department-of-veterans-affairs /
va.gov-team

<> Code   Issues 5k+   Pull requests 108   Discussions   Actions   Projects 29   Wiki   Security

va.gov-team / products / login.gov-adoption / research / 2023-03-Deferred-Identity-Proofing-Round-1-Usability

/ research findings.md

tygindraux Update research findings.md ✓   2 months ago

704 lines (433 loc) · 40.3 KB

Preview   Code   Blame   Raw

Deferred Identity Proofing Round 1: Usability - Research Findings

Office of the CTO - Digital Experience (OCTO-DE), Login.gov Adoption Team

Date: 04/12/2023

Tyler Gindraux [tyler@bluetiger.digital]

Research report deck

Jump to:

Hypotheses and conclusions

Key findings

Recommendations

Who we talked to

Further research needed

Research goals

The key goals of this study were to:

- Review whether Veterans can migrate their accounts from DS Logon to Login.gov (IAL1) without issue.
- Review whether Veterans understand the type of account they've set up and its limitations.
- Review whether Veterans know where to get help or what they will do if they encounter an issue during or after account setup.

Research questions

Review whether Veterans can migrate their accounts from DS Logon to Login.gov (IAL1) without issue:

- Are Veterans motivated to set up a Login.gov account when initially prompted, why or why not?
- Are Veterans more or less motivated when prompted via email or via a (surprise) modal after sign-in?

- How confident do Veterans feel about their ability to set up a Login.gov account when initially prompted?
- Can Veterans successfully initiate the account setup flow?
- Can Veterans successfully create their account, including verifying their email address and setting up multi-factor authentication?
- Can Veterans successfully return back to the VA after setting up their account?
- Do Veterans understand they are now signed into Login.gov?
- Do Veterans have concerns about their data or information now that they use a different sign in method?
- Do Veterans have concerns about their ability to continue accessing VA services, now that they have a new login method?

Review whether Veterans understand what type of account they have set up with Login.gov and its limitations:

- Do Veterans understand why they're being asked to set up a Login.gov account?
- Do Veterans understand the type of Login.gov account they are being asked to set up?
- Do Veterans understand that they should now stop using DS Logon and use Login.gov to sign in moving forward?
- Are Veterans motivated to upgrade to an IAL2 Login.gov account at a later date, why or why not?

Review whether Veterans know where to get help or what they will do if they encounter an issue during or after account setup.

- What will Veterans do first if they encounter an issue?
- Do Veterans know where or how to get help if they encounter an issue?

Methodology

This usability study was conducted remotely on Zoom. We tested on desktop. 2 participants used tablets instead.

We tested two prototypes. In half the sessions, we tested Prototype #1 and in the other half we tested Prototype #2. Both flows are similar but start differently:

- Prototype #1: After signing in to VA.gov, a modal pops up asking Veteran to set up a Login.gov account.
- Prototype #2: Veteran receives an email asking them to sign in to VA.gov to start Login.gov account set up.

Hypotheses and conclusions

Hypotheses	Concusions
Veterans will be motivated to set up a Login.gov account if they understand they will no longer be able to use DS Logon at some point in the future.	Likely True
Veterans who receive an email will be more motivated to set up a Login.gov account than those who see a modal pop-up; because they won't be interrupted while completing another VA task.	Likely True
Veterans will be able to set up an IAL1 Login.gov account, which is less risky and burdensome than setting up an IAL2 Login.gov account.	Likely True
Most Veterans will be able to set up one multi-factor authentication method without issue.	Likely True
Most Veterans will choose to set up text or voice message as their multi-factor authentication method.	Definitely True
Veterans will be motivated to continue to use their Login.gov account moving forward if they understand they should stop using their DS Logon account.	Likely True
Veterans will be motivated to upgrade to an IAL2 account through identity proofing if they understand what an IAL2 account will let them do (access other government websites).	Likely True
Veterans will decide and be able to navigate to contact information on the Login.gov or VA.gov websites if they encounter an issue during account creation.	Definitely True

Key findings

1. Most Veterans are motivated to set up a Login.gov account because they're concerned about losing access to their benefits and healthcare.
2. Veterans are likely to ignore messaging about migrating to Login.gov if it comes at the wrong time, on the wrong device, or without additional context and information for those who need it.
3. Veterans didn't recognize a relationship between their verified DS Logon account and their ability to create a Login.gov without identity verifying right away.
4. Veterans are unfamiliar with the term 'VA Digital Tools' which causes confusion and demotivates them, because they're not sure what they're losing or gaining access to.
5. Not understanding the difference between authentication and verification makes it difficult to know the limitations of an unverified Login.gov account, and how verification works.
6. Veterans prefer when they're given more information about their account, what to expect, and where to get help from VA.
7. If Veterans don't remember that their previous credential is going away, or don't feel a sense of urgency to start using Login.gov, it's likely that they'll continue to use DS Logon.

Details of findings

1. Most Veterans are motivated to set up a Login.gov account because they're concerned about losing access to their benefits and healthcare.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "It doesn't seem like I have much of a choice. I'd have to comply with what it says, otherwise I lose access to what I want, the information I need digitally." Participant 16

> "It looks like it's telling me that the DS Logon will soon stop working. So it wants me to create the Login.gov." Participant 7

> "My original [login] is going to get chucked, so I would use Login.gov now." Participant 15

2. Veterans are likely to ignore messaging about migrating to Login.gov if it comes at the wrong time, on the wrong device, or without additional context and information for those who need it.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "Initially when it said this is going away, you need to create some other stuff for the systems or whatever, I was like yeah, okay, I don't need that right now. I just need to go in and get my stuff. I don't have time." Participant 4

> "If I saw this I'd be like, I'll just do it later. And especially if I'm on the go, I'm on my mobile. I'm just trying to get a message or send something." Participant 5

3. Veterans didn't recognize a relationship between their verified DS Logon account and their ability to create a Login.gov without identity verifying right away.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "At the beginning, it seems like there could be a note there saying, 'if you click on DS Logon you will be asked to create a Login.gov account.' There was no purpose at all to signing in with DS Logon." Participant 16

4. Veterans are unfamiliar with the term 'VA Digital Tools' which causes confusion and demotivates them, because they're not sure what they're losing or gaining access to.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "I have no idea what a VA digital tool is to be honest with you, I mean I would be thinking it's a mouse that I'm moving around and being able to touch a link and press the button. I don't know." Participant 17

> "I'm not really sure. Digital, it means that there's some type of electronic process. And then I guess the tools part – some type of resource to help me get into my information. That was the thing that slowed me down the most. How that language connected to what I was trying to do." Participant 4

5. Not understanding the difference between authentication and verification makes it difficult to know the limitations of an unverified Login.gov account, and how verification works.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "To verify my identity I would choose voice or text." Participant 20

> "I've tried to get a Login.gov account before, but they want you to do this authentication where you have a video with them." Participant 5

> "When you get in, it [will] say, 'okay, so to verify your identity we're gonna send you this code to a text number.'" Participant 15

6. Veterans prefer when they're given more information about their account, what to expect, and where to get help from VA.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "I was wondering how long it was gonna take where it tells me right here, about 20 min. It tells me stuff I need to have so I can gather those things before I continue." Participant 7

> "I would print off this email, so that I can reference it. It's just me. I can't remember things, and I can't go back and forth [between tabs]." Participant 2

> "If I had any questions I would probably call the VA. I'd telephone. I'd go to that website and try to get your phone number for support from the VA." Participant 6

7. If Veterans don't remember that their previous credential is going away, or don't feel a sense of urgency to start using Login.gov, it's likely that they'll continue to use DS Logon.

Labels: `AUD: Veterans` , `PRDT: Login.gov` , `PRDT: Login` , `BNFT: Healthcare` , `VETJNY: Taking care of themselves Veteran` , `RESRCH: Evaluative` , `RESRCH: Interviews` , `RESRCH: Remote`

> "But you can use Login.gov and still keep the same one I have, MHV Premium, right? You can have both, right? Because I want to keep my security blanket until I get used to other sites." Participant 6

> "In my spare time, I would try to go in on Login.gov, just to become familiar. But I have to be familiar with the site in order to use it over and over again." Participant 20

Additional insights

1. Many Veterans benefit from password managers, whether they're using a password manager application or an in-browser password manager that auto fills their details for them.

2. Veterans found it straightforward to close the modal and understood that was all they needed to do in order to navigate to another task they would like to complete on VA.gov.

3. Most Veterans will choose to set up SMS, and are familiar with it. We found this during discovery research and it's further confirmed by data from Login.gov.

4. Most Veterans will not choose to set up a backup multi-factor authentication method. Those that would choose to set up a backup method tend to have experience with losing their phone, or understand there might be circumstances when they're unable to access one method.

Key themes

1. Benefits of deferring identity proofing aren't clear
2. Easy to ignore
3. Confusion between credentials and applications
4. Authentication ≠ verification
5. Transitions take time
6. Help from VA

Benefits of deferring identity proofing aren't clear

As expected, most Veterans meet messaging about the need to adopt a new credential with concern or, at least, frustration.

When you've established a routine for how to sign in, it's frustrating to think of starting over. And Veterans are quickly fearful of losing access to their benefits and healthcare.

> "If the login that I've used for the last 14 years is discontinued then I'm just going to call the VA and leave old fashioned messages with my provider." Participant 19

This concern, however, can be a motivating factor, urging Veterans to set up a new credential as soon as possible so they continue to have access.

If a Veteran recognizes DS Logon as their sign in method and learns they won't be able to use it at some point in the future, they will often choose to take action.

> "It looks like it's telling me that the DS Logon will soon stop working. So it wants me to create the Login.gov." Participant 7

> "It doesn't seem like I have much of a choice. I'd have to comply with what it says, otherwise I lose access to what I want, the information I need digitally." Participant 16

The benefits of migrating deferring identity verification weren't clear. And not recognizing a relationship between DS Logon and Login.gov makes it difficult to understand:

- why you must start by signing in to DS Logon
- why you don't need to verify your identity at first, but later on it's recommended
- why you have access to the VA, but not other government websites for now
- why to verify and how it works

> "At the beginning, it seems like there could be a note there saying, 'if you click on DS Logon you will be asked to create a Login.gov account.' There was no purpose at all to signing in with DS Logon." Participant 16

Easy to ignore

Veterans who saw a modal appear right after signing in to VA.gov, went to close it right away, or admitted that they would usually, out of habit.

> "Initially when it said this is going away, you need to create some other stuff, I was like yeah, okay, I don't need that right now. I just need to go in and get my stuff. I don't have time." Participant 4

Veterans seemed to read through the email more closely. They're hesitance, due to concerns about scams, do lead them to pay closer attention. This tendency to ignore a pop-up or modal also depends on whether the message comes at the wrong time or on the wrong device.

While about 50% of VA.gov traffic is on mobile, Veterans prefer to set up a new credential or account on their desktop or laptop computer.

> "If I saw this I'd be like, I'll just do it later. And especially if I'm on the go, I'm on my mobile. I'm just trying to get a message or send something." Participant 5

Unfamiliar language can also impede a Veteran's motivation to set up a Login.gov account.

Most Veterans were not sure what they were at risk of losing access to, because the term VA Digital Tools was unclear and unfamiliar. This misunderstanding leads to confusion about the relationship between Login.gov and the VA later on.

> "I have no idea what a VA digital tool is to be honest with you, I mean I would be thinking it's a mouse that I'm moving around and being able to touch a link and press the button. I don't know." Participant 17

> "I'm not really sure. Digital, it means that there's some type of electronic process. And then I guess the tools part – some type of resource to help me get into my information. That was the thing that slowed me down the most. How that language connected to what I was trying to do." Participant 4

Some Veterans may struggle to remember the name of the credential they use, which can make it easy to ignore an important message about DS Logon.

And Veterans who do remember which credential they use, may not be aware of, or remember, the names of those they don't use.

This makes it difficult to understand that Login.gov is a sign in option. Referring to it as "VA only Login.gov" account, further complicates things.

> "I know I used to use like DS, or something like that, what was it called?" Participant 7

> "This is basically saying that DS Logon, it's gonna stop working. And you can create a VA healthcare login." Participant 5

Confusion between credentials and applications

At first, most Veterans don't understand that Login.gov is a credential, not a new application.

This confusion between credentials and applications also leads some Veterans to believe that Login.gov will consolidate all VA applications into one place, like a 'one stop shop' portal.

> "I would imagine that [I'm going to set up] a one stop shop for all things VA … Just a login that allows you to access all things VA without having to go to multiple different pages or sites." Participant 5

> "I don't wanna have to log into something, do one thing and then log out of it and log into something else, and then I can do something else. I wanna be able to do all of those things at one time." Participant 4

At the end of account creation, most Veterans weren't sure why Login.gov was sharing their information with the VA.

This is partly because Veterans aren't certain which account they've created, and because many Veterans assume they are creating an account on a VA website, not on Login.gov.

Some referred to their account as a "VA login," "Login for the VA", "Login" or, in a few cases, "DS Logon."

> "You know, I was under the mistaken idea that this was the VA that I was working on? And it's not. It is, I guess, a group that is working either for or in connection with the VA." Participant 17

> "I think it might be a little bit helpful if it said your 'DS Logon' account set up is complete." Participant 19

This confusion also makes it difficult for Veterans to understand how to use Login.gov on other sites, and therefore, how verification works.

After setting up their account, many Veterans assume that they've now 'verified' with the VA. And in order to use Login.gov with other government agencies, they'd follow a similar process on each agencies' website.

Veterans also found this 'out of place' because they would expect to be asked to verify their identity when they're on another government website, not on VA.gov.

> "I've got another account I've got to manage. So VA Login.gov, and all other government agencies Login.gov." Participant 16

> "I created a Login.gov account. It was pretty straightforward. A step by step walkthrough, and then I went through the verification process, verifying my identity with Login.gov. And I was able to get all signed in." Participant 7

Authentication ≠ verification

With changing security requirements, Veterans expect sign in may require an additional step after username and password.

So although it's common to feel overwhelmed at the start of MFA set up, once you find a familiar option it's straightforward.

Most Veterans, like most people who use Login.gov, will choose SMS as their MFA option, because of previous experience with it.

> "Text or voice message, I do that all the time, so that's what I would do." Participant 17

> "I usually have my cell phone on me. So the text is easiest. I can click on that button. Look at my phone, get the 6 digit code, or whatever it is, type it in, and then continue." Participant 5

But familiarity, which comes from repetitive use over time, doesn't build an understanding of the difference between standard authentication, multi-factor authentication and identity verification.

Terms, like, authenticate, sign in, two-factor, login and verify jumble together, with many Veterans using 'authenticate' and 'verify' interchangeably.

This makes it difficult to understand the limitations of a Login.gov account that hasn't been verified.

> "To verify my identity I would choose voice or text." Participant 20

> "I've tried to get a Login.gov account before, but they want you to do this authentication where you have a video with them." Participant 5

> "It sends me a verification, a confirmation code, sometimes I get that." Participant 6

> "I set my email up, and then the next screen was to decide how I wanted to verify my identity, and that's when I chose text." Participant 4

> "When you get in, it [will] say, 'okay, so to verify your identity we're gonna send you this code to a text number.'" Participant 15

> "This is like a double verification. So authentication." Participant 15

> "[We were] logging in, verifying your account and validating your account." Participant 6

Some Veterans assume they are being asked to verify their identity in order to recover their account.

Those who understand that verification allows you to access other government websites – and find it useful to know a timeframe and what to bring – still aren't sure how it actually works or what to do next.

A few Veterans reminded us that a timeframe can be misinterpreted as a session timeout, or, unlikely to represent your personal experience.

> "If they don't recognize the first sign in, then I have to verify." Participant 17

> "I think I would expect to do a process very similar to the Login.gov for the VA. But it sounds like I'd set up an entirely new Login.gov account for another government or entity? Or can I use the same credentials? And then I just need to verify my identity. And I'm not really clear what that means." Participant 16

Transitions take time

After setting up Login.gov, Veterans are confident they can continue using VA services as usual.

If they remember why they were asked to set up a Login.gov account – because DS Logon is going away soon – they're more likely to remember to use Login.gov in future sessions.

> "My original [login] is going to get chucked, so I would use Login.gov now." Participant 15

> "Not DS Logon, so I would click on Login.gov." Participant 16

But if Veterans don't remember that their previous credential is going away, they may to continue to use DS Logon, even after they set up Login.gov.

Or they might use Login.gov, but for less robust reasons, like, 'it's first in the list,' or 'I'll give it a try.'

And because there's no deadline for when to stop using DS Logon, Veterans are more likely to continue using their legacy credential, which they feel more comfortable with. Not having a deadline also makes Veterans more likely to dismiss the modal.

> "In my spare time, I would try to go in on Login.gov, just to become familiar. But I have to be familiar with the site in order to use it over and over again." Participant 20

> "But you can use Login.gov and still keep the same one I have, MHV Premium, right? You can have both, right? Because I want to keep my security blanket until I get used to other sites." Participant 6

Help from VA

Most Veterans will reach out to the VA for support with Login.gov or concerns about migrating. Veterans prefer to get help over the phone.

Veterans might also choose to contact their VA healthcare provider or other Veterans they know.

Only one Veteran mentioned getting support from Login.gov while they were setting up their account, but, this might be a result of Veterans' misunderstanding what account they're setting up.

> "If I had any questions I would probably call the VA. I'd telephone. I'd go to that website and try to get your phone number for support from the VA." Participant 6

> "I would call my doctor, my main provider, and they've been pretty good about responding to questions I had. They would get back to me on the phone." Participant 17

Throughout account creation, many Veterans mention getting help or looking for more information about what they are being asked to do.

Before embarking on setting up an account, Veterans may want to learn more about the process and what to expect, before jumping straight in.

They also to come back to reference information about the migration in case they have questions or need help, which makes an email helpful.

> "I was wondering how long it was gonna take where it tells me right here, about 20 min. It tells me stuff I need to have so I can gather those things before I continue." Participant 7

> "I would print off this email, so that I can reference it. It's just me. I can't remember things, and I can't go back and forth [between tabs]." Participant 2

Recommendations

1. Keep continued access front of mind
2. Better communicate the urgency of the situation
3. Use familiar words rather than trying to educate right now
4. Build greater awareness of Login.gov
5. Consider how the unauthenticated experience fits in
6. Share more up front so Veterans know what to expect
7. Leverage emails to provide detail to Veterans who need it
8. Explore more touchpoints in the authenticated experience

Details of recommendations

1. Keep continued access front of mind

Veterans prioritize ease of use, which comes from familiarity, when it comes to credentials. The pain of switching accounts usually outweighs the fact that Login.gov is secure or recommended.

When we suggest that Veterans create a new account we should stress the importance of maintaining access to VA services.

When it gets closer to the sunset deadline, we should urge Veterans to set up a new account by letting them know they're at risk of losing access.

We recommend:

- emphasizing continued access to VA benefits and healthcare
- increasing the number of channels and notifications as we get closer to the sunset deadline

2. Better communicate the urgency of the situation

Even Veterans who understand that they will lose access are unsure how soon they need to act.

This lack of urgency means they may delay setting up an account, or, choose to set up an account but take their time transitioning over while they continue to use their legacy credential.

We should make it clear that this situation is urgent so that Veterans choose to act soon.

We recommend:

- adding a deadline for DS Logon being sunset
- updating H1 with a more urgent call to action
- increasing the number of channels and notifications as we get closer to the deadline
- requiring Veterans to acknowledge they've read something as we get closer to the deadline

3. Use familiar words rather than trying to educate right now

Veterans' focus should be on creating a Login.gov account so they can maintain access to VA services.

With this in mind, now is not the right time to introduce new terms to Veterans, such as VA Digital tools.

Instead of educating Veterans on new terminology right now, we should explain what they need to do in their own words.

We recommend:

- testing to identify which terms resonate most

- using descriptive language to describe what Veterans need to do, rather than jargon or new terminology such as 'verify your identity'
- removing 'VA Digital tools' and replacing it with something Veterans know or say already
- if we let Veterans defer identity proofing, remove the term 'VA only Login.gov account'

4. Build greater awareness of Login.gov

Veterans who don't currently use Login.gov tend to be unfamiliar with the credential.

We can use different communication channels to help build a greater awareness of Login.gov. This should help Veterans understand what Login.gov is, how it works with the VA and how to set up an account.

Using familiar visual cues, such as the sign in screen which shows Login.gov, will help further contextualize Login.gov for Veterans.

We recommend:

- creating a campaign page and video content in collaboration with VEO
- creating additional blog posts
- adding a banner about Login.gov
- including visual references, for example a screenshot of the sign in screen, when communicating about Login.gov
- considering how MHV coordinators can be empowered to introduce Login.gov to more Veterans

5. Consider how the unauthenticated experience fits in

Focusing on the authenticated experience lets us directly target Veterans who are at risk of losing access to their benefits and healthcare.

But there's an opportunity to communicate with Veterans in the unauthenticated experience, too.

Without alarming current ID.me or Login.gov users, we can still build awareness of Login.gov and let Veterans know that DS Logon is going away soon.

We recommend:

- adding a banner about DS Logon sunset
- elevating Login.gov and ID.me on the sign in screen
- adding an alert about DS Logon on the sign in screen
- building greater awareness that you can create an account on the sign in screen

6. Share more up front so Veterans know what to expect

Veterans find it helpful to have more information before they set up an account.

We should explain what's involved in setting up a Login.gov account, such as, setting up multi-factor authentication and uploading a picture of a state-issued ID.

If we leverage examples that are familiar to Veterans, such as receiving a 6-digit code via text, they'll be more likely to understand what to expect.

We recommend:

- explaining what account creation involves including how long it will take
- creating content that can be referenced later, for example, via email or in outreach materials
- letting Veterans know where to get help
- testing with Veterans to better understand issues with remote identity verification

7. Leverage emails to provide detail to Veterans who need it

Email provides an opportunity to offer more information to Veterans with legacy credentials.

Over email Veterans can learn more while they're not distracted by another task.

If they need to, they'll also be able to come back to the information for reference later on.

This will help prime Veterans when they receive other direct communications within the authenticated experience.

We recommend:

- developing a comprehensive email campaign to eligible Veterans
- testing subject headlines for phishing or scamming concerns
- email Veterans after they set up an account to remind them of what they just did
- letting Veterans know where to get help

8. Explore more touchpoints in the authenticated experience

When Veterans are signed in to VA.gov with DS Logon, we should explore additional ways of reminding Veterans to create a Login.gov account, besides just a modal.

This will help increase awareness through additional channels while also promoting a greater sense of urgency willing Veterans to take action.

We recommend:

- sending notifications in VA profile
- testing alternative ways of using a modal, including how soon after sign in it appears
- letting Veterans click 'remind me later' for reassurance they'll have another chance

Next steps

We are adding research, design and content tasks to our Login.gov Adoption Team backlog with the aim to pick this up in the coming sprints. We will also update our product outlines based on this additional product context.

Further research needed

We recommend:

- testing to identify which terms resonate most
- testing subject headlines for phishing or scamming concerns
- testing alternative ways of using a modal, including how soon after sign in it appears
- testing with Veterans to better understand issues with remote identity verification

We've partnered with the Identity Core Team on an upcoming research study that will address these first 3 recommendations (among other research questions).

We're continuing discussions with Login.gov to learn more about issues with remote identity verification, before we make further recommendations on this.

Appendix

Research plan

Conversation guide #1

Conversation guide #2

Transcripts

Addendum shared with Login.gov

This research tested the Login.gov authenticated flow, aiming to understand whether Veterans are able to set up authenticated (not verified) accounts and any pain points they experience. (This does not cover identity verification).

While our focus at the VA is on implications related to VA applications, we did uncover further detail about the Login.gov authenticated flow that we've compiled to share with Login.gov.

Summary

1. Starting account creation and confirming an email address is familiar
2. Multi-factor authentication is overwhelming at first
3. Veterans who understand risks may add a backup method

1. Starting account creation and confirming an email address is familiar

The sign in and create an account page is familiar and well understood by those who have used their email addresses to set up an account before.

> "I would just go to each box enter your email address, password. Wait a minute. No, I would go to create an account." Veteran (P15)

Similarly, Veterans are used to confirming their email address when they set up an account. When confirming their email address, Veterans might choose to switch devices. For example, it would be common for a Veteran to set up an account from their desktop or laptop, but confirm their email address on their phone.

At this point, we have no recommendations for these steps in Login.gov's account creation.

2. Multi-factor authentication is overwhelming at first

When Veterans first see a long list of MFA options, they're overwhelmed (often sighing out loud).

Veterans, like most users of Login.gov, were most comfortable setting up text message MFA. Once they see this option in the list, they're more comfortable and know what they will do next.

> "It's just the way it looks. That's too much to read." Veteran (P4)

> "Oh good lord! I'm seeing a lot of two-factor authentication options." Veteran (P16)

We recommend:

- elevating text message or phone call to the top of the multi-factor authentication menu
- letting users know that they can choose 2 MFA options earlier on
- giving users an example of an authenticator application they can use, like Authy

3. Veterans who understand risks may add a backup method

Those who have familiarity with MFA may have experience no longer being able to access their MFA. They may choose to setup a backup option.

But, if it's not mandatory, most Veterans will not choose to setup a backup method. And many don't see an option that would work for them, if they did want to set up a second MFA.

> "It says, the second method. I guess it would have to be my email. Send it to my email. I'd rather not get a phone call." Veteran (P17) who chose text message as their 1st MFA

We recommend:

- letting users know that they can choose 2 MFA options earlier on
- helping users know why it can be helpful to set up a second MFA option
- considering how to make it clear that there's no hierarchy to your 1st and 2nd MFA options

Tools used for synthesis

[Mural](#)

Pages and applications used

[Prototype #1](#)

[Prototype #2](#)

Other supporting documents created

[Research report deck](#)

Secondary research

This research builds on:

- [2022-10-Research-LoginGovFieldResearch #185](#)
- [2022-07 MHV transition to Login.gov as a single sign-on #157](#)
- [2022-07 Login Self-Service Tool #156](#)
- [2022-03 Sign-In Accessibility #93](#)

As well as research conducted by Login.gov's product teams.

Who we talked to

Recruitment criteria

Primary criteria (must-haves)

All participants:

- Must be Veterans
- Must have a computer and be willing to complete their sessions on this device (Note: In subsequent rounds, we will include and favour mobile testing)
- Must be willing to share a web browser window on their computer
- Must have a working microphone on their computer
- Must have Zoom downloaded to their computer prior to the session and know how to share their screen
- Must have signed into a VA application (including VA.gov, My HealtheVet or eBenefits) in the last 6 months
- Must use DS Logon (as their credential service provider) to sign in to the VA. If Veterans aren't sure what this means or what they use, this can be confirmed by asking them to sign into VA.gov and confirming how they logged in.

At least 13 participants:

- Must not have a Login.gov or ID.me account set up.

At most 2 participants:

- Must have a Login.gov account set up, but not use it to sign in to the VA. For example, they use Login.gov to sign in to TSA Pre-check or USAJobs, but, when they sign in to VA.gov, they use DS Logon.

Demographic goals:

- At least 50% of people must be over 55
- At least 50% of people must have an identified cognitive disability
- At least 30% of people must identify as Black, Hispanic, or Native
- At least 30% of people must be without a degree or professional certificate
- At least 30% of people must live in a rural or remote area
- At least 20% of people must identify as other than male
- At least 20% of people must be non-native English speakers
- At least 20% of people must identify as gay, lesbian, bisexual, or transgender

Recruitment outcomes

We talked to 10 participants. More information about the participants recruited for this study is in the VA Recruitment Checker for Equality.

Audience segment:

- Veterans: 10
- Caregivers: 0
- Family members of a Veteran: 0

Gender:

- Male: 7
- Female: 3

LGBTQ+:

- Transgender: 0
- Nonbinary, gender fluid, gender queer, Two-Spirit (Indigenous only), or another gender beyond man or woman: 0
- Gay, lesbian, or bisexual: 0

Devices used during study:

- Desktop: 8
- Tablet: 2
- Smart phone: 0
- Assistive Technology: 0

Age:

- 25-34: 0
- 35-44: 0
- 45-54: 3
- 55-64: 3
- 65+: 4
- Unknown: 0

Education:

- High school degree or equivalent: 2
- Some college (no degree): 1
- Associate's degree, trade certificate or vocational training: 2
- Bachelor's degree: 1
- Master's degree: 3
- Doctorate degree: 1

- Unknown: 0

Geographic location:

- Urban: 5
- Rural: 5
- Unknown: 0

Race:

- White: 6
- Black: 5
- Hispanic: 2
- Biracial: 4
- Asian: 0
- Native: 1

Disability and Assistive Technology (AT):

- Cognitive: 4
- AT beginner: 0
- AT advanced user: 0
- Desktop screen reader: 0
- Mobile screen reader: 0
- Magnification/Zoom: 0
- Speech Input Technology like Siri/Dragon Naturally Speaking: 0
- Hearing aids: Unknown
- Sighted keyboard: 0
- Captions: 0

Underserved groups we haven't talked to

This research does not include the perspectives of the following marginalized Veteran groups:

- Asian Veterans
- LGBTQ+ Veterans

We weren't given data on whether participants were other than honorably discharged, of immigrant origin, or expats (living abroad).

We tested a desktop-first prototype, with the aim to test a mobile-first prototype in our next round of research. We did not aim to recruit AT users, with the aim to test a coded prototype with AT users in a subsequent round of research.