Guide des ressources en
matière de cybersécurité

2025 de FCT

FCT[MD]

Table des matières

Introduction

La cybersécurité est devenue un défi majeur de notre ère numérique, qui exige non seulement des solutions techniques, mais aussi une prise de conscience, une responsabilisation et une action à l'échelle du secteur. Chez FCT, nous sommes conscients que chaque transaction représente bien plus que des données : elle représente des personnes, de la confiance et des décisions qui changent le cours d'une vie. Protéger cette confiance n'est pas seulement notre responsabilité, c'est notre engagement.

Le présent guide offre une vue d'ensemble complète de l'évolution des menaces liées à la cybersécurité dans notre secteur. Dans un premier temps, il identifie et explique le langage de ces risques, en clarifiant la terminologie clé en matière de cybersécurité et de cyberfraude afin de favoriser une vigilance éclairée. Il donne ensuite des exemples concrets de réclamations et d'incidents, illustrant comment les menaces se manifestent et comment elles peuvent être interceptées à l'avenir. Enfin, nous nous tournons vers l'avenir en explorant les tendances émergentes et en montrant comment FCT aide ses clients à défendre leurs transactions grâce à des outils proactifs tels que la vérification de l'identité du client.

La cybersécurité est une responsabilité partagée. Grâce à la sensibilisation, à la perspicacité et à l'innovation, nous pouvons bâtir un écosystème plus résilient, où la confiance n'est pas seulement gagnée, mais aussi activement protégée.

Message de notre président

Chez FCT, la protection des personnes est au cœur de toutes nos activités. Derrière chaque transaction se cachent des personnes, comme une famille qui achète sa première maison, un professionnel du droit de confiance qui conseille un client, ou un professionnel du crédit qui aide quelqu'un à franchir une étape importante dans son parcours financier. Dans le monde numérique actuel, cette confiance est confrontée à de nouveaux défis liés à des tactiques de fraude de plus en plus sophistiquées.

La cybersécurité n'est plus seulement une question technique, c'est une question humaine. L'impact émotionnel et financier de la fraude est réel, c'est pourquoi la sensibilisation et la vigilance sont essentielles. En nous unissant en tant que secteur, nous pouvons mieux identifier les menaces émergentes, renforcer nos défenses et protéger ce qui compte vraiment : les personnes qui se cachent derrière chaque transaction. Ce rapport présente des idées, des stratégies et des témoignages qui nous aideront à atteindre cet objectif, en veillant à ce que FCT reste un partenaire de confiance dans chaque transaction.

La cybersécurité ne se limite pas aux systèmes informatiques, elle s'inscrit dans la culture. Quand les gens se sentent en sécurité, en confiance et connectés, ils sont plus enclins à s'exprimer, à repérer les risques et à arrêter les menaces avant qu'elles ne se propagent.

Daniela DeTommaso, LL.B.
Présidente

Détecter

Décoder la cybersécurité : Termes et concepts clés à connaître

FCT croit qu'il est essentiel de comprendre les principes fondamentaux de la cybersécurité pour protéger à la fois les personnes et les transactions. Dans cette section, nous aborderons des termes essentiels tels que le piratage psychologique, l'hameçonnage, l'authentification multifactorielle et les vulnérabilités infonuagiques. Ces concepts sont tous interconnectés et sont au cœur des cybermenaces auxquelles nous sommes confrontés quotidiennement. Par exemple, l'hameçonnage est une tactique de piratage psychologique conçue pour inciter les gens à divulguer des renseignements sensibles, et les vulnérabilités infonuagiques peuvent accroître l'exposition si des protections appropriées, telles que l'authentification multifactorielle, ne sont pas mises en place. En apprenant comment ces menaces interagissent et comment s'en protéger, nous pouvons renforcer la sécurité numérique de tous les professionnels et clients que nous servons.

Cybersécurité 101

Qu'est-ce que le piratage psychologique?

Une forme de cybermanipulation où les pirates exploitent le comportement humain pour accéder à des renseignements ou à des systèmes sensibles. Plutôt que de contourner les défenses techniques, ces stratagèmes s'appuient sur des tactiques psychologiques pour inciter les gens à commettre des actes préjudiciables.

- Les techniques les plus courantes sont l'hameçonnage, l'usurpation d'identité et les demandes urgentes qui contournent les protocoles de sécurité normaux.
- Les cibles sont souvent des professionnels qui traitent des transactions financières ou des données confidentielles.
- Ces attaques peuvent entraîner des pertes financières importantes et sont souvent exclues ou limitées par certains paramètres d'assurance.

Qu’est-ce que l’hameçonnage?

Une tactique trompeuse où les cybercriminels se font passer pour des sources fiables afin d’inciter les gens à partager des renseignements sensibles ou à cliquer sur des liens malveillants, généralement par le biais de courriels ou de messages textes (on parle alors d’« hameçonnage par message texte »). Ces messages sont conçus pour paraître légitimes et sont rédigés de manière à susciter des réponses rapides, avant que le destinataire n’ait le temps d’analyser leur contenu de plus près.

- Ils peuvent prendre la forme de courriels provenant de banques, de clients ou de collègues demandant une action urgente.
- Cliquer sur des liens ou télécharger des pièces jointes peut entraîner le vol d’identifiants ou l’installation de logiciels malveillants.
- L’hameçonnage est souvent utilisé comme point d’entrée pour des stratagèmes de fraude plus importants ou des violations du système.

Qu’est-ce que l’authentification multifactorielle?

Une mesure de sécurité qui exige que les utilisateurs confirment leur identité en utilisant plus d’une méthode d’authentification. Il s’agit généralement d’utiliser quelque chose qu’ils connaissent (questions sur les renseignements personnels), quelque chose qu’ils possèdent (un autre appareil ou canal de communication) ou quelque chose qui les caractérise (renseignements biométriques). Cette couche supplémentaire complique considérablement la tâche des pirates qui souhaitent obtenir un accès non autorisé, même si un mot de passe est compromis.

- L’authentification multifactorielle combine généralement quelque chose que vous connaissez (mot de passe) avec quelque chose que vous possédez (par exemple, un appareil mobile ou une application d’authentification).
- Les formes courantes comprennent les codes à usage unique envoyés par message texte, les notifications poussées ou la vérification biométrique.
- Elle est fortement recommandée pour les courriels, les opérations bancaires et tout système traitant des données sensibles.

Qu’est-ce que la vulnérabilité infonuagique?

Une faiblesse ou une mauvaise configuration dans les systèmes infonuagiques qui peut être exploitée par des cybercriminels pour obtenir un accès non autorisé à des données ou à des services. Ces vulnérabilités sont souvent dues à des contrôles d’accès insuffisants, à des logiciels non corrigés ou à des intégrations de tiers non sécurisées.

- Elles peuvent exposer des renseignements sensibles sur les clients, notamment des données financières et personnelles.
- Elles sont souvent ciblées par le vol d’identifiants, un stockage mal configuré ou des interface de programmation d'application
- (API) non sécurisées.
- Les vulnérabilités infonuagiques nécessitent une surveillance proactive, un cryptage et une gestion rigoureuse des identités afin d’atténuer les risques.

Conversation sur la cybersécurité avec Twane Boettinger

Alors que les cybermenaces continuent de gagner en complexité et en ampleur, les secteurs de l'immobilier et de l'assurance titres sont confrontés à des défis uniques en matière de protection des données sensibles et des transactions de grande valeur. Pour faire la lumière sur ces questions, nous nous sommes entretenus avec Twane Boettinger, directeur de la sécurité de l'information et des risques informatiques chez FCT. Fort d'une expérience dans le domaine de l'application de la loi et d'une expertise approfondie en cybersécurité, Twane brosse un tableau complet du paysage actuel des menaces, de l'hameçonnage et de l'usurpation d'identité à l'avenir de l'authentification multifactorielle et aux vulnérabilités infonuagiques. Cette conversation fournit des renseignements précieux aux professionnels du droit, agents immobiliers et prêteurs qui cherchent à renforcer leurs défenses et à anticiper les risques émergents.

Selon vous, quels sont les risques de cybersécurité les plus urgents auxquels sont confrontés aujourd'hui les secteurs de l'immobilier et de l'assurance titres?

L'un des plus grands risques que nous rencontrons actuellement concerne la compromission des comptes de courriel professionnels. Les fraudeurs sont capables d'usurper l'identité des participants autorisés à une transaction avec une précision croissante, en piratant des comptes de courriel légitimes ou en créant des domaines similaires. Ces tactiques leur permettent de détourner des fonds ou d'isoler les véritables participants des fils de discussion. De plus, comme l'usurpation d'identité devient de plus en plus sophistiquée grâce aux avatars virtuels et à la technologie d'hypertrucage, même les appels vidéo pourraient ne plus être un moyen fiable de vérifier l'identité d'une personne.

Les attaques par hameçonnage et piratage psychologique sont souvent les points d'entrée les plus courants pour les cybercriminels. Quelles sont les tactiques les plus fréquemment utilisées dans ces domaines et comment évoluent-elles au fil du temps?

L'hameçonnage et le piratage psychologique restent les points d'entrée les plus courants. Les fraudeurs sont désormais capables de contourner l'authentification multifactorielle (AMF) en volant des identifiants, le plus souvent à des utilisateurs qui réutilisent leurs mots de passe sur plusieurs plateformes. L'AMF elle-même est menacée, les criminels investissant du temps et des ressources pour intercepter ou détourner les jetons d'authentification. L'essor de l'IA générative a également rendu l'hameçonnage plus convaincant et évolutif, permettant aux pirates de créer des messages hautement personnalisés et crédibles.

En quoi les cybermenaces auxquelles FCT est confrontée diffèrent-elles de celles auxquelles sont confrontés d'autres secteurs, tels que les institutions financières traditionnelles ou d'autres prestataires de services? Y a-t-il un chevauchement important ou sommes-nous confrontés à un ensemble unique de défis?

Les principes fondamentaux sont les mêmes pour nous que pour les autres secteurs : il faut protéger les données et les processus. Ce qui diffère, c'est la manière dont les fraudeurs exploitent ces processus. Dans notre secteur, ils ne volent pas quelques sous sur les transactions aux guichets automatiques; ils ciblent des transactions immobilières de grande valeur, qui se chiffrent en millions. Ainsi, bien que les menaces soient comparables, l'ampleur et la méthode d'exploitation sont uniques dans notre cas.

Selon vous, quelle sera la prochaine vague de cyberattaques la plus probable dans ce secteur? S'agira-t-il de techniques d'hameçonnage et de piratage psychologique plus sophistiquées, d'exploitation des systèmes infonuagiques ou de quelque chose de totalement nouveau?

La prochaine vague impliquera probablement des formes plus sophistiquées d'hameçonnage, une plus grande facilité à contourner les outils d'AMF actuels et une plus grande précision de l'usurpation d'identité grâce à l'utilisation de l'IA. Les criminels utilisent déjà l'IA générative pour créer des messages d'hameçonnage plus convaincants et élaborer des codes d'attaque. Les progrès réalisés dans le domaine de l'informatique quantique constituent également une menace importante pour l'avenir : les données cryptées qui sont volées aujourd'hui sont peut-être sécurisées pour l'instant, mais elles pourraient être décryptées ultérieurement, car l'informatique quantique devrait être disponible dans un contexte grand public d'ici quatre à huit ans. Cela peut conduire à la divulgation de renseignements sensibles tels que les données biométriques ou les dossiers financiers, qui sont actuellement sécurisés.

Comment FCT forme-t-elle ou équipe-t-elle ses employés et partenaires pour reconnaître ces menaces potentielles et y résister?

Chez FCT, nous organisons chaque mois des formations de mise à jour en matière de sécurité pour tous les employés. Le suivi des formations est assuré et tout manquement est signalé à la hiérarchie. Depuis plus de deux ans, nous utilisons une série de vidéos spectaculaires qui intègrent des leçons sur la sécurité dans un scénario, suivies de jeux-questionnaires pour renforcer l'apprentissage. Nous intensifions également nos efforts pendant le Mois de la sensibilisation à la cybersécurité en organisant des événements d'entreprise tels que des jeux d'évasion sur le thème de la cybersécurité et des campagnes de sensibilisation internes. L'objectif est de développer une culture de sensibilisation à la cybersécurité dans toute l'organisation.

Vous avez déjà évoqué l'importance de l'AMF. Quelle est son importance pour protéger les données sensibles des clients et des transactions et comment FCT l'utilise-t-elle actuellement à cette fin?

L'authentification multifactorielle est absolument essentielle pour protéger les données sensibles, en particulier dans des secteurs comme le nôtre où les enjeux financiers sont élevés. Chez FCT, nous avons fait de l'AMF un élément central de notre stratégie de sécurité. Nous utilisons des outils tels que des applications d'authentification et des jetons matériels pour nos pratiques internes d'AMF, tandis que nous décourageons activement l'utilisation des messages textes et des courriels comme outils d'AMF dans notre organisation en raison de leurs vulnérabilités connues. Ces méthodes garantissent que, même si un mot de passe est compromis, tout accès non autorisé sera bloqué. L'AMF ajoute un niveau supplémentaire de défense essentiel et est appliquée à tous les systèmes internes qui traitent des données sensibles relatives aux clients et aux transactions.

Quels sont les défis auxquels les organisations sont confrontées lorsqu'elles déploient l'AMF à grande échelle, et comment atténuer ces défis?

La résistance des utilisateurs est l'un des plus grands défis, en particulier avec les authentificateurs mobiles – tout le monde n'est pas à l'aise avec son téléphone –, c'est pourquoi nous proposons des solutions matérielles comme les clés FIDO. Un autre obstacle consiste à aider les utilisateurs à comprendre les différences de sécurité entre les différentes méthodes d'AMF : les données biométriques (reconnaissance faciale et empreintes digitales) sont les plus sûres, suivies par les applications d'authentification. Les messages textes sont moins sûrs et sont vulnérables à la fraude par usurpation de carte SIM, et les courriels ne doivent jamais être utilisés en raison du risque d'exposition qu'ils présentent. Nous abordons ces questions par le biais d'une formation continue, d'une communication claire et d'options flexibles qui concilient sécurité et facilité d'utilisation, rendant l'AMF efficace sans être contraignante.

Avec l'utilisation croissante des plateformes infonuagiques, quelles sont les principales vulnérabilités infonuagiques qui vous préoccupent le plus?

La principale préoccupation concerne la rapidité des changements dans les environnements infonuagiques. Les fonctionnalités et les contrôles de sécurité sont constamment mis à jour ou supprimés, souvent sans préavis clair. Cela nécessite une surveillance continue afin d'éviter toute faille dans la sécurité. Ce qui prenait auparavant des mois ou des années à changer se transforme désormais en quelques jours ou semaines, et il est essentiel de rester au fait de ces changements.

À l'avenir, pensez-vous que l'AMF évoluera vers des outils de vérification de l'identité plus avancés, tels que l'utilisation régulière de la biométrie?

Absolument. Les données biométriques telles que la reconnaissance faciale et les empreintes digitales constituent actuellement les méthodes d'AMF les plus efficaces. Mais même les données biométriques pourraient être menacées à l'avenir, notamment en raison des progrès réalisés dans des domaines tels que l'informatique quantique et la technologie d'hypertrucage. Les pratiques d'AMF que nous connaissons aujourd'hui devront évoluer pour rester efficaces, d'autant plus que les interactions virtuelles deviennent monnaie courante et qu'il est finalement plus difficile de vérifier s'il s'agit réellement d'une personne réelle à l'autre bout.

Si vous deviez donner un conseil essentiel aux professionnels du droit, agents immobiliers et prêteurs concernant la situation actuelle et future de la cybersécurité, quel serait-il?

La nature même de l'identité est menacée. Avec les progrès réalisés dans le domaine de la technologie d'hypertrucage, même les appels vidéo peuvent être falsifiés avec une précision alarmante. Les organisations doivent trouver des moyens fiables de valider l'identité et de s'assurer qu'elles interagissent avec les personnes autorisées qu'elles prétendent être. Ce sera un défi majeur à court terme, et nous devons nous y préparer. Les mesures de cybersécurité fonctionnent souvent de manière réactive, nous obligeant à nous adapter à la manière dont les nouvelles technologies sont utilisées par les entités criminelles. À l'avenir, nous devons rester proactifs plutôt que réactifs afin d'empêcher ces crimes potentiels avant qu'ils ne se produisent.

Le vocabulaire des fraudeurs : Termes et tactiques essentiels de la cyberfraude

La cyberfraude est la prochaine étape dans la chaîne des risques lorsque les mesures de cybersécurité sont insuffisantes. Nous présenterons ici des termes tels que violation de données, hypertrucages, usurpation d'identité synthétique, fraude numérique liée au titre et fraude électronique. Souvent, ces menaces se renforcent mutuellement : un système compromis dont les données sont exposées peut être utilisé pour créer des hypertrucages et des identités synthétiques dont les fraudeurs se servent pour commettre des délits tels que la fraude numérique liée au titre et la fraude électronique. Comprendre ces risques et leur origine aide FCT et ses partenaires à rester vigilants et à protéger les personnes au cœur de chaque transaction.

Cyberfraude 101

Qu'est-ce qu'une violation de données?

Il s'agit d'un incident au cours duquel des personnes non autorisées accèdent à des données sensibles ou confidentielles, entraînant souvent la divulgation, le vol ou l'utilisation abusive de renseignements personnels ou financiers. Ces violations peuvent se produire par le biais du piratage, de l'hameçonnage ou de vulnérabilités du système.

- Il peut s'agir de dossiers de clients, de données financières ou d'identifiants de connexion.
- Une violation de données peut entraîner une atteinte à la réputation, des conséquences juridiques et des pertes financières.
- Elle peut souvent être évitée grâce à des contrôles d'accès rigoureux, au cryptage et à des audits réguliers des systèmes.

Qu’est-ce qu’un hypertrucage?

Il s’agit des médias générés par l’IA – vidéos, fichiers audio ou images – qui imitent de manière convaincante des personnes réelles, souvent utilisés pour tromper, usurper l’identité ou manipuler des victimes. Ces créations synthétiques peuvent être utilisées à des fins frauduleuses, notamment pour usurper l’identité de personnes de confiance dans le cadre de transactions à fort enjeu.

- Les hypertrucages peuvent reproduire les voix, les expressions faciales et les manières avec une précision déconcertante.
- Ils sont souvent utilisés dans les escroqueries par piratage psychologique ou usurpation d’identité pour gagner la confiance ou autoriser des actions frauduleuses.
- Ils posent des risques croissants dans les secteurs juridique, financier et immobilier où la vérification de l’identité est essentielle.

Qu’est-ce que l’usurpation d’identité synthétique?

Une forme sophistiquée de fraude où les criminels créent une nouvelle identité en combinant des renseignements personnels réels et fictifs. Ces identités sont souvent utilisées pour ouvrir des comptes, demander des prêts ou effectuer des transactions immobilières frauduleuses.

- Il peut s’agir de véritables numéros d’assurance sociale associés à de faux noms, adresses ou renseignements sur l’emploi.
- L’usurpation d’identité synthétique est difficile à détecter, car l’identité n’appartient pas à une seule personne réelle.
- Elle peut entraîner des dommages financiers à long terme et des complications juridiques pour les victimes et les institutions.

Qu’est-ce que la fraude numérique liée au titre?

Une forme de fraude immobilière dans laquelle des criminels utilisent des identités volées ou synthétiques pour transférer illégalement la propriété d’un bien immobilier ou accéder à la valeur nette d’un logement, souvent à l’aide d’outils numériques et de canaux de communication. Ces stratagèmes exploitent les failles dans les processus de vérification de l’identité et de transaction à distance.

- Peut impliquer des documents falsifiés, l’usurpation d’identité de propriétaires ou des demandes de prêt hypothécaire frauduleuses.
- De plus en plus souvent, ces fraudes sont commises par le biais de courriels frauduleux, de plateformes en ligne et de faux identifiants numériques.
- Peut entraîner des pertes financières importantes et des complications juridiques pour les propriétaires et les professionnels.

Qu’est-ce que la fraude électronique?

Un type de fraude financière dans lequel des criminels se font passer pour des parties légitimes – clients, avocats ou prêteurs – afin de rediriger les fonds de clôture vers leurs propres comptes. Ces stratagèmes reposent souvent sur l’usurpation d’adresse courriel et le piratage psychologique pour manipuler des professionnels de confiance lors de transactions de grande valeur.

- Ce type de fraude cible fréquemment les clôtures de transactions immobilières et les transferts de fonds fiduciaires.
- Les pirates peuvent utiliser de fausses adresses courriel ou des comptes piratés pour envoyer des instructions de paiement convaincantes.
- Peut entraîner des pertes financières importantes et nuire à la réputation.

Conversation sur la cyberfraude avec John Tracy

Dans un environnement immobilier de plus en plus numérisé, les fraudeurs perfectionnent leurs méthodes et utilisent toutes sortes de moyens, des identités synthétiques au piratage des courriels, pour exploiter les vulnérabilités des transactions immobilières. Pour mieux comprendre ces nouvelles menaces et la manière dont le secteur peut y répondre, nous nous sommes entretenus avec John Tracy, conseiller juridique principal chez FCT et figure de proue dans le domaine de la prévention de la fraude. Fort de sa vaste expérience dans l'analyse des réclamations en assurance titres, John partage ses idées sur l'évolution du paysage des cybermenaces, le rôle de la technologie et l'importance cruciale de la vigilance humaine. Cet entretien offre des conseils pratiques aux professionnels du droit, aux agents immobiliers et aux clients qui doivent faire face aux réalités complexes de la fraude numérique dans le secteur de l'immobilier.

Comment l'essor des hypertrucages et de l'usurpation d'identité synthétique affecte-t-il le processus de vérification de l'identité des clients et quelles mesures sont prises pour lutter contre ce phénomène?

L'usurpation d'identité synthétique est un problème de plus en plus préoccupant, même s'il reste relativement rare dans nos réclamations. Je me souviens d'un cas, il y a plusieurs années, où une identité fictive – une personne qui n'existait pas – avait été utilisée pour obtenir un prêt hypothécaire auprès d'une grande banque. Ces stratagèmes s'inscrivent dans le long terme; les fraudeurs se constituent progressivement un profil de crédit afin de donner une apparence légitime à leur fausse identité. Cependant, pour être crédible, une identité synthétique doit comporter un lien avec une personne réelle, elle n'est jamais entièrement fictive. Quant aux hypertrucages, nous n'en avons pas encore vu apparaître dans nos réclamations, mais nous les surveillons de près. Les appels téléphoniques et les réunions vidéo jouent toujours un rôle clé dans la vérification de l'identité des clients, et bien que des outils comme Zoom puissent potentiellement être exploités, nous n'avons pas rencontré ce scénario jusqu'à présent.

Comment avez-vous vu évoluer le paysage des cybermenaces au cours de votre carrière chez FCT? Au cours des dernières années en particulier, quelles avancées ont eu le plus grand impact sur la fraude immobilière et la fraude liée au titre?

Au fil des ans, les cybermenaces sont devenues beaucoup plus sophistiquées, notamment avec l'apparition de fausses identités quasi parfaites et de techniques avancées de piratage des courriels. L'un des changements les plus marquants a été le ciblage des professionnels du droit : si l'adresse courriel d'un avocat est piratée, les fraudeurs peuvent détourner des fonds avec une facilité déconcertante. Ces violations sont souvent dues à des vulnérabilités simples telles que la réutilisation de mots de passe ou l'absence d'authentification multifactorielle. Cela dit, l'accès à un compte de courriel ne garantit pas le succès des fraudeurs; le volume considérable de messages quotidiens peut parfois jouer en notre faveur, noyant les tentatives malveillantes dans le bruit ambiant. Pourtant, les risques sont réels et les conséquences peuvent être graves.

Les nouvelles techniques de fraude, comme les hypertrucages et l'usurpation d'identité synthétique, ont-elles remplacé les méthodes traditionnelles, ou y a-t-il un équilibre entre les deux?

Il y a clairement encore un équilibre. Les tactiques de fraude traditionnelles – comme la falsification de documents et l'usurpation d'identité – restent efficaces et nous les observons régulièrement. Ce qui a changé, c'est que de nouvelles technologies, telles que les identités synthétiques et les hypertrucages, sont désormais utilisées pour améliorer ces anciennes méthodes. Les fraudeurs ne délaissent pas les méthodes traditionnelles; ils les perfectionnent pour rendre leurs stratagèmes plus convaincants et plus difficiles à détecter. Il s'agit d'une approche à plusieurs niveaux, et c'est ce qui nous complique autant la tâche.

La fraude électronique est devenue l'un des risques les plus préjudiciables dans les transactions immobilières. Où voyez-vous les plus grandes vulnérabilités pour les avocats, les agents immobiliers et les clients?

Dans toute transaction immobilière, on n'est jamais plus fort que son maillon le plus faible. Les avocats, en particulier, sont soumis à une pression considérable, surtout lors des journées chargées de clôture, où le volume considérable de tâches peut entraîner des lacunes en matière de sécurité de l'information. Si la cybersécurité n'est pas intégrée à chaque étape du processus, cette « activité intense » peut devenir une grave vulnérabilité. Les fraudeurs savent comment exploiter ces moments, et même un petit oubli peut ouvrir la porte à une fraude électronique aux conséquences dévastatrices.

La fraude liée au titre est un risque connu depuis de nombreuses années, mais comment voyez-vous émerger la fraude numérique liée au titre à l'ère des registres électroniques et des systèmes immobiliers en ligne?

Les systèmes numériques ont certes changé la donne, mais ils n'ont pas nécessairement facilité la fraude liée au titre, ils l'ont simplement transformée. Une préoccupation émergente concerne la manipulation des registres d'entreprise en ligne. Les fraudeurs peuvent modifier la liste des dirigeants et administrateurs d'une société propriétaire d'un bien immobilier, puis exploiter cette fausse autorité pour transférer ou hypothéquer le terrain. Si le passage aux dossiers électroniques apporte un gain d'efficacité, il introduit également de nouvelles vulnérabilités. Cela dit, commettre une fraude par voie numérique n'est pas intrinsèquement plus simple que de le faire en personne : cela nécessite toujours un niveau élevé de planification et de précision.

Quelles mesures de protection peuvent être mises en place pour empêcher les fraudeurs d'exploiter les registres numériques et prévenir le risque de violation de données qui en découle?

Il s'agit avant tout de placer la sécurité de l'information au premier plan. Même si cela peut sembler répétitif, les principes fondamentaux restent importants : utiliser des mots de passe forts et uniques, les changer régulièrement, activer l'authentification multifactorielle et faire preuve de prudence quant aux renseignements personnels partagés en ligne. Les médias sociaux, en particulier, peuvent être une mine d'or pour les fraudeurs si les gens partagent trop de renseignements. Ces pratiques élémentaires sont souvent négligées, mais elles sont essentielles pour protéger l'accès aux registres numériques et prévenir les violations susceptibles d'entraîner des fraudes graves.

Pourriez-vous nous donner un exemple de recours à l'usurpation d'identité synthétique et à l'hypertrucage dans le cadre d'un transfert de propriété ou d'une demande de prêt hypothécaire?

La fraude par identité synthétique est une escroquerie à long terme dans laquelle les fraudeurs créent une identité fictive à partir d'informations réelles et fausses, établissant progressivement une solvabilité pour la rendre légitime. Dans le domaine de l'immobilier, il s'agit souvent d'imiter la signature d'un propriétaire pour transférer la propriété d'un bien à l'identité synthétique. Une fois « propriétaire », le fraudeur obtient un prêt hypothécaire et récupère la majeure partie des fonds. Bien que plus courante dans le domaine de la fraude à la carte de crédit en raison d'un accès plus facile, elle existe également dans l'immobilier, même si elle est plus complexe et nécessite davantage de ressources. Il convient de noter que les hypertrucages ne sont généralement pas nécessaires : une fausse pièce d'identité convaincante suffit pour contourner la vérification. Une tactique plus courante est l'usurpation d'identité, où le fraudeur se fait passer pour un véritable détenteur d'hypothèque et draine les fonds propres par le biais d'une hypothèque

Quel rôle les assureurs de titres comme FCT peuvent-ils jouer pour aider les professionnels à atténuer ces risques de fraude électronique?

Les assureurs de titres comme FCT jouent un rôle essentiel tant dans la prévention que dans la protection. Avant tout, nous mettons l'accent sur l'éducation, en aidant les professionnels à comprendre comment une faille de cybersécurité peut avoir un impact direct sur une transaction immobilière. Nos souscripteurs sont formés pour repérer les signaux d'alerte et rechercher activement les signes de fraude électronique ou d'usurpation d'identité au cours du processus. Et lorsque quelque chose tourne mal, l'assurance titre est là pour vous protéger contre les pertes financières, vous offrant un filet de sécurité en cas d'imprévu.

Si une violation de données survient dans un cabinet d'avocats ou une société de courtage, quelles mesures FCT peut-elle prendre pour aider à atténuer l'impact et protéger les transactions futures?

Bien que FCT ne soit pas en mesure de fournir directement des services informatiques à un cabinet d'avocats ou à une société de courtage victime d'une violation, nous pouvons néanmoins jouer un rôle important. Si la violation donne lieu à une réclamation couverte, les clients concernés bénéficieront de la protection offerte par leurs polices d'assurance titre afin de les aider à récupérer les pertes assurées. En outre, FCT possède une grande expérience dans la gestion de ces situations et peut offrir des conseils sur les mesures immédiates à prendre pour réduire ou éviter d'autres pertes. Notre objectif est d'accompagner les professionnels dans les suites de ces événements et de contribuer à Défendreles transactions futures.

Quelles sont actuellement les technologies les plus prometteuses et les plus efficaces pour se protéger contre les cas de fraude numérique?

Il existe des outils prometteurs, tels que Bluink, qui permettent de prévenir l'usurpation d'identité en vérifiant les identités de manière sécurisée, et des programmes de courriel avancés qui peuvent signaler les domaines suspects ou les adresses falsifiées avant qu'ils ne causent des dommages. Mais aucune technologie n'est infaillible. Comme on nous le rappelle souvent, nous devons tous être des pare-feu humains. Cela signifie qu'il faut rester vigilants, adopter de bonnes habitudes en matière de cybersécurité et ne pas compter uniquement sur la technologie pour nous protéger. La meilleure défense est une combinaison d'outils intelligents et de personnes intelligentes.

Désarmer

La grande réclamation : Comment un fraudeur a détourné un remboursement hypothécaire de plusieurs millions de dollars

Tout a commencé par une opération de refinancement de grande valeur, d'une structure classique, mais qui s'est rapidement transformée en l'une des affaires de fraude les plus importantes jamais traitées par FCT. FCT avait émis une police d'assurance titre pour une grande institution financière canadienne, assurant une hypothèque de premier rang à dix chiffres. La transaction devait se dérouler sans encombre, mais elle a plutôt été la cible d'une fraude sophistiquée par usurpation d'identité et de fraude électronique.

La première étape du fraudeur a consisté à accéder au compte de courriel légitime de l'avocat, un acte d'hameçonnage qui a ouvert la voie à une tromperie à plusieurs niveaux. En exploitant le cabinet d'avocats, en créant de fausses adresses courriel et en usurpant l'identité de l'avocat, le fraudeur s'est immiscé dans la transaction, interceptant et manipulant les communications entre les parties. Une fois encore, les fraudeurs ne se sont pas contentés d'usurper l'identité de quelqu'un, ils ont filtré, intercepté et falsifié des courriels légitimes, et ont peut-être même réussi à négocier des documents légitimes en maintenant l'illusion de l'authenticité tout au long du processus de communication.

Au cours de la transaction, le fraudeur a intercepté le véritable relevé de remboursement hypothécaire et les instructions de virement, les a modifiés et a envoyé les documents falsifiés au prêteur. Faisant confiance à la source, le prêteur a transmis les instructions de remboursement frauduleuses à FCT.

Le résultat : Un remboursement hypothécaire très important, de plusieurs millions, a été détourné vers un compte financier contrôlé par le fraudeur. L'hypothèque n'a pas été levée. L'assuré était exposé. La fraude avait réussi.

Cette affaire souligne la nature évolutive de la cybercriminalité dans les transactions immobilières. Il ne s'agissait pas seulement d'une violation, mais d'un piratage et d'une usurpation d'identité à part entière, exécutés avec précision et patience. Le fraudeur ne s'est pas appuyé sur un seul point de défaillance; il a exploité plusieurs niveaux de confiance, de communication et de processus, autant d'éléments caractéristiques des tactiques sophistiquées de piratage psychologique.

Cette affaire nous rappelle avec force que la vérification des adresses courriel ne suffit plus à elle seule. Dans le cadre de transactions de grande valeur, en particulier celles impliquant le remboursement d'un prêt hypothécaire, l'authentification multifactorielle et une vigilance accrue sont essentielles. Remettre en question la source, le moment et le contexte de chaque instruction n'est pas seulement prudent, c'est essentiel.

Il ne s'agissait pas d'une simple réclamation, mais d'une réclamation importante et d'un enseignement majeur : un exemple révélateur de la manière dont la fraude peut infiltrer même les systèmes les plus sécurisés, et de la raison pour laquelle la vigilance doit évoluer au même rythme que les menaces auxquelles nous sommes confrontés.

« Ce qui rend cette affaire si frappante, c'est la sophistication même de la supercherie. Le fraudeur ne s'est pas contenté de pirater un système : il a usurpé une identité, contrôlé les communications et manipulé la confiance à chaque étape de la transaction. C'est un signal d'alarme pour l'ensemble du secteur, qui montre que la cybercriminalité dans l'immobilier a atteint un nouveau niveau de précision et de patience.

Robert Antenore, LL.B.
Vice-président, Solutions commerciales

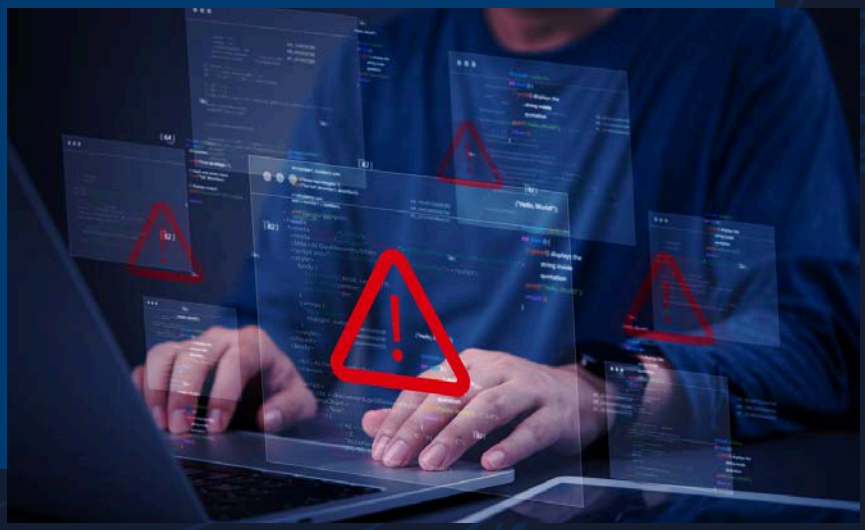
Réclamation : Quand une confirmation ne suffisait pas : un remboursement hypothécaire intercepté par fraude

Ce qui semblait être une transaction ordinaire a rapidement pris une tournure que personne n'avait prévue. L'avocat d'un prêteur a envoyé des instructions de virement mises à jour à l'avocat de l'assuré qui, conformément aux meilleures pratiques, a confirmé le changement en répondant au même fil de discussion par courriel. Mais quelque chose clochait. Le prêteur n'a jamais reçu les fonds.

La suite des événements a révélé une cyberattaque sophistiquée. Le compte de courriel du prêteur avait été piraté, et un fraudeur s'était immiscé dans la conversation. Les instructions de virement étaient fausses, et le paiement hypothécaire, destiné à rembourser le prêt, a été redirigé vers un compte frauduleux. L'hypothèque n'a pas été levée, laissant l'assuré dans une position vulnérable.

L'enquête a révélé non seulement l'impact financier, mais aussi les limites des méthodes de vérification traditionnelles face à l'évolution des cybermenaces.

Si la compromission du courriel avait été détectée plus tôt, ou si un canal secondaire avait été utilisé pour confirmer le changement, cette fraude aurait pu être stoppée avant que les fonds ne soient perdus. Cela nous rappelle avec force que Défendreune transaction ne se limite pas à confirmer les détails; cela implique également de s'interroger sur le contexte, le moment choisi et la source.



Réclamation : Un courriel exposé. Une commission perdue.

Une transaction immobilière était sur le point d'être conclue lorsque l'avocat a reçu une demande apparemment simple : l'agent souhaitait que sa commission lui soit versée par virement électronique plutôt que par chèque. La demande provenait de l'adresse courriel de l'agent et rien ne semblait suspect, jusqu'à ce que les fonds disparaissent.

Le compte de courriel de l'agent avait été piraté. Un fraudeur, se faisant passer pour l'agent, a intercepté la communication et redirigé la commission vers un compte frauduleux. L'avocat, ignorant la violation, a suivi les instructions de bonne foi.

L'enquête a confirmé la couverture après un examen approfondi. Cette affaire nous rappelle brutalement que les cybercriminels ne visent pas uniquement les grosses sommes d'argent, mais exploitent également la confiance et la familiarité dans les transactions quotidiennes.

Dans ce cas précis, la fraude n'a été découverte que lorsqu'il était déjà trop tard. Mais cela a mis en évidence comment une simple mesure, telle que la vérification d'un changement de mode de paiement via un canal distinct, aurait pu mettre fin à la fraude. C'est une leçon qui nous apprend à défendrenon seulement les systèmes, mais aussi les habitudes et les hypothèses sur lesquelles nous nous appuyons chaque jour.

Défendre

Préparer l'avenir : Comprendre les risques futurs et l'évolution des menaces

Principales tendances en matière de fraude :

L'IA transforme l'usurpation d'identité et la fraude

Les transactions à distance ont toujours présenté un risque de fraude, mais la menace s'est complètement transformée grâce aux nouveaux outils basés sur l'intelligence artificielle que les fraudeurs peuvent utiliser pour usurper efficacement l'identité de leur cible. Les professionnels doivent se méfier, même dans ces types de communications :

- Appels téléphoniques : Les outils de synthèse vocale basés sur l'IA et la modulation vocale en temps réel permettent aux fraudeurs de modifier leur âge, leur sexe et leur accent apparents afin de mieux correspondre à leur histoire, tandis que les outils d'usurpation d'identité peuvent faire croire que l'appel provient du numéro de téléphone choisi par le fraudeur.
- Réunions virtuelles : La technologie d'hypertrucage était auparavant limitée à l'usurpation d'identité pré-générée de personnes apparaissant dans de nombreuses séquences vidéo, telles que des politiciens et des célébrités. Elle s'est améliorée au point de pouvoir remplacer le visage d'un fraudeur par celui d'un propriétaire, devant la caméra, en temps réel.

La fraude en personne est en hausse

Avant l'IA, la raison pour laquelle les transactions à distance étaient considérées comme risquées était la distance : un fraudeur lors d'un appel vidéo pouvait brandir une pièce d'identité volée sur laquelle il ressemblait au véritable propriétaire, voire coller sa propre photo sur la carte. Si une transaction pouvait être effectuée au bureau avec des pièces d'identité physiques, la supercherie était plus susceptible d'être découverte. Mais avec l'accès des fraudeurs à des logiciels d'édition et du matériel d'impression plus avancés, les professionnels sont confrontés à une nouvelle réalité : la personne assise en face d'eux, munie d'une pièce d'identité intacte et d'apparence légitime sur laquelle figure sa photo, peut être un imposteur. Les faux documents d'identité sont devenus si sophistiqués que la vérification en personne ne garantit plus l'absence de fraude.

L'usurpation d'identité n'est qu'un début

Les fraudeurs peuvent utiliser de petits éléments de renseignements compromis sur leur cible pour obtenir davantage d'informations sur cette personne auprès d'institutions financières, d'entreprises ou de services gouvernementaux, jusqu'à ce qu'ils en aient suffisamment pour usurper son identité. Les fraudeurs peuvent également se rendre plus difficiles à détecter en créant des identités synthétiques : ils utilisent un seul élément d'identité compromis, comme le numéro d'assurance sociale (NAS) d'une cible, et y ajoutent des informations personnelles fictives. Ils peuvent ensuite utiliser cette fausse identité pour demander de petits prêts et d'autres actifs qui, au fil du temps, confèrent à cette identité une certaine légitimité, voire un historique de crédit.

Un avenir « sans intervention »

Nous pourrions assister au premier cas de fraude hypothécaire commise par un acteur non humain : les outils d'IA utilisés par les fraudeurs peuvent être combinés et gérés par un seul algorithme dont les directives sont définies par le fraudeur, puis déployés pour une exécution « sans intervention ». Les institutions financières investiront probablement dans le développement de défenses contre la fraude et les cyberattaques basées sur l'IA à mesure que la menace grandit. À mesure que les tactiques et les contre-tactiques de fraude commencent à échapper au contrôle humain, leur orientation devient de plus en plus difficile à prévoir.

Conversation sur les risques futurs et l'évolution des menaces avec Marie Taylor

Alors que le secteur immobilier continue de s'adapter à un monde de plus en plus numérique, les menaces qui pèsent sur son intégrité évoluent elles aussi. Pour nous aider à anticiper et à préparer l'avenir de la cybersécurité dans les transactions immobilières, nous nous sommes entretenus avec Marie Taylor, directrice, souscription nationale, Risque juridique et conformité chez FCT. Avec plus de vingt ans d'expérience au sein de l'équipe juridique de FCT, Marie est une experte reconnue à l'échelle nationale dans le domaine de l'assurance titres immobiliers résidentiels et de la prévention de la fraude. En tant qu'auditrice de fraude certifiée et ancienne membre du comité consultatif technique de l'Autorité ontarienne de réglementation des services financiers pour le courtage hypothécaire, Marie apporte une mine d'informations sur les risques émergents et les technologies qui façonnent l'avenir de la fraude liée au titre. Dans la série de questions-réponses qui suit, elle partage son point de vue sur la manière dont l'IA, les identités synthétiques et les plateformes numériques transforment le paysage de la fraude, et sur ce que le secteur doit faire pour garder une longueur d'avance.

Selon vous, quelles techniques émergentes de cyberfraude représenteront la plus grande menace pour les transactions immobilières au cours des trois à cinq prochaines années?

La sophistication croissante des fraudeurs, associée à l'émergence de l'IA, représente la plus grande menace. Il y a quelques années encore, il était facile de détecter l'hameçonnage et l'hameçonnage par message texte grâce aux erreurs grammaticales et typographiques. Aujourd'hui, grâce à l'intelligence artificielle, les fraudeurs rédigent des courriels très authentiques. Les hypertrucages évoluent également, et il n'est plus aussi facile de déterminer si la personne à l'autre bout de l'écran est bien celle à qui vous pensez parler. Le clonage vocal est également devenu très convaincant. L'évolution de l'IA a rendu le travail des fraudeurs beaucoup plus facile qu'avant la Covid.

Avec la numérisation croissante des registres fonciers et des documents juridiques, quelles sont les vulnérabilités que vous identifiez et auxquelles le secteur devrait commencer à se préparer dès maintenant?

Avec la numérisation des registres fonciers et des documents juridiques, l'une des vulnérabilités les plus importantes est le risque de cyberattaques, en particulier les rançongiciels. Comme ces systèmes stockent des données hautement sensibles, il est essentiel de mettre en place des mesures de sécurité robustes, notamment des protocoles d'authentification résilients, des sauvegardes de données fiables et une surveillance proactive des menaces, afin de garantir l'intégrité et la disponibilité des enregistrements face à l'évolution des menaces numériques.

Comment voyez-vous évoluer les outils basés sur l'IA, tels que les hypertrucages et le clonage vocal, dans leur capacité à contourner les systèmes de vérification de l'identité utilisés dans les transferts de propriété?

Les fraudeurs utilisent de plus en plus l'IA pour créer des fichiers audio et vidéo synthétiques convaincants, leur permettant d'usurper l'identité de cadres supérieurs ou d'utilisateurs autorisés afin d'accéder à des systèmes sécurisés ou d'approuver des transactions. Les hypertrucages peuvent imiter les traits du visage, tandis que le clonage vocal reproduit les voix pour tromper l'authentification biométrique. Une récente escroquerie qui a fait l'objet d'une importante couverture médiatique a vu un employé du secteur financier de Hong Kong se faire piéger et envoyer 25 millions de dollars lors d'une réunion en ligne avec de faux participants utilisant des hypertrucages pour se faire passer pour de vraies personnes. Les criminels peuvent désormais falsifier des documents, des égoportraits et des voix pour créer de fausses identités numériques et commettre des fraudes. Avec cette technologie, on imagine facilement un fraudeur créer une pièce d'identité réaliste et utiliser des hypertrucages pour se faire passer pour un avocat conseillant à un client d'envoyer des fonds afin de conclure une transaction immobilière.

Selon vous, quel rôle la chaîne de blocs ou les technologies décentralisées pourraient-elles jouer dans la prévention ou la facilitation des fraudes liées au titre à l'avenir?

Personnellement, je pense que l'utilisation de la technologie de chaînes de blocs pourrait aider à prévenir les futures fraudes liées au titre. Je ne suis pas particulièrement versée dans la technologie de chaînes de blocs, mais d'après ce que j'ai lu, c'est un concept intéressant. Imaginez disposer d'une base de données pour une transaction immobilière où toutes les données, depuis la conclusion d'un accord d'achat et de vente jusqu'à l'obtention d'un prêt hypothécaire, en passant par la préparation des documents juridiques et l'envoi des fonds, sont stockées dans un endroit sécurisé et inviolable.

Pensez-vous que la fraude par identité synthétique se généralisera dans le secteur immobilier, et comment les fraudeurs pourraient-ils adapter leurs tactiques actuelles pour exploiter plus efficacement les systèmes hypothécaires?

La fraude par identité synthétique est déjà largement répandue dans les transactions immobilières. Equifax Canada a rapporté en 2024 que les cas avaient triplé en seulement un an. Grâce aux nouvelles techniques et technologies, les fraudeurs disposent de plus de moyens pour exploiter les vulnérabilités des systèmes. Nous sommes passés des demandes de prêt hypothécaire en personne et des remises de chèques dans les bureaux d'enregistrement foncier à des processus entièrement numériques (demandes en ligne, signatures électroniques et virements bancaires) sans jamais nous rencontrer en personne. Cette évolution crée un environnement idéal pour les fraudeurs, qui peuvent se cacher derrière la technologie et se faire passer pour des professionnels, ce qui facilite plus que jamais la fraude immobilière.

Comment les assureurs de titres comme FCT peuvent-ils mieux aider les professionnels du droit et les agents immobiliers à se préparer à la prochaine vague de cybermenaces?

Je pense que la formation et l'utilisation de logiciels de vérification de l'identité tels que Bluink et Fintracker contribuent grandement à aider nos clients. Les systèmes que nous utilisons sont hautement sécurisés et surveillés en temps réel afin de détecter toute menace potentielle. FCT a été le tout premier assureur de titres à recourir à la souscription anti-fraude il y a plus de 20 ans, et nous travaillons sans relâche pour rester au fait des dernières tendances en matière de fraude afin d'atténuer les risques pour les avocats, les professionnels du crédit et, bien sûr, pour nous-mêmes.

Quels sont les principaux risques associés aux plateformes tierces (par exemple, les outils de signature électronique, les logiciels de réunions virtuelles) dans le contexte des transactions immobilières sécurisées? Y a-t-il quelque chose que nous puissions faire pour atténuer les risques liés à l'utilisation de ces outils?

Les principaux risques que nous voyons associés à l'utilisation de ces plateformes sont les menaces liées à la cybersécurité, les violations de données et la fraude. Certains systèmes mal conçus peuvent ne pas disposer de pistes d'audit complètes ou d'un enregistrement suffisant des données. Pour atténuer ce risque, il faut utiliser des plateformes dotées d'un cryptage puissant, d'une authentification multifactorielle et de pistes d'audit complètes. Vous devez faire preuve de diligence raisonnable envers le fournisseur : renseignez-vous sur la manière dont les informations sont stockées, comprenez et apprenez ses politiques de sécurité et ses pratiques en matière de traitement des données.

Existe-t-il, selon vous, des technologies émergentes ou des innovations susceptibles de révolutionner la prévention de la fraude dans le domaine de l'assurance titres?

Je crois que la prévention de la fraude nécessite une combinaison de technologie, de vigilance et de proactivité. Je pense que la chaîne de blocs et la vérification biométrique robuste contribueront grandement à la prévention de la fraude, mais il en va de même pour la bonne vieille méthode qui consiste à connaître son client et à se fier à son instinct. Il est important de garder à l'esprit que, si la technologie améliore notre capacité à prévenir la fraude, elle fournit également aux fraudeurs davantage d'outils pour la commettre. En tant qu'industrie, nous devons tous travailler ensemble pour faire tout notre possible afin de prévenir ce phénomène et essayer de garder une longueur d'avance.

Alors que les progrès technologiques aident les cybercriminels à mieux s'organiser et à collaborer, comment FCT devrait-elle faire évoluer ses stratégies internes de détection et de prévention de la fraude pour garder une longueur d'avance?

Je pense que FCT a déjà pris des mesures importantes pour faire évoluer ses stratégies internes de détection des fraudes. Nous disposons d'une équipe dédiée composée de personnes expérimentées qui suivent une formation continue sur la manière de détecter les nouveaux types de fraude potentielle. Nous travaillons en étroite collaboration avec notre service des réclamations afin d'analyser nos réclamations de fraude et de voir s'il existe des tendances qui nous obligent à modifier notre souscription. Nous utilisons également un logiciel de vérification de l'identité qui analyse de nombreux attributs différents afin de détecter les identités frauduleuses.

À l'avenir, quels changements culturels ou comportementaux au sein du secteur vous semblent nécessaires pour renforcer la cyberrésilience de toutes les parties prenantes?

Je pense que le secteur doit accepter le fait que la fraude est là pour durer et qu'elle ne fera que devenir plus facile pour les fraudeurs. Nous devons nous informer sur la manière dont cela se produit et sur les moyens de l'empêcher. Nous devons renforcer nos pratiques en matière de sécurité personnelle en utilisant des mots de passe forts, une authentification multifactorielle, des pare-feu et des logiciels de vérification de l'identité sécurisés. Vérifiez, vérifiez, vérifiez– et ne vous reposez jamais sur vos lauriers, car tout le monde peut être victime d'une fraude.

Comment FCT peut être votre partenaire pour des transactions immobilières sécurisées

Le rôle de la vérification de l'identité des clients dans la cybersécurité

Sur le marché immobilier actuel, où le numérique occupe une place prépondérante, la vérification de l'identité des clients n'est plus seulement une obligation réglementaire, mais aussi une ligne de défense essentielle contre les cybermenaces et la fraude. Les cybercriminels continuent d'exploiter les faiblesses à l'aide de tactiques telles que l'hameçonnage, le piratage psychologique et l'usurpation d'identité synthétique, mettant ainsi en péril les données sensibles des clients et les transactions immobilières. Une solution robuste de vérification de l'identité des clients permet de protéger toutes les parties en garantissant que les personnes sont bien celles qu'elles prétendent être. Grâce à des outils avancés tels que les contrôles biométriques, l'authentification multifactorielle et le traitement crypté des données, ces systèmes créent une couche de sécurité supplémentaire qui empêche les fraudeurs d'exploiter les vulnérabilités. Pour les professionnels de l'ensemble du secteur, des professionnels du droit aux agents immobiliers, la vérification de l'identité est synonyme de tranquillité d'esprit, de conformité réglementaire et de protection contre les risques croissants de cyberfraude.

Fintracker : Un partenaire de conformité pour les agents immobiliers

Fintracker est conçu pour les agents immobiliers et les courtiers. Plus qu'un simple outil de vérification de l'identité, Fintracker offre une plateforme numérique complète de conformité qui s'intègre parfaitement aux processus immobiliers. Il numérise et authentifie les pièces d'identité délivrées par les gouvernements, remplissant automatiquement certaines des informations requises sur les formulaires CANAFE et effectue des vérifications complètes par rapport aux listes de surveillance de la lutte contre le blanchiment d'argent, aux sanctions et aux sources médiatiques défavorables. En conservant des dossiers cryptés et prêts à être vérifiés, Fintracker réduit la paperasserie et garantit que les courtiers et les agents immobiliers sont toujours prêts pour les contrôles réglementaires. Ce qui rend Fintracker unique, c'est sa capacité à simplifier la conformité dans un marché en constante évolution, ce qui renforce la confiance des agents immobiliers. Avec Fintracker, la vérification de l'identité n'est pas seulement une mesure de sécurité, c'est aussi un puissant catalyseur d'efficacité, de confiance et de responsabilité professionnelle.

Bluink : Un outil de confiance pour les professionnels du droit

a solution de vérification de l'identité des clients de FCT, optimisée par **Bluink**, vise à créer une expérience sécurisée et conforme pour les professionnels du droit. Bluink utilise essentiellement la vérification biométrique et l'authentification avancée des documents pour confirmer l'identité des clients à l'aide de pièces d'identité délivrées par le gouvernement. Ce qui distingue Bluink, c'est l'importance accordée à la confidentialité dans sa conception. Les identifiants vérifiés sont stockés en toute sécurité sur l'appareil mobile du client dans son portefeuille numérique, et non sur des serveurs centraux, ce qui réduit le risque de violation des données. Pour les avocats et les notaires, cela signifie une conformité simplifiée avec les exigences du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) en matière de connaissance du client et celles du Barreau, tout en garantissant la protection des renseignements sensibles. Bluink allie facilité d'utilisation et normes de sécurité de pointe, permettant ainsi aux professionnels du droit de se concentrer sur le service à la clientèle en toute confiance, sachant que leurs transactions sont soutenues par des identités fiables et vérifiées.

Ensemble, des solutions comme Bluink et Fintracker renforcent les défenses du secteur immobilier contre la cyberfraude. En adaptant la vérification de l'identité aux besoins uniques des professionnels du droit et des agents immobiliers, FCT contribue à garantir que chaque transaction est sécurisée, conforme et fondée sur la confiance.

Mot de conclusion de notre Chef de la direction FCT

Comme nous l'avons vu, les cybermenaces constituent un risque en constante évolution, mais notre meilleure défense consiste à rester informés et proactifs. Quand on sait comment **détecter** les signaux, prendre des mesures pour **désarmer** les activités suspectes et mettre en place des mesures de protection pour **défendre** les renseignements sensibles, on peut créer des transactions immobilières plus sûres. Pour continuer à développer vos connaissances et votre résilience face aux cybermenaces, nous vous invitons à consulter les articles de notre blogue ci-dessous, où vous trouverez des renseignements pratiques et des ressources qui vous aideront à garder une longueur d'avance sur les risques émergents :

Chaque solution que nous commercialisons est conçue dans un souci d'innovation et de sécurité, car le progrès sans protection ne devrait jamais être une option. Nos clients nous font confiance pour leur fournir des outils fiables et tournés vers l'avenir. Cette confiance, nous la gagnons en veillant à ce que chaque innovation reflète le même niveau de sécurité qui caractérise FCT.

Michael LeBlanc, LL.B.
Chef de la direction, FCT.

Poursuivre l'apprentissage :

Pour continuer à développer vos connaissances et votre résilience face aux cybermenaces, nous vous invitons à explorer nos articles de blog ci-dessous, où vous trouverez des informations et des ressources pratiques pour vous aider à garder une longueur d'avance sur les risques émergents:

- Ce que vos clients et vous devez savoir au sujet de la vérification de l'identité
- Comment la technologie a-t-elle transformé la fraude liée au titre?
- Quelles sont les prochaines étapes? L'avenir de la prévention de la fraude
- Vérification de l'identité numérique : comment connaître son client?

Restez informé des dernières informations de FCT en matière de prévention de la fraude :

Centre d'information sur la fraude