A Secret Shared: Expectations and Realities of Sharing Passwords (Industry Report)

Pilar Garcia
1Password

Abstract

Once a password has been shared with someone it must be assumed that the recipient has it and is able to use it until it is changed. However, we have learned that users of password managers sometimes believe otherwise. We present misconceptions that we have identified in users of 1Password related to sharing passwords and the ability to revoke them.

1 Introduction

"When Alice tells Bob a secret and later regrets doing so, she cannot make Bob forget that secret without resorting to brain surgery."

If you tell someone your password, you can't take it back. Few people would disagree with that statement. Yet expectations change as soon as a password manager is involved, especially one that supports sharing. Through our interactions with 1Password users, we have identified two misconceptions: first, that passwords can be shared without being visible to the recipient, and second, that passwords can be taken back once shared.

2 Sharing passwords without exposing them

In 1Password, passwords are concealed by default, only appearing in clear text if the user chooses to reveal them. This behaviour is familiar and provides a bit of privacy from shoulder surfing. Passwords can also be shared with other users in a family or team. Permissions can be applied to shared passwords, for instance, the ability to edit them.

Who Are You?! Adventures in Authentication (WAY) 2020.
August 7, 2020, Virtual Conference.

One permission goes a step further and prevents shared passwords from being revealed by their recipients. The goal of this permission is to prevent casual viewing. It is not cryptographically enforced and can be easily bypassed. This is by design; there is no reason to share a password if it cannot be used by the recipient to log in to websites. Problems arise when users believe it should be possible to allow someone to use a password without being able to see it.

Once a password has left the password manager and been filled into the browser it is no longer in the control of the password manager. The boundary between where the password manager ends, and the browser begins, is often lost on users. It is not uncommon to receive bug reports about passwords being visible once they have been filled or dragged into a browser or app. Users believe they have found a serious security vulnerability that has escaped our notice and that must be patched. It is difficult to explain that the feature is working as intended, and how it would be impossible to fill a password that other apps cannot see.

Even if the password never leaves the app there are still circumstances where it can be viewed by someone who does not have the permission to reveal it. Consider the scenario where viewing is disabled but sharing is enabled: the sharer can copy the password to another vault to which they have full access in order to view it. An argument could be made that revealing passwords is already trivial so the password manager shouldn't pretend to make it more difficult. On the other hand, unlike the scenario with the browser, it's at least possible for the password manager to be stricter about permissions. Even our developers disagree on how these permissions should interact with each other. They have taken different approaches depending on the client app and version.

3 Revoking access to passwords

If the source of all confusion stemmed from permissions alone, those permissions could simply be removed or changed. We have found, however, that the misunderstanding goes much deeper. Consider the action of revoking access to a

shared password. Users conflate the ability to access a password with the ability to access the services associated with that password. Of course that's not the case: a password will remain usable unless additional effort is taken to change it, even after it is deleted from a password manager. Even if an employee is completely removed from their company's 1Password account, any passwords they kept copies of are still valid.

But users don't need to go out of the way to make copies of their passwords, 1Password holds on to deleted passwords longer than users may think, for instance in the trash or password history. This again is by design. When someone deletes a password, one of two things might be true: either they hope it is gone forever, or they made a mistake which they expect to be able to undo. We err on the side of data availability, but finding the right balance is an ongoing struggle.

Offline availability of passwords provides another opportunity for misunderstanding. Employers are often surprised to discover that revoked passwords do not immediately disappear from the offline devices of employees who have been terminated. Our explanation that shared data will remain shared indefinitely, or at least until all devices re-authenticate, is often not well received. The only way to change this behaviour would be to implement online-only access, increasing the risk of data loss.

Conclusion

When it comes to sharing passwords, it really is all or nothing. Either you don't share a password at all, or you share it in full, and forever. Password managers like 1Password offer fine-grained sharing features to help users collaborate, but these same features sometimes give users the wrong impression. We must work harder to find a balance between empowering users and making fundamental limitations clear.