ACI
L'ASSOCIATION CANADIENNE DE L'IMMOBILIER

Sécurité des courtiers et agents immobiliers
Sensibilisation à la cybersécurité –
Document de référence

En adoptant des mesures de sécurité et en restant au fait des arnaques et menaces les plus récentes, les courtiers et agents immobiliers peuvent se protéger et protéger leur entreprise des cyberattaques.

Sécurité sur les appareils mobiles

Les appareils mobiles sont d'une aide précieuse pour les professionnels de l'immobilier, mais leur commodité à un prix.

Voici des mesures à prendre pour sécuriser votre appareil mobile :

- choisissez des mots de passe forts et activez l'authentification multifactorielle, par exemple à l'aide d'une empreinte digitale ou d'un code numérique;
- ayez recours au chiffrement pour sécuriser les données client;
- désactivez la localisation avant de prendre des photos;
- définissez un mot de passe unique pour chaque compte;
- utilisez les fonctionnalités de sécurité intégrées à votre téléphone, comme celles de localisation de l'appareil et d'appels d'urgence;
- vérifiez les réglages de confidentialité de votre téléphone et ceux des applications pour vous assurer de partager de l'information intentionnellement et avec parcimonie (emplacement, photos, microphone, vidéo, etc.).

Sécurité sur les médias sociaux

Les courtiers et agents immobiliers peuvent se servir des médias sociaux pour communiquer avec leurs clients, tisser des relations, et maximiser leur présence en ligne et leur potentiel de croissance. Ils devraient toutefois toujours le faire avec prudence, car la confidentialité et la sécurité peuvent facilement être compromises sur ces plateformes.

Voici des mesures de sécurité à prendre pour les médias sociaux :

- choisissez des mots de passe forts et uniques, et activez l'authentification multifactorielle;
- assurez-vous que l'information que vous partagez est exacte et qu'elle vient d'une source fiable;
- vérifiez les réglages de confidentialité régulièrement et ajustez-les au besoin;
- évitez de diffuser trop d'information ou de publier du contenu présentant des renseignements personnels ou de nature délicate;
- désactivez le partage de la localisation avant de publier une information;
- évitez de montrer les objets de valeur des propriétaires-vendeurs sur les photos;
- ne cliquez jamais sur les liens et ne téléchargez pas de pièces jointes provenant de sources inconnues;
- restez au fait des arnaques courantes, comme l'hameçonnage et l'hameçonnage par message texte;
- tenez-vous au courant des tactiques de piratage psychologique, qui visent à nous inciter à transmettre des renseignements de nature délicate.

Cybercriminalité : arnaques et fraudes

La cybercriminalité pose problème dans le monde entier. Les arnaques et les fraudes électroniques représentent une menace certaine dont les courtiers et agents immobiliers, les acheteurs et les propriétaires-vendeurs peuvent être la cible.

En voici des exemples communs :
Fraude par virement électronique : Des criminels pourraient tenter de tromper des professionnels de l'immobilier et leurs clients en leur envoyant de fausses directives de virement, détournant les fonds vers leur propre compte.

Compromission de messagerie d'entreprise : Les criminels se présentent comme des expéditeurs de confiance et incitent le destinataire à leur envoyer de l'argent ou à leur transmettre de l'information financière.

Fraude sur titre : Les cybercriminels utilisent des pièces d'identité contrefaites pour se présenter comme les propriétaires d'une résidence dont le prêt hypothécaire est remboursé, et demander une deuxième hypothèque sur cette propriété.

Arnaques employant l'intelligence artificielle (IA) : L'IA aide les criminels à raffiner leurs stratagèmes, en créant pour eux de fausses identités ou en automatisant leurs activités frauduleuses.

Tactiques communes de piratage psychologique

Les pirates trompent leurs victimes pour leur soutirer des renseignements personnels. Cette pratique, employée souvent sur les médias sociaux, se présente sous forme de messages amusants et interactifs, mais peut aussi être employée dans un courriel, un message direct ou un message texte.

Les pirates tentent généralement de subtiliser des renseignements personnels en employant l'une de ces méthodes.

- **Hameçonnage –** Des courriels qui semblent provenir d'une source de confiance dirigent les destinataires vers de faux sites Web où ils entreront des renseignements personnels et financiers, ce qui les expose à une fraude financière et à un vol d'identité.
- **Hameçonnage téléphonique –** Les cybercriminels utilisent de faux numéros de téléphone, des logiciels pour modifier la voix et d'autres tactiques pour inciter les gens à divulguer des renseignements personnels au téléphone.
- **Hameçonnage par message texte –** Les pirates se servent de messages textes pour inciter les destinataires à transmettre de l'information en y répondant ou en cliquant sur un lien compromis.
- **Rançongiciel –** Selon le Centre canadien pour la cybersécurité, les rançongiciels sont la cybermenace la plus commune à laquelle la population canadienne est exposée. Les cybercriminels utilisent un logiciel malveillant pour chiffrer, supprimer ou voler des données, puis exigent une rançon pour les restituer.

Voici des mesures de sécurité à prendre dans un environnement virtuel :

- utilisez des modes de communication sécurisés, comme des courriels chiffrés;
- restez au fait des risques pour la cybersécurité et des pratiques exemplaires pour les atténuer;
- recourez à l'authentification multifactorielle;
- mettez régulièrement à jour leurs logiciels;
- utilisez des réseaux Wi-Fi sécurisés et protégés par un mot de passe;
- faites régulièrement des copies de sauvegarde des données essentielles.

Menaces découlant de l'intelligence artificielle

Nous ne connaissons pas encore tout le potentiel de l'IA, mais cela n'empêche pas les cybercriminels de l'exploiter avec malveillance. Les courtiers et agents immobiliers ont intérêt à se tenir au courant des dangers associés à l'IA, et des types d'arnaques dont ils doivent se méfier.

Inscriptions frauduleuses : À l'aide de l'IA, les cybercriminels créent des inscriptions immobilières frauduleuses qui pourraient tromper les courtiers et agents immobiliers et leurs clients. Cherchez des incohérences dans le texte (par exemple, des fautes d'orthographe et du contenu vague et répétitif) et vérifiez l'identité des parties concernées.

Désinformation : L'IA peut servir à simuler des évaluations, des témoignages, des inscriptions, des courriels et d'autres renseignements qui peuvent induire en erreur les acheteurs et les propriétaires-vendeurs et ternir la réputation des professionnels de l'immobilier.

Hameçonnage : Les courriels produits par l'IA peuvent avoir l'air authentiques, incitant leurs destinataires à divulguer des renseignements personnels ou financiers.

Rançongiciels : L'IA peut aider à repérer les failles du réseau d'une société immobilière et à diffuser un rançongiciel, ce qui pourrait entraîner la perte de précieuses données client.

Hypertrucage : L'IA permet de produire du contenu multimédia hypertruqué qui présente des événements inventés. Une vidéo hypertruquée peut simuler une situation impliquant un professionnel de l'immobilier, un prêteur, un acheteur ou un propriétaire-vendeur, entraînant des transactions frauduleuses et des pertes financières. Des images hypertruquées d'une propriété peuvent donner lieu à une fausse représentation et à des conséquences juridiques, tandis que des hypertrucages audio, qui reproduisent la voix d'une source fiable, peuvent servir à convaincre une cible de révéler des renseignements personnels et financiers au téléphone.

Grâce à leur capacité à repérer les tendances et les incohérences, les technologies d'IA et d'apprentissage machine commencent à jouer un rôle important dans la détection des fraudes. L'IA, par l'intermédiaire d'outils de vérification des faits, de détecteurs d'hypertrucages et d'authentificateurs de vidéos, peut aider les courtiers et agents immobiliers à repérer l'information trompeuse.

Vous pouvez utiliser l'IA en toute sécurité pour :
- détecter les vidéos et les images truquées;
- vérifier le contenu trompeur;
- repérer les inscriptions frauduleuses.

Logiciels malveillants, rançongiciels et virus

La première étape pour protéger votre entreprise et vous-même : comprendre les cybermenaces les plus communes.

Un logiciel malveillant est conçu pour endommager des systèmes informatiques. Il en existe plusieurs types : virus, logiciel espion, logiciel publicitaire et rançongiciel.

Un rançongiciel est un logiciel malveillant qui chiffre les dossiers de l'utilisateur et menace celui-ci de les diffuser ou de lui en bloquer l'accès à moins qu'il lui paye une rançon.

Les virus sont des logiciels malveillants qui se répliquent et attaquent d'autres ordinateurs et systèmes.

Voici des mesures à prendre pour atténuer les risques de cyberattaques :
- gardez vos logiciels à jour et activez les mises à jour automatiques sur vos appareils;
- choisissez des mots de passe forts, et activez l'authentification multifactorielle;
- faites une copie de sauvegarde des données importantes;
- restez au fait des pratiques exemplaires en matière de cybersécurité;
- utilisez un logiciel antivirus et des pare-feu;
- mettez en place un plan d'intervention en cas d'atteinte à la protection des données.

Pratiques exemplaires de création des mots de passe

Pour assurer la confidentialité et la sécurité de vos données en ligne, vous devez adopter de bonnes pratiques de gestion des mots de passe.

Suivez notamment ces conseils :
- Choisissez un mot de passe de 12 caractères alliant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
- Utilisez une phrase dont vous vous souviendrez en substituant les chiffres aux lettres, ou vice-versa.
- N'utilisez pas le même mot de passe pour plusieurs comptes.
- Ne divulguez pas vos mots de passe à qui que ce soit.