MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #101

Mars 2024

LES RISQUES ASSOCIÉS AUX ESCROQUERIES PAR USURPATION D'IDENTITÉ

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

LES RISQUES ASSOCIÉS AUX ESCROQUERIES PAR USURPATION D'IDENTITÉ

Les entreprises françaises sont régulièrement ciblées par des escroqueries ou des tentatives d'escroqueries impliquant l'usurpation de l'identité d'un salarié, d'un dirigeant, d'un client ou encore d'un prestataire. Les acteurs malveillants ont recours à des techniques de plus en plus sophistiquées, qui s'appuient notamment sur les technologies de l'intelligence artificielle, rendant plus difficile la détection des usurpations. Le développement rapide du télétravail et la multiplication des échanges professionnels à distance ont également augmenté la vulnérabilité des entreprises face aux fraudes et aux escroqueries.

Ce « flash ingérence » évoque le cas de trois entreprises françaises visées par des tentatives d'escroqueries par usurpation d'identité afin d'obtenir des transferts de fonds ou des informations sensibles.

1 UNE ENTREPRISE FRANÇAISE A ÉTÉ VICTIME D'UNE TENTATIVE D'ESCROQUERIE UTILISANT L'INTELLIGENCE ARTIFICIELLE

Le responsable d'un site industriel d'un groupe français a reçu un courrier électronique lui indiquant que le dirigeant du groupe souhaitait s'entretenir avec lui en visio-conférence, par le biais d'une application de messagerie instantanée.

Au cours de la même journée, le responsable de site a effectivement reçu un appel, et démarré une visio-conférence avec un individu dont l'apparence physique et la voix étaient bien celles du dirigeant du groupe. Insistant sur le caractère très confidentiel de cet appel et sur la confiance qu'il plaçait en son interlocuteur, l'individu usurpant l'apparence du dirigeant a demandé au responsable de site de procéder à un transfert de fonds dans le cadre d'un projet d'acquisition.

Surpris par le caractère inhabituel de cette démarche, le responsable du site a mis un terme aux échanges et a alerté la direction de sa société. Cette dernière lui a confirmé qu'il avait été victime d'une tentative d'escroquerie par hypertrucage (*deepfake*) associant le visage et la voix du dirigeant grâce à l'usage d'une intelligence artificielle.

2 UNE START-UP DE HAUTE TECHNOLOGIE A ÉTÉ VICTIME D'INGÉNIÉRIE SOCIALE ET D'UNE TENTATIVE DE CAPTATION D'INFORMATIONS SENSIBLES

Une start-up française proposant des solutions de gestion innovantes a vu son activité se développer fortement grâce à la signature de plusieurs contrats avec de nouveaux clients, dont certains opèrent dans des secteurs d'activité sensibles.

Dans ce contexte, le service comptable de la start-up a été contacté *via* une fausse adresse électronique, semblable à celle de son dirigeant, afin que des virements bancaires soient effectués. Toutefois, le service comptable, surpris de cette demande non conforme aux procédures habituelles, a remarqué que l'extension de l'adresse électronique de l'expéditeur renvoyait à un pays étranger, et n'a pas procédé au virement.

En parallèle, la start-up a également été ciblée *via* un réseau social professionnel par des individus se faisant passer pour des salariés d'une société partenaire. Ils ont cherché, en vain, à obtenir des informations sensibles, notamment sur des contrats et des appels d'offres en cours.

3 LE FOURNISSEUR D'UN GROUPE STRATÉGIQUE FRANÇAIS A FAIT L'OBJET D'UNE TENTATIVE DE FRAUDE PAR USURPATION DE NOM DE DOMAINE

Le principal fournisseur d'un groupe stratégique français a été contacté par téléphone par un individu se présentant comme un employé du service comptabilité du groupe.

Cet individu a indiqué que le compte de facturation de son groupe avait été piraté, et qu'il était urgent que le fournisseur renvoie toutes les factures à payer sur une nouvelle adresse électronique. Cette adresse, présentée comme une adresse de récupération temporaire, utilisait le nom de domaine de l'ancienne raison sociale du groupe stratégique français.

Face au caractère inhabituel de cette demande, le fournisseur s'est rapproché de ses interlocuteurs habituels au sein du groupe français et a pu établir qu'il s'agissait d'une escroquerie. Aucun document n'a été transmis et l'ensemble des fournisseurs du groupe a été mis en alerte.

Commentaires

Les sollicitations par des individus usurpant l'identité d'une personne morale ou de son dirigeant peuvent cibler tous types de structures : start-up, PME, grand groupe industriel ou encore un laboratoire de recherche. Si les modes opératoires des escroqueries peuvent être anciens, à l'image de l'ingénierie sociale et de la « fraude au président », ils se renouvellent constamment et améliorent sans cesse leur sophistication en s'appuyant sur de nouvelles technologies, à l'image de l'intelligence artificielle, afin de gagner en crédibilité. L'essor et la démocratisation des nouvelles technologies nécessitent une vigilance accrue de la part de tous les salariés d'une société.

Ainsi, en amont de toute transmission d'information ou opération financière demandée par un tiers, l'identité du donneur d'ordre doit faire l'objet d'une vérification rigoureuse, particulièrement lorsque l'action demandée est susceptible d'affecter fortement l'entreprise. Une adresse électronique douteuse, un nom de domaine inhabituel ou une prise de contact singulière doivent constituer des facteurs d'alerte systématiques.

Prévenir les tentatives d'escroquerie :

- **Réserver les noms de domaine s'approchant de celui de son entreprise.**
  Réserver les noms de domaine proches de celui du nom de son entreprise permet d'en bloquer l'utilisation par des acteurs malveillants et de limiter leur usage à des fins d'escroquerie.

- **Avoir un usage prudent des réseaux sociaux professionnels et personnels.**
  Les réseaux sociaux constituent une source précieuse d'informations pour les individus cherchant à cibler des sociétés à des fins malveillantes. La nature des informations partagées sur les réseaux sociaux doit être étudiée avec attention, et toute approche par ce biais doit faire l'objet d'une vigilance renforcée.

- **Faire appliquer les procédures de façon stricte et sans dérogation.**
  Les acteurs malveillants cherchent à tirer profit de la méconnaissance, totale ou partielle, par certains salariés, des procédures internes de contrôle et de sécurité de la société. Le caractère d'urgence, très souvent mis en avant par les acteurs malveillants, ne doit pas constituer une dérogation à ces procédures.

- **Sensibiliser la totalité des salariés de l'entreprise aux risques d'escroquerie.**
  La sensibilisation et la formation restent les moyens les plus efficaces pour se prémunir d'escroqueries, notamment celles faisant appel à l'ingénierie sociale. La DGSI peut être sollicitée afin d'effectuer des conférences de sensibilisation, notamment sur le thème de la protection de l'information sensible à l'ère numérique.

- **Organiser des tests d'intrusion plusieurs fois par an.**
  Ces tests peuvent consister en l'envoi de faux messages piégés aux salariés ou au dépôt de fausses clés USB piégées sur des lieux de passage de l'entreprise. Simples à mettre en œuvre et complémentaires aux actions de sensibilisation, les tests d'intrusion permettent au service informatique ou au service sûreté d'une entreprise d'identifier rapidement ses failles et de faire prendre conscience, à des fins pédagogiques, aux cadres et salariés de leurs propres vulnérabilités.

En cas de suspicion d'escroquerie :

- **Vérifier systématiquement l'origine des demandes qui vous sont adressées.**
  Même si la nature des demandes peut sembler légitime ou habituelle, l'identité de la personne à l'origine de la demande doit toujours être vérifiée. Une adresse électronique peut notamment être falsifiée en changeant quelques lettres du nom de domaine ou en utilisant des caractères en alphabet cyrillique, dont certains sont proches de l'alphabet latin. L'extension de l'adresse (« .fr », « .com », etc.) peut également être modifiée.

- **Mettre rapidement un terme aux échanges avec le demandeur en cas de suspicion d'escroquerie.**
  En cas de suspicion d'usurpation de l'identité de son interlocuteur, il est préférable de mettre rapidement un terme aux échanges, afin de limiter son exposition aux risques de captations de données et d'atteintes à la réputation.

- **Alerter rapidement son service informatique et/ou son service sûreté.**
  La détection d'une tentative d'escroquerie par un salarié d'une entreprise doit rapidement être diffusée au sein de l'entreprise. Il est en effet fréquent qu'une escroquerie vise plusieurs salariés en même temps. La rapidité du signalement est ainsi déterminante. Par ailleurs, en cas d'usurpation d'identité, la personne dont l'identité a été usurpée doit être immédiatement informée afin qu'elle puisse alerter tous ses interlocuteurs habituels.

- **Déposer plainte auprès des services locaux de police ou de gendarmerie.**
  Même en l'absence de tout préjudice, cette démarche permet de signaler ces agissements, de procéder à des recoupements et de caractériser les modes opératoires des auteurs. En cas de préjudice, la plainte sera le préalable à toute procédure d'indemnisation engagée auprès des banques ou des assurances. Il est conseillé de joindre aux déclarations tous les éléments justificatifs (journaux de connexions, messages échangés, coordonnées bancaires, numéros de téléphone, etc.) permettant de prouver l'escroquerie.

- **Contacter la DGSI afin de signaler l'incident.** Le service dispose d'une adresse électronique dédiée aux ingérences économiques : **securite-economique@interieur.gouv.fr.**

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité