Liste de vérification à l'intention en cas de fraude

Dans quelle mesure votre pratique est-elle sécuritaire?

Cochez tous les énoncés qui s'appliquent à votre pratique.
Plus vous cochez de cases, plus votre pratique comporte des aspects qui demandent votre attention.

- ☐ Nos systèmes de courriel ne sont pas dotés de contrôles de sécurité rigoureux ni d'une surveillance centralisée.
- ☐ Les instructions de télévirement ou de paiement sont confirmées par courriel seulement.
- ☐ Les changements de dernière minute apportés aux renseignements sur les paiements ne sont pas vérifiés de façon indépendante.
- ☐ Les demandes de paiement urgentes ou sous pression ne sont pas régulièrement remises en question.
- ☐ Les renseignements sur l'expéditeur de courriels et les domaines ne sont pas systématiquement examinés pour déceler des variations subtiles.
- ☐ Les employés ne savent pas comment reconnaître les tentatives d'hameçonnage ou de redirection de courriels.
- ☐ Les liens et les pièces jointes sont parfois ouverts sans vérification indépendante.
- ☐ Les numéros de confirmation des paiements ne sont pas toujours obtenus ou conservés.
- ☐ La réception des fonds transférés n'est pas confirmée régulièrement auprès du destinataire visé.
- ☐ Il n'y a pas de plan d'intervention clairement documenté en cas de fraude ou de compromission du système.

FCT

Liste de vérification à l'intention en cas de fraude

Comprendre les risques et la façon de les gérer

1. Renforcer les contrôles de sécurité des courriels
Les comptes de courriel sont un point d'entrée courant pour la fraude. L'utilisation de systèmes dotés de mesures d'authentification, de surveillance et de reprise solides peut contribuer à réduire le risque d'accès non autorisé. Examiner régulièrement les paramètres de compte, y compris les règles de transmission, peut aider à repérer les changements non autorisés.

2. Vérifier les instructions de paiement par l'intermédiaire d'une méthode de confiance
Confirmer les instructions de télévirement en composant un numéro de téléphone de confiance (provenant d'une source indépendante plutôt que d'un courriel) peut aider à prévenir l'usurpation d'identité et les tentatives de redirection.

3. Traiter les changements de dernière minute comme un risque plus élevé
Apporter des changements aux renseignements sur les paiements tard dans le processus constitue une tactique frauduleuse fréquente. Le fait de ralentir pour vérifier de façon indépendante ces demandes peut contribuer à réduire le risque de fraude.

4. Ralentir les demandes urgentes
Les tentatives de fraude reposent souvent sur la création d'une pression pour agir rapidement, surtout lorsque les échéances des transactions approchent. Prévoir du temps pour vérifier les demandes peut aider à prévenir les décisions précipitées concernant les fonds.

5. Examiner attentivement les adresses courriel et les domaines
Les messages frauduleux s'appuient souvent sur de petites variations dans les adresses courriel ou les domaines. Vérifier l'adresse complète de l'expéditeur (pas seulement le nom affiché) peut vous aider à repérer de potentielles usurpations d'identité.

6. Favoriser la sensibilisation et la formation du personnel
Une formation régulière aide les employés à reconnaître les tentatives d'hameçonnage, l'usurpation d'identité, les problèmes de vérification et les tentatives de redirection de courriels, y compris la réticence à parler au téléphone ou les incohérences dans les documents.

7. Vérifier les liens ou les pièces jointes avant de les ouvrir
Les liens et les pièces jointes ne doivent être ouverts qu'après avoir confirmé l'identité de l'expéditeur au moyen d'une méthode de communication connue et fiable, surtout lorsqu'il est question de renseignements financiers.

8. Obtenir et conserver les numéros de confirmation des paiements
Les numéros de confirmation des paiements aident à confirmer que les fonds ont été envoyés et reçus comme prévu. Autrement, il pourrait y avoir de l'incertitude quant à savoir si les fonds sont définitifs ou s'ils ont été réaffectés.

9. Confirmer la réception des fonds dans la mesure du possible
Confirmer que le destinataire prévu a reçu des fonds transférés ajoute une étape de vérification supplémentaire et aide à cerner les problèmes rapidement.

10.Établir un plan d'intervention clair
Un plan d'intervention documenté –indiquant avec qui communiquer, comment sécuriser les systèmes et quand faire appel au soutien des TI– peut aider à limiter l'incidence d'une fraude présumée.

Contexte supplémentaire

Les mesures de suivi ou les questions de couverture liées à la fraude par télévirement peuvent dépendre des circonstances de la transaction et du fait que les fonds ont été vérifiés au moyen des meilleures pratiques financières. Dans certains cas, des étapes de confirmation supplémentaires peuvent être requises.