CYBER SECURITY MEMO

L'une des responsabilité s de l'é quipe de cybersé curité de Sirva est d'identifier et de combattre le dé ferlement constant de nouvelles menaces de cybersé curité . Dans le cadre des efforts continus de Sirva pour maintenir la sé curité et tenir nos clients informé s des dé veloppements importants dans le domaine de la cybersé curité , nous voulons nous assurer que vous connaissez et comprenez les mesures que vous pouvez prendre pour diminuer les risques.

Des escroqueries ont é té ré alisé es par des criminels qui ont tenté de falsifier les instructions bancaires utilisé es dans des transactions en ligne. Les auteurs peuvent s'infiltrer dans un compte de messagerie ou mê me dans l'ordinateur de l'une des parties à la transaction. Une fois infiltré , l'auteur cré e un compte de messagerie qui imite le compte de l'expé diteur ré el. Il envoie ensuite de faux courriels contenant des instructions frauduleuses de virement bancaire ou d'ACH. Cela peut entraîner des pertes financiè res importantes. Dans certaines circonstances, l'auteur intercepte et supprime les courriels entre les parties ré ellement impliqué es dans la transaction. Bien que des cybermenaces puissent apparaître à tout moment et en tout lieu, ce type de piratage apparaît actuellement comme un problè me particulier dans les transactions immobiliè res en Amé rique du Nord.

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

En outre, nous avons é numé ré ci-dessous certaines mesures que vous pouvez prendre pour vous proté ger contre ce type de vol. Ces mesures ne sont pas applicables à toutes les situations, mais elles se sont avé ré es efficaces pour minimiser le risque de cyber-vol. Avant tout, l'essentiel est de rester vigilant lors des transactions financiè res et des activité s connexes et de signaler immé diatement toute activité suspecte.

- Maintenez à jour les abonnements ou les logiciels de cybersé curité (gé né ralement appelé s « logiciels antivirus ») de votre ordinateur, qui comprennent une protection contre le piratage des emails. La plupart des grands fournisseurs de courrier é lectronique, tels que Yahoo, MSN, Google et AOL, disposent d'une cybersé curité solide pour l'activité de courrier é lectronique au sein mê me des serveurs de domaine. Toutefois, cette protection ne s'é tend 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 cybersé curité de votre fournisseur de messagerie. Achetez un logiciel ou un abonnement de protection cybersé curité qui vous fournit des mises à jour constantes pour faire face à toutes les nouvelles menaces qui existent.
- Les systè mes de messagerie de l'entreprise disposent souvent de logiciels de protection de pointe en matiè re de cybersé curité . Renseignez-vous auprè s de votre entreprise sur ces protections et envisagez d'utiliser un ordinateur proté gé 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 é quipe 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 dé clarent avoir des fonctions de cybersé curité . Ne visitez pas les sites qui sont douteux, qui pré sentent de nombreuses fenê tres publicitaires ou qui vous dirigent vers d'autres sites web.
- Lorsque vous envoyez ou recevez des informations financiè res, confirmez verbalement les informations qui ont é té transmises auprè s d'une source connue chez l'expé diteur ou le destinataire. Si vous ne connaissez pas l'expé diteur ou le destinataire du courriel ou si vous n'avez jamais eu de contact avec eux, contactez une source connue (votre conseiller en ré installation ou votre courtier) pour confirmer le nom et le numé ro 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'affû t des fonds. Confirmez que tous les fonds sont envoyé s par un virement unique ou par ACH dè s que les fonds sont envoyé s.
- Lorsque vous envoyez des fonds par voie é lectronique (par opposition à l'envoi d'un chè que bancaire) pour couvrir une transaction financiè re importante, envisagez d'envoyer les fonds par câ ble plutô t que par ACH. Le virement a un coû t, mais pré sente des caracté ristiques de sé curité supplé mentaires, notamment la correspondance entre le nom du compte et le numé ro.
- Regardez attentivement l'adresse de tous les e-mails que vous recevez (y compris en plaç ant votre curseur sur l'adresse) pour vous assurer qu'ils sont lé gitimes 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 supplé mentaire que vous pouvez prendre pour contribuer à pré venir la fraude.
- Assurez un suivi verbal de toute communication par courriel (ou autre transmission sé curisé e) contenant des informations ou des instructions financiè res et confirmez l'exactitude ou la ré ception 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 immé diatement toute activité suspecte à votre banque, aux autorité s locales, à Sirva et à toute autre partie concerné e, dè s que possible. Plus tô t la fraude est identifié e, plus grandes sont les chances de l'arrê ter.

Le transfert é lectronique de fonds par le biais d'un virement ou d'une transaction ACH pré sente de nombreux avantages. Toutefois, ces types de transactions sont susceptibles d'escroqueries

en matiè re de cybersé curité . Pour é viter d'ê tre victime d'une escroquerie, il est essentiel d'utiliser des moyens sé curisé s pour transmettre et recevoir des instructions bancaires et des informations personnelles, et de suivre des procé dures de vé rification sé curisé es.

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 SÉ CURISÉ SI VOUS N'Ê TES PAS EN MESURE DE FOURNIR DES INFORMATIONS VIA NOTRE PORTAIL D'INFORMATIONS SÉ CURISÉ , CONTACTEZ VOTRE CONSULTANT SIRVA PAR TÉ LÉ PHONE POUR DISCUTER DE LA MEILLEURE FAÇ ON DE FOURNIR LES INFORMATIONS. CHAQUE FOIS QUE DES INFORMATIONS OU DE L'ARGENT SONT ENVOYÉ S OU REÇ US EN DEHORS DE NOTRE PORTAIL D'INFORMATION SÉ CURISÉ (SOIT AVEC SIRVA, SOIT AVEC UNE AUTRE PARTIE), CONTACTEZ IMMÉ DIATEMENT L'AUTRE PARTIE POUR CONFIRMER VERBALEMENT L'EXACTITUDE DES INFORMATIONS ET DES INSTRUCTIONS DE COMPTE BANCAIRE AVEC UNE SOURCE PRÉ CÉ DEMMENT CONNUE CHEZ L'EXPÉ DITEUR/LE DESTINATAIRE, ET POUR VÉ RIFIER É GALEMENT LE MONTANT DES FONDS ENVOYÉ S OU REÇ US PAR LA CONTREPARTIE DE LA TRANSACTION. N'ENVOYEZ PAS DE FONDS AVANT D'AVOIR CONFIRMÉ VERBALEMENT AUPRÈ S D'UNE SOURCE CONNUE AU PRÉ ALABLE QUE LES INSTRUCTIONS ONT É TÉ CORRECTEMENT TRANSMISES.

Sirva s'engage à offrir la meilleure expé rience de relocation possible grâ ce à son expertise en matiè re de mobilité , à son assistance personnalisé e et à ses outils et ressources pour diminuer les difficulté s à chaque é tape du processus. Veuillez contacter votre repré sentant Sirva si vous avez des questions sur cette communication.

John Kirk
Directeur gé né ral de l'Information et de la Technologie
Sirva Worldwide, Inc.