Fraude par compromission d'adresse e-mail professionnelle

Avertissement de sécurité destiné aux fournisseurs.

MSD traite les fraudes et la protection des informations avec le plus grand sérieux.

Veuillez noter que, du fait de notre utilisation croissante des communications virtuelles, les cas de compromission d'adresse e-mail professionnelle (Business Email Compromise, BEC) sont en augmentation. Dans un scénario de BEC, l'acteur malveillant utilise l'adresse e-mail professionnelle et d'autres moyens de communication électronique pour usurper l'identité d'un cadre dirigeant, d'un employé ou autre personne responsable.
Des demandes de paiement ou d'accès aux informations relatives au registre du personnel ou au formulaire fiscal W2 (États-Unis uniquement) sont ensuite émises de manière frauduleuse au nom d'une entreprise.

À savoir

MSD s'engage à protéger votre entreprise et vos informations bancaires. Conformément à notre service de protection des données personnelles, à nos processus et directives concernant les technologies de l'information et conformément aux réglementations locales et régionales, notre personnel formé applique des processus et des contrôles stricts à la collecte, la validation et la capture des données, en mettant en œuvre de nombreux points de contrôle et des audits réguliers de nos procédures et de nos pratiques.

Pour mieux protéger votre entreprise :

- Utilisez des canaux secondaires ou une authentification à deux facteurs, pour vérifier de manière indépendante les demandes de modification des informations relatives à un compte.
- Assurez-vous que les adresses URL contenues dans les e-mails sont bien associées à l'entreprise dont elles se réclament.
- Soyez vigilants pour repérer les liens hypertexte qui contiennent une version mal orthographiée d'un nom de domaine réel.
- Vérifiez que l'adresse e-mail utilisée pour envoyer un message correspond bien à celle de l'expéditeur annoncé, en particulier lorsque vous utilisez un appareil mobile ou portable.
- Créez des filtres pour votre système de détection d'intrusions de manière à ce qu'ils puissent repérer et signaler les e-mails dont l'extension ressemble à celle du courriel de l'entreprise. Par exemple, si l'adresse ceo@abc_company.com est légitime, un e-mail provenant de ceo@abc-company.com devrait être signalé comme frauduleux.
- Surveillez régulièrement les comptes financiers et recherchez toute irrégularité, comme des dépôts manquants.
- Gardez tous les correctifs logiciels activés et maintenez tous vos systèmes à jour.

- Assurez-vous que les paramètres des ordinateurs de vos employés leur permettent d'afficher l'intégralité des extensions des adresses e-mail.
- Prenez note des coordonnées de contact de votre Centre de résolution local et alertez-le si vous pensez être victime d'une BEC concernant Merck ou MSD ; sinon, contactez vos services de police locaux.

En dehors des États-Unis et du Canada, Merck est connu sous le nom de MSD.