TOP FIVE SECURITY FINDINGS FOR SMALL BUSINESSES

Early results are in. Here’s what we learned from employees at small businesses about how their organizations are approaching security in a changing hybrid work environment.

01 Most small businesses adopted new security policies or increased cybersecurity training since the shift to remote work.
75% of small businesses made some security changes since the COVID-19 pandemic caused an increase in remote work, with 43% adopting new security policies, 40% increasing cybersecurity training, and 31% investing in digital security tools like password managers.

02 Recent large-scale data breaches caused small business employees to feel more concerned about their company’s security practices.
89% of employees feel their organizations are paying more attention to security after recent data breaches.

03 More small business employees want digital security tools that will help them practice better cybersecurity to protect their organization.
Half of employees believe their organizations need a password management solution.

04 Many small business employees are wrangling more than five work account passwords regularly.
About half of employees have 1–5 password-protected accounts, and one-third have 6–10 accounts.

05 Those who work at small businesses with access to a password manager feel more secure.
Employees whose companies require password manager use were more likely to describe their organization as more secure, with 60% believing their organization was not at risk of being hacked or breached.

For more information on how to keep your business secure in the meantime, [start a free trial](https://www.dashlane.com) or check out our password playbook for small businesses.

We distributed our survey to potential respondents and received 618 qualified responses from employees and managers in small-to-medium businesses. Respondents were distributed evenly across organizations with 51–100, 101–200, and 201–500 full-time employees.