FRAUDE AU PRÉSIDENT

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

COMMENT ÇA MARCHE ?

Par téléphone ou courriel, un fraudeur se fait passer pour un dirigeant de la société ou un directeur administratif et financier.

Les fraudeurs connaisssent bien l'entreprise ciblée.

L'arnaqueur réclame un paiement urgent.

L'arnaqueur demande des paiements internationaux vers des banques en dehors de l'Europe.

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

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

Les expressions courantes utilisées: «confidentialité», «la société vous fait confiance».

Ils font référence à une situation sensible (par ex. contrôle fiscal, fusion, acquisition).

COMMENT DÉTECTER L'ARNAQUE ?

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

QUE FAIRE EN CAS DE TENTATIVE D'ESCROQUERIE ?

SI VOUS ÊTES DIRIGEANT/E D'UNE SOCIÉTÉ

Soyez attentif/ve aux risques et assurez-vous que les collaborateurs soient conscients de ce type de risque.

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.

Ne dérogez jamais aux procédures que vous avez mises en place.

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 du process de validation d'un paiement.

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

SI VOUS ÊTES COLLABORATEUR

Appliquez strictement les procédures de sécurité 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 ordinateur de la société.

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

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

Si vous recevez un courriel ou appel douteux, informez toujours votre service informatique.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLICE NATIONALE | FÉDÉRATION BANCAIRE FRANÇAISE

#CyberScams