LastPass pour les agences immobilières et les courtiers

Le secteur de l'immobilier se concentre sur l'achat, la vente, la location et la gestion de terrains et de bâtiments, qu'ils soient commerciaux, résidentiels ou industriels. Il porte également sur des activités comme la gestion des terres et les investissements.

Les identifiants sont les clés d'accès aux organisations

Les les agences immobilières et les courtiers sont confrontés à de nombreuses cybermenaces, le vol d'identifiants étant la tactique principale exploitée par les acteurs malveillants pour infiltrer les systèmes. Ces organisations, qui gèrent des données hautement sensibles sur les clients, comme des informations personnelles et financières et des titres de propriété, sont une cible privilégiée des cybercriminels. Les conséquences d'une fuite ne se limitent pas aux interruptions de fonctionnement, mais peuvent aussi nuire à la réputation de l'agence et à la confiance des clients. Dans un secteur sous haute pression et très concurrentiel, où les relations et les transactions sont primordiales, tout compromis en matière de sécurité peut entraîner une perte d'activité et de fidélité des clients, et avoir des effets à long terme.

Avec l'adoption croissante du numérique sur le secteur de l'immobilier, les réseaux sociaux, les outils SaaS et les applications collaboratives complexifient la gestion des accès et de la sécurité. De nombreuses agences, les petites équipes au sein d'organisations plus importantes, dépendent de ces outils pour partager des informations en temps réel, gérer les contrats et communiquer avec leurs clients et partenaires. Ce qui augmente le nombre de points d'accès à sécuriser, d'où l'importance de la gestion des identifiants

Lorsque les équipes travaillent sur plusieurs plates-formes et appareils et qu'elles subissent une rotation permanente dans un environnement en perpétuel mouvement, assurer la sécurité des accès et empêcher le partage non sécurisé d'identifiants est un problème permanent qui doit pourtant être résolu pour protéger tant le fonctionnement des agences que les données des clients.

Avec la transition récente vers le télétravail et la PropTech (technologies et logiciels de gestion des propriétés conçus pour le secteur), la maîtrise de la sécurité des données est un facteur de différenciation essentiel pour les professionnels de l'immobilier qui souhaitent conserver la confiance de leurs clients et la protection de leurs données, tout en stimulant les transactions numériques.

Il est essentiel de protéger vos actifs

LastPass fournit une solution robuste qui résout les problèmes rencontrés par les courtiers et les agences immobilières. Il permet la création, le stockage, la gestion et le partage simple et sécurisé d'identifiants entre les équipes, assurant une sécurité robuste qui n'entrave pas l'accessibilité. En centralisant la gestion des identifiants, LastPass simplifie le contrôle des accès, l'application de pratiques saines et le respect de la réglementation.

Les agences immobilières dépendent de plus en plus des outils SaaS, des réseaux sociaux et des plates-formes collaboratives, et LastPass atténue les risques associés à cette transition numérique. Sa solution native dans le cloud s'intègre avec ces outils pour renforcer la sécurité, tout en simplifiant l'adoption de pratiques vertueuses par les utilisateurs, quel que soit leur niveau de compétence technique. Des fonctionnalités comme le partage sécurisé, la MFA et les rapports détaillés fournissent une visibilité en temps réel et permettent la détection rapide de vulnérabilités, diminuant ainsi le poids de la gestion des accès tout en renforçant la productivité et la conformité.

Les avantages de LastPass pour les agences immobilières et les courtiers

Le moyen le plus simple, abordable et fiable pour les courtiers et les agences immobilières de diminuer radicalement les risques de cyberattaques et opérationnels consiste à standardiser la gestion des mots de passe avec LastPass à l'échelle de l'entreprise.

Sécuriser	**Empêcher les accès non autorisés**	Empêchez les acteurs malveillants et les utilisateurs non autorisés d'accéder aux applications, aux comptes en ligne et aux informations et systèmes sensibles.
	Stopper les détournements de comptes et les fuites de données	Assurez la fiabilité et l'accessibilité des comptes et applications en ligne, et la confidentialité des identifiants.
	Contrôler le shadow IT	Donnez aux organisations une visibilité et la maîtrise des applications SaaS non approuvées et surprovisionnées, en permettant aux administrateurs de suivre le partage d'identifiants, de gérer les droits d'accès et de repérer les vulnérabilités.
	Renforcer la gestion sécurisée des accès	Intégrez de manière transparente avec les principaux fournisseurs d'identité (IdP) comme Microsoft Entra, pour améliorer la gestion des utilisateurs tout au long du cycle de vie des employés.
Se conformer	**Répondez aux conditions de cyberassurance**	Simplifiez la tâche aux organisations qui doivent répondre aux exigences de gestion des mots de passe et des accès pour obtenir une cyberassurance.
	Favoriser la conformité	Aide les organisations à répondre aux normes de conformité et réglementaires comme RGPD, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA et SOX, ainsi que les cadres de cybersécurité comme NIST, CISA, Zero Trust et NERC-CIP.
	Répondre aux exigences de sécurité des partenaires	Aide les organisations à respecter les normes de sécurité strictes de partenaires grâce à un contrôle efficace des accès, des règles de partage de mots de passe, des mécanismes d'authentification forte et des rapports exploitables.
Rationaliser	**Offrir une expérience intuitive à chaque utilisateur**	Fournit des centaines de stratégies personnalisables, des autorisations souples, des rapports détaillés et plusieurs options d'authentification, pour devenir un outil indispensable de la pile technologique.
	Standardiser la protection par mot de passe	Simplifiez la gestion des identifiants pour les employés à l'échelle de l'organisation.
	Alléger la frustration du service d'assistance	Diminuez le fardeau du service d'assistance informatique dû aux problèmes de mots de passe, comme les mots de passe oubliés et les comptes verrouillés.
Collaborer	**Maximiser le travail d'équipe grâce au partage**	Rationalisez le partage de mots de passe et d'informations à l'intérieur et à l'extérieur de l'organisation, pour stimuler la productivité et l'efficacité des partenaires, des indépendants et des télétravailleurs.
	Maximiser adoption et l'utilisation	Boostez l'adoption et l'utilisation chez les employés en offrant une interface utilisateur intuitive qui simplifie les tâches de gestion des mots de passe.
	Promouvoir une culture de la sécurité	Aidez les administrateurs à s'assurer que tous les employés contribuent activement à une culture de la sécurité, pour se protéger contre les menaces courantes comme le vol ou le piratage d'identifiants afin d'assurer la responsabilité fiduciaire.