

1Password

HOW TO SECURE YOUR

HYBRID WORKFORCE



“

“If you aren’t making it easy on your users to do the right thing, you can expect them to ignore security altogether.”

As security professionals, we often forget that security isn’t our colleagues’ first priority. They have work to do, so if they have to make a choice between security and productivity, they’re going to choose productivity.

Making security easy

Instead of making security harder by imposing burdensome requirements and motivating with fear, our goal should be to make it easy to do the right thing. That means creating a security-positive culture that removes roadblocks, makes security personnel available to solve problems, educates employees, and rewards security-centric decisions.

This only gets more important as we transition to a hybrid work model, because shadow IT is here to stay.

According to 1Password research:

64% of workers have created at least one account in the past 12 months that their IT department doesn’t know about.

33% of workers who have created shadow IT accounts reuse memorable passwords, and **48.2%** use a pattern of similar passwords.

37% of workers have shared an account or website login with a colleague.

89% of people who share passwords through insecure digital methods either use password patterns or reuse passwords.

How do I cultivate a culture of security?

- ✓ **Foster an open relationship between security and the rest of the organization.** Your employees won't care about security if they don't believe that your security team cares about them.
- ✓ **Treat your employees like humans.** Educate your employees, and trust them to use common sense and make the right decisions.
- ✓ **Praise and reward security-minded behavior.** Praise team members for raising security issues or concerns so they're more likely to share future issues. Thank them for doing the right thing.
- ✓ **Provide the tools your employees need to make informed decisions.** Employees will always take the path of least resistance, so make sure that the path of least resistance is also the most secure path.

Two easy wins to get started

1. **Reevaluate your security policies** in light of the challenges presented by a hybrid workforce. Start with BYOD policies, network security protocols, and travel policies. Keep an eye out for infeasible policies.
2. **Utilize the Principle of Least Privilege where possible.** For example, ensure that employees only have access to the data they need to do their job, and nothing more. If it's easier on them, the policy is more likely to succeed.



Harlie Hardage
Senior Security Specialist, 1Password