

onelogin

DANGER!

**Unprotected laptops:
A growing security nightmare**



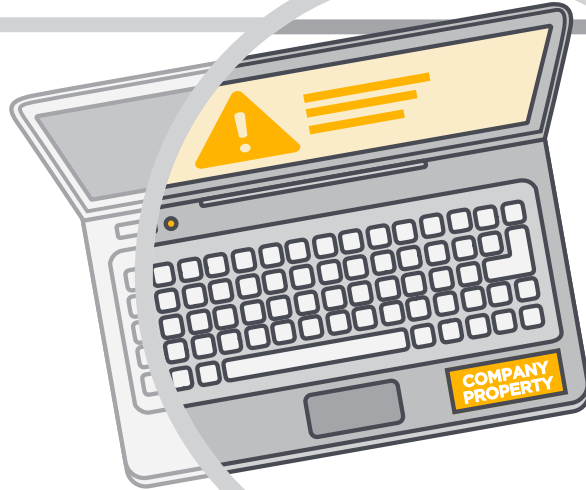
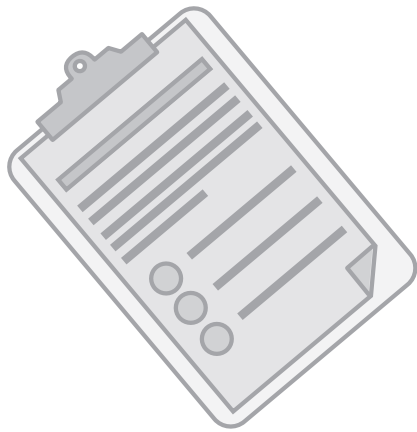


More and more, people are working remotely.

53% work remotely at least half of the week.¹



70% work remotely at least one day a week.



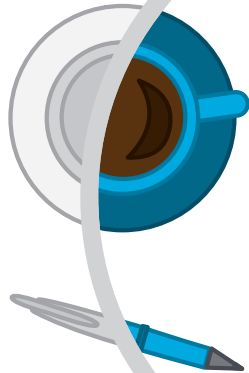
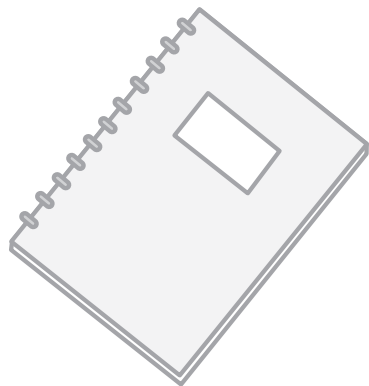
And endpoints like laptops
are a big security risk.

42% of IT
professionals said
their endpoints have
been breached.²



69% of those
breaches happened
on corporate
laptops.

The average cost of a breach is **\$148** per
record—and most breaches are a result of
weak or insecure passwords.³



It's not just your corporate laptops at risk.

42% of IT professionals said their breaches involved employee-owned laptops.



25% of executives reported that an external vendor was the cause of a data breach at their company.

Even aside from vendors and contractors, the problem will continue to grow.

The number of employees using personal computers doubled over one year.⁴

FROM

44%

TO

88%



WIFI:
CoolBean123

The laptop security problem is exacerbated by employee behavior.

83% percent of respondents in one study reported using a computing device in a public place.⁵



25% of employees leave their computer unlocked and unattended.⁶



25% of employees report using insecure passwords because they're easier to remember.⁷



86% of Americans track passwords by memorizing them—suggesting they are simple, insecure passwords.





Keep employee laptops secure with **OneLogin**

Available for both Mac and Windows machines, OneLogin Desktop helps secure users' machines from unauthorized access. It extends OneLogin to user machines and offers easy access to corporate apps and data through the OneLogin portal.

[Read more about OneLogin Desktop](#)