THE POWER OF BEING UNDERSTOOD
AUDIT | EXPERTISE | CONSEIL

Insights

Nos experts vous informent

L'ESSENTIEL A RETENIR

Risque de fraude en période estivale : comment rester vigilant ?

Quelques exemples de fraudes les plus courantes

FRAUDE AU PRÉSIDENT

Une personne mal intentionnée contactant le service comptabilité en se faisant passer pour le Président ou un Administrateur, en se montrant insistant pour déclencher un virement d'un montant élevé, en urgence.

FRAUDE AU FOURNISSEUR

Des escrocs se faisant passer pour un fournisseur et demandant de procéder à un changement de RIB

HAMEÇONNAGE ET HARPONNAGE

Un lien ou une pièce jointe frauduleuse dans un e-mail imitant celui d'une société (« phishing »), et déclenchant l'installation d'un logiciel espion via un fichier exécutable.

RANSOMWARE

Un type particulier de logiciel malveillant qui, une fois installé (via un lien ou une pièce jointe dans un mail par exemple), chiffre les données qu'elle abrite pour les rendre inaccessibles.

FRAUDE AU FAUX TECHNICIEN

L'usurpation d'identité d'un technicien informatique de votre banque (pour effectuer un test sur des coordonnées bancaires) ou de votre prestataire informatique pour payer un pseudo-dépannage informatique.

AUTRES

Vol de données, déni de service, vishing, etc.

Nos conseils pour se prémunir contre le risque de fraude

Faites attention aux messages douteux
Objet plausible mais vague, expéditeur avec une adresse mail de faussaire (.com au lieu de .fr), lien cliquable, pièce jointe, fautes d'orthographes et syntaxe surprenante.

Vérifiez l'authenticité des demandes financières
Soyez prudent lorsqu'il s'agit de paiements, de transferts ou de demandes de modification des coordonnées bancaires. En cas de doute, contactez directement la personne ou l'organisation concernée en utilisant des coordonnées déjà enregistrées et ne répondez jamais à des e-mails non sollicités demandant des informations sensibles.

Sensibilisez vos collaborateurs
Assurez-vous que tous les collaborateurs de votre entreprise sont informés des risques de fraude et des bonnes pratiques de sécurité.

Renforcez les procédures internes
Mettez en place des contrôles internes solides pour réduire les risques de fraude comme des approbations multiples pour les transactions financières importantes et une séparation claire des tâches pour éviter les conflits d'intérêts

Surveillez vos comptes et vos transactions
Effectuez régulièrement des vérifications détaillées de vos comptes bancaires et des transactions pour détecter rapidement toute activité suspecte.

Protégez vos informations sensibles
Assurez-vous que vos données confidentielles sont sécurisées en utilisant des solutions de protection appropriées (pare-feu, antivirus, systèmes de détection des intrusions) et en mettant en place une politique de gestion des mots de passe adéquate.

RSM vous accompagne

Chez RSM, nous accompagnons nos clients dans l'évaluation et la maîtrise des risques de fraude et d'escroquerie. Nous avons la capacité de vous proposer des solutions rapides et efficace en matière de prévention : diagnostic flash, formation des collaborateurs, sécurisation des processus, etc.

Thomas DE GIGORD
Directeur Pôle Risque et Performance

STD : +33 (0)4 72 69 19 19
MOB : +33 (0)6 35 22 58 00
Mail : thomas.degigord@rsmfrance.fr

2b rue Tête d'Or - 69006 Lyon