MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #116

Novembre 2025

APPROCHES MALVEILLANTES SUR LES RÉSEAUX SOCIAUX PROFESSIONNELS

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes.

Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

> securite-economique@interieur.gouv.fr

APPROCHES MALVEILLANTES SUR LES RÉSEAUX SOCIAUX PROFESSIONNELS

Désormais considérés comme incontournables dans les processus de recherche d'emploi, d'évolution des parcours de carrière et de mise en relation entre individus, les réseaux sociaux professionnels incitent, par leur fonctionnement, au partage et à la diffusion de nombreuses informations personnelles et professionnelles.

L'usage non-contrôlé des réseaux sociaux professionnels peut exposer leurs utilisateurs, qu'il s'agisse de chercheurs, d'entreprises ou de salariés de tous niveaux de responsabilités, à des approches malveillantes à des fins d'escroqueries, de déstabilisation ou encore de captations d'informations.

Les approches malveillantes effectuées par le biais des réseaux sociaux professionnels sont souvent élaborées à partir des informations partagées et publiées par les cibles elles-mêmes. Les acteurs malveillants à l'origine de ces approches, qui peuvent être issus de réseaux criminels et/ou dirigés par des puissances étrangères, exploitent de façon croissante ces informations facilement accessibles pour cibler leurs démarches.

Ce flash présente différents types d'approches malveillantes sur les réseaux sociaux professionnels qui doivent inciter à la prudence dans les informations partagées et la réponse apportée à toute approche suspecte.

1 UNE START-UP SE VOIT PROPOSER UN INVESTISSEMENT PAR UN INTERMÉDIAIRE AU PROFIL DOUTEUX À LA SUITE D'ÉCHANGES SUR UN RÉSEAU SOCIAL PROFESSIONNEL

Le dirigeant d'une start-up en difficultés financières, évoluant dans un secteur sensible, a été approché sur un réseau social professionnel par un cabinet de conseil étranger déclarant opérer en qualité d'intermédiaire pour un fonds d'investissement.

Le cabinet de conseil a rapidement exprimé le souhait d'obtenir une présentation détaillée des activités de la start-up française dans la perspective d'un investissement que son client pourrait effectuer. Le dirigeant français s'est montré intéressé et a notamment dévoilé un projet de conception d'un nouveau produit. Sans poser davantage de questions, ni demander d'éléments chiffrés sur la santé financière de la start-up, le cabinet a communiqué une offre d'investissement particulièrement intéressante faite par son client.

Toutefois, à l'occasion d'un processus de due diligence initié par le service juridique de la start-up, de nombreuses incohérences ont pu être identifiées : les adresses électroniques des membres du cabinet de conseil ne correspondaient pas à la dénomination du cabinet, l'identité de l'investisseur final n'était pas vérifiable et le mode d'investissement comportait de nombreuses incohérences. La DGSI a également pu confirmer que le cabinet de conseil et le fonds d'investissement ne disposaient pas d'une existence légale et n'étaient référencés dans aucune base de données de leurs pays d'origine.

Le dirigeant de la start-up a mis fin à ses échanges avec ces intermédiaires douteux.

2 UN CHERCHEUR EST APPROCHÉ SUR UN RÉSEAU SOCIAL PROFESSIONNEL PAR UN INDIVIDU PRÉTENDANT QU'UNE CÉLÉBRITÉ INTERNATIONALE SOUHAITE FINANCER SES TRAVAUX

Le responsable d'un centre de recherche a été approché sur un réseau social professionnel par un individu prétendant être le chargé de communication d'une célébrité internationale. Or, le chercheur avait justement partagé sur le réseau social professionnel son intérêt pour cette célébrité.

L'individu a indiqué au chercheur que la célébrité souhaitait financer ses travaux à hauteur de plusieurs millions d'euros en justifiant cette démarche par ses engagements caritatifs. Facilement vérifiables en sources ouvertes, les récentes actions de soutien menées par la célébrité sous forme de dons financiers correspondaient bien au domaine d'activité du centre de recherche et étaient largement relayées sur les réseaux sociaux.

Rassuré par ces éléments identifiés sur Internet et estimant qu'ils crédibilisaient le narratif du prétendu chargé de communication, le chercheur a poursuivi les échanges. Afin de procéder au versement du don, le chargé de communication a demandé au chercheur de régler au préalable une taxe locale correspondant à plusieurs milliers d'euros afin de permettre le versement des fonds. Face à ce mode opératoire classique des escroqueries sur Internet, la DGSI a vivement conseillé au chercheur de mettre définitivement fin à ses échanges avec l'individu.

3 APRÈS AVOIR CRÉÉ UN FAUX PROFIL SUR UN RÉSEAU SOCIAL PROFESSIONNEL, UN INDIVIDU PARVIENT À OBTENIR DES INFORMATIONS SENSIBLES AUPRÈS DE SALARIÉS D'UNE SOCIÉTÉ

Le dirigeant d'une société développant des technologies sensibles a constaté l'existence d'un faux profil sur un réseau social professionnel, créé par un individu se faisant passer pour un comptable de leur entreprise. Ce faux profil a cherché à solliciter un grand nombre de salariés de la société par le biais du réseau social, sans succès, grâce à un message d'alerte rapidement diffusé en interne.

Quelques mois plus tard, un second faux profil a été créé en qualité de salarié de la même société. Ce nouveau profil a réussi à entrer en contact avec plusieurs salariés et à engager des discussions sur des sujets plus ou moins sensibles.

L'un des salariés de l'entreprise, récemment recruté, a fait preuve d'imprudence et a révélé des informations stratégiques relatives au calendrier de développement de certaines activités de l'entreprise et à l'état de ses progrès technologiques.

Le salarié a été mis en garde et sensibilisé par le service sûreté de l'entreprise, et le second faux profil a été signalé à tout le personnel.

Commentaires

L'accroissement des approches malveillantes sur les réseaux sociaux professionnels doit inciter à la plus grande prudence, d'autant plus que ces évènements, perçus au niveau individuel comme isolés, s'inscrivent bien souvent dans une stratégie plus large susceptible de cibler différents profils.

En outre, le besoin évident de discrétion de tout chercheur, salarié ou dirigeant dans leurs recherches d'emploi ou de partenariat peut complexifier l'identification de telles campagnes au sein d'une structure.

Les risques associés aux approches sur les réseaux sociaux professionnels sont souvent sous-estimés par rapport aux approches physiques. En effet, le caractère dématérialisé de ces approches entraîne une baisse de la vigilance chez les personnes ciblées et atténue l'impression de risque encouru. De telles opérations sur les réseaux sociaux professionnels sont pourtant porteuses de nombreux risques à l'image de pertes financières (ingénierie sociale, escroquerie), de captations de données ou encore d'atteinte à la réputation.

Prévenir les risques d'approches sur les réseaux sociaux professionnels

- **Effectuer des sensibilisations régulières sur l'hygiène numérique.**
  Des formations peuvent être animées en interne par le service chargé de la sécurité des systèmes d'information. Le personnel peut également être encouragé à suivre les modules numériques et le guide des bonnes pratiques de l'Agence nationale de la sécurité des systèmes d'information (Anssi). La DGSI effectue également des conférences de sensibilisation sur les risques numériques dans les entreprises et les laboratoires de recherche.

- **Inciter à une utilisation réfléchie des réseaux sociaux professionnels.**
  Il est recommandé d'ajuster les paramètres de sécurité et de confidentialité afin de restreindre l'accès du grand public aux informations du profil. Il est vivement déconseillé aux personnes occupant des postes stratégiques de partager des informations personnelles ou des éléments professionnels trop détaillés sur les réseaux sociaux.

Identifier les profils et sollicitations à risques

- **Analyser les profils.**
  Les profils de création récente, qui présentent un faible nombre de relations professionnelles et un parcours incomplet ou incohérent, sont autant d'indices devant attirer l'attention. De plus, l'emploi d'outils de recherche d'images inversées permet d'identifier celles qui proviennent de banques d'images ou qui auraient été usurpées. Enfin, des vérifications élémentaires sur Internet ou sur le réseau intranet de l'entreprise ou de l'organisme de recherche peuvent permettre de vérifier la fiabilité d'un contact.

- **Rester vigilant sur les échanges avec de nouveaux contacts.**
  Toutes demandes d'informations, personnelles ou professionnelles, formulées par un individu sur un réseau social professionnel doit systématiquement interroger l'utilisateur. L'identité de l'interlocuteur doit impérativement être vérifiée. En l'absence de confirmation de son identité, le téléchargement et l'ouverture de fichiers envoyés doivent être proscrits.

- **Confirmer la réputation de l'individu avant d'entamer une relation d'affaires.**
  Un faux profil créé par un individu cherchant à être crédible et aguerri à l'usage des réseaux sociaux reste parfois difficile à détecter. Il peut être pertinent de chercher à confirmer la réputation de l'individu, notamment auprès d'autres membres de votre réseau, de son propre réseau ou sur Internet. Il peut également s'avérer utile d'effectuer un premier contact, par téléphone ou en visio-conférence.

Adopter la bonne réaction en cas d'approche

- **Ignorer une invitation plutôt que la refuser.**
  Une demande de contact ignorée empêche le faux profil d'envoyer de nouvelles invitations ultérieurement.

- **Signaler le faux profil au sein de son entreprise ou de son organisme de recherche.**
  Les individus ciblés par un faux profil sur un réseau social sont encouragés à signaler l'approche au responsable sûreté, au fonctionnaire de sécurité défense ou à la direction de leur entité. Ceux-ci pourront alors alerter l'ensemble des collaborateurs et détecter d'éventuels cas similaires.

- **Prendre attache avec le service d'assistance du réseau social professionnel.**
  Les services-client des principaux réseaux sociaux professionnels sont particulièrement vigilants vis-à-vis des contenus douteux ou frauduleux et disposent d'une plateforme spécifiquement dédiée aux signalements de faux profils.

- **Contacter la DGSI en cas d'approche par un faux profil.**
  Lorsqu'une société ou un organisme de recherche opérant dans des domaines sensibles détectent des approches suspectes, ils sont encouragés à prendre contact avec la DGSI via l'adresse **securite-economique@interieur.gouv.fr** , qui pourra ensuite les accompagner dans leurs démarches.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité