

L'une des responsabilités de l'équipe de cybersécurité de SIRVA est d'identifier et de combattre le déferlement constant de nouvelles menaces de cybersécurité. Dans le cadre des efforts continus de SIRVA pour maintenir la sécurité et tenir nos clients informés des développements importants dans le domaine de la cybersécurité, nous voulons nous assurer que vous connaissez et comprenez les mesures que vous pouvez prendre pour diminuer les risques.

Des escroqueries ont été réalisées par des criminels qui ont tenté de falsifier les instructions bancaires utilisées dans des transactions en ligne. Les auteurs peuvent s'infiltrer dans un compte de messagerie ou même dans l'ordinateur de l'une des parties à la transaction. Une fois infiltré, l'auteur crée un compte de messagerie qui imite le compte de l'expéditeur réel. Il envoie ensuite de faux courriels contenant des instructions frauduleuses de virement bancaire ou d'ACH. Cela peut entraîner des pertes financières importantes. Dans certaines circonstances, l'auteur intercepte et supprime les courriels entre les parties réellement impliquées dans la transaction. Bien que des cybermenaces puissent apparaître à tout moment et en tout lieu, ce type de piratage apparaît actuellement comme un problème particulier dans les transactions immobilières en Amérique du Nord.

Afin de minimiser le risque associé aux transactions financières sur Internet, SIRVA a mis en place de nouvelles procédures internes pour lutter directement contre les tentatives des pirates informatiques de falsifier les instructions bancaires.

En outre, nous avons énuméré ci-dessous certaines mesures que vous pouvez prendre pour vous protéger contre ce type de vol. Ces mesures ne sont pas applicables à toutes les situations, mais elles se sont avérées efficaces pour minimiser le risque de cyber-vol. Avant tout, l'essentiel est de rester vigilant lors des transactions financières et des activités connexes et de signaler immédiatement toute activité suspecte.

- Maintenez à jour les abonnements ou les logiciels de cybersécurité (généralement appelés « logiciels antivirus ») de votre ordinateur, qui comprennent une protection contre le piratage des e-mails. La plupart des grands fournisseurs de courrier électronique, tels que Yahoo, MSN, Google et AOL, disposent d'une cybersécurité solide pour l'activité de courrier électronique au sein même des serveurs de domaine. Toutefois, cette protection ne s'étend pas à votre ordinateur de bureau, à votre ordinateur portable ou à d'autres ordinateurs portables. Vous ne devez pas vous fier uniquement à la protection de la cybersécurité de votre fournisseur de messagerie. Achetez un logiciel ou un abonnement de protection cybersécurité qui vous fournit des mises à jour constantes pour faire face à toutes les nouvelles menaces qui existent.
- Les systèmes de messagerie de l'entreprise disposent souvent de logiciels de protection de pointe en matière de cybersécurité. Renseignez-vous auprès de votre entreprise sur ces protections et envisagez d'utiliser un ordinateur protégé par l'entreprise et votre compte de messagerie d'entreprise pour toutes les questions relatives à votre activité de relocation.
- Lorsque vous travaillez avec SIRVA ou ses fournisseurs, nous attendons des membres de notre équipe et des fournisseurs qu'ils utilisent leurs comptes de messagerie d'entreprise. S'ils ne le font pas, faites-le nous savoir.
- Essayez de limiter votre activité sur Internet à des sites connus qui déclarent avoir des fonctions de cybersécurité. Ne visitez pas les sites qui sont douteux, qui présentent de nombreuses fenêtres publicitaires ou qui vous dirigent vers d'autres sites web.

- Lorsque vous envoyez ou recevez des informations financières, confirmez verbalement les informations qui ont été transmises auprès d'une source connue chez l'expéditeur ou le destinataire. Si vous ne connaissez pas l'expéditeur ou le destinataire du courriel ou si vous n'avez jamais eu de contact avec eux, contactez une source connue (votre conseiller en réinstallation ou votre courtier) pour confirmer le nom et le numéro du contact.
- Chaque fois que vous envoyez des fonds, assurez-vous que le destinataire sait que les fonds arrivent et qu'il est à l'affût des fonds. Confirmez que tous les fonds sont envoyés par un virement unique ou par ACH dès que les fonds sont envoyés.
- Lorsque vous envoyez des fonds par voie électronique (par opposition à l'envoi d'un chèque bancaire) pour couvrir une transaction financière importante, envisagez d'envoyer les fonds par câble plutôt que par ACH. Le virement a un coût, mais présente des caractéristiques de sécurité supplémentaires, notamment la correspondance entre le nom du compte et le numéro.
- Regardez attentivement l'adresse de tous les e-mails que vous recevez (y compris en plaçant votre curseur sur l'adresse) pour vous assurer qu'ils sont légitimes et ne proviennent pas d'un compte frauduleux. (Par exemple, si le courriel est censé provenir de "agent@broker.com," regardez attentivement pour vous assurer qu'il ne s'agit pas de "agent@broker.co" ou d'une autre variante). Bien qu'il ne s'agisse pas d'une solution infaillible, c'est une mesure supplémentaire que vous pouvez prendre pour contribuer à prévenir la fraude.
- Assurez un suivi verbal de toute communication par courriel (ou autre transmission sécurisée) contenant des informations ou des instructions financières et confirmez l'exactitude ou la réception de ces informations.
- Il est peu probable que l'on vous demande un jour de modifier des directives bancaires. Si vous recevez des instructions pour modifier des informations bancaires ou fournir de nouvelles informations, contactez une source connue pour interroger et confirmer un tel changement.
- Signalez immédiatement toute activité suspecte à votre banque, aux autorités locales, à SIRVA et à toute autre partie concernée, dès que possible. Plus tôt la fraude est identifiée, plus grandes sont les chances de l'arrêter.

Le transfert électronique de fonds par le biais d'un virement ou d'une transaction ACH présente de nombreux avantages. Toutefois, ces types de transactions sont susceptibles d'escroqueries en matière de cybersécurité. Pour éviter d'être victime d'une escroquerie, il est essentiel d'utiliser des moyens sécurisés pour transmettre et recevoir des instructions bancaires et des informations personnelles, et de suivre des procédures de vérification sécurisées.

VEUILLEZ NOTER QUE NI SIRVA NI VOTRE BANQUE NE DOIVENT VOUS FOURNIR DES INSTRUCTIONS DE VIREMENT. SEUL LE DESTINATAIRE DES FONDS DOIT VOUS FOURNIR DES INSTRUCTIONS DE VIREMENT. SIRVA N'ACCEPTERA DES INSTRUCTIONS BANCAIRES DE VOTRE PART QUE VIA NOTRE PORTAIL D'INFORMATION SÉCURISÉ SI VOUS N'ÊTES PAS EN MESURE DE FOURNIR DES INFORMATIONS VIA NOTRE PORTAIL D'INFORMATIONS SÉCURISÉ, CONTACTEZ VOTRE CONSULTANT SIRVA PAR TÉLÉPHONE POUR DISCUTER DE LA MEILLEURE FAÇON DE FOURNIR LES INFORMATIONS. CHAQUE FOIS QUE DES INFORMATIONS OU DE L'ARGENT SONT ENVOYÉS OU REÇUS EN DEHORS DE NOTRE PORTAIL D'INFORMATION SÉCURISÉ (SOIT AVEC SIRVA, SOIT AVEC UNE AUTRE PARTIE), CONTACTEZ IMMÉDIATEMENT L'AUTRE PARTIE POUR CONFIRMER VERBALEMENT L'EXACTITUDE DES INFORMATIONS ET DES INSTRUCTIONS DE COMPTE BANCAIRE AVEC UNE SOURCE PRÉCÉDEMMENT CONNUE CHEZ L'EXPÉDITEUR/LE DESTINATAIRE, ET POUR VÉRIFIER ÉGALEMENT LE MONTANT DES FONDS ENVOYÉS OU REÇUS PAR LA CONTREPARTIE DE LA TRANSACTION. N'ENVOYEZ PAS DE FONDS AVANT D'AVOIR CONFIRMÉ VERBALEMENT AUPRÈS D'UNE SOURCE CONNUE AU PRÉALABLE QUE LES INSTRUCTIONS ONT ÉTÉ CORRECTEMENT TRANSMISES.

SIRVA s'engage à offrir la meilleure expérience de relocation possible grâce à son expertise en matière de mobilité, à son assistance personnalisée et à ses outils et ressources pour diminuer les difficultés à chaque étape du processus. Veuillez contacter votre représentant SIRVA si vous avez des questions sur cette communication.

John Kirk
Directeur général de l'Information et de la Technologie
SIRVA Worldwide, Inc.