OUCH ! Août 2025

La lettre d'information mensuelle de sensibilisation à la sécurité pour vous

Détecter les arnaques à l'emploi en ligne

Le "travail de rêve" de Maria s'est transformé en cauchemar

Maria venait juste de terminer ses études supérieures et avait hâte de commencer son premier emploi à distance à temps plein. Alors, lorsqu'elle a reçu un message sur LinkedIn d'une personne prétendant être un recruteur pour une entreprise technologique internationale, elle était ravie. Le travail était un poste "d'assistant administratif à distance", à 4 000€ par mois, des horaires flexibles et tout équipement fourni. Le recruteur l'a contactée en lui disant que son profil était impressionnant et qu'il souhaitait lui faire rapidement passer un entretien.

L'interview s'est déroulée le jour d'après, via une application de messagerie. Cela paraissait étrange, mais le recruteur a expliqué que l'entreprise était en train de passer à un système complètement à distance. Après 20 minutes d'échange, il a annoncé à Maria qu'elle avait obtenu le poste. Puis sont arrivées les prochaines étapes : elle devait remplir des documents administratifs, notamment son numéro d'identification fiscale, des informations bancaires et une photo de son permis de conduire pour les dossiers des RH.

Quelques jours plus tard, elle a reçu un chèque d'une valeur de 5 000€ pour l'achat d'un ordinateur portable et d'un logiciel. Il lui a été indiqué de déposer le chèque, puis d'envoyer 3 800 dollars par virement bancaire à leur fournisseur d'ordinateurs portables "agréé" et de garder le reste de l'argent pour des dépenses supplémentaires.

Maria a suivi les instructions, mais trois jours plus tard, elle a reçu un message de sa banque. Le chèque était frauduleux. Maria avait non seulement perdu de l'argent, mais elle avait également partagé des informations sensibles qui pouvaient être utilisées pour du vol d'identité. L'excitation d'une opportunité de carrière l'avait empêchée de voir les signaux d'alerte.

Comment l'arnaque à l'emploi fonctionne

Les escroqueries à l'emploi sont efficaces parce qu'elles exploitent vos émotions et votre sentiment d'urgence. Si vous êtes au chômage, sous pression ou simplement excité par une opportunité prometteuse, il est facile de négliger les signes avant-coureurs. Les escrocs utilisent également des emails et des sites web d'apparence professionnelle, voire des numéros de téléphone usurpés, pour paraître légitimes. Ils commencent souvent par créer des offres convaincantes sur les réseaux sociaux, souvent pour des postes à distance ou flexibles. Ils vous contactent ensuite par email ou vous envoient un message pour vous proposer un emploi. Ces escrocs prétendent souvent représenter de vraies entreprises pour gagner votre confiance. Après quelques échanges, les escrocs peuvent organiser un faux entretien par email, message ou application de chat. "L'offre d'emploi" suit peu de temps après.

Leur objectif final est de vous soutirer de l'argent, comme dans le cas de Maria, ou d'obtenir vos informations très sensibles afin de voler votre identité et de commettre des fraudes en votre nom.

Les signes à repérer

Bien que ces escroqueries soient de plus en plus sophistiquées, il existe des signaux d'alarme constants à connaître.

- **Trop beau pour être vrai** : une paie trop élevée, une offre d'emploi sans entretien, des propositions de poste qui sont bien au-dessus de vos qualifications, ou des promesses d'embauche rapide.
- **Une pression d'agir vite** : les escrocs veulent que vous commetiez l'erreur avant d'avoir le temps de réfléchir ou faire des recherches.
- **Une description vague** : si l'offre d'emploi n'est pas claire ou trop générique, méfiez-vous. Les employeurs légitimes fournissent généralement des descriptions détaillées et les qualifications requises.
- **Demandes de paiement** : vous ne devriez jamais avoir à payer en avance la formation professionnelle, la vérification des antécédents ou l'équipement.
- **Des moyens de communication étranges** : méfiez-vous des offres provenant de Gmail, Yahoo ou d'autres domaines de messagerie personnelle similaires. Les recruteurs légitimes utilisent généralement des comptes de messagerie d'entreprise. Attention à l'utilisation excessive des applications de messagerie et à l'absence d'appels téléphoniques ou vidéo. Soyez toujours très prudent lors des communications dont vous n'êtes pas à l'origine.
- **Des informations cachées sur l'entreprise** : si vous ne trouvez pas l'entreprise en ligne, ou si son site web, son profil LinkedIn ou sa présence en ligne vous semblent suspects, soyez prudent.

Comment se protéger

Vous pouvez toujours profiter des offres d'emploi en ligne tout en sécurité. Il suffit de prendre quelques précautions :

- Vérifiez toujours l'identité de l'employeur en effectuant des recherches indépendantes et en visitant le site web officiel de l'entreprise pour confirmer que l'emploi y figure.
- Tenez-vous-en à des sites web de recherche d'emploi et à des réseaux professionnels réputés Il y a moins de chance qu'ils contiennent des arnaques à l'emploi, mais cela peut quand même arriver.
- Ne donnez pas votre numéro d'identification fiscale, vos coordonnées bancaires ou des copies de votre pièce d'identité lors des premières conversations.

En fin de compte, si quelque chose vous paraît bizarre, c'est probablement le cas. Prenez du recul et consultez une personne de confiance. Plus le sentiment d'urgence et l'opportunité sont grands, plus il est probable qu'il s'agisse d'une escroquerie.

Rédacteur invité

Donna Ross est vice-présidente exécutive et responsable de la sécurité de l'information chez Radian. Avec plus de 25 ans d'expérience dans la cybersécurité, la conformité et la gestion des risques d'entreprise dans de nombreux secteurs, notamment la finance, la santé, l'assurance et la fabrication, elle dirige les fonctions de Radian en matière de sécurité de l'information, d'atténuation des risques et de protection de la vie privée, en mettant l'accent sur la stratégie, la résilience et la gouvernance.

Ressources

Les escroqueries à l'investissement fondées sur le romantisme : https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Comment les cybercriminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Reprise de compte : Les prédateurs émotionnels : https://www.sans.org/newsletters/ouch/account-takeovers-emotional-predators/

Traduit pour la communauté par : Juliette Busson