FRAUDE CEO

La fraude CEO consiste à piéger un collaborateur habilité à effectuer les paiements de l'entreprise, le but étant qu'il paie une fausse facture/réalise un transfert non autorisé.

COMMENT CELA SE PASSE-T-IL ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société (par ex. CEO ou CFO).

Il connaît bien l'organisation.

Il réclame un paiement urgent.

Ses expressions courantes : « confidentialité », « la société vous fait confiance », « pour l'instant indisponible ».

Il fait référence à une situation sensible (par ex. contrôle fiscal, fusion, acquisition).

Le collaborateur est invité à ne pas respecter les procédures d'autorisation prévues.

Les instructions visant la procédure pourront être données plus tard, par courriel/un tiers.

L'employé transfère les fonds vers un compte géré par le fraudeur.

Sont souvent demandés des paiements internationaux vers des banques en dehors de l'Europe.

QUELS SONT LES SIGNES ?

- Courriel/appel non sollicités
- Contact direct d'un dirigeant avec lequel vous n'êtes normalement pas en contact
- Demande de confidentialité absolue
- Pression et sentiment d'urgence
- Demande inhabituelle contraire aux procédures internes
- Menaces ou flatteries/promesses de récompense inhabituelles

QUE FAIRE ?

EN TANT QUE SOCIETE

Soyez attentif/ve aux risques et assurez-vous que les collaborateurs sont informés/conscients.

Invitez votre personnel à la prudence concernant les demandes de paiement.

Prévoyez des protocoles internes pour les paiements.

Prévoyez une procédure pour vérifier l'authenticité des demandes de paiement reçues par courriel.

Prévoyez des routines de notification pour contrer les fraudes.

Contrôlez les informations publiées sur le site de votre société, limitez-les et soyez prudent/e vis-à-vis des médias sociaux.

Actualisez et améliorez la sécurité technique.

Contactez toujours la police en cas de tentative de fraude, même si vous n'êtes pas tombé/e dans le piège.

EN TANT QUE COLLABORATEUR

Appliquez strictement les procédures prévues pour les paiements et les acquisitions. **Ne sautez aucune étape et résistez à la pression.**

Vérifiez toujours attentivement les adresses courriel lorsque vous traitez des informations sensibles/paiements.

En cas de doute sur un ordre de transfert, **consultez un collègue compétent.**

N'ouvrez jamais de liens/documents attachés douteux reçus par courriel. Soyez très vigilant/e lorsque vous vérifiez vos courriels privés sur un pc de la société.

Limitez les informations et soyez attentif/ve en ce qui concerne les médias sociaux.

Ne partagez jamais d'informations sur la hiérarchie dans l'entreprise, la sécurité ou les procédures.

Si vous recevez un courriel ou appel douteux, informez toujours votre département IT.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · Politie Police · febelfin · Cyber Security Coalition · #CyberScams