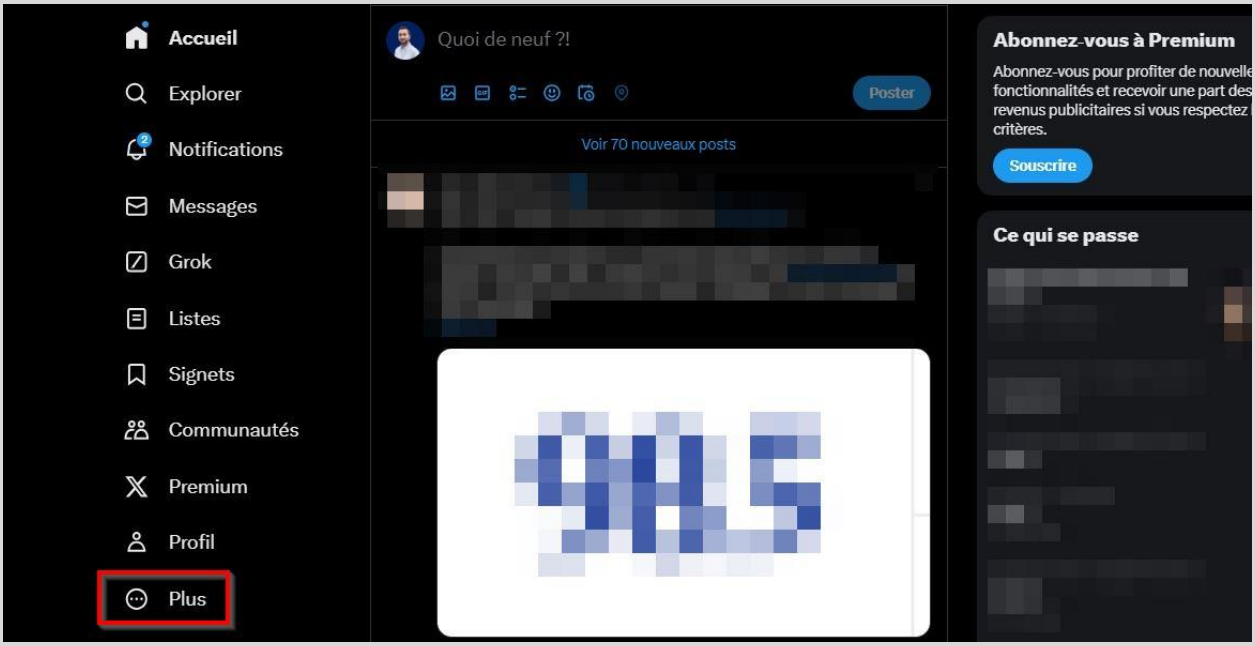
TABLE DES MATIÈRES

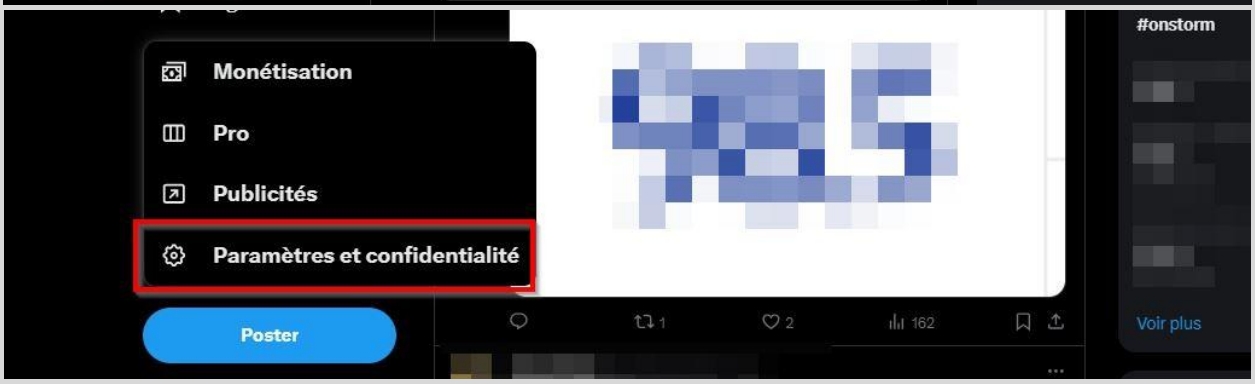
Où se trouvent les paramètres (à partir d'un ordinateur)

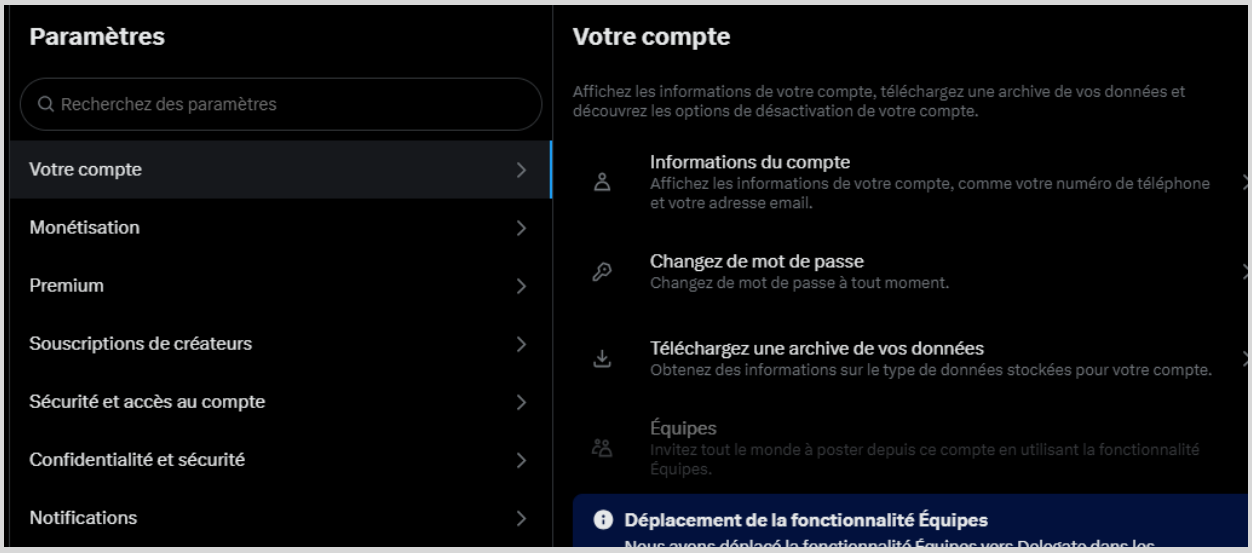
La première étape pour gérer efficacement les paramètres de confidentialité et de sécurité disponibles, c'est bien évidemment de savoir où ils se trouvent.

Voici la marche à suivre pour accéder aux paramètres de X à partir d'un ordinateur :

1. Cliquez sur l'onglet « Plus » en bas à gauche de l'écran.
2. Cliquez sur l'onglet « Paramètres et confidentialité ».





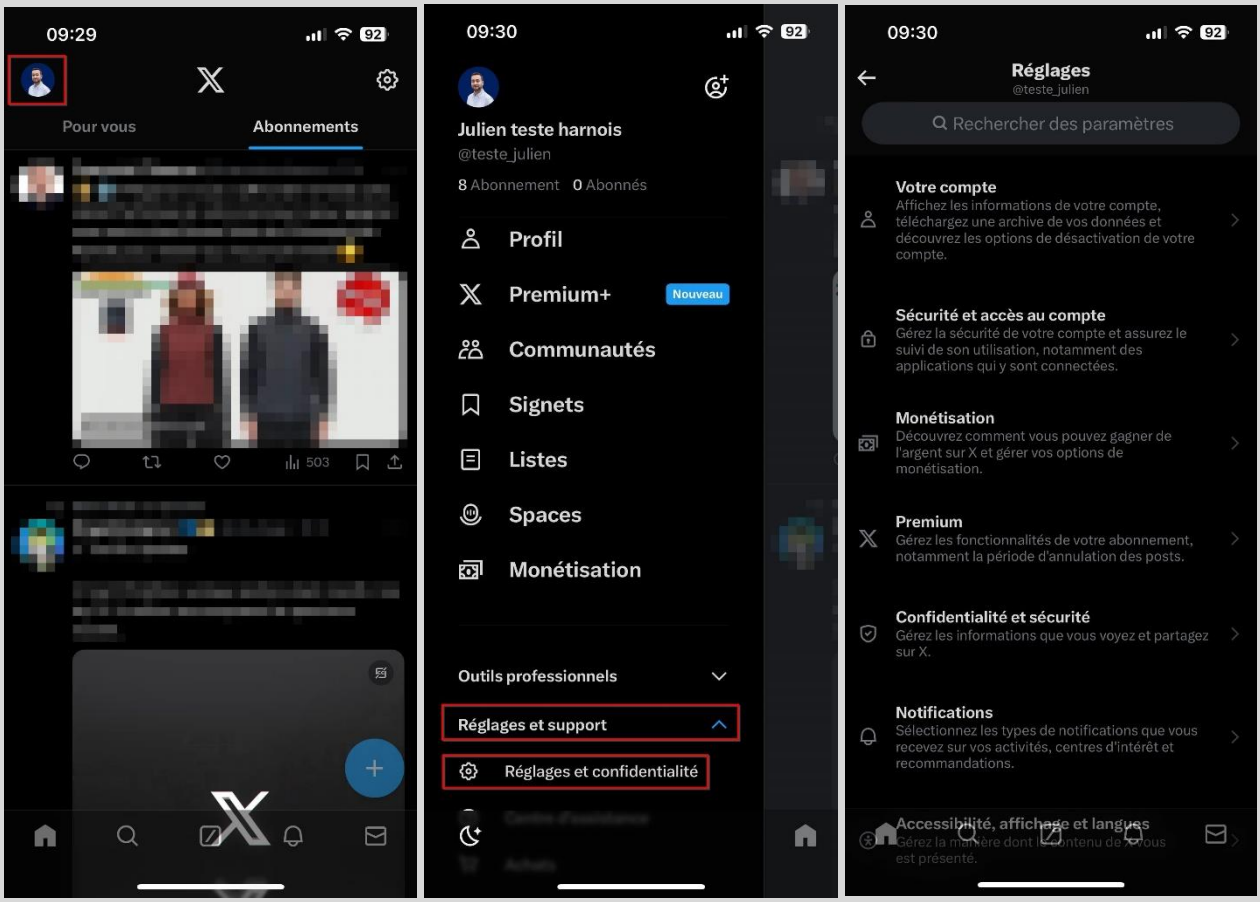


Où se trouvent les paramètres (iOS et Android)

Voici la marche à suivre pour accéder aux paramètres de X à partir de l'application mobile :

1. Appuyez sur l'icône de votre photo de profil en haut à gauche de l'écran.
2. Appuyez sur « Réglages et support » puis sur l'onglet « Réglages et confidentialité ».

* Il est possible qu'il soit écrit « Paramètres » au lieu de « Réglages » sur votre application.



Explication de la section réglages de X

Une fois que vous avez atteint la zone des réglages, vous remarquerez différentes sections. Dans ce guide, nous allons principalement nous concentrer sur les paramètres localisés dans les sections votre compte, sécurité et accès au compte ainsi que confidentialité et sécurité.

Comment sécuriser votre compte X

Deux mesures cruciales doivent être prises pour renforcer la sécurité de votre compte X. La première est l'utilisation d'un mot de passe robuste, tandis que la seconde consiste à configurer et activer le double facteur d'authentification.

Important : Pour une sécurité optimale, n'oubliez pas d'activer le double facteur d'authentification sur l'adresse e-mail associée à votre compte X.

Utiliser un mot de passe robuste

On ne le dira jamais assez, une pratique fondamentale en matière de cybersécurité, valable non seulement pour les réseaux sociaux, mais aussi au-delà, est l'utilisation de mots de passe robustes pour tous vos comptes.

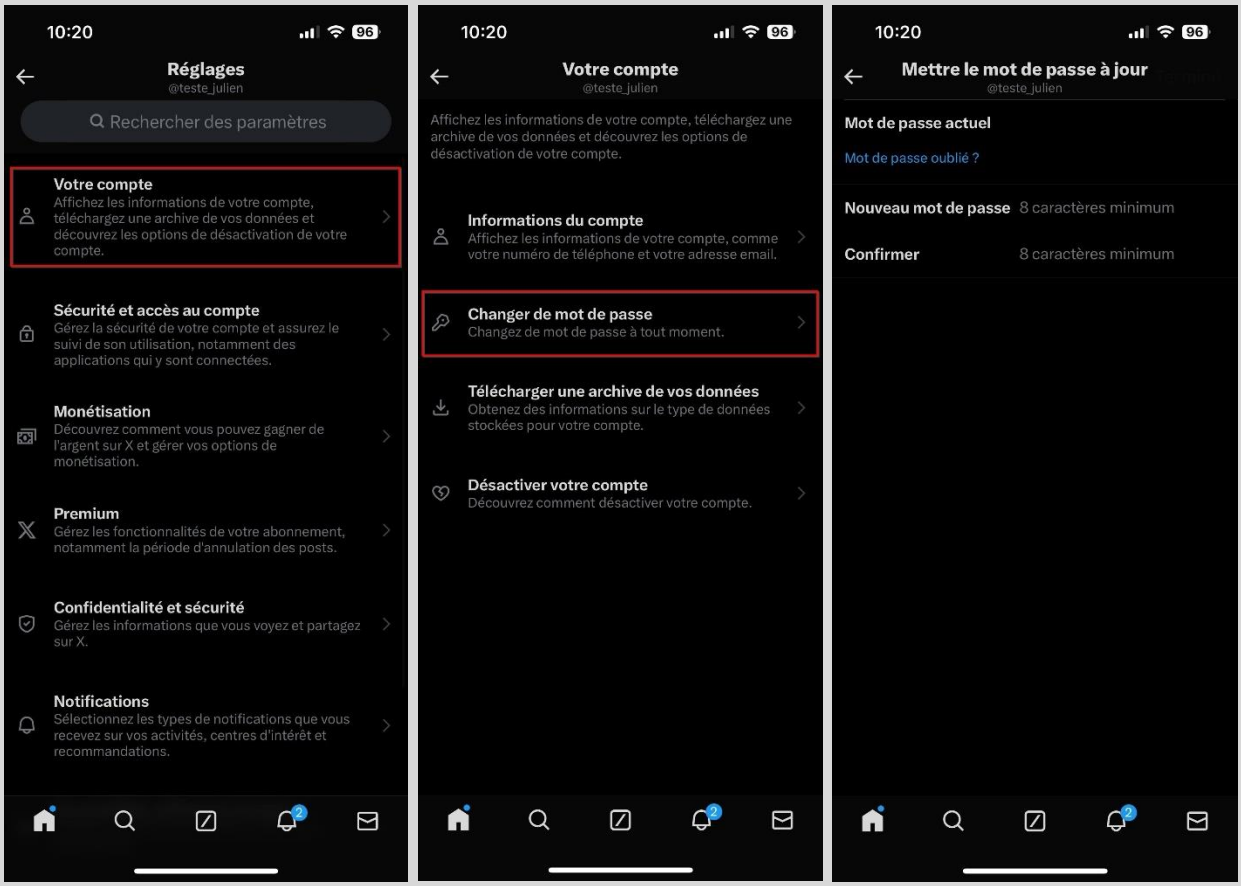
Un mot de passe robuste c'est :

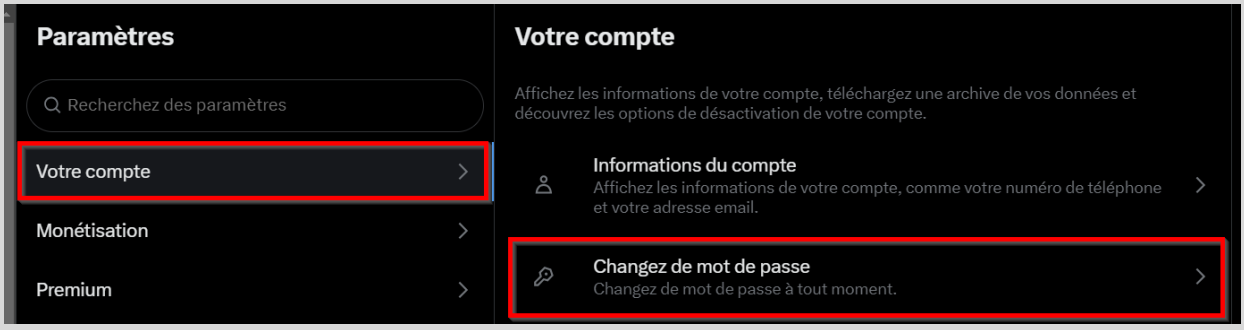
- Au minimum 12 caractères (idéalement 18).
- Composé de minuscules, de majuscules, de chiffres et de caractères spéciaux.
- Unique et utilisé pour un seul compte.

Si le mot de passe actuel de votre compte X respecte ces critères, félicitations. Si ce n'est pas le cas, je vous recommande très fortement de procéder au changement de celui-ci.

Voici la marche à suivre pour changer le mot de passe de votre compte X :

1. Allez dans les réglages au niveau de la section « Votre compte ».
2. Appuyez sur l'onglet « Changer de mot de passe ».





Explication du double facteur d'authentification (2FA)

Le double facteur d'authentification est un mécanisme de sécurité qui ajoute une couche supplémentaire de protection à vos comptes en ligne.

En général, pour accéder à un compte en ligne, vous devez fournir un identifiant et un mot de passe. Cependant, ces informations peuvent être compromises si elles sont divulguées ou piratées. Le double facteur d'authentification ajoute une étape supplémentaire pour vérifier votre identité. Cela peut inclure une clé de sécurité physique, un code généré par une application ou un code envoyé par SMS à votre téléphone portable.

Son activation peut grandement aider à protéger vos comptes de réseaux sociaux contre les tentatives d'accès non autorisées, même si votre identifiant et mot de passe sont compromis. En effet, un pirate informatique qui aurait réussi à obtenir votre mot de passe ne pourra pas accéder à votre compte sans valider cette étape supplémentaire de vérification.

Comme vous l'avez probablement compris, mettre en place le double facteur d'authentification constitue une action **extrêmement importante** afin de sécuriser vos comptes de réseaux sociaux ainsi que vos données personnelles.

Important : L'utilisation de l'option du SMS envoyé à votre téléphone portable est déconseillée, car une fraude connue sous le nom de « SIM Swap » la rend plus vulnérable. À la place, privilégiez l'utilisation d'une application génératrice de code comme Google Authenticator ou Microsoft Authenticator.

Configurer et activer le double facteur d'authentification (2FA)

Comme démontré dans les explications ci-dessus, l'utilisation du double facteur d'authentification est une autre pratique fondamentale en matière de cybersécurité, à mettre en place sur tous vos comptes lorsque cette option est disponible.

Voici donc la marche à suivre pour configurer et activer le double facteur d'authentification sur votre compte X avec une application génératrice de code :

1. Si ce n'est pas déjà fait, télécharger et installer l'application Google Authenticator ou Microsoft Authenticator sur votre téléphone à partir du Play Store ou de l'App Store.

2. Si l'une de ces applications est déjà installée et que vous en maîtrisez l'utilisation, passez à la page suivante. Sinon, continuez avec l'étape 3.

3. Si vous venez d'installer l'une de ces applications, il est fort probable que vous ne sachiez pas comment l'utiliser. Je vous fournis ci-dessous deux liens qui vous guideront dans la configuration et le fonctionnement des applications.

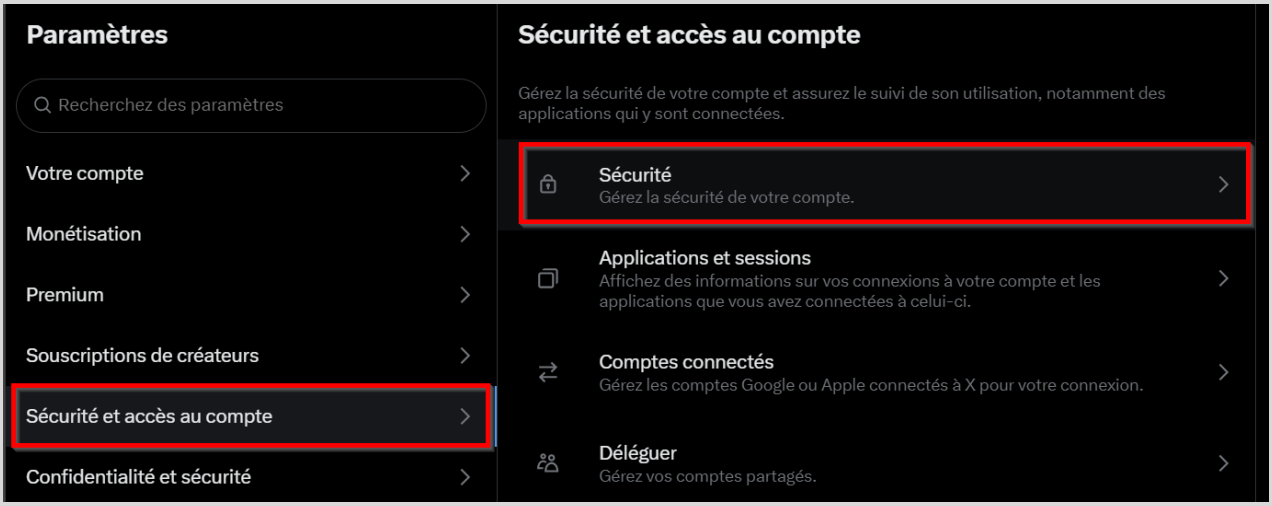
- Procédure pour Microsoft Authenticator (iOS et Android)
  Lien : Procédure pour Microsoft Authenticator (iOS et Android).pdf

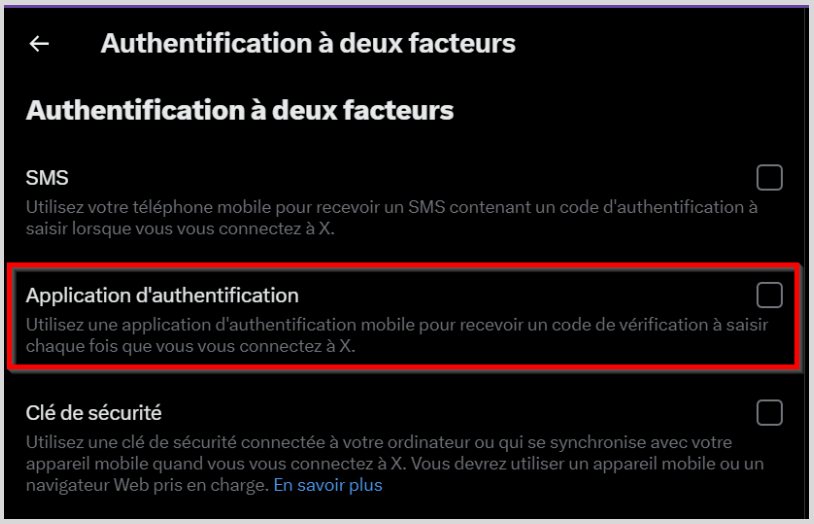
- Procédure pour Google Authenticator (iOS et Android)
  Lien : Procédure pour Google Authenticator (iOS et Android).pdf

Important : La procédure de configuration ci-dessous est réalisée depuis un **ordinateur**. Si vous souhaitez activer le double facteur d'authentification via **l'application mobile**, allez directement à la page 10 de ce guide.

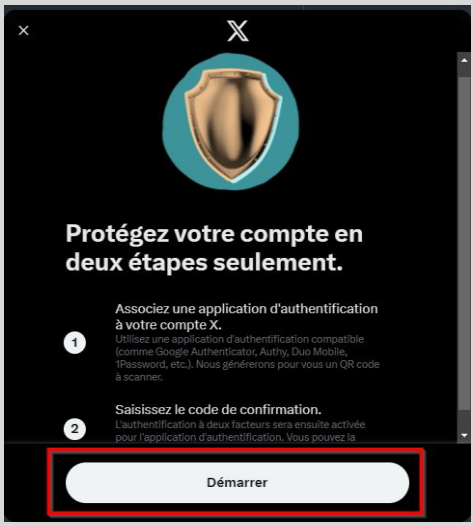
Configuration depuis un ordinateur :

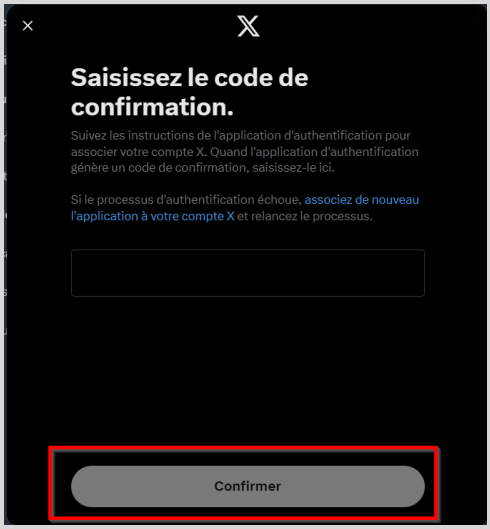
1. Allez dans les réglages au niveau de la section « Sécurité et accès au compte ».
2. Cliquez sur l'onglet « Sécurité » puis sur « Authentification à deux facteurs ».
3. Cochez le bouton « Application d'authentification ».



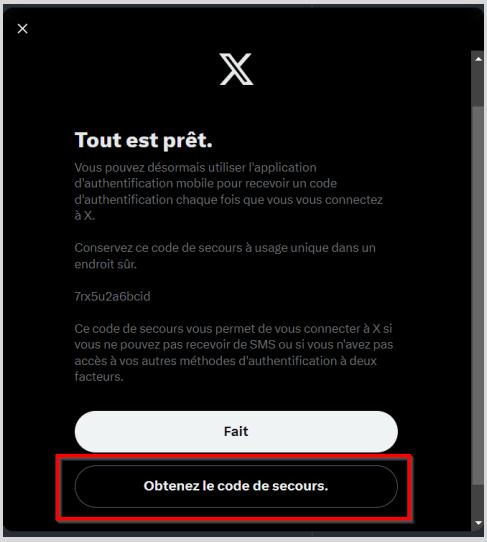


4. Inscrivez le mot de passe de votre compte et appuyez sur « Confirmer »
5. Cliquez sur « Démarrer ».
6. Scannez le code QR à l'aide de l'application choisie puis cliquez sur « Suivant ».
7. Saisissez le code généré à partir de l'application et cliquez sur « Confirmer ».



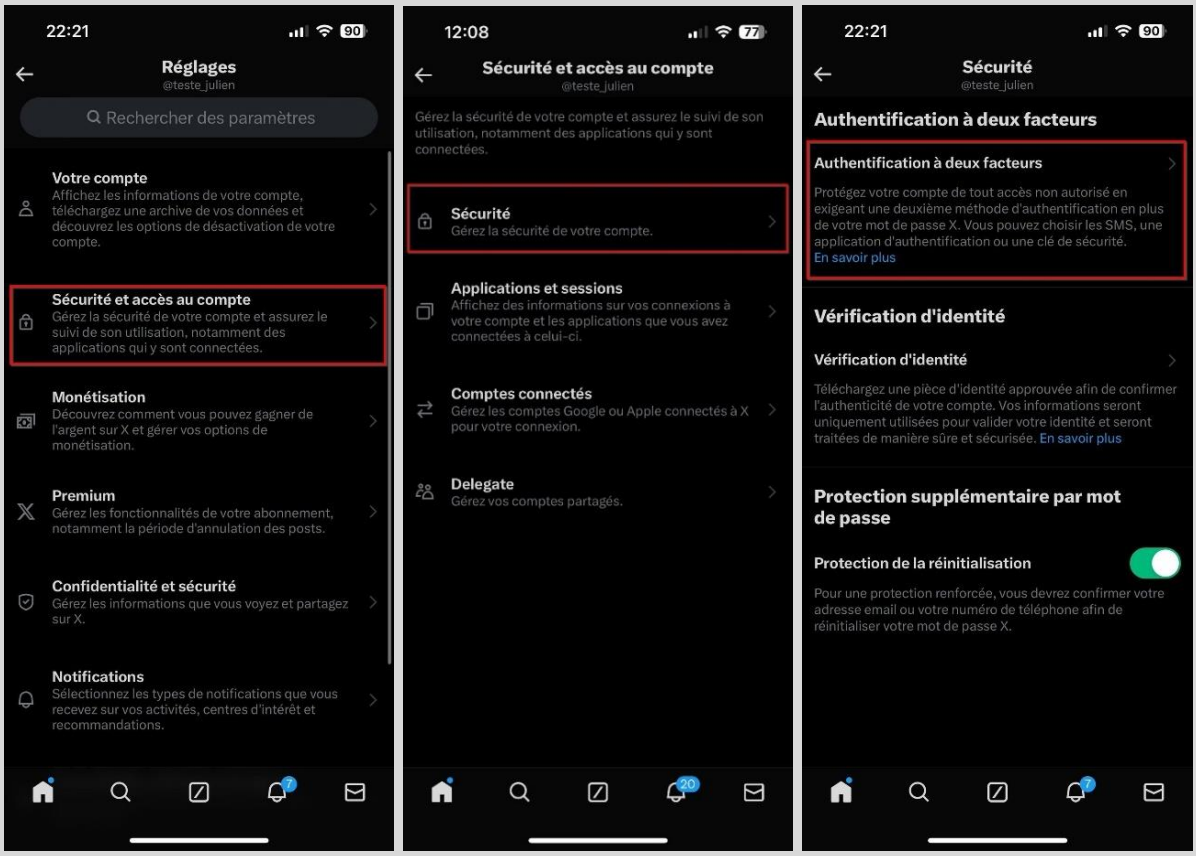


8. Cliquez sur « Obtenez le code de secours » et conservez-le dans un endroit sûr. Rendez-vous à la page 12 pour des explications sur cette fonctionnalité.

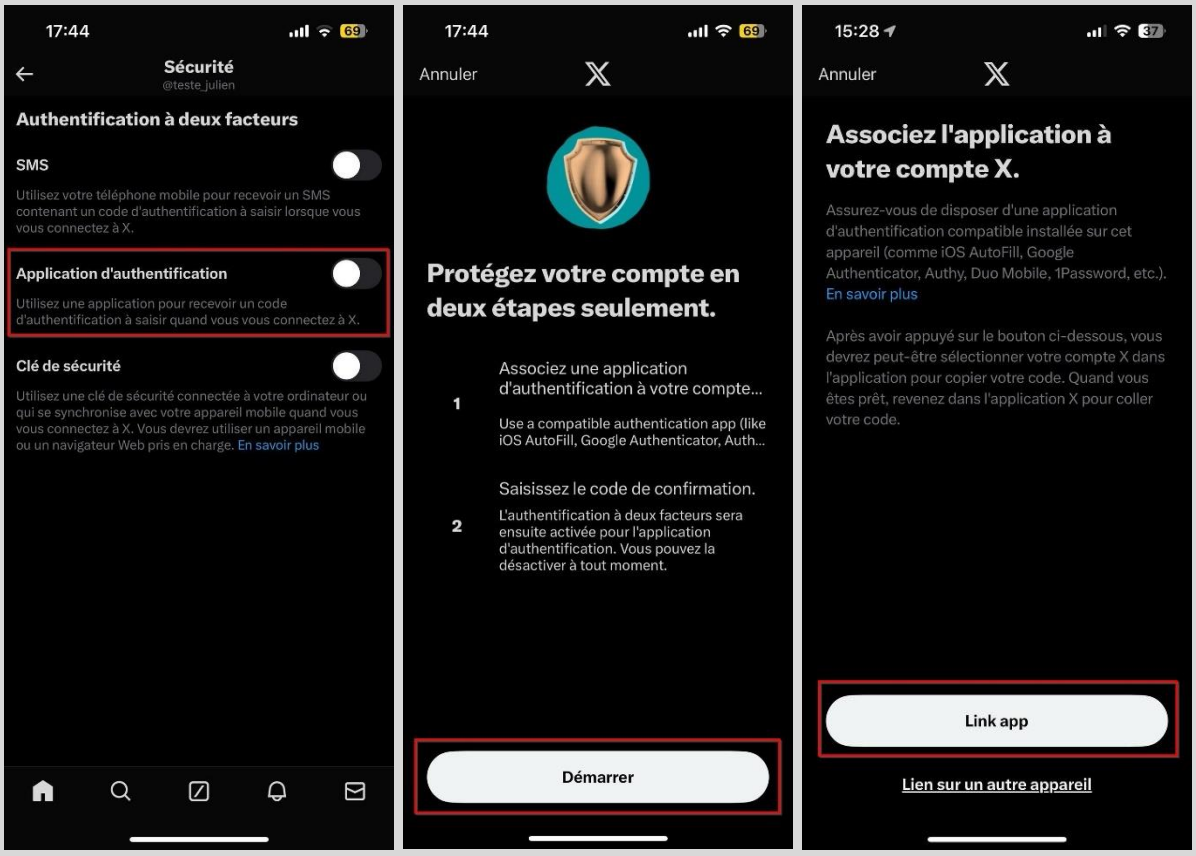


Configuration via l'application mobile :

1. Allez dans les réglages au niveau de la section « Sécurité et accès au compte ».
2. Appuyez sur l'onglet « Sécurité » puis sur « Authentification à deux facteurs »

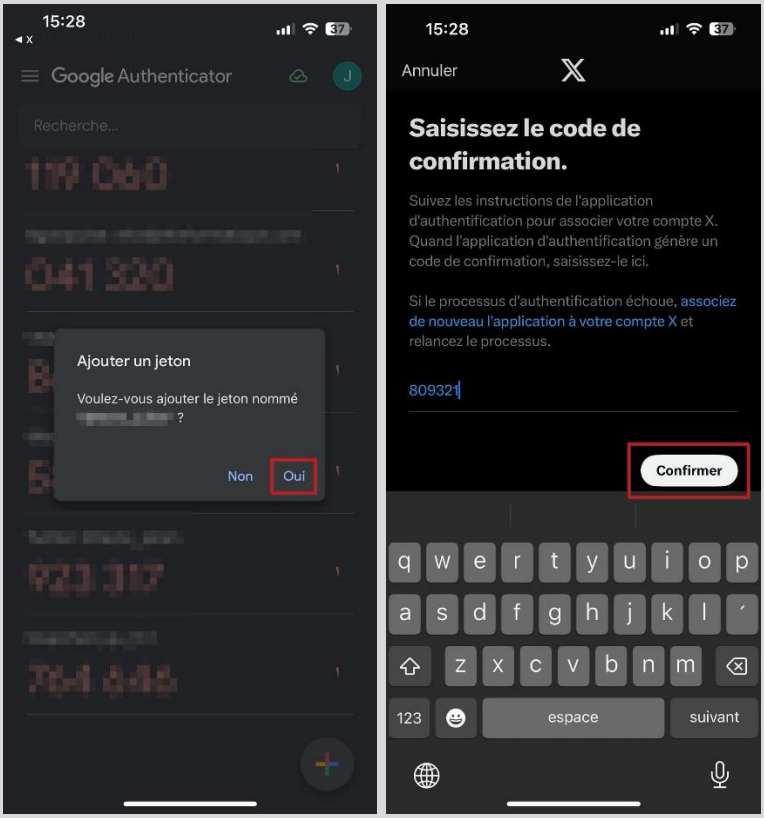


3. Cochez le bouton « Application d'authentification » puis appuyez sur « Démarrer ».
4. Appuyez sur « Link app ». Vous serez alors redirigé sur l'application 2FA utilisée. *

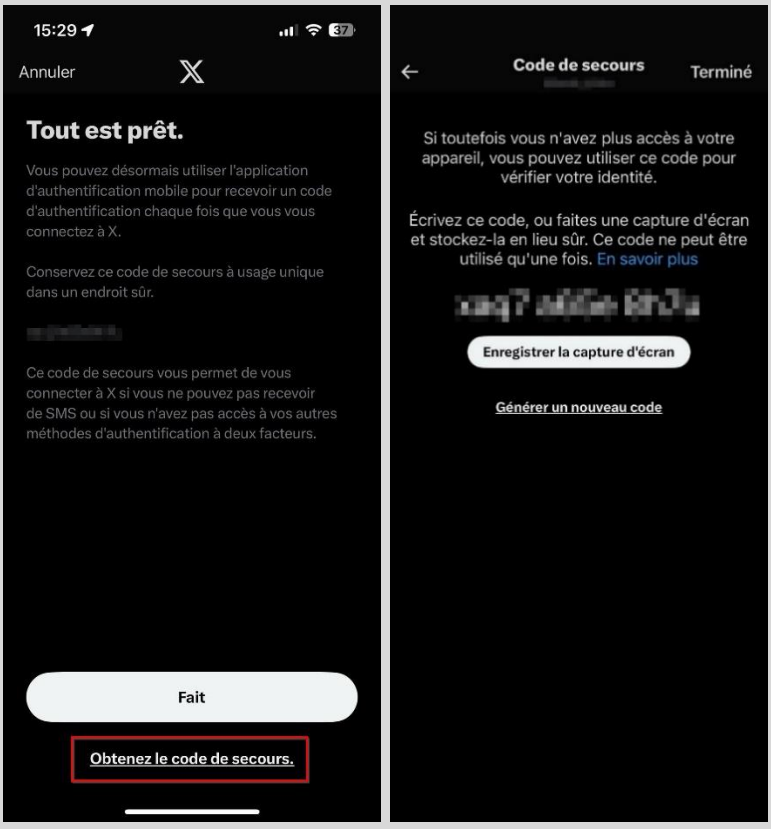


* Pour les utilisateurs d'iOS, voici la procédure pour choisir votre application 2FA par défaut.

5. Appuyez sur « Oui » pour confirmer l'ajout du compte.
6. Copiez le code aléatoire généré à partir de l'application et retournez sur X.
7. Saisissez le code aléatoire précédemment copié et appuyez sur « Confirmer ».



8. Appuyez sur « Obtenez le code de secours » et conservez-le dans un endroit sûr.



Explication de la fonction code de secours

Le code de secours est une série de chiffres générée lors de la configuration du double facteur d'authentification. Il sert de solution de secours pour accéder à votre compte en cas de perte de votre appareil principal ou de problèmes techniques empêchant la réception de codes d'authentification.

Important : Le code de secours ne devrait en aucun cas être exclusivement conservé sur votre téléphone. Il est recommandé de le stocker ailleurs, de manière sécurisée. Si le code de secours est uniquement sauvegardé sur votre téléphone et que vous perdez cet appareil ou qu'il devient inutilisable, l'accès à vos comptes pourrait être sérieusement compromis. Il est préférable d'opter pour des solutions telles qu'un gestionnaire de mots de passe, une note manuscrite conservée dans un lieu sûr et confidentiel, ou encore un fichier protégé par mot de passe sauvegardé sur le cloud, comme iCloud ou Google Drive par exemple.

Gérer le double facteur d'authentification (2FA) après la configuration

Après avoir finalisé la configuration, revenez à la section des réglages et appuyez à nouveau sur l'onglet « Authentification à deux facteurs », vous pourrez alors accéder à divers paramètres.

- **SMS** : Si vous souhaitez tout de même configurer le double facteur d'authentification par l'envoi de codes par SMS, cochez l'option et vous pourrez configurer cette méthode en associant le numéro de téléphone de votre choix. Il est cependant important de noter qu'il faut un abonnement premium pour utiliser cette option.

- **Application d'authentification** : Si vous souhaitez désactiver le double facteur d'authentification par application génératrice de code, décochez l'option.

- **Clé de sécurité** : Si vous souhaitez configurer le double facteur d'authentification avec une clé de sécurité, cochez l'option et vous pourrez configurer cette méthode.

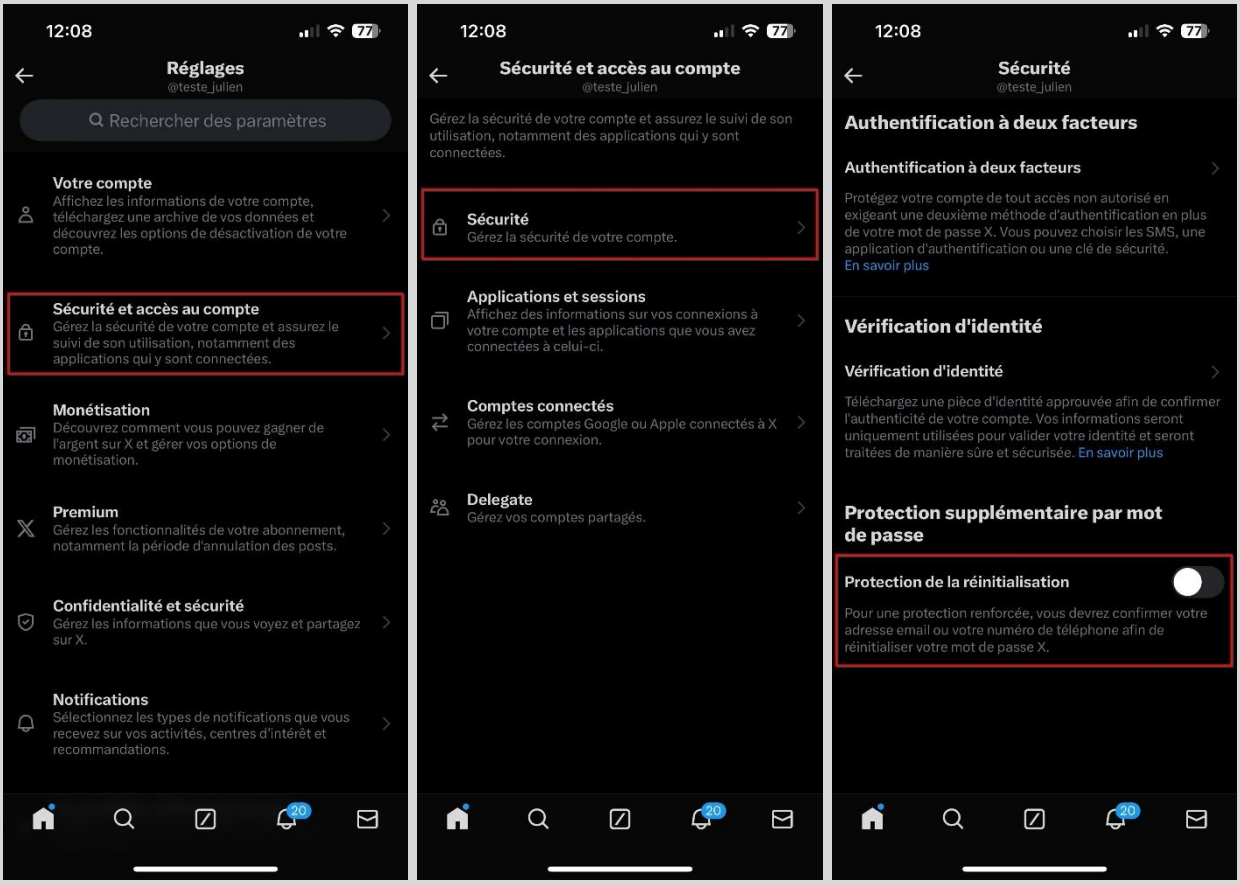
- **Code de secours**: Si vous avez perdu le code de secours généré initialement lors de la configuration du double facteur d'authentification, vous pouvez le récupérer à cet endroit. Il est aussi possible de générer un nouveau code.

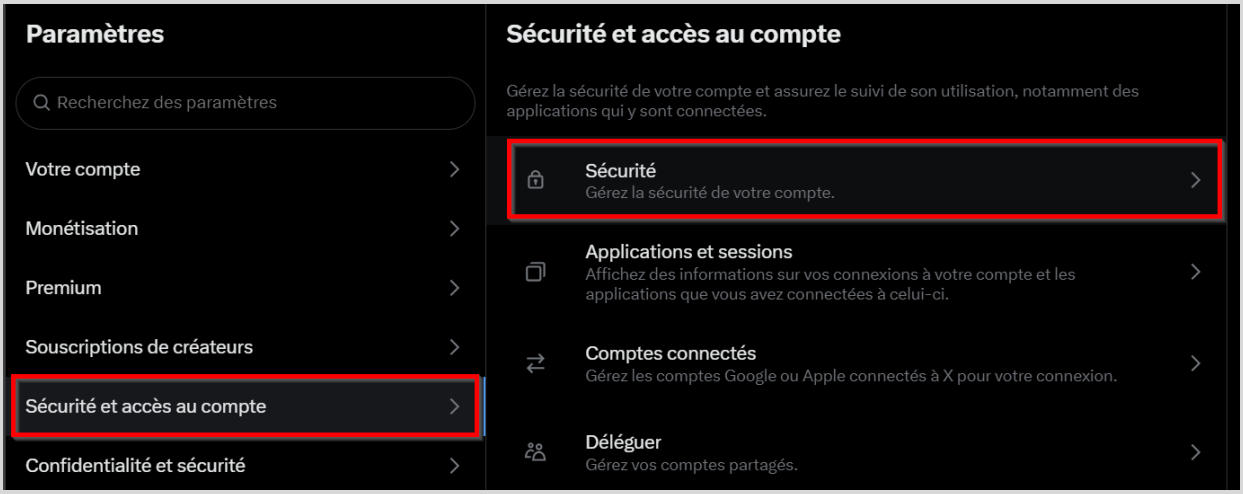
Protection de la réinitialisation du mot de passe

Cette fonctionnalité permet d'ajouter une couche de protection en exigeant des informations supplémentaires pour réinitialiser votre mot de passe. Si elle est activée, vous devrez fournir l'adresse e-mail et le numéro de téléphone associé à votre compte X pour réinitialiser votre mot de passe. Il ne s'agit pas d'une solution miracle, mais elle contribue à rendre plus ardue la tâche des individus malintentionnés qui tentent de compromettre votre compte en exploitant la fonction de réinitialisation de mot de passe.

Vous trouverez la marche à suivre pour activer ou désactiver cette fonctionnalité à la page suivante.

1. Allez dans les réglages au niveau de la section « Sécurité et accès au compte ».
2. Appuyez sur l'onglet « Sécurité ».
3. Cochez le bouton « Protection de la réinitialisation » pour activer la fonctionnalité.





Comment protéger votre vie privée sur X

Plusieurs paramètres de confidentialité sont à votre disposition pour vous aider à contrôler ce que vous partagez avec les autres. Pour chaque paramètre que nous passerons en revue, je partagerai avec vous mon opinion sur la meilleure configuration à appliquer.

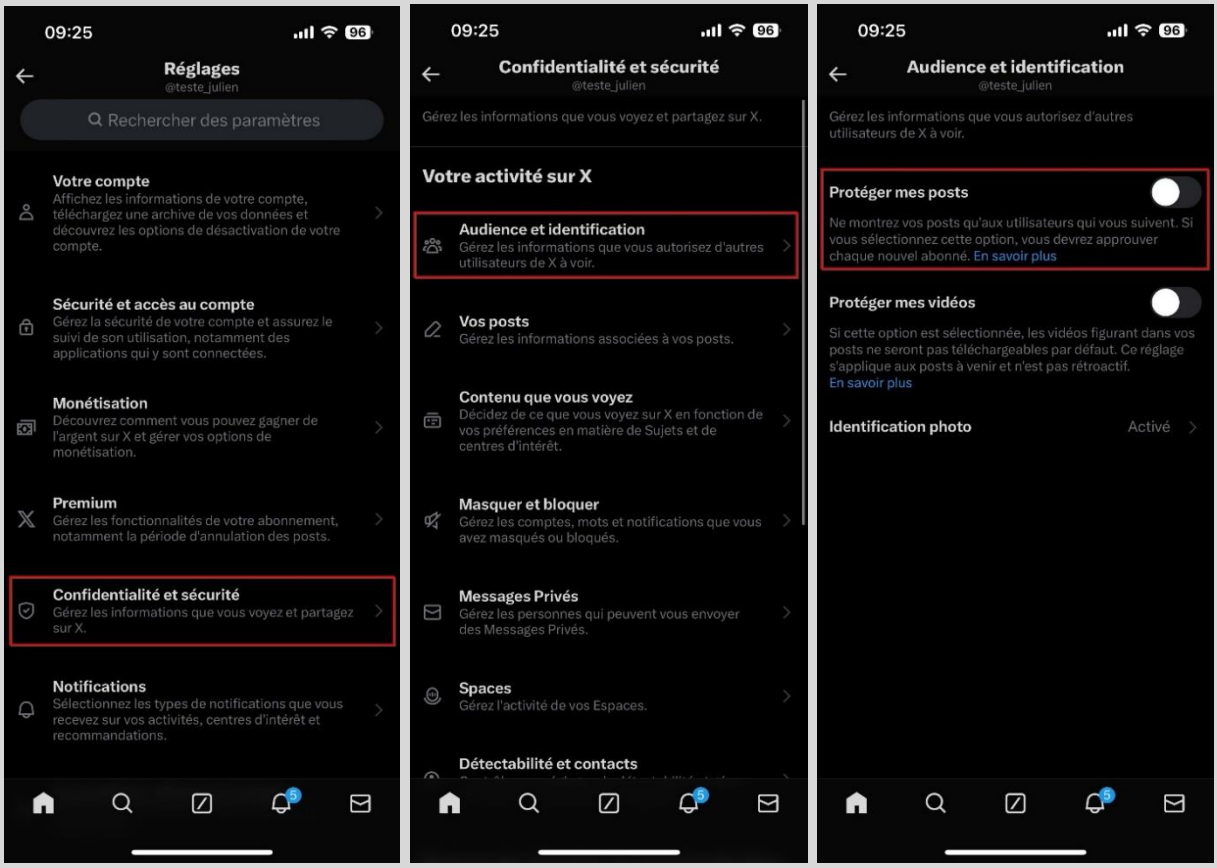
Afin d'éviter les redondances dans les étapes de gestion des paramètres, les captures d'écran présentées seront issues uniquement de l'application mobile, car la procédure est identique sur un ordinateur. En cas d'oubli sur la manière d'accéder aux différents paramètres depuis un ordinateur, n'hésitez pas à consulter la page 4.

Protéger mes posts

Cette fonctionnalité permet de masquer l'intégralité du contenu de votre profil aux utilisateurs qui ne sont pas abonnés à votre compte, à l'exception de votre biographie. Pour accéder à votre contenu, les utilisateurs doivent envoyer une demande d'abonnement que vous pouvez accepter ou refuser. Il est important de comprendre que vos tweets apparaitront uniquement dans le fil d'actualité de vos abonnés et qu'ils ne pourront pas les retweeter. Si vous n'activez pas cette fonctionnalité, votre compte demeurera public, ce qui permettra à tous les utilisateurs de voir vos tweets.

Voici la marche à suivre pour activer ou désactiver cette fonctionnalité :

1. Allez dans les réglages au niveau de la section « Confidentialité et sécurité ».
2. Appuyez sur l'onglet « Audience et identification ».
3. Cochez le bouton « Protéger mes posts » pour activer la fonctionnalité.



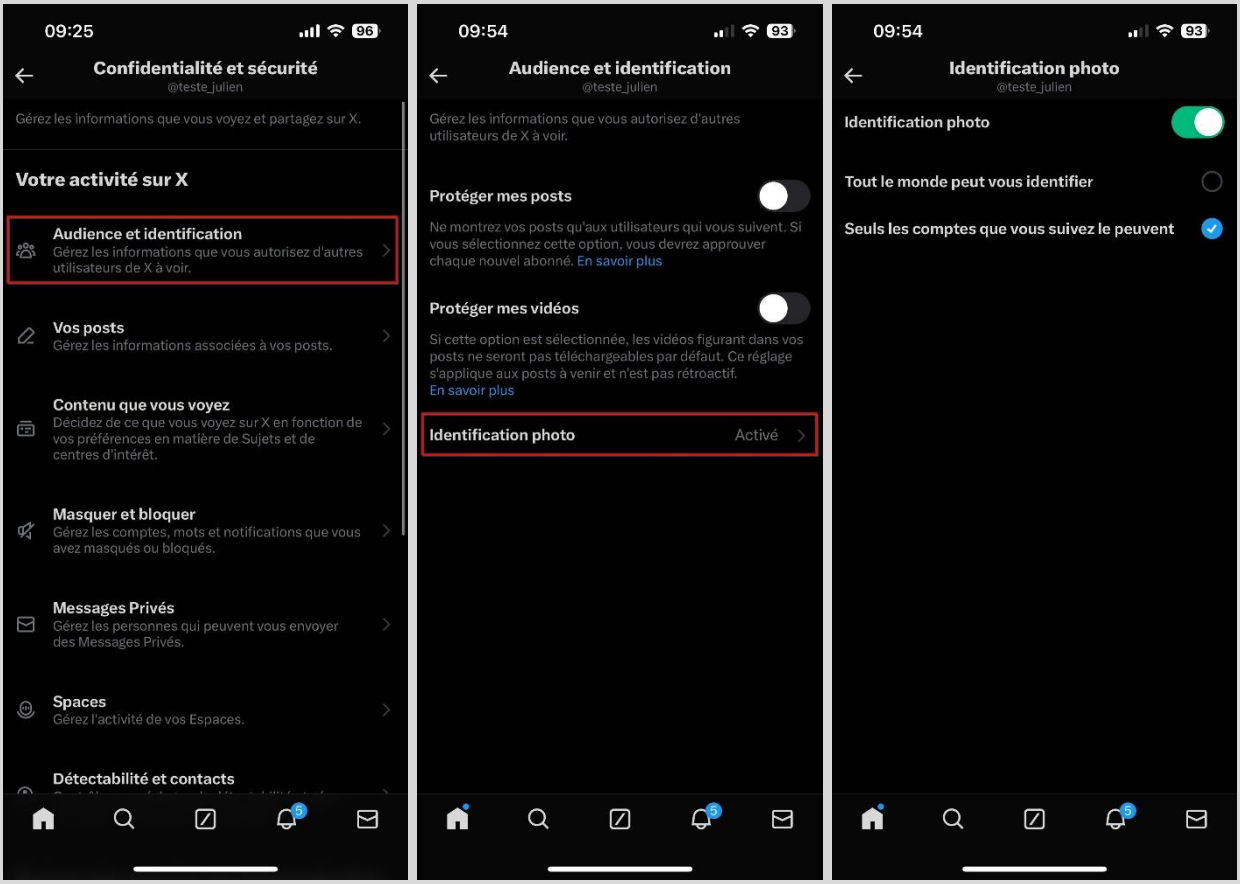
Mon opinion: Si vous n'êtes pas une personnalité publique et que votre but sur X n'est pas de gagner en visibilité ou d'augmenter votre nombre d'abonnés, je recommande d'activer cette fonctionnalité. Cela vous permettra de mieux contrôler qui peut accéder au contenu que vous publiez. Pensez aussi aux employeurs : ils consultent souvent les réseaux sociaux pour en savoir plus sur les candidats ou les employés actuels. Vous ne souhaitez probablement pas qu'ils puissent connaître toutes vos opinions émises sur X par exemple.

Identification photo

Cette fonctionnalité vous permet de choisir qui est autorisé à vous identifier sur leurs photos.

Voici la marche à suivre afin d'effectuer votre choix :

1. Allez dans les réglages au niveau de la section « Confidentialité et sécurité » (voir la page précédente si vous avez oublié où elle se trouve).
2. Appuyez sur l'onglet « Audience et identification ».
3. Appuyez sur « Identification photo ». À partir de là, vous pouvez désactiver ce paramètre ou sélectionner l'option de confidentialité qui vous convient.



Ci-dessous, les différentes options de confidentialité disponibles.

- **Désactivé**: Si vous désactivez cette fonctionnalité, aucun utilisateur ne peut vous identifier sur leurs photos.

- **Tout le monde peut vous identifier**: Vous l'aurez compris, tous les utilisateurs peuvent vous identifier sur leurs photos.

- **Seules les personnes que vous suivez peuvent vous identifier**: Seuls les utilisateurs que vous suivez, sans qu'ils aient nécessairement besoin de vous suivre en retour, peuvent vous identifier sur leurs photos.

Mon opinion: Je recommande d'activer cette fonctionnalité, mais de limiter l'autorisation d'identification en sélectionnant l'option de confidentialité « Seules les personnes que vous suivez peuvent vous identifier ». À moins que vous ne soyez une personnalité publique, il est peu probable qu'une personne totalement inconnue souhaite vous identifier sur une photo.

Messages privés

Sur X, vous pouvez envoyer et recevoir des messages privés. Ce paramètre permet de choisir qui peut vous envoyer une demande de message. Il est important de comprendre que les utilisateurs que vous suivez auront toujours la possibilité de vous envoyer un message privé. En fonction de l'option de confidentialité choisie, les utilisateurs que vous ne suivez pas pourront également vous envoyer des messages privés, mais ceux-ci apparaîtront en tant que demandes. Vous aurez alors la possibilité d'accepter ou de supprimer ces messages. *

* Tant que vous n'acceptez pas une demande de message, l'utilisateur ne saura pas que vous avez lu son message.

Ci-dessous, les différentes options de confidentialité disponibles.

- **Personne**: Aucun utilisateur ne peut vous envoyer une demande de message. Les utilisateurs que vous suivez pourront cependant toujours vous envoyer un message privé.

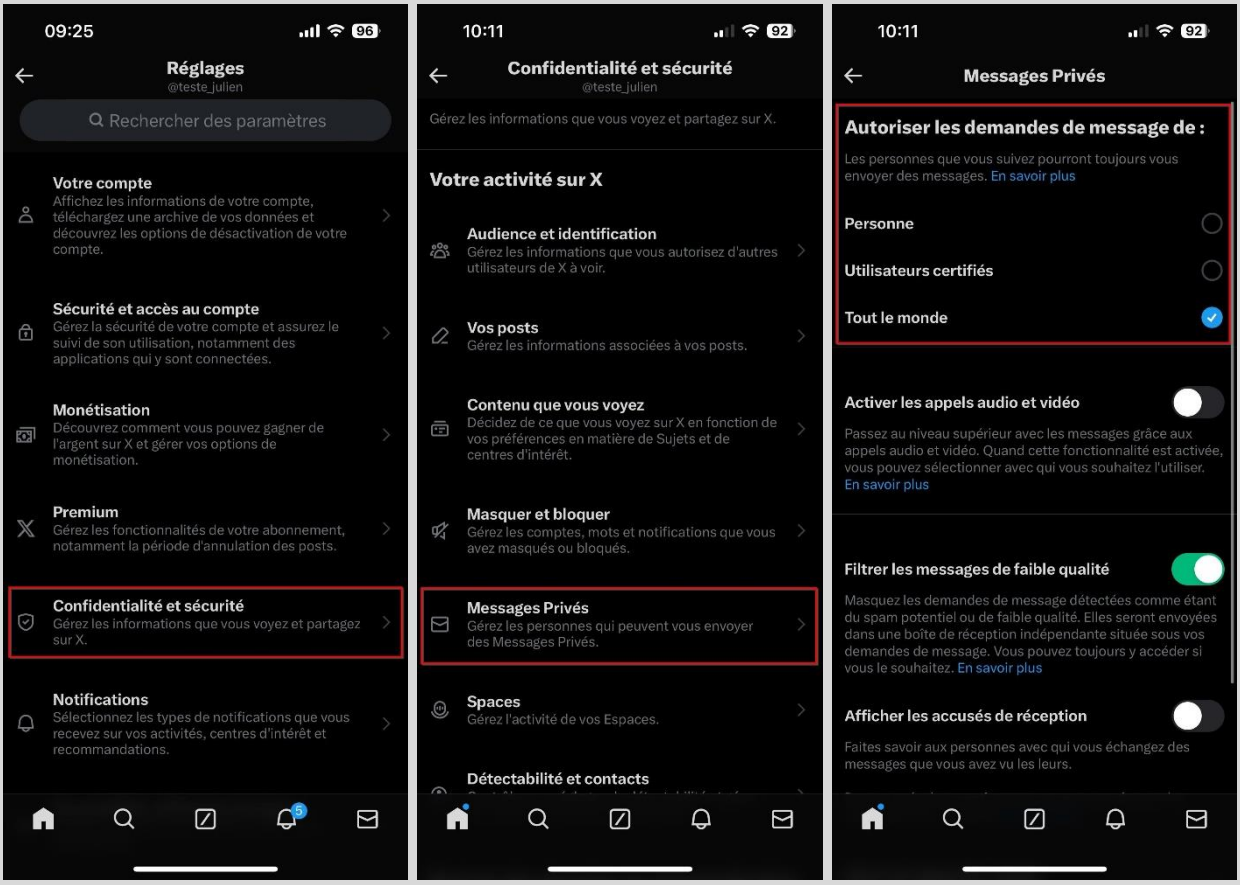
- **Utilisateurs certifiés**: Seuls les utilisateurs certifiés peuvent vous envoyer une demande de message.

- **Tout le monde**: Tous les utilisateurs peuvent vous envoyer une demande de message.

Mon opinion: Ce choix dépend de plusieurs facteurs. Si vous souhaitez limiter les interactions avec les utilisateurs que vous ne connaissez pas, optez pour l'option « Personne ». Si vous êtes ouvert à une interaction plus large, en sachant que vous avez toujours la possibilité de refuser une invitation par message, alors l'option « Tout le monde » est une bonne alternative.

Vous trouverez la marche à suivre afin d'effectuer votre choix à la page suivante.

1. Allez dans les réglages au niveau de la section « Confidentialité et sécurité ».
2. Appuyez sur l'onglet « Messages Privés ».



Vous avez peut-être remarqué que, en plus de l'option permettant de choisir qui peut vous envoyer une demande de message, on retrouve d'autres paramètres très intéressants.

Filtrer les messages de faible qualité: Ce paramètre vous offre la possibilité de filtrer les messages contenant un langage inapproprié ou considéré par X comme du spam. Vous ne serez pas notifié de ces messages, mais vous avez toujours la possibilité de vérifier la section des messages filtrés pour voir s'il y en a.

Mon opinion: Je recommande d'activer cette fonctionnalité de sécurité pour mettre de côté les messages désobligeants ou violents.

Afficher les accusés de réception : À l'image de Messenger sur Facebook, X offre aux utilisateurs la possibilité de savoir quand leur message privé a été lu. Ce paramètre permet de choisir si vous souhaitez activer ou désactiver cette fonctionnalité. Si vous la désactivez, personne ne pourra voir quand vous avez lu leurs messages, et vous ne pourrez pas non plus savoir quand quelqu'un a lu vos messages.

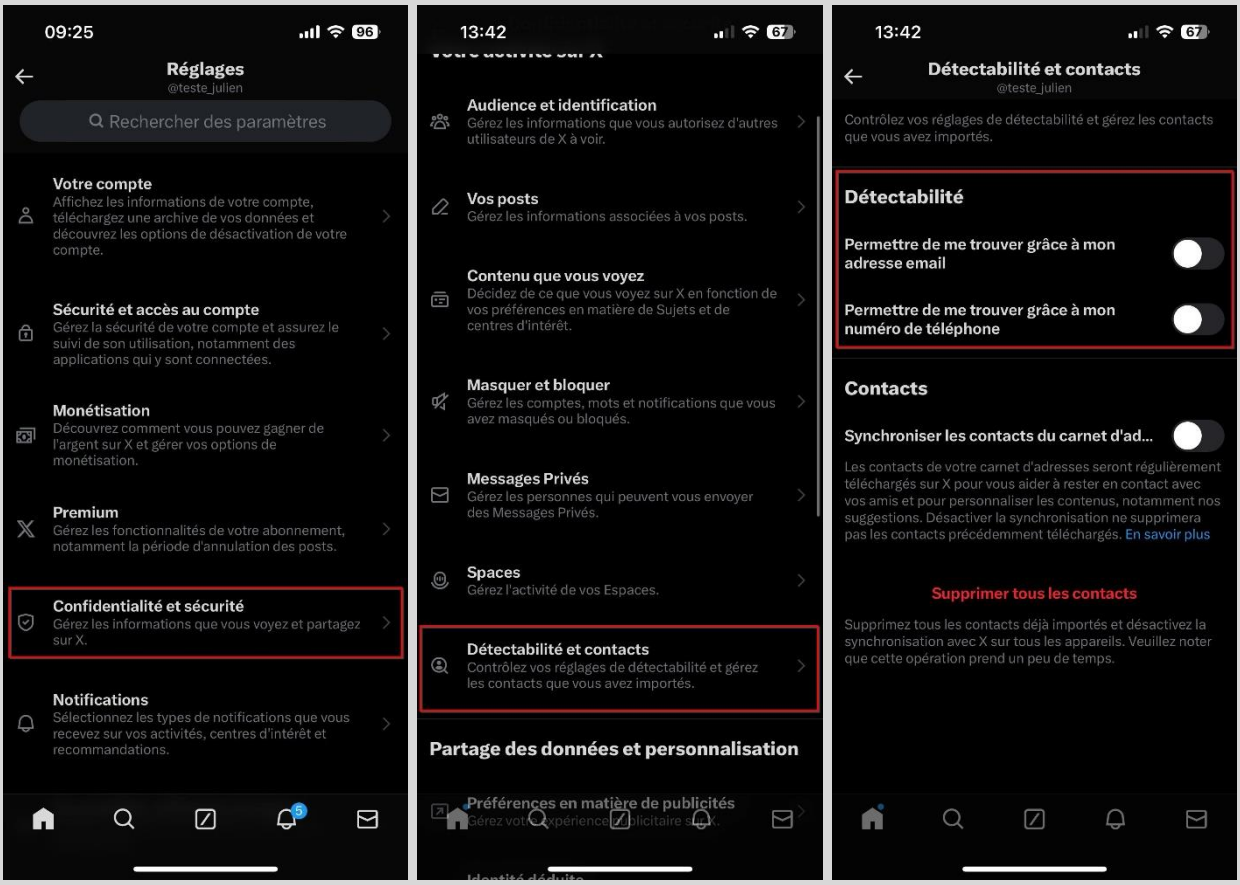
Mon opinion: Je n'ai pas de recommandation spécifique pour ce paramètre, car il relève d'une préférence personnelle. Cependant, je pense que dans le monde actuel où tout va très vite, en particulier en ligne, désactiver ce paramètre peut être une excellente idée. Cela peut en effet contribuer à alléger la charge mentale, à la fois pour vous-même et pour les autres utilisateurs, en éliminant la possibilité de savoir quand quelqu'un a vu votre message.

Permettre aux autres utilisateurs de me trouver

Sur X, une fonctionnalité permet aux utilisateurs de repérer votre compte via votre numéro de téléphone ou votre adresse e-mail liés à celui-ci. En résumé, si quelqu'un possède vos coordonnées dans ses contacts et donne à X l'autorisation d'accéder à ceux-ci, votre compte s'affichera alors pour cette personne, lui donnant la possibilité de vous suivre. Il est important de noter que vous avez le choix d'activer ou de désactiver cette fonctionnalité.

Voici la marche à suivre pour activer ou désactiver cette fonctionnalité :

1. Allez dans les réglages au niveau de la section « Confidentialité et sécurité ».
2. Appuyez sur l'onglet « Détectabilité et contacts ».
3. À partir de là, vous pouvez cocher ou décochez les boutons « Permettre aux personnes qui ont votre adresse email de vous trouver sur X » et « Permettre aux personnes qui ont votre numéro de téléphone de vous trouver sur X ».



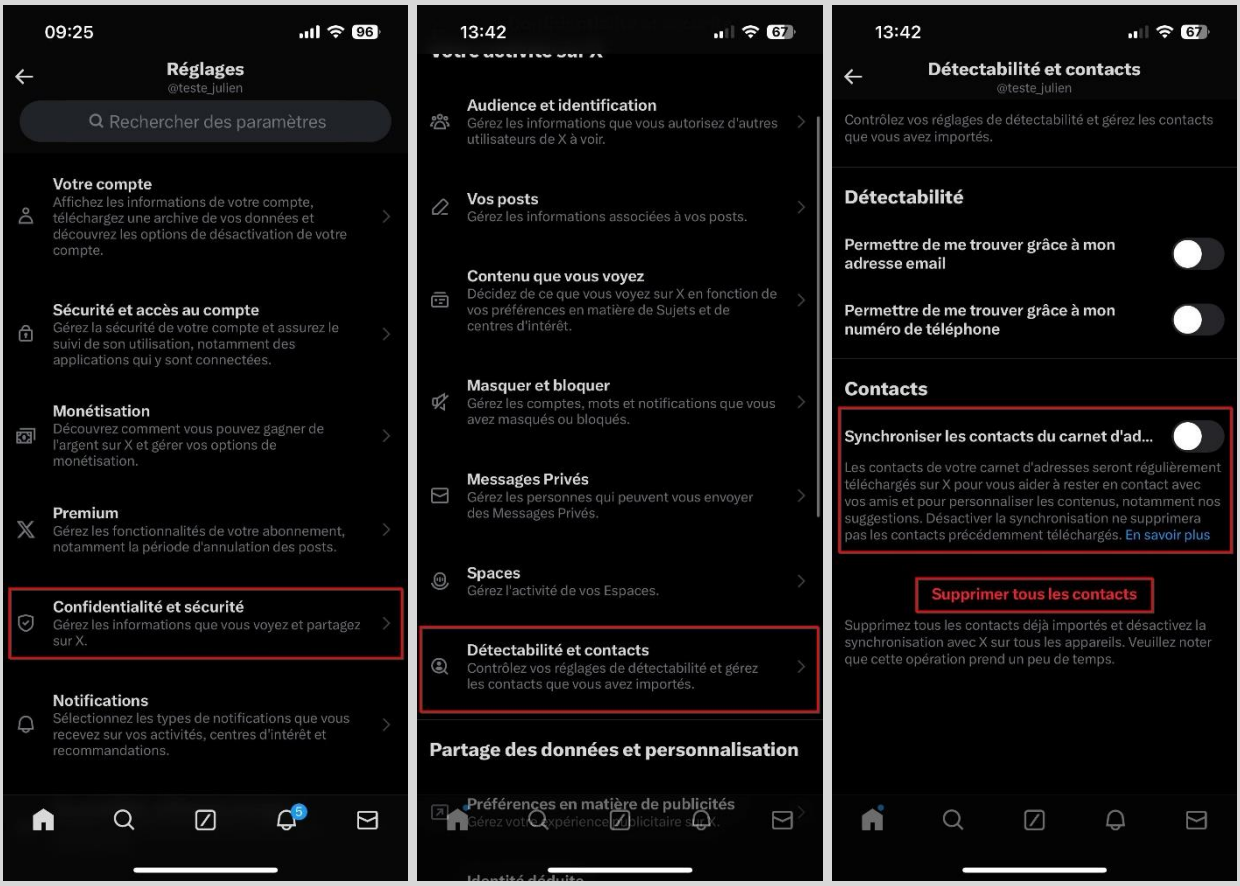
Mon opinion: Je recommande de désactiver cette fonctionnalité parce qu'il est peu probable que seuls vos amis aient votre numéro de téléphone et votre adresse e-mail. Vous les avez probablement aussi partagés avec des clients, des collègues, entre autres. Par conséquent, vous ne voulez pas que quiconque vous ayant dans ses contacts puisse trouver votre compte.

Synchroniser les contacts du carnet d'adresses

Comme discuté précédemment, il est possible d'autoriser X à accéder à vos contacts. Il est cependant important de noter qu'il est possible de révoquer cette autorisation.

Voici la marche à suivre pour accorder ou révoquer l'accès à vos contacts :

1. Allez dans les réglages au niveau de la section « Confidentialité et sécurité ».
2. Appuyez sur l'onglet « Détectabilité et contacts ».
3. Cochez ou décochez le bouton « Synchroniser les contacts du carnet d'adresses » selon vos préférences.



Il est important de noter que si vous avez déjà synchronisé vos contacts avec X par le passé, vous avez la possibilité de supprimer le tout en appuyant sur « Supprimer tous les contacts ».

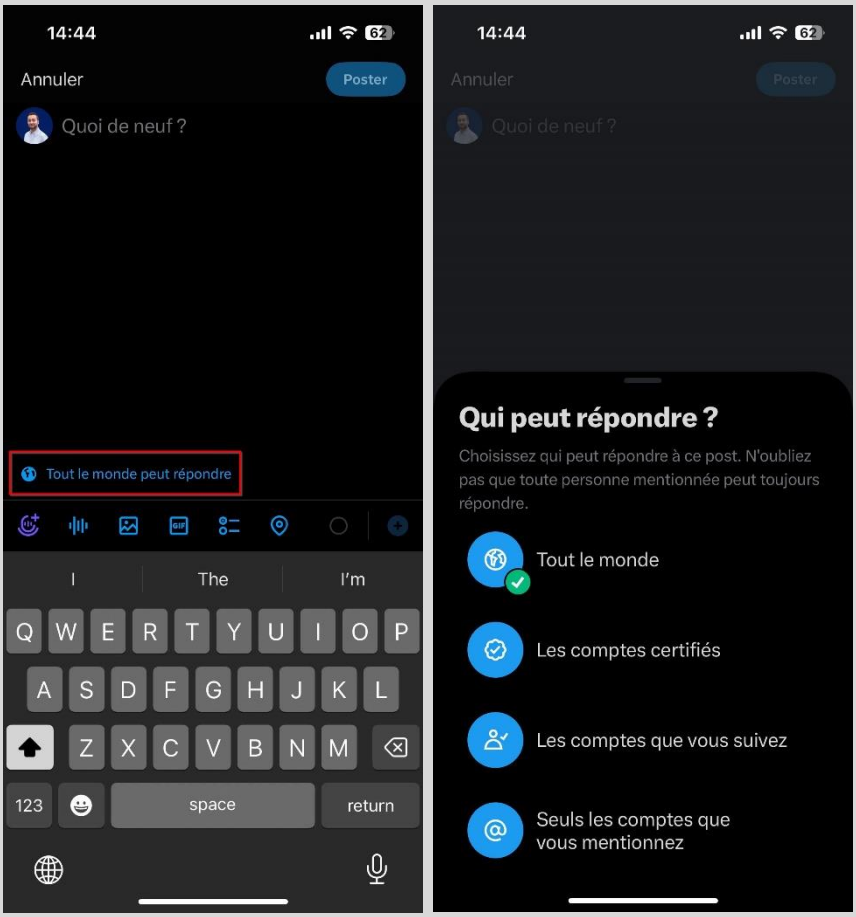
Mon opinion: Je recommande de ne pas synchroniser vos contacts avec X, à moins que vous souhaitiez absolument tenter de trouver le compte de l'un de vos contacts de cette manière.

Qui peut répondre à votre post

Lorsque vous publiez un tweet sur X, les utilisateurs peuvent répondre à celui-ci. Ce paramètre permet de choisir qui est autorisé à le faire.

Voici la marche à suivre afin d'effectuer votre choix:

1. Lorsqu'une fenêtre de rédaction est ouverte, appuyez sur « Tout le monde peut répondre » afin de faire apparaître les différentes options.



Ci-dessous, les différentes options de confidentialité disponibles.

- **Tout le monde**: Tous les utilisateurs peuvent répondre à votre tweet.

- **Les comptes que vous suivez** : Seuls les utilisateurs que vous suivez peuvent répondre à votre tweet.

- **Comptes certifiés**: Seuls les utilisateurs certifiés peuvent répondre à votre tweet.

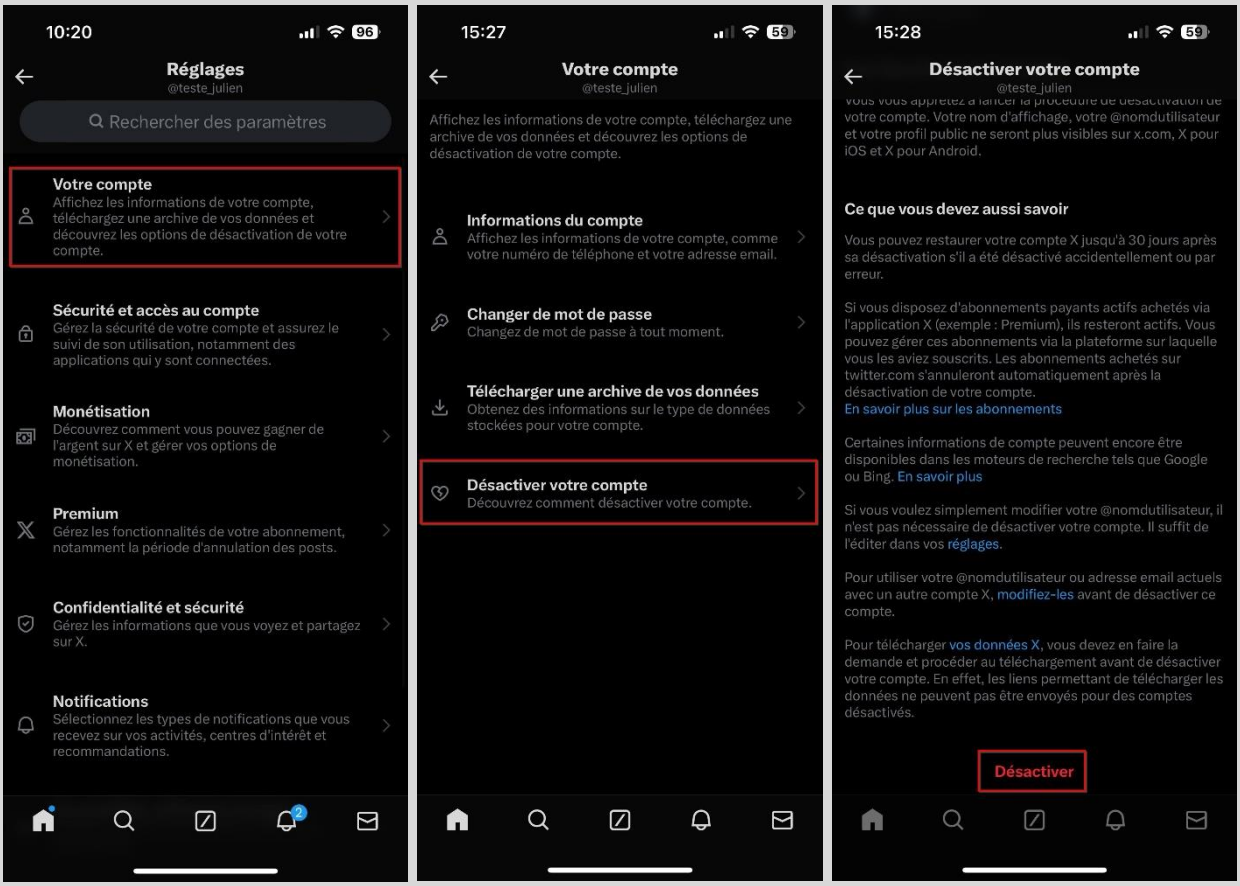
- **Seuls les comptes que vous mentionnez** : Seuls les utilisateurs que vous mentionnez sur votre tweet peuvent y répondre. Si vous désirez empêcher toute réponse à votre tweet, choisissez cette option en n'identifiant personne.

Mon opinion: Ce choix dépend de plusieurs facteurs. Si vous disposez d'une large communauté sur X et souhaitez limiter les interactions avec les utilisateurs que vous ne connaissez pas, optez pour l'option « Les comptes que vous suivez ». Si vous êtes ouvert à une interaction plus large, « Tout le monde » est alors une bonne option.

Comment supprimer votre compte X

Voici la marche à suivre afin de procéder à la suppression de votre compte X :

1. Allez dans les réglages au niveau de la section « Votre compte ».
2. Appuyez sur l'onglet « Désactiver votre compte ».
3. Appuyez sur « Désactiver ».
4. Saisissez votre mot de passe et confirmez votre décision en appuyant « Désactiver ».



Ce qu'il est important de comprendre, c'est que X ne va pas supprimer votre compte immédiatement; il va en fait le désactiver durant 30 jours. C'est seulement passé ce délai qu'il sera officiellement supprimé.

Durant ces 30 jours où votre compte est désactivé, vous avez la possibilité de le réactiver. Pour ce faire, simplement vous connecter à celui-ci et il sera réactivé, annulant du même coup la demande de suppression.

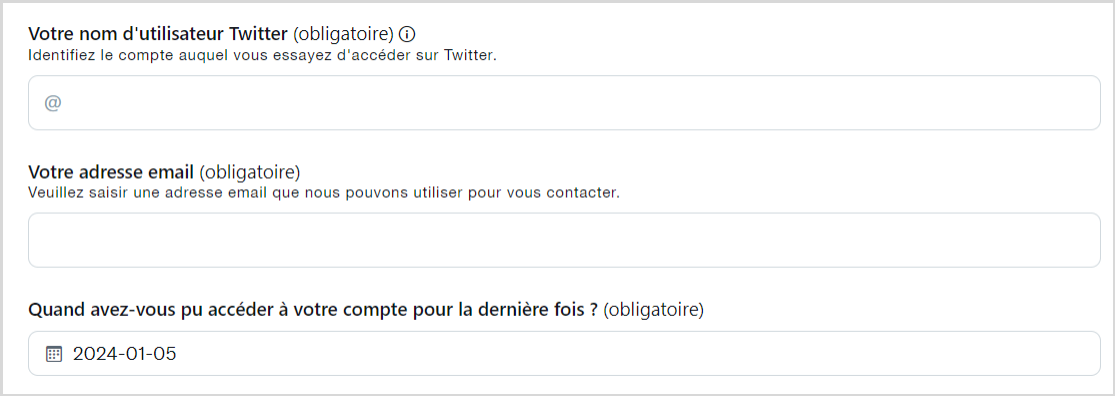
Que faire si votre compte a été piraté

Si votre compte X a été piraté et que vous n'y avez plus accès, vous pouvez aller sur le site ci-dessous pour soumettre une demande d'assistance.

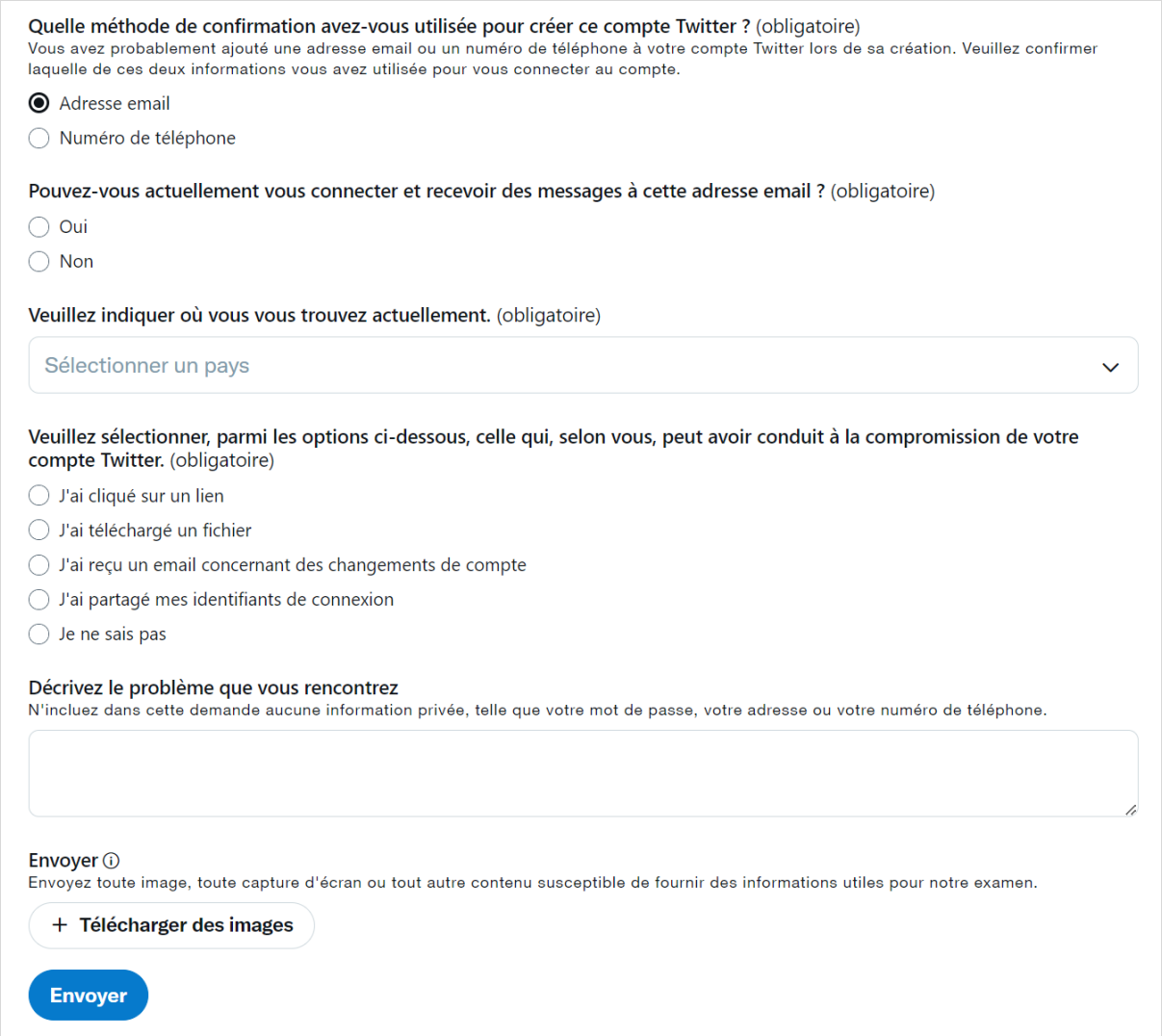
Lien : https://help.twitter.com/fr/forms/account-access/regain-access/hacked-or-compromised

1. Sélectionnez « J'ai besoin de restaurer l'accès à mon compte Twitter ».
2. Sélectionnez « Je pense que mon compte a été piraté ou compromis ».
3. Sélectionnez « Non » à la question « Pouvez-vous vous connecter à votre compte ».

4. Renseignez votre nom d'utilisateur, l'adresse e-mail liée à votre compte et la dernière fois que vous avez été en mesure d'accéder à celui-ci.



5. Précisez si vous avez utilisé une adresse e-mail ou un numéro de téléphone lors de la création de votre compte, puis répondez aux questions qui vous seront posées. Vous serez notamment invité à détailler comment vous croyez avoir été victime du piratage de votre compte X.



La bonne nouvelle de la journée

Si vous avez lu dans son intégralité la section Comment sécuriser votre compte X de ce guide, et surtout que vous avez appliqué TOUS les conseils que j'y donne :

- Avoir un mot de passe complexe et unique;
- Activer le double facteur d'authentification avec une application génératrice de codes;
- Activer le double facteur d'authentification sur l'adresse e-mail associée à votre compte X.

Eh bien malgré le fait que le risque 0 n'existe jamais en cybersécurité, je vous annonce qu'il est peu probable que vous ayez un jour à vous poser la question « Que faire si mon compte a été piraté » 😉

À propos de l'auteur

Titulaire d'un Baccalauréat en cybersécurité de Polytechnique Montréal et certifié en cybersécurité (CC) par l'organisme (ISC)², Julien Teste-Harnois est le fondateur de Resolock, une firme spécialisée dans la sécurisation des réseaux sociaux des entreprises et OBNL.

Son désir de contribuer à un cyberespace plus sûr l'a amené à partager ses connaissances et son expérience à travers divers canaux. Entrevues télévisées et radiophoniques, podcasts, conférence au Hackfest, rédaction d'articles, ne sont que quelques exemples.

N'hésitez pas à ajouter Julien sur LinkedIn et à vous abonner à sa page Facebook ⚡

LinkedIn: https://www.linkedin.com/in/julien-teste-harnois/

Page Facebook: https://www.facebook.com/resolock

Les principaux services de Resolock

🔍 *Audit de vulnérabilités des réseaux sociaux*

Vise à évaluer la posture de sécurité actuelle d'une entreprise par rapport à l'utilisation de ses réseaux sociaux et l'aider à identifier les différentes vulnérabilités présentes.

🤝 *Accompagnement personnalisé*

Peut prendre diverses formes selon les besoins des clients :

- Remédiation des vulnérabilités.
- Mises en place et configuration de plateformes de gestion.
- Élaboration et mise en œuvre de politiques pour l'octroi, la revue et la révocation des accès aux réseaux sociaux.

Pour en savoir plus sur les différents services : https://www.resolock.com/services