Secure Password Request: User Research

Interview Notes & Findings

OVERVIEW

Most password managers offer a way to share a password securely, but how does that help when the sender does not use a password manager? Freelance designers and developers, along with professionals across all fields who work in organizations with people of varying levels of tech savviness, often find themselves in situations where they need access to an account, and the account holder cannot quickly and easily share the credentials securely.

To address the above issue, I'm proposing adding a feature, using the password manager RememBear as a model, that would allow for secure password request, initiated by the recipient.

RESEARCH GOALS

The following questions will be answered via SME interview, competitive analysis, and user interviews:

1. What are the technological and legal considerations of a password request feature?
2. What are the password sharing habits of people who do not use password managers?
3. What methods currently exist to send information securely without signing up for an app or service?
4. What are the pain points of working with people who don't take online security precautions, and would a secure password request feature alleviate them?

SUBJECT MATTER EXPERT INTERVIEW SUMMARY

I contacted Eliot, a developer currently working on a password manager app, to clarify the legal and technical considerations of this feature. His response:

> "Generally, as long as you're not trying to trick someone into giving information to you (either by saying it'll be used for something else or by pretending to be someone you're not), you should be in the clear.
>
> From a technical perspective as well, there's ways to allow for only the person who gave the password in the first place and the receiving party to see the information. For example, there's no ability for us as employees to look into our database and figure out what someone's password is. There's a bunch of math that goes into the encryption that prevents us from doing something like that. I'd expect a tool that works in the way you describe to work in a similar way."

With this expert's sign-off, I'm prepared to call the proposed feature viable.

USER INTERVIEW PARTICIPANTS

The target demographic for this research is users who use password managers for professional pursuits but may work with people who don't—namely freelance designers and developers, and those with tech roles in non-tech focused organizations. Participants include;

1. Adam, 35M: Graphic & web design, IT
2. Chris, 33M: Graphic & web designer
3. Leilani, 22F: Graphic design intern
4. Sean, 43M: Creative director

INTERVIEW QUESTIONS

1. Do you use a password manager?
2. If so, which one? / If not, how do you store your passwords?
3. Have you worked in a position where you've needed clients or coworkers to share passwords with you?
4. Have you ever struggled to get others to send you passwords securely?
5. What are some of the methods others have used to send you passwords?
6. Have you ever experienced negative consequences from insecure password sharing?
7. Would you use a feature that allowed you to receive a password securely?

SUMMARY OF INTERVIEW FINDINGS

Goals:

Improve the security of password sharing in professional settings

Needs:

- Easy organization of passwords
- Separation of work and personal passwords
- Something that can be used easily with non-tech savvy people who will not sign up for services

Pains:

- Security breaches

- Lost passwords, lost account access
- Frustration of working with others who place convenience over security
- Feeling of responsibility if a breach occurs due to your password sharing behavior

Motivations:

- Improve overall security
- Decrease/eliminate personal liability
- Easy/convenient password storage and access
- Encouraging safe behavior in others

Behaviors:

- Use a personal password manager
- Use other methods of encrypting password sends
- Keep passwords offline out of strong distrust of the internet
- Resign oneself to employer's substandard security practices
- Make suggestions to colleagues

DETAILED INTERVIEW NOTES

Adam:

- Current profession: graphic and web designer at a small company, formerly designer and IT manager with a religious nonprofit organization
- Currently uses RememBear for password management
- Has worked in multiple organizations where no thought was given to password security
- Methods for receiving passwords have included: email, Skype, text, phone, yelling across the office, passing post-it notes
- Has experienced email and website breaches possibly due to insecure password sharing and storage in his organizations
- Has struggled to get colleagues to adopt more secure practices; attempts at greater security eventually overruled and turned off for being "too annoying"
- Would use a password request feature

Chris:

- Current profession: graphic and web designer
- Does not use a password manager; keeps personal passwords in a notebook in a drawer written in code only he understands, keeps work passwords in a spreadsheet on his local drive
- Works in an organization with lax password security, but doesn't give it much thought because he does not use a password manager himself
- Methods for receiving passwords have included: email, Skype, text, phone
- Has experienced email and website breaches possibly due to insecure password sharing and storage in his organizations; also experienced boss's personal email which also contained sensitive workplace information being compromised
- Would not change personal password management habits but would prefer a better system for storing and sharing passwords in the workplace

Leilani:

- Currently uses LastPass, but only for personal password management
- Has worked in an organization with no password management system
- Has received work related passwords primarily through unsecured email. One colleague would take it upon himself to use a service to encrypt passwords he sent, but this was not standard practice across the organization.
- Company passwords stored on one hard drive on a spreadsheet
- Has not experienced security breaches, but organization frequently lost access to accounts due to poor password management; usernames and passwords were easily lost when employees left the company.

Sean:

- Currently works as a creative director at a small company; has a long history of agency and freelance work as well
- Uses Chrome's built-in password manager
- Has worked in organizations with no password management
- Has used password vaults for external clients, but mostly experiences insecure sharing internally
- Methods for receiving passwords have included: email, Skype, text, phone
- Has experienced email and website breaches possibly due to insecure password sharing
- Would like to have secure password request as part of his workflow

My experience:

Additionally, I have ample experience in both freelance and office settings that is relevant to this project, including:

- Struggling to get others to adopt secure practices
- Having passwords sent to me via Skype, email, and text message
- Encouraging clients to separate usernames and passwords, i.e. text one and email the other
- Encouraging clients to use self destructing link sites, i.e. One Time Secret, etc
- Experiencing email security breaches at work
- Delaying the launch of a project because the organization needed a method for securely receiving information from partners and didn’t have one