# L’attaque informatique contre l’agence nationale des titres sécurisés et la fuite massive de données relancent le débat sur l’identification obligatoire sur les réseaux sociaux

20/04/2026 à 16h18



*L'Agence nationale des titres sécurisés (ANTS), qui gère les demandes de pièces d'identité, a "détecté un incident de sécurité" le 15 avril qui pourrait impliquer des données de particuliers et de professionnels, a indiqué lundi le ministère de l'Intérieur. #JT20h pic.twitter.com/V5fbPOJIHa*

*— Le20h-France Télévisions (@le20hfrancetele) April 20, 2026*

*L'agence nationale des titres sécurisés n'est donc pas sécurisée.*

*Le tout à quelques mois de demander aux millions de Français d'envoyer une pièce d'identité pour se connecter à Facebook.*

> *Auprès de BFMTV, le ministère de l'Intérieur ne confirme en revanche aucun chiffre. https://t.co/25DJMBVtJq*
>
> *— Raphael Grably (@GrablyR) April 20, 2026*

Le ministère de l’Intérieur a révélé ce lundi qu’un incident de sécurité avait touché Agence nationale des titres sécurisés, organisme chargé notamment des cartes d’identité, passeports et permis de conduire. L’alerte a été détectée le 15 avril.

Selon les premières constatations, des données personnelles d’usagers pourraient avoir été compromises. Sont évoqués les noms, prénoms, adresses électroniques, dates de naissance, identifiants de connexion, et dans certains cas l’adresse postale, le lieu de naissance ou le numéro de téléphone.

Un forum cybercriminel affirme détenir les informations de 19 millions de personnes et proposerait ces données à la vente. Ce chiffre n’est toutefois pas confirmé à ce stade. Le parquet de Paris indique avoir été saisi après un signalement transmis par l’ANTS le 16 avril. Office anti-cybercriminalité mène les investigations.

Le ministère assure que les pièces jointes déposées lors des démarches administratives ne sont pas concernées et que la fuite ne permettrait pas d’accéder illégitimement aux comptes. Les usagers concernés reçoivent une information personnalisée et sont appelés à redoubler de vigilance face au phishing.

BFM