FUTURA

Gare au vol de salaire !

Podcast écrit et lu par Adèle Ndjaki

[Générique d'intro, une musique énergique et vitaminée.]

Votre salaire dans le viseur des arnaqueurs ! C'est le décryptage de la semaine dans *Vitamine Tech*.

[Fin du générique.]

C'est un véritable cauchemar ! Un seul email, et votre salaire disparaît ça [*un claquement de doigts*]! Vous pensez que ça n'arrive qu'aux autres ? Attendez de voir avec quelle facilité des centaines de milliers de personnes sont tombées dans le piège. Bonjour à toutes et à tous, je suis Adèle Ndjaki et aujourd'hui dans *Vitamine Tech*, on vous parle d'une arnaque qui touche de plus en plus de salariés en France : la fraude au virement de salaire.

[Une musique électronique calme.]

Le principe est assez simple, mais terriblement efficace. Des escrocs se font passer pour un employé d'une entreprise, contactent le service RH, souvent par e-mail, en prétendant avoir changé de compte bancaire. Ils fournissent alors un nouveau RIB qui est en réalité le leur. Résultat : au moment du versement de la paie, c'est l'arnaqueur qui touche l'argent à la place du salarié. Le pire c'est qu'environ 200 000 personnes seraient concernées chaque année en France. En fait, ce n'est souvent que quand la personne attend son salaire et ne voit rien arriver qu'elle comprend qu'il y a un souci. Et l'employeur, de son côté, est tout aussi surpris : car il reçoit un mail parfaitement crédible, un message du style : "Bonjour, voici mon nouveau RIB, merci de faire le changement dès que possible." signés du nom du salarié,. Mais comment les escrocs font-ils pour être aussi convaincants ? Eh bien, ils préparent leur coup. Ils collectent des informations précises comme le nom, le poste, l'adresse mail professionnelle... Et pour obtenir ces données, ils utilisent plusieurs techniques comme le phishing (ces fameux mails piégés qui vous poussent à cliquer ou à donner vos identifiants), les faux appels où ils se font passer pour un collègue ou un prestataire, ou encore l'usurpation d'identité, en se faisant passer pour un salarié ou un membre du service RH.

[Virgule sonore, une cassette que l'on accélère puis rembobine.]

[Une musique de hip-hop expérimental calme.]

Comment une arnaque aussi simple peut-elle encore fonctionner aujourd'hui ? Une des explications données, c'est l'évolution du travail lui-même. Eh oui, le monde du travail a changé et ça, les escrocs l'ont bien compris. Avec la généralisation du télétravail qui concerne aujourd'hui près d'un salarié sur trois en France, les échanges internes sont

devenus moins directs, plus numériques, et parfois moins sécurisés. Autre point faible : certaines entreprises externalisent leur service RH, parfois même à l'étranger. Résultat : les relations sont plus impersonnelles, et la vérification des informations peut devenir un peu plus compliquée. C'est donc une porte d'entrée idéale pour les fraudeurs. Pourtant, des garde-fous existent. Certaines entreprises exigent par exemple que tout changement de RIB soit remis en main propre, contre une signature. D'autres demandent une confirmation par appel ou visio, depuis une adresse mail déjà connue. Mais en réalité, ces bonnes pratiques ne sont pas toujours appliquées, surtout en période de paie où les services RH sont souvent sous pression. Au fond, selon les spécialistes, les escrocs ne font pas qu'exploiter des failles techniques, ils sont plutôt à la recherche, en réalité, d'une faille humaine ! L'art de manipuler des gens, vous connaissez ?! Les escrocs jouent sur la confiance, l'urgence, ou même la politesse, pour pousser quelqu'un à agir sans trop réfléchir. Ce qui n'est pas très étonnant. Alors oui, les mails peuvent être crédibles, les procédures parfois floues, mais face à ça, une seule vraie défense existe : la vigilance à tous les niveaux. Et en cas de fraude au virement de salaire, la première chose à faire, c'est de réagir et très vite. Une enquête interne doit être lancée pour comprendre comment la fraude a pu se produire : analyser les échanges, identifier l'origine du mail frauduleux, vérifier les adresses utilisées, et détecter d'éventuelles autres tentatives. Si des données personnelles ont été compromises, alors l'entreprise a une obligation légale importante : elle doit alerter la CNIL, la commission nationale chargée de protéger les données personnelles, dans un délai de 72 heures. Il faut aussi informer les personnes concernées, leur expliquer quelles sont les données touchées, les risques potentiels, et les mesures déjà prises pour y répondre. Mais rien n'est perdu d'avance. Pour limiter les risques à l'avenir, la CNIL recommande plusieurs actions concrètes comme restreindre la diffusion des informations personnelles des employés, notamment en ligne ou dans les supports de communication externes ; Renforcer les procédures internes (tout changement de coordonnées bancaires doit passer par un portail RH sécurisé, accessible uniquement via le réseau interne ou un VPN) ; Exiger une vérification systématique, en présentiel ou par visio, surtout si la demande ne vient pas d'une adresse professionnelle connue ; Mais le plus important c'est qu'il faut que ces règles soient bien connues de tous les salariés parce qu'en matière de fraude, la meilleure défense, c'est la prévention.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de *Vitamine Tech*. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le dernier épisode de Futura Récap' dans lequel Melissa Lepoureau vous présente les 5 actus scientifiques de la semaine à ne surtout pas rater ! Pour le reste, je vous remercie pour votre fidélité à Vitamine Tech, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

[*Un glitch électronique ferme l'épisode.*]