

SOCIAL - HARDERING - LinkedIn

HYGIÈNE NUMÉRIQUE & RÉSEAUX SOCIAUX.....	2
LE CLOISONNEMENT (EMAIL & IDENTITÉ).....	2
VISIBILITÉ PUBLIQUE & OBSCURCISSEMENT (STEALTH MODE).....	3
DURCISSEMENT DES POINTS D'ENTRÉE (EMAIL).....	4
DURCISSEMENT DES POINTS D'ENTRÉE (GSM).....	5
CONFIGURATION DU "MUR" (PARAMÈTRES DE CONFIDENTIALITÉ).....	6
NAVIGATION FURTIVE (GHOST MODE).....	6
SEGMENTATION DU RÉSEAU (CONNECTIONS LIST).....	7
DÉSACTIVATION DES API PARTENAIRES (MICROSOFT/TIERS).....	8
TÉLÉMÉTRIE & EXFILTRATION DE DONNÉES (OPT-OUT).....	9
PREVENTION : INGESTION PAR L'IA (LLM TRAINING).....	9
PREVENTION : PARTAGE TIERS & RECHERCHE.....	10
AUDIT DE CONFORMITÉ (VALIDATION).....	11

HYGIÈNE NUMÉRIQUE & RÉSEAUX SOCIAUX

Dans le cadre d'une stratégie de visibilité professionnelle, la présence sur les réseaux (LinkedIn) est obligatoire. Cependant, cela expose l'Admin à des vecteurs d'attaque (OSINT, Phishing ciblé). Ce module détaille le durcissement (Hardening) d'un compte LinkedIn pour maintenir l'étanchéité entre la vie privée et la vitrine publique.

LE CLOISONNEMENT (EMAIL & IDENTITÉ)

Règle d'or : Ne jamais utiliser l'email racine (perso ou root pro) pour un réseau social.

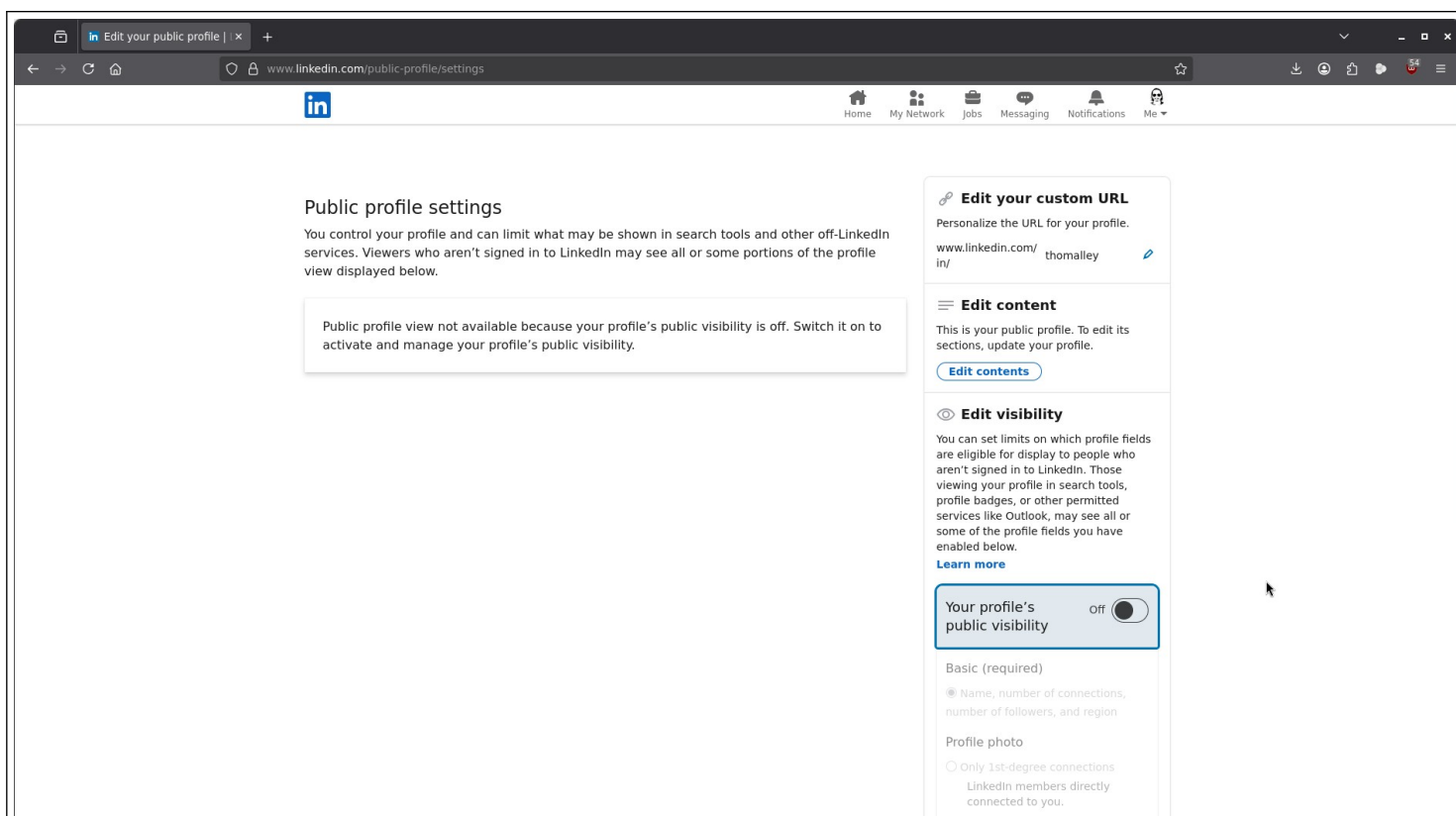
Action : Utilisation d'un alias dédié (ex: linkedin@domaine.fr ou une adresse SimpleLogin).

- *Intérêt* : Si cet email reçoit du spam ou une tentative de phishing ailleurs que via LinkedIn, l'alerte de fuite de données est immédiate.

Le Masque : Utilisation d'une photo professionnelle mais non-biométrique (stylisée, N&B, filtres) pour empêcher la reconnaissance faciale automatisée par des tiers.

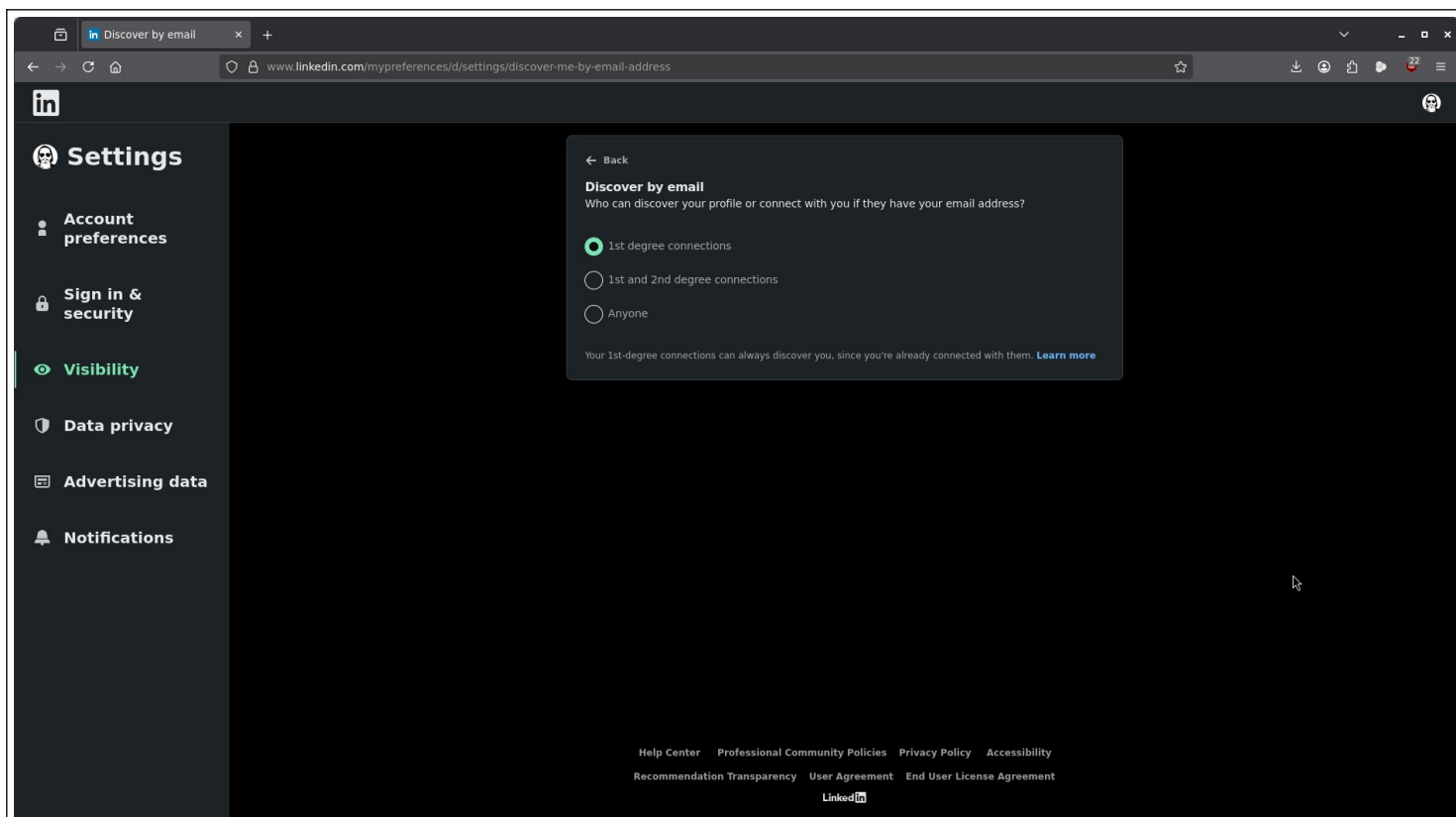
VISIBILITÉ PUBLIQUE & OBSCURCISSEMENT (STEALTH MODE)

- **Paramètre** : *Visibilité > Modification de votre profil public*



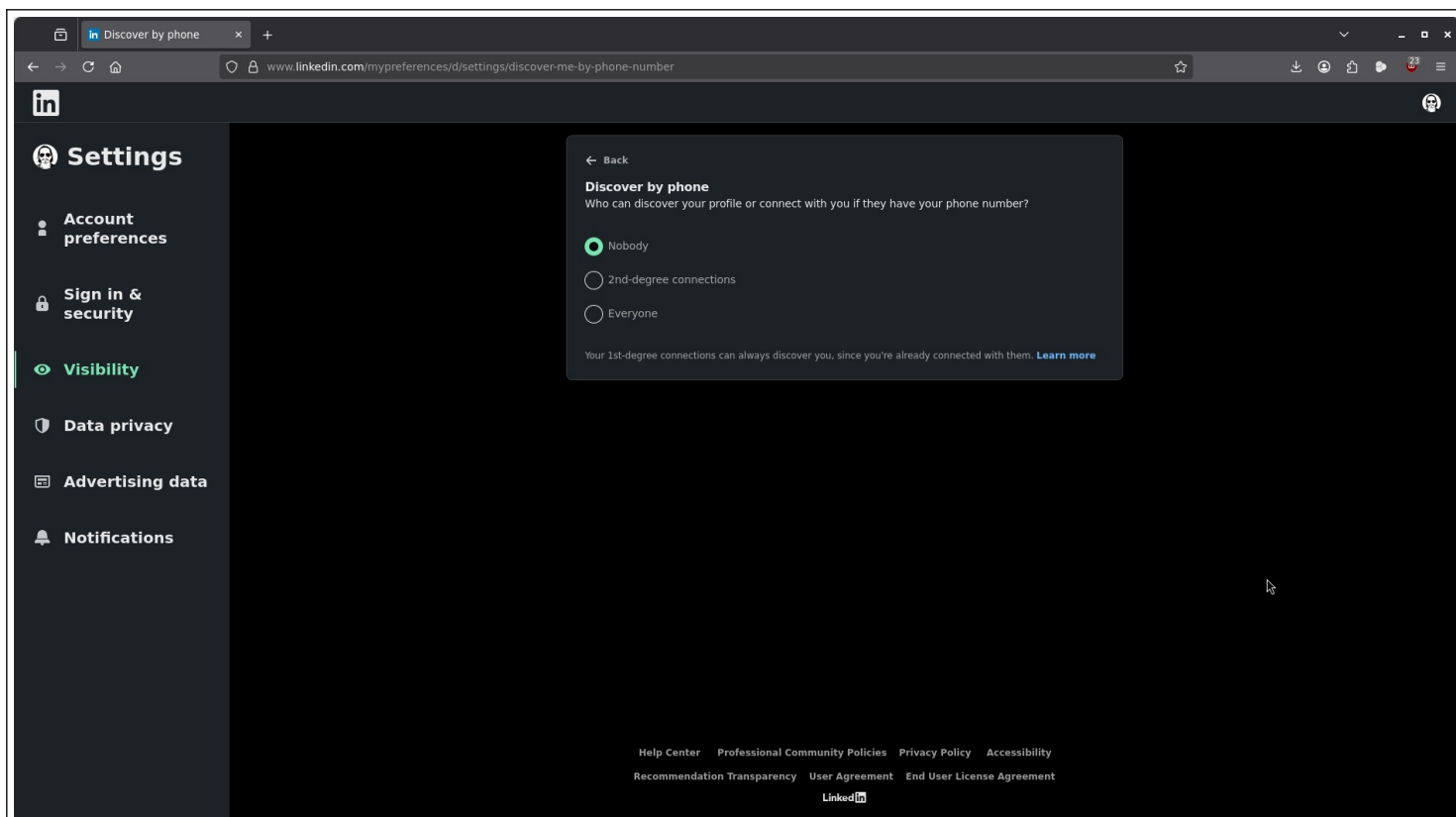
- **Paramètre** : *Modifier la visibilité public de votre profil*
- **Valeur** : Désactivé (OFF)
- **Effet** : Le profil n'est plus indexé par les moteurs de recherche (Google, Bing). Il n'existe que *dans* l'intranet LinkedIn. Empêche la corrélation automatique "Nom Prénom" -> "Profil LinkedIn" depuis une recherche web externe.
- **Paramètre (bonus)** : Modifier votre URL personnalisée
- **Action** : Cliquez sur le crayon et définissez votre alias
- **Effet** : Remplace l'identifiant numérique aléatoire par un lien lisible et mémorisable. Indispensable pour faire "pro" sur le CV papier et faciliter le partage du profil sans passer pour un bot.

DURCISSEMENT DES POINTS D'ENTRÉE (EMAIL)



- **Paramètre** : *Visibilité* > Découverte du profil via l'adresse e-mail
- **Valeur** : 1st degree connections
- **Effet** : Empêche les inconnus et les robots de trouver votre profil en utilisant votre adresse email. Seules les personnes DÉJÀ connectées avec vous (Relations de 1er niveau) peuvent faire le lien. Bloque l'énumération par des tiers malveillants.

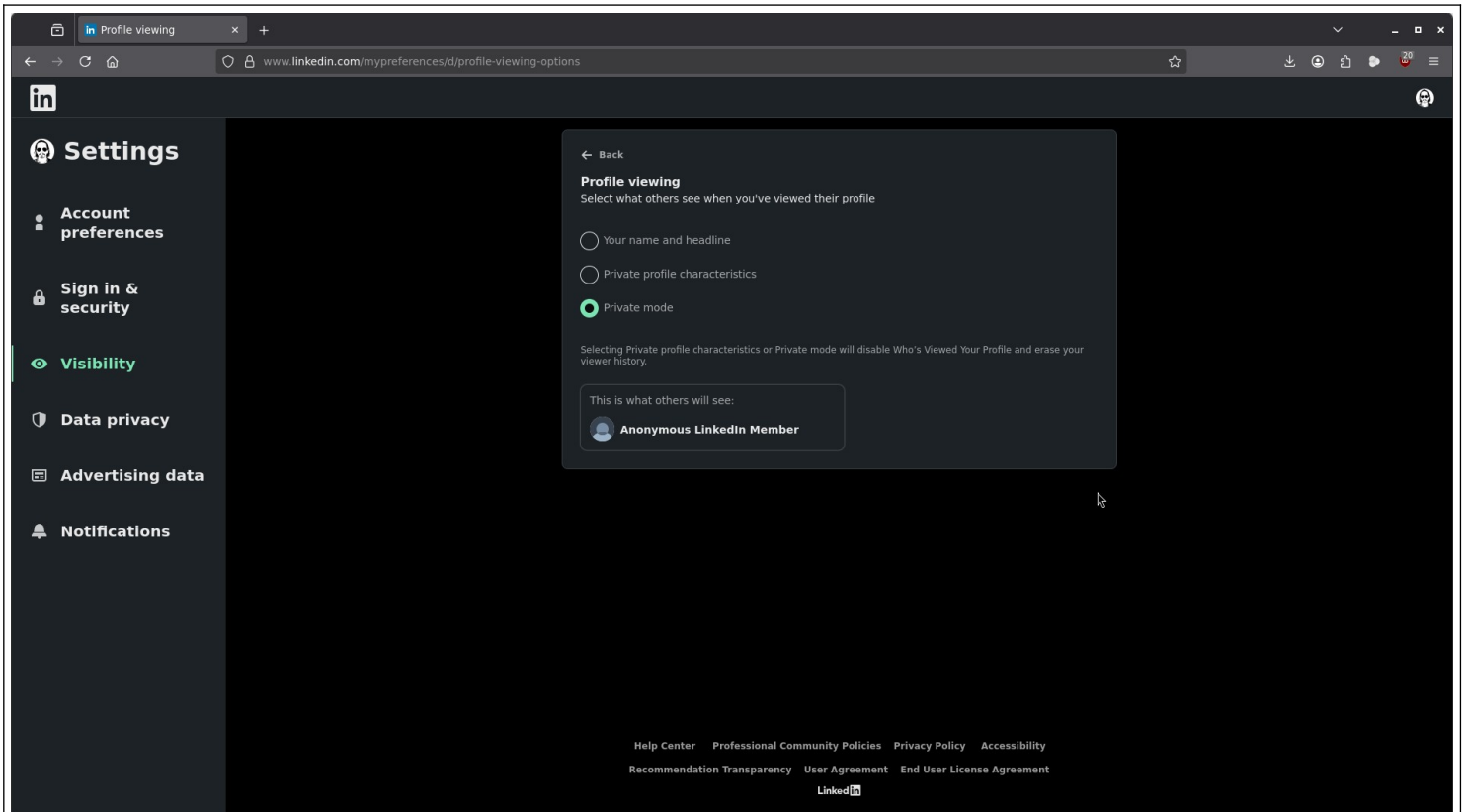
DURCISSEMENT DES POINTS D'ENTRÉE (GSM)



- **Paramètre** : *Visibilité* > Découverte du profil via le numéro de téléphone
- **Valeur** : Personne (Nobody)
- **Effet** : Verrouille totalement la recherche par numéro. Même si un tiers (recruteur, ancien collègue, spammeur) possède votre numéro mobile dans son répertoire, LinkedIn ne lui suggérera **jamais** votre profil. C'est une barrière essentielle pour empêcher la corrélation entre votre vie privée (téléphone) et votre vitrine publique.

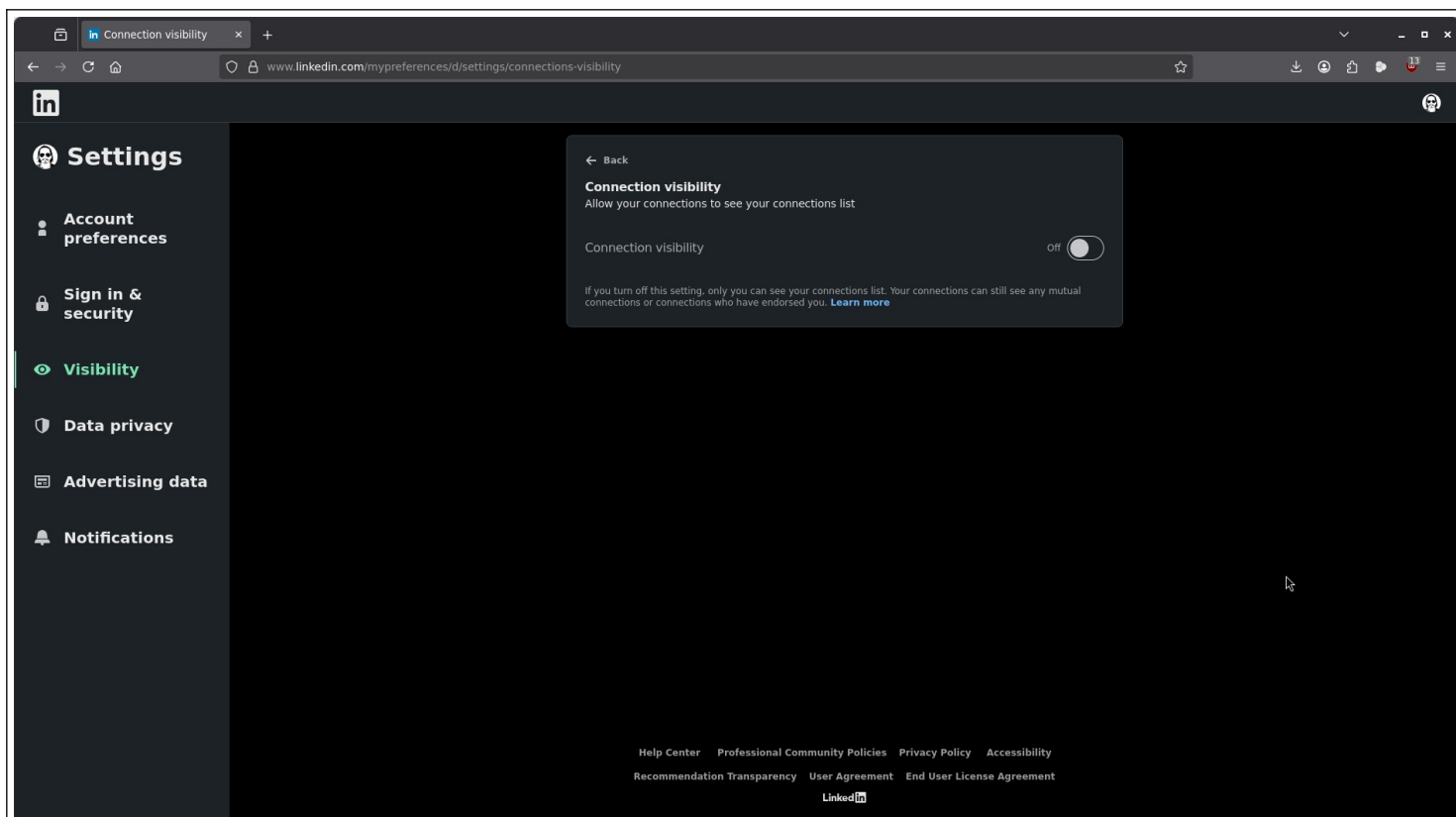
CONFIGURATION DU "MUR" (PARAMÈTRES DE CONFIDENTIALITÉ)

NAVIGATION FURTIVE (GHOST MODE)



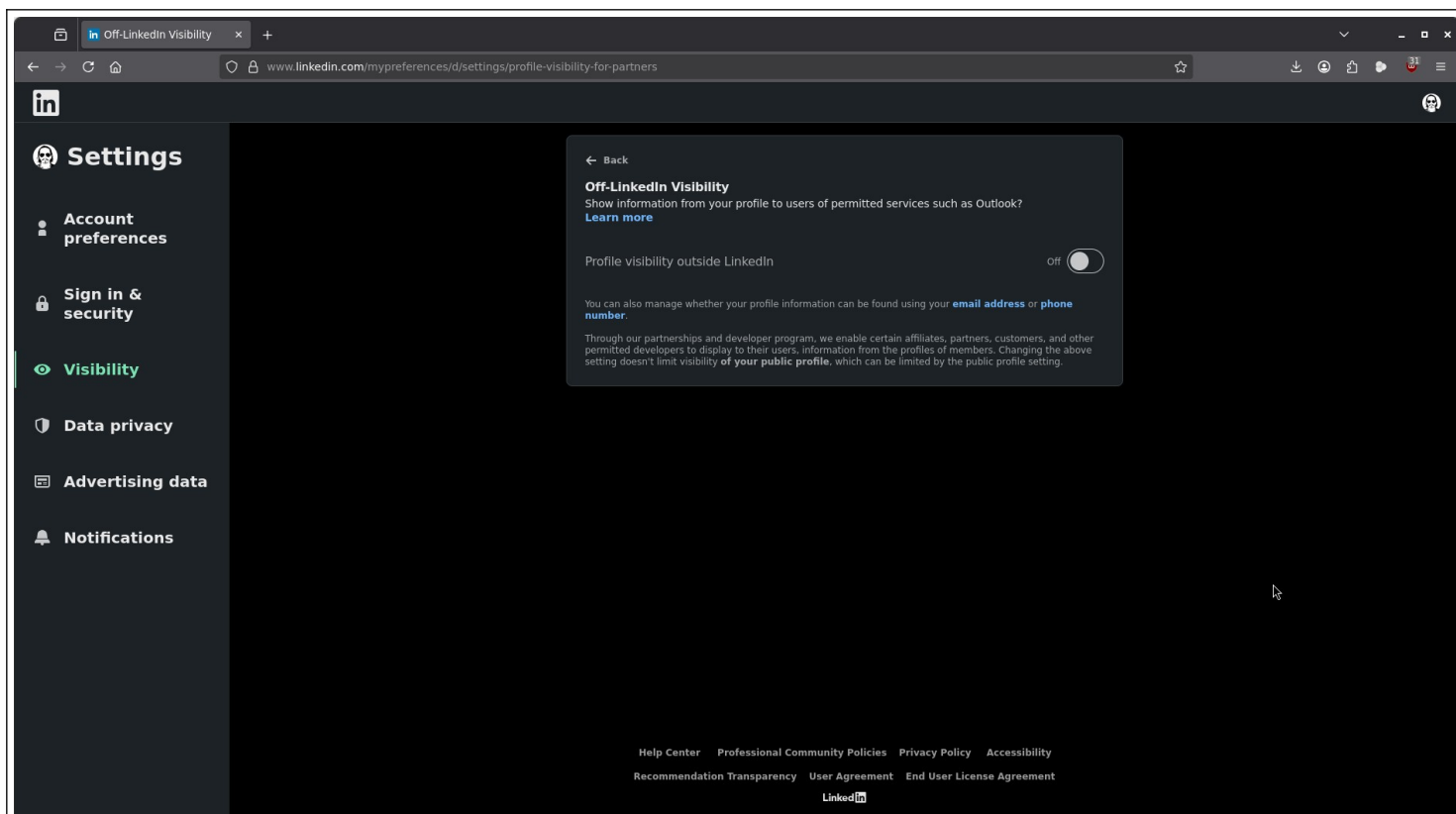
- **Paramètre** : *Visibilité > Options d'affichage du profil*
- **Valeur** : Private mode
- **Effet** : Tu peux visiter n'importe quel profil pour faire tes recherches. La cible verra juste "Un membre de LinkedIn" dans ses statistiques, sans ton nom ni ta photo. C'est de l'invisibilité active.

SEGMENTATION DU RÉSEAU (CONNECTIONS LIST)



- **Paramètre** : *Visibilité > Qui peut voir vos relations*
- **Valeur** : Désactivé (OFF)
- **Effet** : Empêche un concurrent ou un recruteur agressif de "scraper" (aspirer) votre réseau pour contacter vos partenaires.

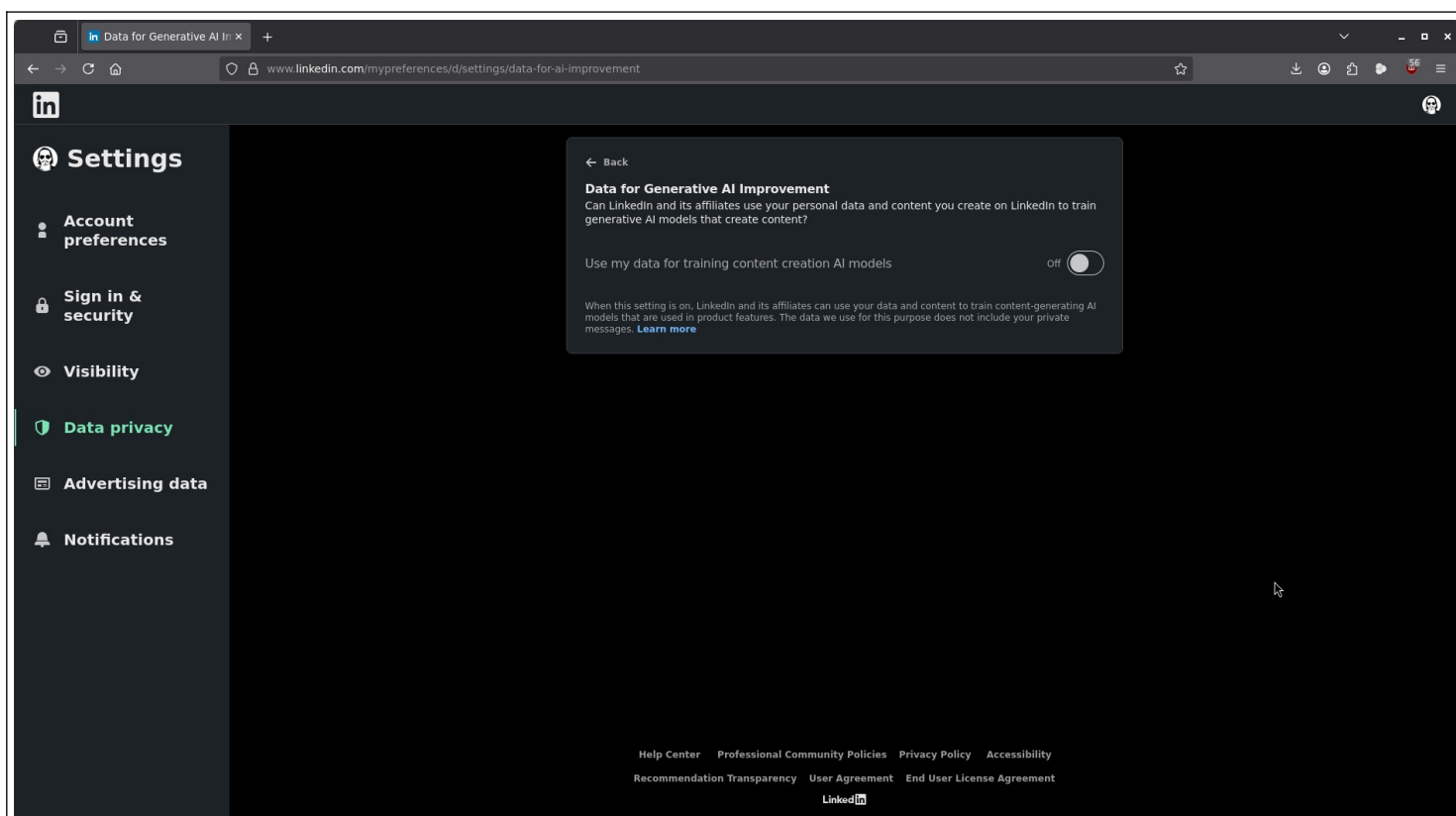
DÉSACTIVATION DES API PARTENAIRES (MICROSOFT/TIERS)



- **Paramètre** : *Visibilité* > Découverte et visibilité du profil hors LinkedIn
- **Valeur** : Désactivé (OFF)
- **Effet** : Coupe le flux de données vers les applications partenaires (principalement l'écosystème Microsoft : Outlook, Teams, Office). Empêche votre profil d'apparaître automatiquement dans le carnet d'adresses ou les fiches de contact d'utilisateurs tiers simplement parce qu'ils ont votre email. Garantit que vos données restent confinées à la plateforme LinkedIn.

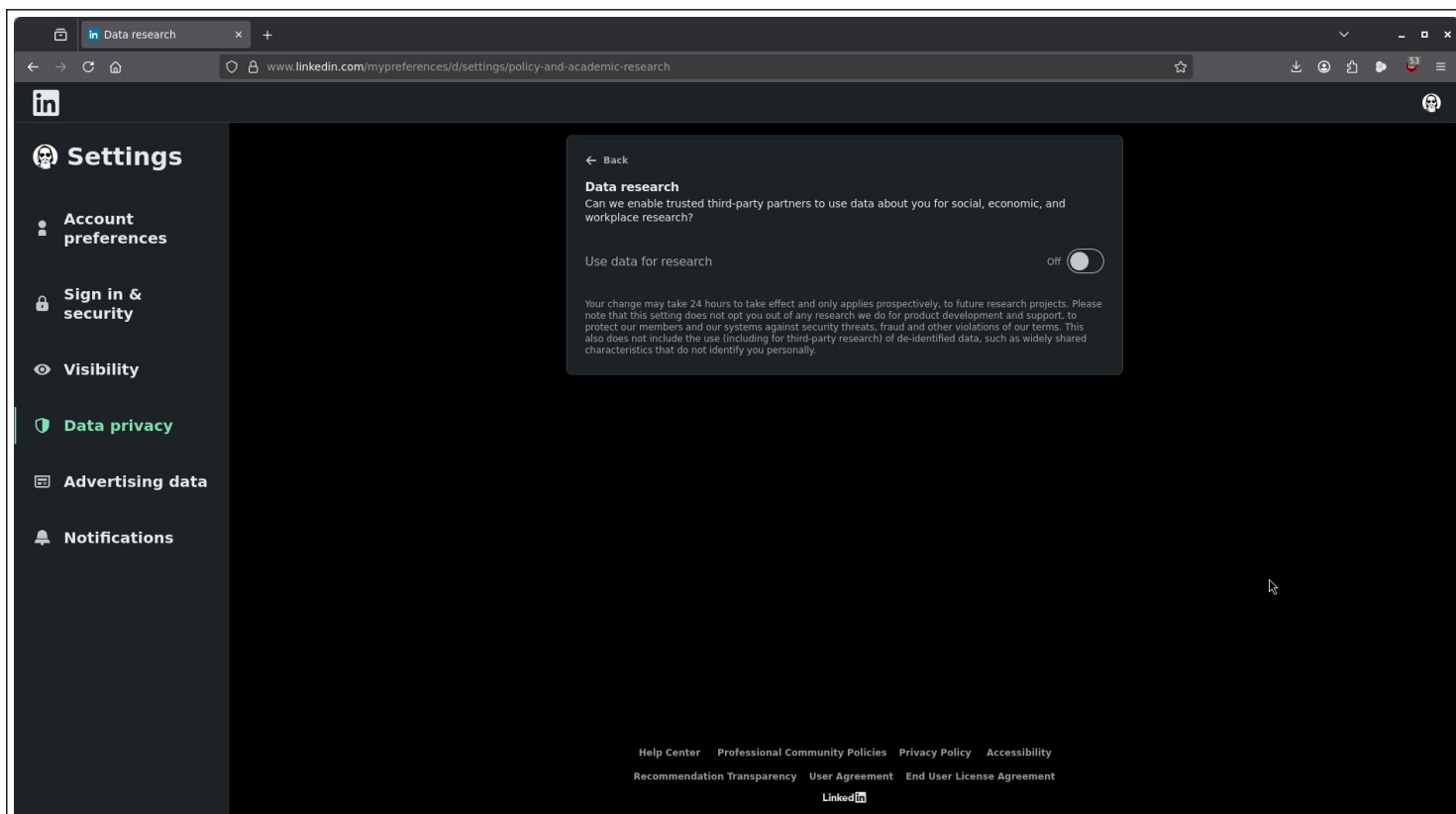
TÉLÉMÉTRIE & EXFILTRATION DE DONNÉES (OPT-OUT)

PREVENTION : INGESTION PAR L'IA (LLM TRAINING)



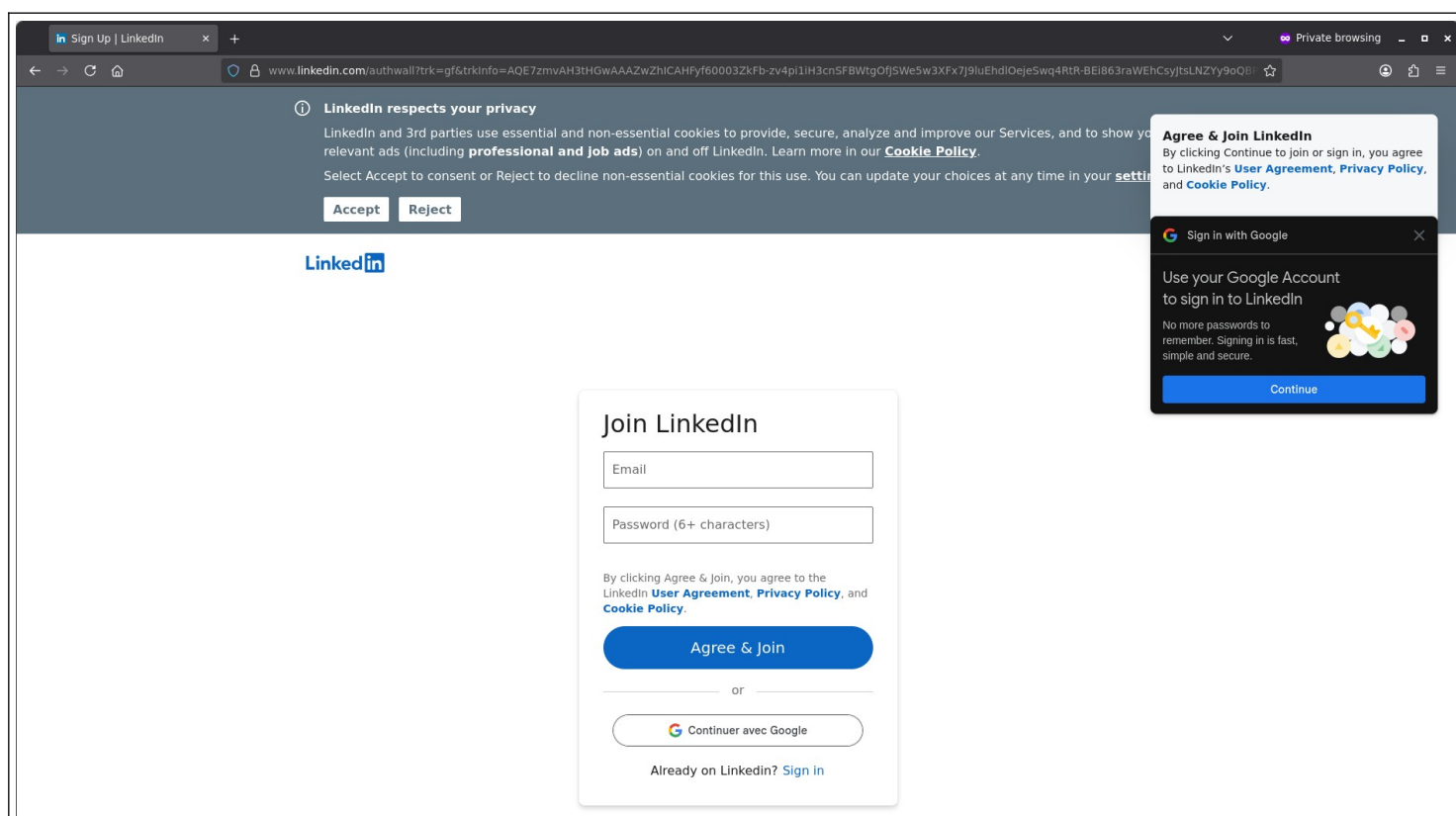
- **Paramètre** : *Visibilité > Données pour l'amélioration de l'IA générative*
- **Valeur** : Désactivé (OFF)
- **Effet** : Interdit formellement à LinkedIn (et par extension Microsoft) d'ingérer vos données personnelles, vos articles et vos posts pour entraîner leurs modèles d'Intelligence Artificielle.

PREVENTION : PARTAGE TIERS & RECHERCHE



- **Paramètre** : *Visibilité* > Études de recherche
- **Valeur** : Désactivé (OFF)
- **Effet** : Interdit à LinkedIn de partager vos données avec des tiers (universités, instituts économiques) pour des études de marché ou sociologiques. Même si ces données sont censées être anonymisées, cela réduit la surface d'exposition de vos informations personnelles hors des serveurs de LinkedIn. Vos données ne servent qu'à vous, pas de cobaye pour les statistiques mondiales.

AUDIT DE CONFORMITÉ (VALIDATION)



- Se déconnecter du compte.
- Taper l'URL directe du profil dans un navigateur en "Navigation Privée".
- **Résultat attendu** : Page de connexion LinkedIn générique (Demande de login). Le profil ne doit pas s'afficher publiquement.