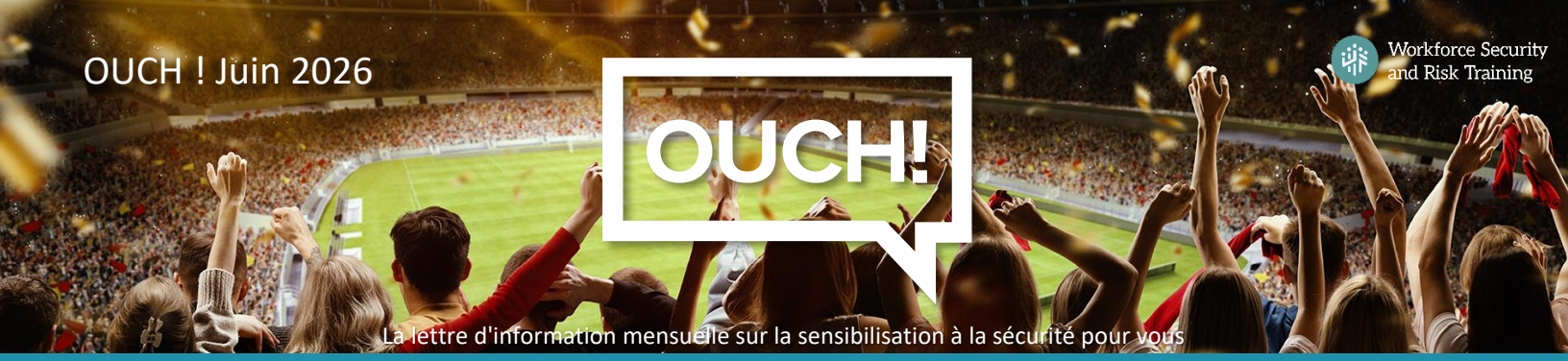

Workforce Security and Risk Training

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

La fièvre de la Coupe du monde : ne laissez pas les arnaqueurs gagner

La chance d'une vie - volée

Diego avait attendu des années pour ce moment. La Coupe de monde 2026 était enfin là, et pour la première fois il avait enfin le temps et l'argent pour s'y rendre. Lorsqu'il a vu une publication sur les réseaux sociaux proposant "des tickets dernière minute" pour un match complet, il s'est senti chanceux. Le vendeur affirmait travailler avec un distributeur autorisé et partageait même ce qui semblait être un e-mail de confirmation de la part des organisateurs de la compétition.

Le prix était élevé mais pas choquant. Le vendeur l'a averti que les tickets étaient presque "tous vendus", et que plusieurs acheteurs étaient intéressés. Comme Diego ne voulait pas rater sa chance, il a payé les tickets via une application de paiement instantané.

Les tickets ne sont jamais arrivés. Et le compte du vendeur a disparu. Le site dont il parlait dans les messages s'est fermé dans les jours qui ont suivi. Diego n'avait pas seulement perdu de l'argent, il était aussi passé à côté de l'opportunité d'une vie de se rendre à l'événement.

Pourquoi les grands événements sportifs attirent les arnaqueurs

Les événements mondiaux comme la Coupe du monde constituent un terrain propice aux arnaques. Il y a une demande massive de tickets, de trajets, de marchandise et d'accès de diffusion. Les gens sont excités, investis émotionnellement et agissent souvent rapidement. La combinaison de l'urgence et de l'émotion aide les attaquants à manipuler leurs victimes.

Les criminels connaissent le comportement humain. Ils savent que lorsqu'un bien se fait rare, les gens agissent plus rapidement. Ils savent que lorsque des millions de personnes recherchent la même chose, les faux sites et les messages d'hameçonnage se fondent facilement dans la masse. Les attaquants exploitent constamment l'urgence, la peur et l'excitation pour pousser les gens à prendre des décisions rapides qui mènent à une perte financière ou personnelle.

À quoi ressemblent ces attaques ?

La vente de faux billets : les escrocs créent des sites ou des publications sur les réseaux sociaux d'apparence professionnelle qui semblent légitimes. Certains copient les marques et logos officiels, tandis que d'autres achètent des publicités en ligne afin que leurs sites frauduleux apparaissent en tête des résultats de recherche. Les victimes payent pour des tickets qui ne sont jamais envoyés, ou recoivent des tickets dématérialisés qui ne marchent pas à l'entrée du stade. Souvent, les escros demandent un paiement par virement, en cryptomonnaie ou via des applications de paiement entre particuliers, qui sont des moyens difficiles à annuler.

Les messages urgents : vous recevez des e-mails ou des messages affirmant venir des organisateurs de l'événement, des lignes d'avion, des hôtels ou des services de diffusion. Ces messages indiquent souvent que l'achat de votre billet a échoué ou que votre réservation sera annulée si vous ne confirmez pas le paiement immédiatement. Ces messages sont conçus pour paraître urgents et crédibles afin d'inciter l'acheteur à agir rapidement, sans réfléchir de manière rationnelle. Le lien mène en fin de compte à une fausse page de connexion conçue pour voler vos identifiants. Tout comme dans d'autres campagnes frauduleuses, les attaquants misent beaucoup sur le sentiment d'urgence et la crainte de perdre l'accès.

Les arnaques de streaming : les criminels créent de fausses plateformes offrant "une retransmission en direct gratuite" des matchs. Pour regarder, vous devez créer un compte et entrer vos détails de paiement. Et plutôt que pouvoir voir le match, vous avez installé un maliciel sans le savoir, qui vous a volé vos informations financières.

La mauvaise marchandise : même la marchandise et les cadeaux deviennent un outil d'exploitation. Par exemple, les faux concours peuvent promettre des maillots officiels ou des prix exclusifs en échange d'informations personnelles. Les boutiques en ligne proposant des contrefaçons peuvent vendre des articles à prix réduit, mais elles envoient soit des contrefaçons de mauvaise qualité, soit rien du tout.

Comment vous protéger

La bonne nouvelle, c'est qu'il est possible d'éviter ces arnaques si vous prenez le temps de réfléchir et de vérifier avant d'agir. N'achetez des billets, des trajets et des produits dérivés qu'auprès de partenaires officiels ou de vendeurs réputés. Au lieu de cliquer sur les liens contenus dans les e-mails, les publications sur les réseaux sociaux ou d'autres sources non vérifiées, saisissez directement l'adresse du site officiel dans votre navigateur ou utilisez une application mobile de confiance. Ajoutez les sites fiables à vos favoris une fois que vous les avez vérifiés, afin de toujours revenir au bon endroit.

Soyez particulièrement vigilant face à tout message qui vous pousse à agir immédiatement. Les arnaqueurs dépendent de l'urgence. Si vous recevez un message d'avertissement concernant une réservation annulée ou un paiement qui n'a pas abouti, ne cliquez pas sur le lien. Contactez plutôt directement l'entreprise en utilisant les coordonnées vérifiées.

Enfin, méfiez-vous des méthodes de paiement inhabituelles. Toute demande concernant des cryptomonnaies, des virements bancaires ou des cartes-cadeaux doit immédiatement susciter la méfiance. Les vendeurs sérieux exigent rarement ces modes de paiement. De plus, les principales cartes de crédit ou les systèmes de paiement en ligne reconnus, tels que PayPal, vous offrent des garanties supplémentaires lors de vos achats.

Faites preuve de prudence dans vos achats et vos actions ; les cybercriminels profitent du fait qu'ils poussent les gens à commettre des erreurs dans la précipitation.

Rédacteur invité

Karyn DiMassa est une spécialiste en cybersécurité, audit interne, gestion des risques et des contrôles, dotée d'une expertise dans les domaines suivants : gestion des incidents, reprise après sinistre et gestion de la continuité des activités ; évaluations de la cybersécurité, analyse des lacunes et mesures correctives ; identification, évaluation et correction des risques et des contrôles internes ; gestion des risques d'entreprise ; et audit interne.

Ressources

Comment les cyber-criminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Top trois des manières dont les cyber-attaquants vous ciblent : https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you
Comment les cyber-criminels volent votre mot de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords
Traduit pour la communauté par : Juliette Busson

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : https://www.sans.org/newsletters/ouch