



LastPass voor makelaars en vastgoedhandelaars

Onroerend goed is een breed werkveld, met koop, verkoop, verhuur en beheer van land en gebouwen, voor wonen, werk en industrie. Vaak gaat het om forse investeringen en grote bedragen.

Aanmeldingsgegevens zijn de sleutel tot een organisatie

Makelaars en vastgoedhandelaars hebben te maken met ernstige cyberrisico's. Diefstal van aanmeldingsgegevens is een van de belangrijkste aanvalstactieken die hackers gebruiken om binnen te komen in systemen. De onroerendgoedsector is een geliefd doelwit voor cybercriminelen, met veel gevoelige klantgegevens, financiële gegevens, eigendomsregisters en grote transacties. Een gegevenslek heeft vaak directe gevolgen voor de operationele activiteiten, maar ook indirecte gevolgen voor de reputatie en het vertrouwen van klanten. In een sector waar veel afhangt van goede relaties en deals, leidt een probleem met de beveiliging al snel tot gemiste omzet en verlies van klanten. En dat werkt lang door.

Voor alles wat te maken heeft met vastgoed, is er specifieke technologie. En al die accounts voor social media, SaaS-tools, toepassingen voor samenwerking, klantenportals, en natuurlijk ook bankrekeningen vragen om goed toegangsbeheer en een sterke beveiliging. Veel van deze tools zijn onmisbaar voor kleinere teams: uw mensen moeten snel gegevens kunnen delen, contracten beheren, communiceren met klanten en partners. Maar dat betekent ook dat uw organisatie veel toegangspunten heeft. En één zwak beveiligd toegangspunt kan de deur openzetten voor hackers, dus goed wachtwoordbeheer is absoluut essentieel.

Teams werken vaak vanaf verschillende locaties, apparaten en besturingssystemen. Nieuw personeel heeft toegang nodig, maar vertrekkende medewerkers mogen juist geen wachtwoorden meenemen, want dat is een risico voor uw activiteiten en voor de gegevens van uw klanten. Dat maakt het lastig om veilige toegang te waarborgen en ongeoorloofd delen van wachtwoorden te blokkeren – maar het moet wel.

De vastgoedsector werkt steeds meer op afstand, en steeds vaker met gespecialiseerde software. Dat betekent dat goede gegevensbeveiliging onmisbaar is voor iedereen die met onroerend goed werkt. Klanten verwachten dat hun gegevens veilig zijn, en ondernemers kunnen niet zonder goed digitaal toegangsbeheer.

Beveiliging is een must



LastPass vormt een krachtige oplossing voor de cyberbeveiliging in de onroerendgoedsector. De software maakt het makkelijk om sterke wachtwoorden te maken, op te slaan, te beheren en veilig te delen in teams. Zo levert LastPass gebruiksgemak en beveiliging in één. Door het beheer van aanmeldingsgegevens te centraliseren, vereenvoudigt LastPass de toegangscontrole. Het dwingt best practices af en ondersteunt compliance met relevante wet- en regelgeving.



Makelaars en vastgoedhandelaars werken steeds meer met online toepassingen, social media en verschillende platformen. LastPass houdt de risico's van deze digitale transformatie beheersbaar. Het is een cloud-native oplossing die integreert met vrijwel al uw tools. En het is handig: medewerkers met en zonder IT-kennis kunnen dankzij LastPass probleemloos veilig werken. Ook voor uw IT-afdeling zijn er veel voordelen: LastPass ondersteunt veilig delen, MFA en gedetailleerde rapporten voor real-time inzicht en snelle detectie van kwetsbaarheden. Toegangsbeheer kost veel minder tijd, de productiviteit gaat omhoog en compliance wordt een stuk eenvoudiger.



Voordelen van LastPass voor de onroerendgoedsector

De makkelijkste, meest betaalbare en meest betrouwbare manier voor makelaars en vastgoedhandelaren om hun cyberrisico en operationele risico terug te dringen, is door hun wachtwoordbeheer bedrijfsbreed te organiseren met LastPass.

Beveiliging	Voorkom ongeoorloofde toegang	Houd hackers en ongeoorloofde gebruikers buiten uw toepassingen, online accounts, gevoelige gegevens en systemen.
	Blokkeer overnames van uw accounts en gegevenslekken	Zorg dat online accounts en toepassingen betrouwbaar toegankelijk zijn voor geautoriseerde gebruikers en dat aanmeldingsgegevens beschermd blijven.
	Krijg schaduw-IT onder controle	Krijg zicht op toepassingen die medewerkers gebruiken zonder toestemming en beheer van de IT-afdeling. Voorkom onnodige abonnementen en volg wie er aanmeldingsgegevens deelt voor welke accounts. Beheer de toegangsrechten en herken kwetsbaarheden in het systeem.
	Breid veilig toegangsbeheer uit	Integreer naadloos met identiteitsproviders als Microsoft Entra en verbeter het gebruikersbeheer van inhuur tot aan vertrek.
Naleving	Voldoe aan voorwaarden van cyberverzekeraars	Toon eenvoudig aan dat u voldoet aan de vereisten die cyberverzekeraar stellen aan wachtwoord- en toegangsbeheer.
	Ondersteun compliance	Voldoe aan de vereisten van wet- en regelgeving, onder andere voor de AVG, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA en SOX, en voor kaders voor cyberbeveiliging zoals NIST, CISA, Zero Trust, en NERC-CIP.
	Garandeer de beveiliging die partners vereisen	Voldoe aan de strenge beveiligingsvereisten van partners, met krachtige systemen voor toegangscontrole, regels voor het delen van wachtwoorden, sterke verificatiemechanismen en nuttige rapportages.
Optimalisatie	Bied iedereen een intuïtieve gebruikservaring	Profiteer van uitgebreide instelbare beleidsregels, flexibele machtigingen, gedetailleerde rapportages, en verschillende opties voor de verificatie.
	Standaardiseer de wachtwoordbeveiliging	Vereenvoudig het wachtwoordbeheer voor alle medewerkers binnen de organisatie.
	Verlaag de werkdruk voor de helpdesk	Verlos de helpdesk van problemen door aanmeldingsgegevens, zoals vergeten wachtwoorden en geblokkeerde accounts.
Samenwerking	Stroomlijn teamwerk met gedeelde toegang	Maak het makkelijk om wachtwoorden en andere informatie zowel intern als extern veilig te delen, voor meer productiviteit en efficiency voor partners, freelancers en thuiswerkers.
	Optimaliseer aanname & gebruik	Bevorder de aanname en het gebruik door medewerkers met een intuïtieve, gebruiksvriendelijke interface, die alle taken rondom wachtwoordbeheer makkelijker maakt.
	Bouw een veiligheidscultuur	Zorg ervoor dat alle medewerkers actief bijdragen aan een hoog veiligheidsbewustzijn en de organisatie beschermen tegen veel voorkomende bedreigingen rondom gestolen of gelekte aanmeldingsgegevens.