CONSEILS SUR LA CYBERSÉCURITÉ ET LA PRÉVENTION DES FRAUDES

Les attaques par hameçonnage et autres formes de cyberfraude occasionnent de plus en plus souvent des pertes pour les avocats. L'évolution constante de la technologie et des stratagèmes des fraudeurs nécessite une vigilance et une adaptation permanentes. Voici quelques conseils pour la protection de vos renseignements et de ceux de vos clients, et pour la prévention des fraudes.

1. ADOPTEZ DES PRATIQUES ÉPROUVÉES DE SÉCURITÉ INFORMATIQUE ET TÉLÉPHONIQUE

- Appliquez des protocoles de mots de passe rigoureux et formez votre personnel à l'usage de mots de passe alphanumériques complexes et à l'authentification à deux facteurs.
- Dotez vos ordinateurs d'une protection antivirus adéquate et effectuez une mise à jour régulière. Lorsque vous transmettez des données par Internet, servez-vous du chiffrement de bout en bout.
- Sauvegardez souvent vos données sur un serveur ou un espace de stockage sécurisé pour empêcher les fraudeurs de prendre vos données en otage dans une attaque par rançongiciel.
- Essayez des outils de test d'intrusion pour évaluer la vulnérabilité du réseau.

2. FORMER LE PERSONNEL SUR LES CHÈQUES SANS PROVISION ET LES MESSAGES HAMEÇONS

- Formez-vous, ainsi que votre personnel, à détecter les signaux d'alerte associés aux chèques sans provision et aux attaques par hameçonnage.
- Pour accéder à la fiche d'information de LAWPRO sur les fraudes et des conseils sur la détection de celles-ci, visitez la page Web de practicePRO sur la prévention des fraudes (voir la vidéo en français ici).

3. VÉRIFIEZ LES INSTRUCTIONS REÇUES PAR COURRIEL

- Les attaques des fraudeurs par hameçonnage ciblé prennent souvent la forme d'instructions par courriel qui semblent provenir d'un client, du cabinet qui représente la partie adverse ou d'une autre partie digne de confiance. Avant de donner suite à des instructions envoyées par courriel, surtout des demandes de transfert de fonds, appelez l'expéditeur pour confirmer sa demande.

4. DISPOSEZ D'UNE CYBERASSURANCE SUFFISANTE

- L'assurance contre la faute professionnelle protège seulement de certains cyberrisques, et les cabinets ne doivent pas supposer que leur assurance responsabilité civile générale couvrira tous ces genres de risques. Voyez si votre cabinet devrait souscrire une police d'assurance pour couvrir directement les coûts liés à une cyberattaque.

5. DISPOSEZ D'UN PLAN D'INTERVENTION EN CAS D'INCIDENT

- Comme une cyberattaque peut causer des dommages importants, les cabinets d'avocats doivent pouvoir réagir sur-le-champ. Un plan d'intervention en cas d'incident décrit les étapes à suivre pour détecter, endiguer et éradiquer une cyberattaque, pour reprendre les activités normales et pour effectuer une analyse de suivi. Les ressources de LAWPRO sur les plans d'intervention en cas d'incident (*en anglais seulement*) peuvent vous aider à concevoir ce plan.

EN SAVOIR PLUS SUR LA CYBERSÉCURITÉ ET LA PRÉVENTION DES FRAUDES

Voir les pages Web sur la prévention des fraudes (practicePRO) et **les dangers du cyberespace**.