



LastPass voor de financiële dienstverlening

De financiële dienstverlening is een breed werkveld, met boekhouders, accountants, banken, vermogensbeheerders, kredietverstrekkers, cryptobeurzen, FinTech-bedrijven, investeerders, betalingsplatformen en nog veel meer.

Wachtwoorden vormen een uniek risico voor financiële dienstverleners

Financiële dienstverleners zijn een geliefd doelwit voor cyberaanvallen: er valt simpelweg veel te halen, van klantgegevens tot geld. Dat betekent dat bedrijven in deze sector zich moeten wapenen tegen hardnekkige, geavanceerde cyberbedreigingen, die zich continu ontwikkelen. Hackers gebruiken infostealers, phishing, en social engineering met behulp van AI om wachtwoorden en digitale identiteiten te veroveren. En met succes: regelmatig slagen cybercriminelen erin om accounts over te nemen, rekeningen te plunderen of ransomware te lanceren.

Ook voor het dagelijkse werk is het een uitdaging om wachtwoorden en digitale toegang goed te beheren: SaaS-toepassingen zijn wijd verbreid en bedrijven in de financiële sector hebben vaak honderden accounts. Dat leidt vaak tot een wirwar aan software en schaduw-IT, die medewerkers gebruiken zonder toestemming of toezicht van de IT-afdeling. Onnodige abonnementskosten en productiviteitsverlies door vergeten wachtwoorden liggen op de loer.

Door de overstap naar hybride werk hebben systemen nog meer toegangspunten gekregen, digitale samenwerking betekent dat collega's toegang moeten delen, en hackers maken gericht misbruik van kwetsbaarheden. Tools voor samenwerking op afstand hebben vaak geen centraal overzicht en dat maakt het lastig om activiteiten van gebruikers te volgen. Maar als medewerkers ongeautoriseerde communicatietoepassingen gebruiken (bijvoorbeeld hun privémail), omzeilen ze beveiligingsprotocollen. En dat is een probleem voor een dekkende gegevensbeveiliging. Alles bij elkaar lopen consumenten het risico op fraude en social engineering, medewerkers verliezen tijd door vergeten wachtwoorden, en de organisatie riskeert gegevenslekken, ransomware, reputatieschade en boetes voor ontbrekende compliance.

Het Data Breach Investigations Report voor 2024 van Verizon meldt dat 78% van de inbraken in de financiële dienstverlening te herleiden zijn tot infiltratie in systemen, diverse fouten en social engineering.

Geavanceerde wachtwoord-beveiliging en goede controle



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en kan de dagelijkse uitdagingen rondom cyberbeveiliging voor financiële dienstverleners effectief aanpakken. De software is speciaal gemaakt voor de complexe behoeften van werkplekken met veel accounts en systemen. Met LastPass kunnen organisaties sterke wachtwoorden maken, opslaan en beheren, en veilig toegang delen waar nodig. De handige interface versterkt de beveiliging en verhoogt tegelijkertijd het gebruiksgemak.



Financiële dienstverleners moeten een evenwicht zien te vinden tussen compliance en strenge beveiliging enerzijds, en gebruiksgemak voor beheerders en medewerkers anderzijds. LastPass is de perfect oplossing. Het werkt in de cloud en houdt gevoelige gegevens veilig, zodat compliance gewaarborgd wordt. Inloggen en onderling toegang delen en beheer is geen probleem meer, en de IT-afdeling kan een toegangsbeleid met sterke beveiliging uitrollen, voor meer inzicht en controle.



Belangrijke stakeholders kunnen met geavanceerde rapportages audits voorbereiden en bijvoorbeeld nagaan wie er wanneer toegang heeft tot welke items. Dat maakt het een stuk makkelijker om ongeoorloofde toegang te voorkomen, digitale bedreigingen af te weren, en het vertrouwen in uw organisatie te vergroten.



Voordelen van LastPass voor de financiële dienstverlening

De makkelijkste, meest betaalbare en meest betrouwbare manier voor financiële dienstverleners 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	Standaardiseer de wachtwoordbeveiliging	Profiteer van uitgebreide instelbare beleidsregels, flexibele machtigingen, gedetailleerde rapportages, en verschillende opties voor de verificatie.
	Breid veilig toegangsbeheer uit	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.