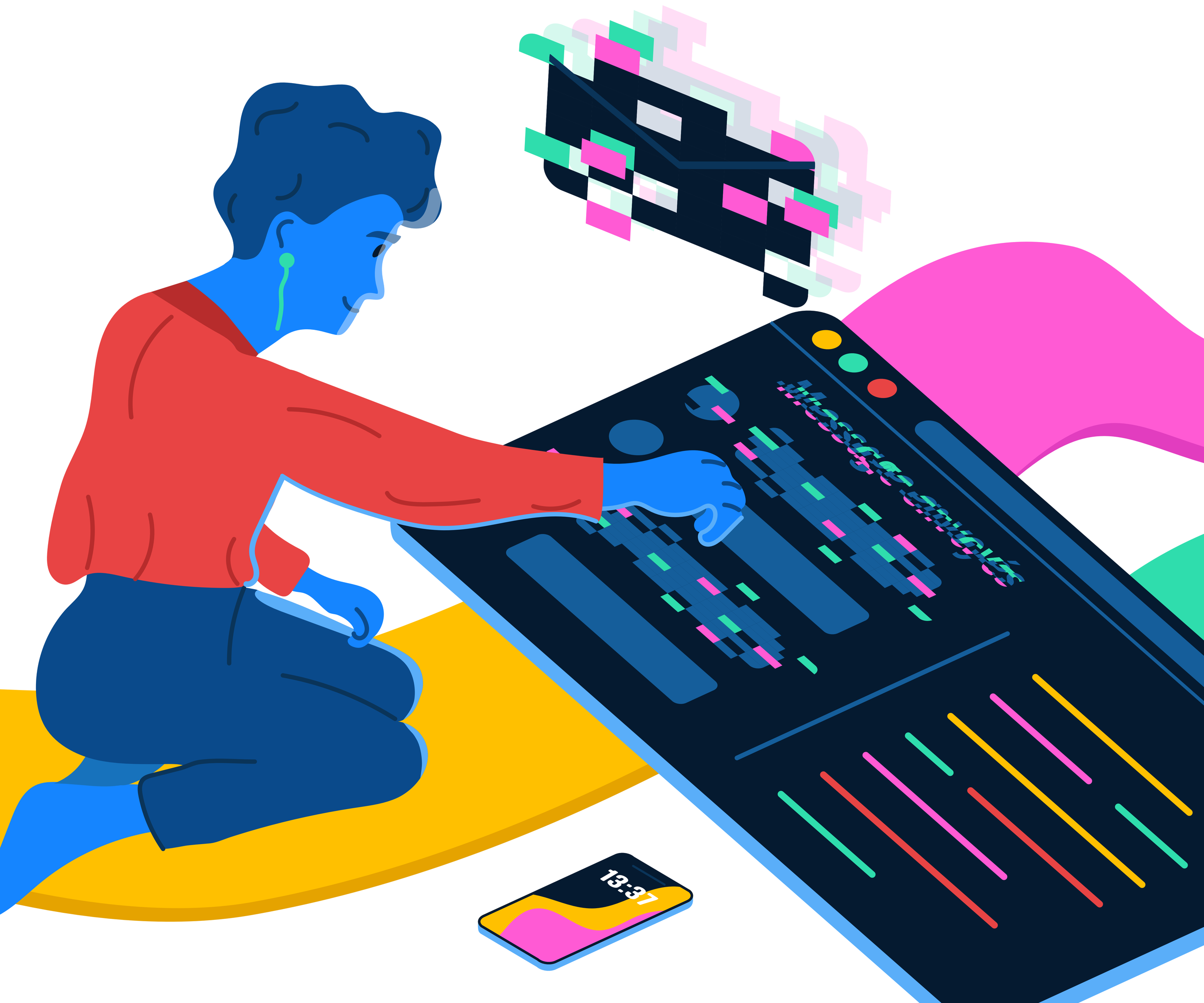
Escroquerie aux données bancaires en période estivale : comment réagir ?

CNIL.

À l’approche de la saison estivale, Jérôme réserve et paie son séjour dans un hôtel sur une plateforme de réservation en ligne. La veille du départ, il reçoit un message urgent de l’hôtel lui demandant de refournir ses informations bancaires en cliquant sur le lien présent, car le premier paiement n’est pas passé.

Trouvant la situation étrange, Jérôme vérifie l’adresse de l’expéditeur : c’est bien celle de la plateforme utilisée dans la confirmation de réservation. Dans le doute, il appelle l’hôtelier en question. Celui-ci lui confirme que tout est déjà réglé et qu’il n’aurait pas dû recevoir ce message de la plateforme de gestion.

Après avoir raccroché, l’hôtelier se connecte à la plateforme et s’aperçoit d’une anomalie dans l’onglet « messages envoyés » : ceux-ci disparaissent sans action de sa part.



L’hôtelier contacte le support de la plateforme. Le Centre des Opérations de Sécurité détecte des connexions ne provenant pas de l’adresse IP de l’établissement, mais cela ne semble pas lié à une attaque massive sur son système d’information. Cependant, une mauvaise gestion des mots de passe a compromis le compte utilisateur lié à la plateforme.

Le prestataire retrouve les traces des actions effectuées sur la plateforme, il est ainsi possible de savoir quels clients les attaquants ont pu cibler. L'hôtelier adresse un message d'information et de sensibilisation aux personnes concernées sous forme de questions/réponses. Enfin, il sensibilise son personnel à la protection des données.