Protégez-vous

Contre la cyberfraude immobilière

Les informations de nature sensible jouent un rôle essentiel dans vos transactions immobilières, et il est impératif que ces informations demeurent sécurisées et protégées. Lorsque vous commandez des polices d'assurance titres Stewart, vous pouvez le faire en sachant que les informations confidentielles et personnelles sont protégées par nos méthodes de sécurité des données robustes. Mais, en tant que professionnel du droit, vous pouvez également prendre des mesures pour vous protéger contre la cyberfraude.

Récemment, il y a eu une vague de cyberfraude. Les cybercriminels piratent les comptes de messagerie de professionnels du droit ou d'autres personnes qui sont parties aux transactions immobilières. Ces pirates, ou « hackers », sont patients; ils attendent de découvrir des renseignements utiles pour leur plan d'escroquerie et vous convaincre d'envoyer de l'argent par virement électronique à un compte bancaire qui semble appartenir légitimement à une partie à la transaction (mais qui ne l'est pas). Les pirates envoient un courriel qui semble provenir d'une personne qui est partie à la transaction (une pratique appelée usurpation).

À première vue, ces adresses courriel bidons semblent légitimes, mais comportent souvent une lettre supplémentaire ou une autre variation mineure par rapport à l'adresse courriel réelle.

Exemple : msmith@stewartttitle.com
au lieu de
msmith@stewarttitle.com

Ces courriels bidons informent le destinataire d'une modification de dernière minute apportée aux instructions de virement ou de paiement et demandent que les fonds soient envoyés au moyen des nouvelles coordonnées de compte fournies. En suivant ces instructions, les fonds sont virés par inadvertance au compte du pirate informatique et, le plus souvent, perdus à jamais.

Autres types de cyberfraude

Rançongiciel

Ce type d'attaque implique le vol de données ou le blocage de l'accès aux systèmes de données de l'entreprise. Le criminel exige alors le paiement d'une « rançon » (souvent en bitcoin) pour libérer vos données.

Ces attaques se produisent généralement lorsque quelqu'un ouvre involontairement un courriel ou une pièce jointe, ou qu'il clique sur des liens sur des sites Web non sécurisés. Les rançongiciels peuvent également provenir de fournisseurs tiers qui ne savent pas qu'ils sont infectés.

Exemple :

En 2017, un cabinet d'avocats mondial a été victime d'une attaque de rançongiciel qui a paralysé le cabinet. Cette attaque a nécessité plus de 15 000 heures supplémentaires de services informatiques pour récupérer les systèmes informatiques, et a affecté la capacité à servir les clients pendant l'attaque.

Les escroqueries par hameçonnage

Ces escroqueries proviennent de faux courriels ou de fenêtres contextuelles de sites Web contenant des liens incitant le destinataire à télécharger par inadvertance des logiciels malveillants.

Exemple :

Un commis a reçu un courriel accompagné d'une facture. La facture s'est révélée fausse et a mené au téléchargement de logiciels espions sur le réseau. Les criminels pouvaient alors surveiller les activités informatiques du commis et obtenir des renseignements sur les comptes bancaires, mots de passe et informations de virement bancaire. À l'insu du commis, des fonds ont alors été virés du compte en fiducie de l'avocat/notaire à l'étranger.

En apprendre davantage

stewart™
TITLE

Reconnaître les indicateurs courants de la cyberfraude

- Les courriels demandant que des modifications de dernière minute soient apportées aux informations de virement bancaire (p. ex. des changements concernant le nom du bénéficiaire et/ou de la banque réceptrice);
- Des demandes de virements électroniques en fin de journée, en semaine ou en dehors des heures de bureau;
- Des courriels contenant des erreurs de grammaire et/ou typographiques;
- Des modifications légères, généralement imperceptibles au premier coup d'œil, de l'adresse courriel.

Meilleures pratiques suggérées pour transmettre et recevoir des renseignements de nature sensible

- Envoyez des courriels contenant des renseignements personnels de nature sensible uniquement par courriel crypté;
- Vérifiez les demandes de modifications des instructions de virement bancaire au moyen d'une méthode fiable (comme un numéro de téléphone préalablement vérifié); n'utilisez jamais le numéro de téléphone contenu dans le courriel;
- Vérifiez les demandes de virement bancaire vers des emplacements en dehors des zones commerciales habituelles;
- Ne cliquez jamais sur aucun lien dans un courriel non vérifié ou inattendu;
- Méfiez-vous toujours des pièces jointes et des liens envoyés non cryptés.

Conseils supplémentaires pour réduire au minimum les cyberrisques

- Organisez une formation annuelle sur la cybersécurité pour tout le personnel;
- N'ouvrez pas les courriels que vous ne reconnaissez pas tant qu'ils n'ont pas été vérifiés;
- Ne suivez pas les instructions inhabituelles concernant les informations bancaires ou les virements de fonds, etc. sans d'abord en vérifier la légitimité;
- N'utilisez jamais les adresses courriel ou les numéros de téléphone indiqués dans des communications suspectes pour effectuer une vérification;
- Recherchez les erreurs d'orthographe et de grammaire dans les courriels (p. ex. les noms de société ou les termes standard);
- Passez votre curseur sur les hyperliens sans cliquer pour voir l'URL réelle du lien. Si l'adresse est différente de celle affichée, il s'agit probablement d'une arnaque par hameçonnage;
- Assurez-vous d'avoir accès à des services de TI appropriés pour les systèmes informatiques;
- Assurez-vous que l'antivirus est à jour;
- Utilisez le cryptage pour les données de nature sensible;
- Assurez-vous d'avoir en place des politiques de protection des mots de passe et de les appliquer;
- Conservez des sauvegardes appropriées de vos données électroniques;
- Prévoyez un plan en cas d'atteinte à vos systèmes et sachez qui joindre et comment récupérer efficacement les données de sauvegarde;
- Envisagez de souscrire à une assurance pour les pertes découlant d'une atteinte à vos systèmes.

Que faire si vous pensez être victime de cyberfraude

- Si de l'argent a été transféré en réponse à des instructions de virement frauduleuses, appelez immédiatement toutes les banques et institutions financières qui pourraient mettre un terme au virement ou bloquer vos fonds;
- Communiquez avec votre service de police local ou la division de fraude immobilière de votre municipalité;
- Contactez toute autre partie qui peut avoir été exposée à la cyberfraude afin que des mesures appropriées puissent être prises;
- Modifiez tous les noms d'utilisateur et mots de passe associés à tout compte que vous pensez avoir été compromis;
- l'Unité nationale de coordination de la lutte contre la cybercriminalité de la GRC https://www.rcmp-grc.gc.ca/fr/gnc3.

Communiquez avec nous pour plus de renseignements.

866.235.9152

stewart.ca

stewart™ TITLE