

Guide des ressources en
matière de cybersécurité

2026 de FCT



Tabale des matières

Introduction	Décoder la cybersécurité : Termes et concepts clés à connaître	Conversation sur la cybersécurité avec Cory Woods
1	4	7
Le vocabulaire des fraudeurs : Termes et tactiques essentiels de la cyberfraude		Conversation sur la cyberfraude avec John Tracy
10		13
La grande réclamation : Comment un fraudeur a détourné un remboursement hypothécaire de plusieurs millions de dollars	Autres histoires de réclamations pour fraude	Préparer l'avenir : Comprendre les risques futurs et l'évolution des menaces
17	19	22
Conversation sur les risques futurs et l'évolution des menaces avec Matt Cunnington	Comment FCT peut être votre partenaire pour des transactions immobilières	Conclusion
24	29	31

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 Cory Woods



La complexité et l'ampleur des cybermenaces continuent d'évoluer et les entreprises des secteurs de l'immobilier et des services financiers sont confrontées à des défis croissants par rapport à la protection des renseignements sensibles et au maintien de la confiance et de la sécurité des transactions de grande valeur.

Pour faire la lumière sur ces questions, nous avons discuté avec Cory Woods, chef du service de l'information chez FCT. Fort de ses années d'expérience en cybersécurité et en gestion du risque, Cory nous a donné son point de vue sur l'évolution des menaces, les technologies émergentes et l'importance de maintenir la confiance dans un monde de plus en plus numérique.

Cet entretien contient de précieux renseignements pour les professionnels du droit, les agents immobiliers, les prêteurs et tous ceux qui souhaitent comprendre comment la cybersécurité continue de façonner les affaires modernes.

■ À votre avis, quels sont les risques les plus importants auxquels font face les industries de l'immobilier et de l'assurance titres à l'heure actuelle?

L'un des risques les plus importants demeure la fraude fondée sur l'identité.

Les cybercriminels parviennent de mieux en mieux à se faire passer pour des personnes de confiance, que ce soit au moyen de comptes compromis, de communications frauduleuses ou de techniques d'ingénierie sociale complexes. Dans les industries qui reposent beaucoup sur la confiance, les communications et les transactions financières, la capacité d'usurper, de façon crédible, l'identité de personnes réelles suscite des risques importants.

Il ne suffit plus de protéger les systèmes et les renseignements. Les entreprises doivent également tenir compte de leur façon de valider l'identité des gens avec lesquels ils font affaire.

■ Les attaques d'hameçonnage et d'ingénierie sociale sont les points d'entrée les plus couramment utilisés par les cybercriminels. D'après vos observations, quelles sont les stratégies les plus souvent utilisées dans ces domaines et comment évoluent-elles?

L'hameçonnage et l'ingénierie sociale demeurent très efficaces, car ils ciblent des gens plutôt que des technologies.

Ce qui change, c'est la complexité et l'ampleur de ces attaques. Grâce aux progrès de l'intelligence artificielle, les attaquants peuvent plus facilement créer des messages très convaincants qui semblent authentiques et pertinents à leurs destinataires.

Les cybercriminels consacrent de plus en plus de temps à étudier leurs cibles et à personnaliser leurs attaques. Plus la technologie évolue, plus les entreprises et les particuliers doivent demeurer vigilants et traiter avec prudence les demandes imprévues, particulièrement celles qui portent sur des renseignements sensibles ou des transactions financières.

■ Quelles sont les différences entre les cybermenaces auxquelles FCT est exposée et celles auxquelles font face d'autres industries, comme celles des institutions financières traditionnelles ou d'autres fournisseurs de services?

De façon générale, de nombreuses entreprises font face à des problèmes de cybersécurité semblables. Le besoin de protéger les renseignements tout en préservant la résilience opérationnelle et la confiance des clients est universel.

Ce qui diffère selon les industries, c'est souvent la façon dont les activités criminelles se présentent. Les attaquants ont tendance à mettre l'accent sur les secteurs où ils peuvent obtenir des montants importants et où les interactions fondées sur la confiance créent des occasions de fraude. Les menaces sous-jacentes peuvent être semblables, mais les processus opérationnels ciblés diffèrent souvent d'une industrie à l'autre.

■ Selon vous, quelle sera la prochaine vague de cyberattaques dans notre industrie?

Je crois que nous continuerons de voir une progression rapide des attaques fondées sur l'identité, surtout celles qui utilisent l'intelligence artificielle.

La capacité de générer du texte, des images et du contenu audio et vidéo convaincant crée de nouvelles occasions de fraude et d'usurpation d'identité. Les technologies que l'on considérait comme très fiables pour établir la confiance pourraient devenir de plus en plus difficiles à utiliser en vase clos.

Les entreprises devront donc mettre un plus grand accent sur la vérification de l'identité, les cadres de confiance et les approches de sécurité à plusieurs niveaux conçues pour contrer les menaces émergentes.

■ Comment les entreprises peuvent-elles outiller leurs employés et leurs partenaires pour leur permettre de reconnaître ces éventuelles menaces et d'y résister?

La technologie ne peut suffire à régler les problèmes de cybersécurité.

Les entreprises doivent entretenir une culture dans le cadre de laquelle la sensibilisation à la cybersécurité est considérée comme une responsabilité partagée. La formation, la communication et le renforcement constant demeurent des éléments essentiels de tout programme de sécurité efficace.

L'objectif n'est pas que tout le monde devienne expert en cybersécurité, mais plutôt d'aider les gens à repérer les éventuels risques, à poser les bonnes questions et à savoir quand demander de l'aide.

■ Vous avez déjà parlé de l'importance de l'authentification multifacteur (AMF). À quel point est-elle essentielle pour protéger les données confidentielles?

Les méthodes d'authentification rigoureuses sont l'une des mesures les plus efficaces pour réduire le risque d'accès non autorisé.

Plus les cybermenaces évoluent, plus les entreprises doivent adopter des méthodes d'authentification aussi sécuritaires que conviviales, en fonction des besoins liés à leurs activités. Bien qu'aucune mesure de contrôle ne soit à toute épreuve à elle seule, les approches de la gestion de l'identité et des accès qui comportent plusieurs niveaux sont des composantes essentielles des programmes de cybersécurité modernes.

■ Quel genre de difficultés les entreprises doivent-elles surmonter lorsqu'elles adoptent l'authentification multifacteur?

L'un des plus grands défis consiste à trouver un équilibre entre la sécurité et l'expérience utilisateur.

En fin de compte, toutes les mesures de contrôle de sécurité doivent être acceptées et utilisées par les gens qu'elles visent à protéger. Les entreprises qui mettent exclusivement l'accent sur la sécurité sans tenir compte de la convivialité ont souvent des difficultés sur le plan de l'adoption.

Les mesures les plus réussies sont celles qui combinent d'excellentes pratiques en matière de sécurité, une communication claire, la formation et une compréhension pratique des méthodes de travail.

■ De plus en plus d'entreprises adoptent des technologies infonuagiques. Quels sont les risques connexes qui vous préoccupent le plus?

L'un des plus grands défis est le rythme des changements technologiques.

Les technologies infonuagiques procurent de grands avantages aux entreprises, mais elles nécessitent aussi une attention, une gouvernance et une gestion des risques constantes. La technologie évolue et les entreprises doivent s'assurer de comprendre l'incidence de leurs nouvelles capacités, de l'évolution des exigences opérationnelles et du fait que l'écosystème numérique est de plus en plus interconnecté.

Quelle que soit la plateforme technologique utilisée, il est important de continuer à observer et à comprendre comment l'information circule dans l'entreprise.

■ Selon vous, l'authentification évoluera-t-elle vers des formes plus avancées de vérification de l'identité?

Absolument.

Les technologies d'authentification continueront d'évoluer en même temps que la technologie et les auteurs de menaces. À l'avenir, il faudra probablement utiliser une combinaison de techniques qui amélioreront simultanément la sécurité et l'expérience utilisateur, tout en réduisant le recours aux mots de passe traditionnels.

De façon plus générale, on commence déjà à parler d'assurance de l'identité plutôt que d'authentification. Les entreprises doivent de plus en plus s'assurer qu'en plus d'être authentifiés, les gens sont aussi vraiment ceux qu'ils prétendent être.

■ Si vous pouviez donner un conseil essentiel aux professionnels du droit, aux courtiers en immeubles et aux prêteurs sur l'état actuel et futur de la cybersécurité, que leur diriez-vous?

La nature de la confiance est en train de changer. Autrefois, pour établir la confiance, on se fiait à des signaux familiers : une adresse de courriel, un appel téléphonique ou même une conversation en personne. Avec l'évolution de la technologie, bon nombre de ces signaux deviendront plus faciles à imiter.

Les entreprises et les particuliers devraient mettre un plus grand accent sur la vérification, la validation et un sain scepticisme lorsqu'il est question de renseignements sensibles ou de transactions financières.

La cybersécurité est avant tout une question de confiance. Ceux qui adapteront leurs processus et leurs pratiques pour préserver la confiance dans notre environnement numérique en rapide évolution seront les mieux préparés pour l'avenir.

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 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.

■ **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.

■ **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 Défendre les 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



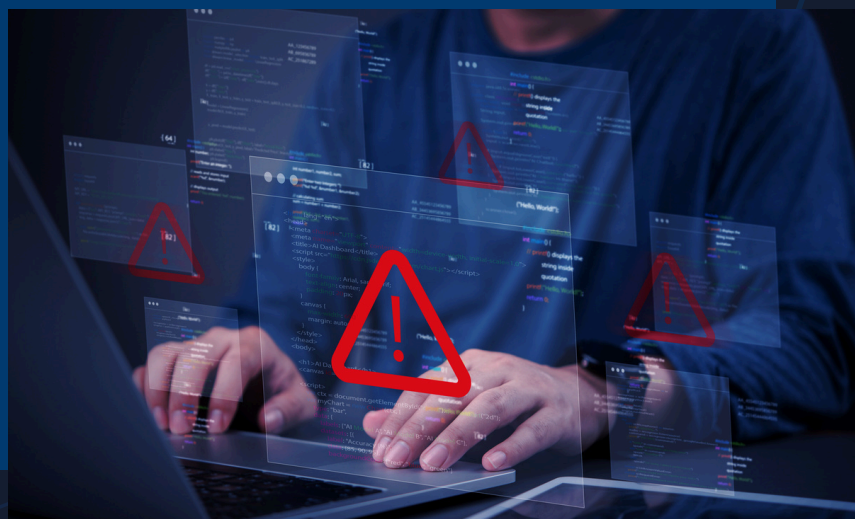
Réclamation : Quand une confirmation ne suffisait pas : un remboursement hypothécaire intercepté par fraude

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 Défendre une 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 défendre non 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.



Un point de vue d'expert sur le terrain: Questions-réponses avec Matt Cunningham, Service de police regional de Halton



Matt Cunningham, gendarme-détective, compte plus de 23 ans d'expérience dans le domaine de l'application de la loi et travaille actuellement à l'unité des crimes financiers du service de police régional de Halton, où il enquête sur des fraudes et des crimes financiers complexes. Il détient les attestations d'examineur de fraude certifié (CFE), de Certified Financial Crime Investigator (CFCI) et de Crypto Fundamentals Certification de TRM (TRM-CFC), ce qui l'aide à protéger le public et à maintenir la confiance au sein de la communauté. Il a également de l'expérience dans les domaines des crimes graves, de la maltraitance et des agressions sexuelles envers les enfants, de la violence conjugale et des enquêtes sur les homicides, ce qui lui permet d'amener une approche disciplinée et axée sur les détails aux dossiers complexes et délicats.

■ Quels signes précoces de fraude sont souvent négligés dans les situations quotidiennes?

L'un des premiers signes les plus courants de fraude est le sentiment d'urgence et la pression. Lorsque des fraudeurs communiquent avec une victime (souvent par téléphone), ils visent délibérément à l'empêcher de prendre une pause, de raccrocher ou de penser de façon critique. Les victimes se font souvent dire des choses comme : « Cette offre prend fin aujourd'hui », « Votre compte sera verrouillé » ou « Ne le dites à personne ou vous empirerez les choses ». L'objectif est de créer de la panique et de forcer l'action immédiate, ce qui laisse peu de place à la réflexion ou à la vérification.

Un autre signal d'alarme est lorsque l'on nous demande d'effectuer des paiements inhabituels ou non conventionnels. Les demandes de cartes-cadeaux, de téléversements ou de cryptomonnaies sont particulièrement révélatrices, même lorsqu'elles sont présentées comme une « solution de rechange temporaire » ou une « option plus rapide ».

Dans bien des cas, ces demandes commencent par de petits montants pour éviter d'éveiller les soupçons tôt dans le processus. Les montants grossissent progressivement une fois la confiance établie. Les contacts inattendus suivis de demandes de renseignements personnels sont aussi chose courante. Les fraudeurs peuvent communiquer avec les victimes sans préavis et, après avoir établi une relation, commencer à demander des renseignements personnels sous prétexte de vérification. Des phrases comme « Nous avons juste besoin de confirmer quelques renseignements » peuvent sembler habituelles, mais elles sont souvent utilisées pour extraire des renseignements qui peuvent être exploités par la suite.

Enfin, la fraude repose souvent en grande partie sur la manipulation émotionnelle. Cela peut prendre la forme de peur, comme des menaces d'actions en justice ou de compromission d'un compte; d'enthousiasme, y compris des promesses de prix ou d'occasions de placement; ou de confiance, comme on peut le voir dans les arnaques amoureuses ou l'usurpation d'une autorité comme la police ou l'Agence du revenu du Canada. Lorsque les émotions prennent le dessus, la pensée logique peut disparaître et les petits signaux d'alarme sont plus facilement ignorés ou rationalisés.

■ Dans les cas d'usurpation d'identité, comment les fraudeurs paraissent-ils légitimes, et que devrait-on vérifier pour confirmer l'identité d'une personne?

Ce que nous voyons habituellement à l'Unité des crimes financiers, c'est l'utilisation fréquente de pièces d'identité frauduleuses, le plus souvent sous la forme d'un permis de conduire de l'Ontario. Les fraudeurs falsifient de mieux en mieux ces documents. Dans bien des cas, la personne qui vérifie la pièce d'identité peut sentir que quelque chose n'est pas tout à fait correct, même si elle ne peut pas expliquer immédiatement le problème. Les fraudeurs sont habiles pour reconnaître cette hésitation et l'exploiteront souvent en exerçant de la pression pour faire avancer l'interaction.

Un exemple courant est celui des prises de contrôle de comptes. Un fraudeur peut s'adresser à un caissier de banque et lui présenter une pièce d'identité frauduleuse. Le caissier pourrait remarquer que quelque chose semble faux et faire une pause instinctive, mais sans raison claire d'interrompre la transaction. À ce moment-là, le fraudeur peut intensifier la situation en créant un sentiment d'urgence, en devenant visiblement frustré ou en semblant en colère. Le caissier, qui ressent la pression liée à la situation et qui est possiblement inquiet que le client fasse une plainte ou que la situation cause du retard ailleurs, peut effectuer la transaction rapidement et passer outre son instinct initial. La façon la plus efficace de vérifier si une pièce d'identité est frauduleuse est d'utiliser un appareil de détection. Ce type d'outil représente un petit investissement, mais peut éviter d'importantes pertes financières. Il permet de valider ou de réfuter rapidement les préoccupations qu'un employé peut avoir lors de la vérification d'une pièce d'identité, ce qui lui donne la confiance nécessaire pour interrompre une transaction lorsqu'elle ne semble pas légitime.

■ Quelles méthodes de contact les fraudeurs utilisent-ils le plus souvent et comment ces canaux influencent-ils le déroulement de la fraude?

La plupart des cas sur lesquels j'ai enquêté avec mon équipe impliquaient des fraudeurs qui appelaient des victimes au hasard. Comme nous l'avons déjà mentionné, ces personnes se

présentent souvent comme des représentants de la banque, du gouvernement ou du personnel de soutien technique. Les appels téléphoniques sont particulièrement efficaces en raison de leur nature personnelle et directe, ce qui permet aux fraudeurs d'exercer une pression psychologique en temps réel. Ils peuvent créer un sentiment d'urgence, orienter la conversation et manipuler les victimes pour qu'elles communiquent des renseignements personnels ou effectuent des paiements. Lorsque cela est combiné à la mystification par téléphone, l'appel peut sembler légitime, ce qui augmente la probabilité que la victime fasse ce qu'on lui demande.

Les fraudeurs sont aussi très habiles pour s'adapter à la volée en fonction de la réaction d'une victime, ce qui rend l'interaction plus authentique et convaincante. Ces arnaques ont tendance à être particulièrement efficaces lorsque le fraudeur utilise une technologie inhabituelle, comme la cryptomonnaie, et se présente comme un guide utile tout au long du processus. Dans bien des cas, la confiance se bâtit progressivement à mesure que le fraudeur accompagne la victime étape par étape dans une transaction, ce qui renforce l'illusion de légitimité et fait en sorte qu'il est plus difficile pour la victime de reconnaître la situation comme étant frauduleuse.

■ Quelles vulnérabilités les fraudeurs recherchent-ils, et adaptent-ils leurs tactiques à certains groupes d'âge ou à des situations particulières?

Selon mon expérience, les fraudeurs ciblent le plus souvent les personnes âgées de 60 ans et plus, en particulier par des fraudes liées aux placements, des tentatives d'hameçonnage et des escroqueries amoureuses. Les personnes appartenant à ce groupe sont fréquemment ciblées, car elles peuvent avoir accumulé plus d'actifs financiers au fil du temps et, dans certains cas, elles sont moins familières avec l'évolution des dangers en ligne. Les fraudeurs adaptent délibérément leurs approches pour paraître crédibles et dignes de confiance, ce qui augmente la probabilité que ces arnaques réussissent.

La vulnérabilité émotionnelle est un autre facteur que les fraudeurs exploitent souvent. Les situations liées au veuvage, à la solitude, au deuil, à la peur ou à l'excitation peuvent nuire au jugement des gens et les rendre plus vulnérables à la manipulation. Les arnaques comme la fraude amoureuse, les arnaques bancaires, les arnaques liées aux cryptomonnaies, les arnaques liées à la loterie et la fraude liée aux héritages sont souvent conçues pour exploiter ces états émotionnels et encourager les victimes à agir rapidement ou à garder le secret.

Le manque de connaissances numériques et les lacunes dans les connaissances en matière de cybersécurité peuvent aussi accroître l'exposition à la fraude, surtout lorsqu'il est question de fraudes techniques. Les tentatives d'hameçonnage, les arnaques liées au soutien technique et le vol d'identité reposent souvent sur une méconnaissance des outils ou des processus numériques. Lorsque les victimes ne sont pas certaines du fonctionnement de certaines technologies, les fraudeurs peuvent se positionner en tant qu'aides ou autorités, ce qui réduit davantage la probabilité que l'arnaque soit remise en question.

■ Avez-vous déjà vu des cas de fraude qui brisent les hypothèses courantes, et qu'est-ce qui aurait pu les prévenir?

Au cours de la dernière année, une nouvelle arnaque appelée « banker's fraud » (fraude du représentant de banque) a fait son apparition. Dans le cadre de ce stratagème, les fraudeurs appellent des victimes au hasard en se faisant passer pour des représentants de la banque. En utilisant un langage persuasif et des tactiques de pression, ils convainquent les victimes que leurs cartes de débit et de crédit ont été compromises. On dit aux victimes qu'un représentant de la banque viendra chercher leurs cartes et on leur demande de les découper et de les déposer dans une enveloppe aux fins de ramassage. Pendant l'appel, les fraudeurs obtiennent également le NIP de la victime, ce qui leur donne un accès complet aux comptes associés.

En réalité, la personne qui recueille l'enveloppe est souvent un conducteur d'Uber qui ignore qu'il participe à une fraude. Le conducteur livre l'enveloppe à un complice, souvent en le rencontrant dans un lieu public comme un coin de rue. Une fois que les cartes sont en leur possession, les fraudeurs commencent à les utiliser presque immédiatement. Dans ces cas, les répercussions financières sont importantes, avec des pertes moyennes de 35 000 \$ à 40 000 \$ par victime.

La façon la plus efficace de prévenir ce type de fraude commence par la compréhension qu'une banque ne demandera jamais de NIP par téléphone. Un NIP ne doit en aucun cas être communiqué. Si une personne prétend appeler de votre banque, la mesure la plus sécuritaire est de raccrocher et de communiquer de façon indépendante avec la banque en utilisant le numéro de téléphone officiel indiqué au verso de votre carte ou sur un relevé bancaire. Tout numéro de téléphone fourni par l'appelant doit être traité avec prudence, car il pourrait faire partie de la fraude.

■ Au-delà des pertes financières, quels sont les impacts plus larges de la fraude sur les victimes?

Les victimes de fraude subissent souvent d'importantes répercussions émotionnelles et pratiques, y compris du stress, de l'anxiété et des sentiments de honte ou d'embarras, même si le crime n'est jamais de leur faute. L'accès aux fonds peut être perturbé, ce qui peut compliquer le paiement des factures ou la gestion des dépenses quotidiennes. Dans certains cas, la fraude peut aussi nuire à la cote de crédit d'une personne, ce qui nuira à l'obtention de prêts, de prêts hypothécaires ou de certains types d'emploi.

La fraude peut aussi avoir des répercussions sur les relations personnelles, car les victimes subissent le stress émotionnel et les conséquences financières du crime. Le recouvrement est rarement immédiat et exige souvent beaucoup de temps et d'efforts, notamment pour communiquer avec les institutions financières, travailler avec les forces de l'ordre et surveiller de près les comptes en vue de toute autre activité suspecte. Bien que certaines victimes deviennent plus prudentes à la suite d'un incident, d'autres demeurent vulnérables et risquent d'être de nouveau ciblées.

Les enquêteurs du Service de police régional de Halton travaillent fréquemment avec l'Unité des services aux victimes pour aider les personnes touchées par la fraude. Cette collaboration permet de s'assurer que les victimes ont accès à des ressources et à des conseils appropriés tout au long du processus de recouvrement.

■ **Quelles actions des victimes peuvent compliquer les enquêtes, et pourquoi certaines personnes tardent-elles à signaler une fraude?**

L'une des plus grandes préoccupations que nous avons du point de vue de l'enquête est lorsque les victimes continuent de communiquer avec le fraudeur après le signalement à la police. Les victimes peuvent se sentir gênées, anxieuses ou désespérées de récupérer leur argent et croire qu'elles peuvent persuader le fraudeur de les rembourser. Dans certains cas, elles peuvent aussi tenter de mener leur propre « enquête » pour aider la police. Malheureusement, les contacts continus mènent souvent à l'aggravation de la situation et peuvent compliquer considérablement l'enquête en alertant le fraudeur, en altérant des preuves ou en minant les stratégies d'enquête.

Un autre défi se pose lorsque les victimes ne connaissent pas le processus judiciaire canadien. Si des accusations sont portées, un manque de compréhension du fonctionnement du système juridique peut entraîner de la confusion, des attentes irréalistes ou des erreurs qui pourraient avoir une incidence sur le dossier.

Il est important de bien comprendre le processus afin que les victimes sachent à quoi s'attendre et comment leurs actions peuvent avoir une incidence sur les procédures.

Enfin, l'embarras ou la peur du jugement peuvent amener certaines victimes à ne pas divulguer certains renseignements clés ou à les minimiser au moment de signaler la fraude. L'omission de renseignements, intentionnelle ou non, peut créer des problèmes d'intégrité et de crédibilité plus tard au cours de l'enquête. Si des renseignements supplémentaires sont révélés après le fait, cela peut affaiblir le dossier dans son ensemble et, dans certaines situations, entraîner le retrait des accusations. La franchise et la transparence totales sont essentielles au moment de signaler une fraude, car des renseignements complets et exacts donnent aux enquêteurs les meilleures chances de poursuivre l'enquête efficacement.

■ **En cas de soupçon de fraude, quelles mesures immédiates faut-il prendre pour limiter les dommages?**

Une fois qu'une fraude est soupçonnée, la première étape la plus importante est de cesser immédiatement tout contact avec le fraudeur et de préserver toute preuve potentielle. Cela comprend la conservation des courriels, des messages textes, des numéros de téléphone, des noms ou des noms fournis, des dossiers bancaires et de cartes de crédit, des reçus de transaction et de tout autre renseignement pertinent. Les victimes doivent éviter de supprimer, de modifier ou de modifier des fichiers de quelque façon que ce soit, car cela peut compromettre l'intégrité de la preuve. Il est essentiel de maintenir une chaîne de possession claire afin que les renseignements demeurent fiables et, au besoin, admissibles devant les tribunaux.

Parallèlement, les autorités compétentes doivent être avisées le plus rapidement possible. Cela comprend communiquer avec la police locale, les institutions financières et les sociétés émettrices de cartes de crédit, et signaler l'incident au Centre antifraude du Canada. Un avis rapide permet à ces organisations de prendre des mesures immédiates pour limiter les pertes futures, signaler les activités suspectes et soutenir toute enquête ultérieure.

Dans la mesure du possible, les victimes ou les témoins devraient également être encouragés à fournir des déclarations écrites ou enregistrées sur vidéo à la police ou à l'organisme d'enquête pertinent. Recueillir les déclarations rapidement permet d'aider à préserver l'exactitude des souvenirs des événements et de leur chronologie ainsi que des interactions, ce qui peut être crucial à mesure que les enquêtes progressent. Lorsqu'on leur fournit rapidement des renseignements clairs et complets, les enquêteurs disposent de bases solides pour évaluer l'incident et prendre les mesures appropriées.

■ Quelles habitudes ou pratiques à long terme permettent de réduire de façon significative le risque de fraude?

La sensibilisation proactive est l'un des outils les plus efficaces pour réduire l'incidence de la fraude. Les membres du service de police régional de Halton travaillent activement à renseigner les citoyens, les groupes communautaires, les institutions financières et les entreprises sur la prévention de la fraude. Ces efforts visent à aider les gens à reconnaître les tactiques courantes, à comprendre les risques émergents et à savoir comment réagir si quelque chose semble incorrect. Lorsque de nouvelles tendances en matière de fraude commencent à toucher la communauté, en particulier celles qui font plusieurs victimes, l'unité responsable des crimes financiers publie également des communiqués de presse pour sensibiliser les gens. Ces communications visent à alerter rapidement le public, à communiquer des conseils pratiques en matière de prévention et à réduire le risque de nouvelles victimes en veillant à ce que des renseignements exacts parviennent rapidement à la communauté.

■ Comment prévoyez-vous l'évolution des tactiques de fraude, et à quoi les gens devraient-ils être plus attentifs à l'avenir?

L'une des tendances les plus importantes au cours des dernières années a été l'utilisation accrue de la cryptomonnaie dans les activités liées à la fraude. Les monnaies numériques étant de plus en plus largement adoptées, elles sont aussi utilisées plus fréquemment par les fraudeurs pour déplacer et dissimuler des fonds illicites. Les transactions de cryptomonnaies peuvent être difficiles à retracer et à récupérer, ce qui les rend particulièrement intéressantes pour les activités criminelles et désavantage les enquêteurs.

Par conséquent, les organisations qui participent à la prévention et aux enquêtes sur la fraude devraient accorder la priorité à la sensibilisation et à la formation de leurs employés sur le fonctionnement de la cryptomonnaie. À l'heure actuelle, les criminels sont souvent bien en avance sur les efforts de prévention en ce qui concerne la compréhension et l'utilisation de ces outils. Mieux connaître la façon dont la cryptomonnaie est acquise, transférée et utilisée à mauvais escient peut aider à combler cette lacune et à mieux outiller les organisations pour reconnaître, prévenir et réagir à la fraude à mesure que ces tactiques continuent d'évoluer.

Cette séance de questions-réponses est fournie à des fins d'information générale seulement. Les points de vue et opinions exprimés par [le détective Cunningham] lui sont propres et ne reflètent pas nécessairement ceux d'un service de police ou d'un organisme gouvernemental. La participation à cette séance ne constitue pas une approbation de First Canadian Title Company Limited, ni de ses produits ou services.



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



Les assurances sont offertes par la **Compagnie d'assurances FCT Itée**. Les services sont offerts par la **Compagnie de titres First Canadian limitée**. La société de services n'offre pas de produits d'assurance. Ce document n'a pour but que de fournir des renseignements généraux. Pour connaître la couverture et les exclusions exactes, reportez-vous à la police. Des exemplaires sont disponibles sur demande. Certains produits et services peuvent varier selon la province. Les prix ainsi que les produits et services peuvent changer sans préavis.

^{MD} Marque de commerce déposée de **First American Financial Corporation**.