

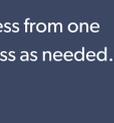
10 Ways to Increase Security and Productivity During Remote Work



Remote work presents many opportunities for businesses, but also has its challenges:

- How do you maintain security throughout the business?
- How do you ensure employees have access to the resources they need to stay productive?

#1 Deploy single sign-on

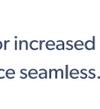


Single sign-on gives IT the ability to manage access from one view, all with the flexibility to add or revoke access as needed.



90% of businesses say managing user access is very important to the overall security of the organization.¹

#2 Add multi-factor authentication



MFA adds an additional layer of authentication for increased security and biometrics make the login experience seamless.

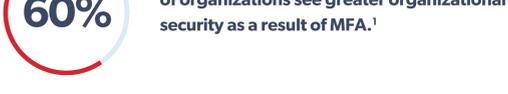


59% of businesses ranked strengthening user authentication as a top area for IAM improvement.¹

#3 Use contextual factors



Contextual policies can enforce authentication requirements that adapt with the login for greater flexibility and control.



60% of organizations see greater organizational security as a result of MFA.¹

#4 Lock down your VPN



Strong passwords and MFA on the VPN increase security to ensure employees are who they say they are before gaining access.



80% of data breaches are caused by weak, reused or stolen passwords alone.²

#5 Protect your workstation

MFA on workstations ensures only legitimate employees can authenticate, even if the workstation is compromised.



30% of data breaches involved employee workstations.²

Securely Share

Password sharing helps employees securely share credentials and ensures everyone has access to what they need to get their work done.



185 shared folders are used in a business on average.³

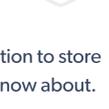
#7 Reduce passwords

Passwordless authentication removes the password from the login experience, creating a more streamlined and secure way to work.



95% of IT security professionals believe their company should better emphasize strong password behavior.¹

#8 Tackle shadow IT



A password manager offers employees a secure location to store all their credentials – the ones IT does and does not know about.



77% of employees use a 3rd-party cloud app without the approval or knowledge of IT.⁴

#9 Prevent phishing schemes



Password management can help mitigate the risk of phishing by never auto-filling on suspicious sites.



On average, 26.5% of recipients who were sent a malicious email clicked on a link in the email.⁵

#10 Maintain complete insight



Through detailed reporting, you can monitor activity with insights to make access and authentication adjustments as needed.



53% of businesses prioritize monitoring user activity as a key priority for their IAM capabilities.¹

Remote work, made simple and secure with IAM

Remote work doesn't need to be a challenge with the right IAM strategy in place.



Learn how LastPass Identity can secure and empower your remote workforce to keep employees productive and the business secure.

Please contact us to learn more.

Sources:

- 1 LastPass SMBs Guide to Modern Identity
- 2 2019 Verizon Data Breach Investigations Report
- 3 LastPass State of the Password Report 2019
- 4 NTT Com, "Shadow IT Survey", 2016.
- 5 IBM State of the Phish Research 2019