In the name of security! Misconceptions of security features

Pilar Garcia
1Password

Abstract

Caring about security is not the same as understanding security. It can be challenging enough to foster a culture of security within an organization, but once that has been accomplished the work of the security team is not over. New problems arise when motivated individuals make insecure choices in pursuit of better security. Proposals for new policies or features can be motivated by appropriate concerns, and may seem sensible on their surface, but can contain flaws when examined closely. At best these flaws can render the proposed changes ineffectual. At worst, they can undermine previous policies and weaken organizational security in unforeseen ways.

1 Introduction

"Change your password often, so if it's ever exposed in a leak it's not a threat for very long." "Use special characters and numbers to make sure your password is complex and therefore hard to guess." We are all familiar with the history behind this kind of security advice. Most of us still cross paths with the occasional site that disables pasting in an attempt enforce the rule "don't ever write your passwords down" and in the process makes it harder to use a password manager.

What all these policies have in common is that they're both well-intended and ineffective, or even harmful. We know they're ineffective with the benefit of hindsight: they sounded reasonable once upon a time, until real life use and research uncovered their shortcomings. But not all such policies have fallen out of favour. Within organizations, new security policies are proposed and adopted which sound reasonable but which would also not stand up to scrutiny.

1Password customers aren't shy when it comes to sharing with us what they believe to be "the most secure" configuration for their password manager solution. We present a compilation of some of the most common feature requests from clients and IT managers, along with the trade-offs that would need to be made to implement them, and the ways in which they could backfire and compromise security.

2 I want to stop shadow IT

Most organizations have a process to vet the software that can be used by their employees. Apps or services that haven't been properly scrutinized by security can lead to data leaks. Since the password manager stores credentials for apps and services, it's common for our customers in IT and security departments to enlist our help in restricting employee access. The request is typically for a feature which would allow admins to create list of "approved domains". When an employee creates a password for a domain not on the list, the admin gets a notification that a login was created for an account outside of the list of allowed domains.

Superficially this feature makes sense. Technically speaking it could be implemented in a secure way that doesn't leak the domains outside of1Password account. But what it doesn't take into account is the reality of human behaviour. An employee who is trying to hide something from their company will not save their credentials in a password manager if they are aware that it will notify their IT department. The employee will bypass IT and the password manager entirely by creating a weak, possibly reused password and storing it somewhere unsafe. The risk is now significantly higher: not only is there an account that IT knows nothing about, but it is also protected by a weak, easy to guess password.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

3 I want to remain in control of the passwords shared

We have discussed before that there's no such thing as partially sharing a password. That doesn't stop customers from requesting certain features that they believe will help them achieve this goal. One that has surfaced recently is the ability to prevent employees from using multiple 1Password accounts – business and personal – in the same app.

The rationale is that credentials will be better protected if they can't easily be moved or copied out of a business account and into a personal account. It is true that the app makes it easy to move items between accounts, but there is no need for an admin to restrict the ability to use multiple accounts in order to prevent doing so. There are already admin controls to disable "copy" and "move" between accounts for this purpose.

A restriction on multiple accounts may reduce the chances of passwords being saved in the wrong account accidentally. While this benefit is not negligible, it doesn't actually give the employer their desired level of control. Users can still copy passwords manually if they are motivated to do so. And the restriction is bad policy for another reason: if an employee ever needs to access personal sites from their work computer they are now less likely to keep good password hygiene.

4 I want to keep credentials from being shared

One of the original motivations for creating the hosted version of 1Password was to offer a good solution for sharing. Customers requested this regularly after going through the pains of sharing vaults manually. But now that we have made sharing easy and secure, we are surprised to learn that a different set of users would like for us to disable it all together and disallow credential sharing.

Unique credentials are generally preferable to shared credentials, of course. They allow for proper accountability. But they aren't always an option. Social media sites are the most common offenders. The entire social team needs to have access to a single password. In the absence of a proper place to store this shared password, it is likely to find itself living on a sticky note on someone's desk.

But even when a service allows for separate accounts, we cannot discount the odd emergency when something simply needs to be done and the one person who can do it is about to board a plane for the next ten hours. If an exception needs to be made it's always preferable to do so via secure means, taking advantage of encryption, usage auditing, and the ability to access controls. Organizations which forbid password sharing will soon discover that their employees' shared passwords have migrated to Slack DMs instead of being kept safe in their password manager.

5 Conclusion

It is encouraging to see organizations place a greater emphasis on security than at any time in the past. However, we have also witnessed the consequences of overzealousness when applied to new policies which sound secure, but in fact are anything but secure. Any proposal for a secure policy change or a new security feature must be considered in light of its possible consequences and side effects to ensure that it doesn't backfire and make the organization less secure than it was before.