LES FRAUDEURS DE PLUS EN PLUS CRÉATIFS !

Les paiements étant de plus en plus sécurisés, les fraudeurs sont contraints de faire preuve de plus en plus de créativité. Plutôt que de violer la sécurité des ordinateurs, les escrocs s'efforcent à présent d'abuser de la confiance des employés. Prenez tout particulièrement garde aux 2 techniques de fraude expliquées ci-dessous.

La fraude « CEO »

De quoi s'agit-il ?

Dans un premier temps, un malfaiteur téléphone ou envoie un e-mail à des entreprises en se faisant passer pour un auditeur ou un réviseur chargé d'analyser les processus de paiement internes. Dans d'autres cas, il s'agit soi-disant d'une étude pour le compte des pouvoirs publics. Cela leur permet de répertorier les employés habilités à effectuer des paiements.

Dans un deuxième temps, ils contactent les employés qui ont l'autorisation de signer des paiements importants en se faisant passer pour le CEO ou le CFO, appelant souvent d'un siège situé dans un autre pays, et évoquent le rachat d'une entreprise étrangère ou un contrôle fiscal. Dans tous les cas, un paiement urgent est demandé. Celui-ci doit rester strictement confidentiel : personne ne peut être au courant.

L'opération frauduleuse est réussie lorsque l'employé effectue finalement le paiement demandé. Le fraudeur peut alors retirer l'argent du compte étranger et disparaître sans laisser de traces.

Conseils

- Informez les collaborateurs de votre entreprise de l'existence de cette technique de fraude.
- Ne répondez jamais aux questions d'inconnus qui tenteraient de savoir qui effectue les paiements dans votre entreprise.
- Soyez particulièrement attentif dans les situations suivantes :
  - Si la transaction est présentée comme étant urgente et confidentielle ;
  - Si les personnes qui disposent des compétences de signature ne sont pas toutes présentes ;
  - Si la transaction est adressée par mail et qu'elle fait suite à une conversation téléphonique avec un avocat, un notaire, un consultant… avec lequel le collaborateur de l'entreprise n'a jamais eu de contact dans le passé ;
  - Si le CEO communique subitement qu'il peut être contacté via une autre adresse e-mail.
- Faites en sorte que les procédures normales soient toujours suivies.

La fraude aux factures

De quoi s'agit-il ?

De vraies factures sont interceptées lors de leur expédition chez le client. Elles sont remplacées par des factures identiques sur lesquelles seul le numéro de compte change. Le client qui reçoit la facture effectue donc le paiement sur le numéro de compte frauduleux. Les fonds récoltés sur ce compte font généralement l'objet d'un retrait immédiat ou sont envoyés à l'étranger.

Une technique équivalente existe également pour des factures envoyées par mail au départ d'une adresse e-mail piratée ou qui ressemble à la vraie adresse.

Enfin, dans certains cas, il s'agit tout simplement de fausses factures qui font référence à des prestations de services inexistantes. Étant donné leur montant peu élevé, la personne chargée du paiement des factures n'effectue que très peu voire aucun contrôle.

Conseils

Les contrôles suivants peuvent être réalisés :

- Contrôle du numéro de compte sur la base de paiements réalisés dans le passé. En cas de doute, prenez toujours contact avec le fournisseur sur la base des données de contact mentionnées sur d'anciens documents et non sur la base des données indiquées sur la facture présumée frauduleuse.
- Est-ce que le montant et le délai de paiement correspondent à ce qui est mentionné sur le bon de commande ? Ici également, prenez contact avec le fournisseur en cas de doute.