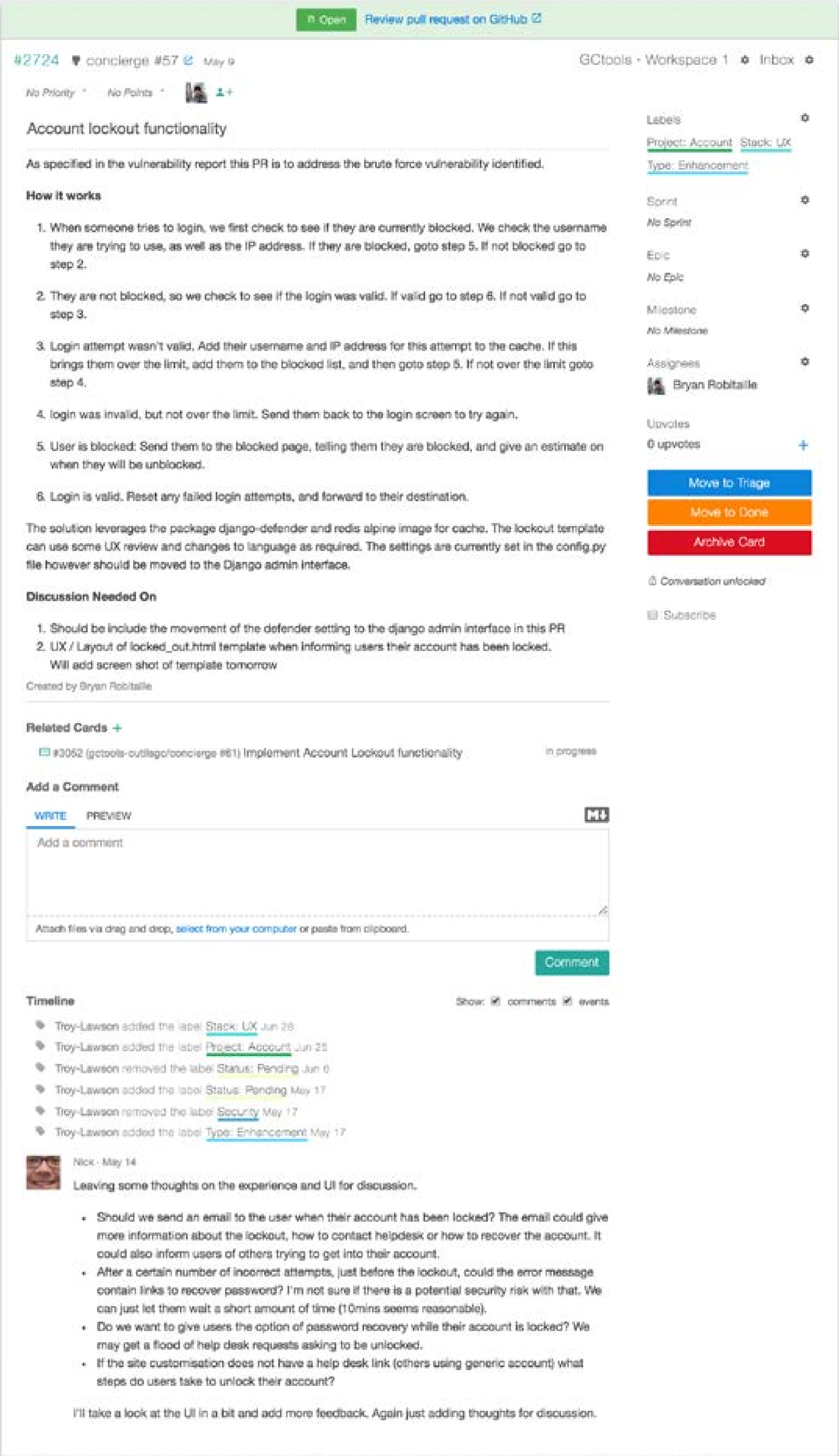
THE MOMENT WHEN
YOU GET LOCKED OUT YOUR ACCOUNT BECAUSE YOU ENTERED THE WRONG PASSWORD TOO MANY TIMES
imgflip.com

Account - Lockout functionality
Sprint #42



Account lockout functionality

As specified in the vulnerability report this PR is to address the brute force vulnerability identified.

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

The solution leverages the package django-defender and redis alpine image for cache. The lockout template can use some UX review and changes to language as required. The settings are currently set in the config.py file however should be moved to the Django admin interface.

Discussion Needed On

1. Should be include the movement of the defender setting to the django admin interface in this PR
2. UX / Layout of locked_out.html template when informing users their account has been locked.
   Will add screen shot of template tomorrow

Created by Bryan Robitaille

Related Cards +

#3052 (gctools-outilsgc/concierge #61) Implement Account Lockout functionality — in progress

Add a Comment

Attach files via drag and drop, select from your computer or paste from clipboard.

Timeline

Show: ☑ comments ☑ events

- Troy-Lawson added the label Stack: UX Jun 28
- Troy-Lawson added the label Project: Account Jun 28
- Troy-Lawson removed the label Status: Pending Jun 6
- Troy-Lawson added the label Status: Pending May 17
- Troy-Lawson removed the label Security May 17
- Troy-Lawson added the label Type: Enhancement May 17

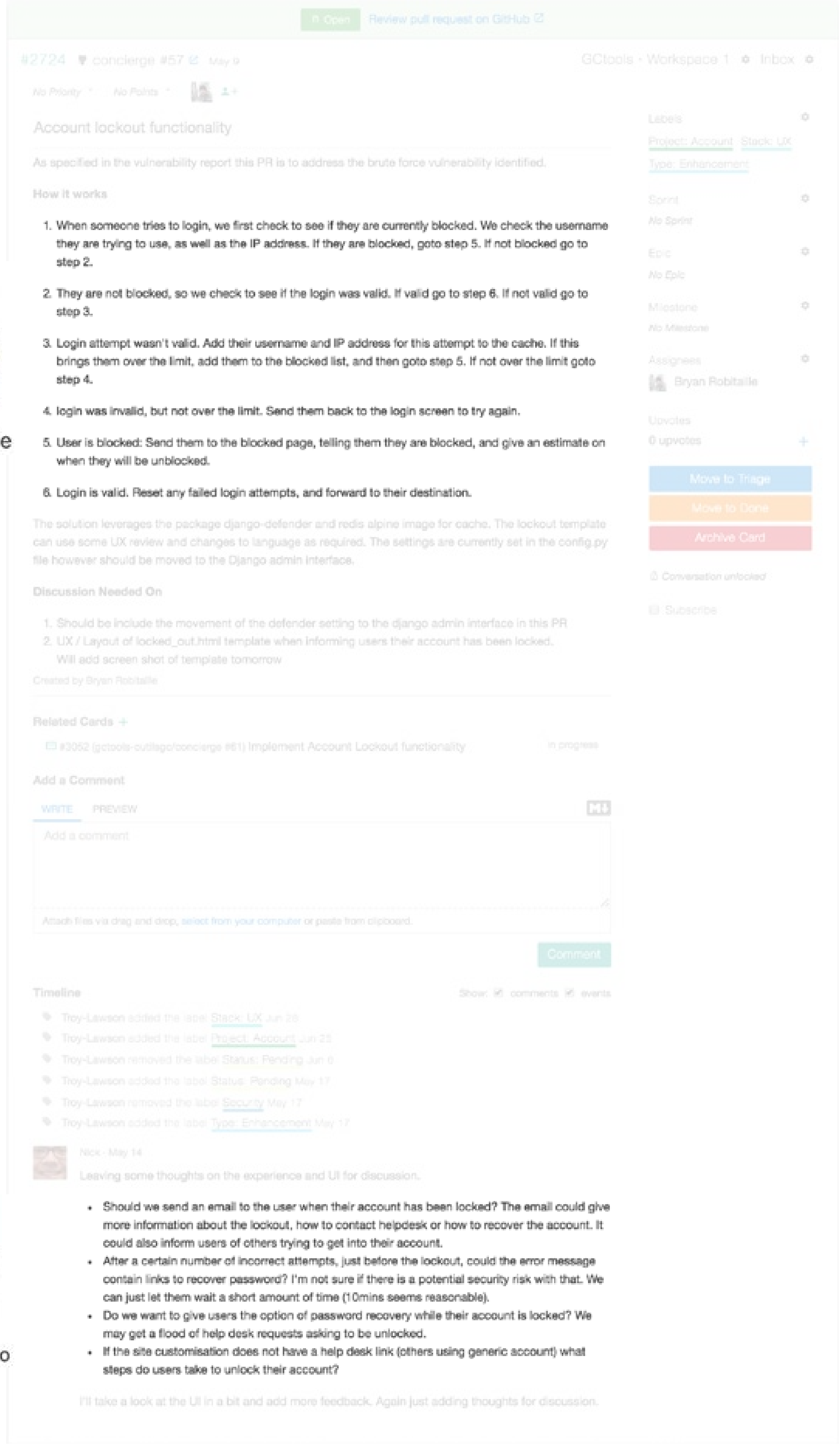
Nick · May 14

Leaving some thoughts on the experience and UI for discussion.

- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?

I'll take a look at the UI in a bit and add more feedback. Again just adding thoughts for discussion.

Bryan Robitaille



Account lockout functionality

As specified in the vulnerability report this PR is to address the brute force vulnerability identified.

How it works

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

The solution leverages the package django-defender and redis alpine image for cache. The lockout template can use some UX review and changes to language as required. The settings are currently set in the config.py file however should be moved to the Django admin interface.

Discussion Needed On

1. Should be include the movement of the defender setting to the django admin interface in this PR
2. UX / Layout of locked_out.html template when informing users their account has been locked.
   Will add screen shot of template tomorrow

Created by Bryan Robitaille

Related Cards +

#3052 (gctools-outilsgc/concierge #61) Implement Account Lockout functionality — in progress

Add a Comment

Add a comment

Attach files via drag and drop, select from your computer or paste from clipboard.

Timeline

- Troy-Lawson added the label Stack: UX Jun 26
- Troy-Lawson added the label Project: Account Jun 25
- Troy-Lawson removed the label Status: Pending Jun 6
- Troy-Lawson added the label Status: Pending May 17
- Troy-Lawson removed the label Security May 17
- Troy-Lawson added the label Type: Enhancement May 17

Nick · May 14

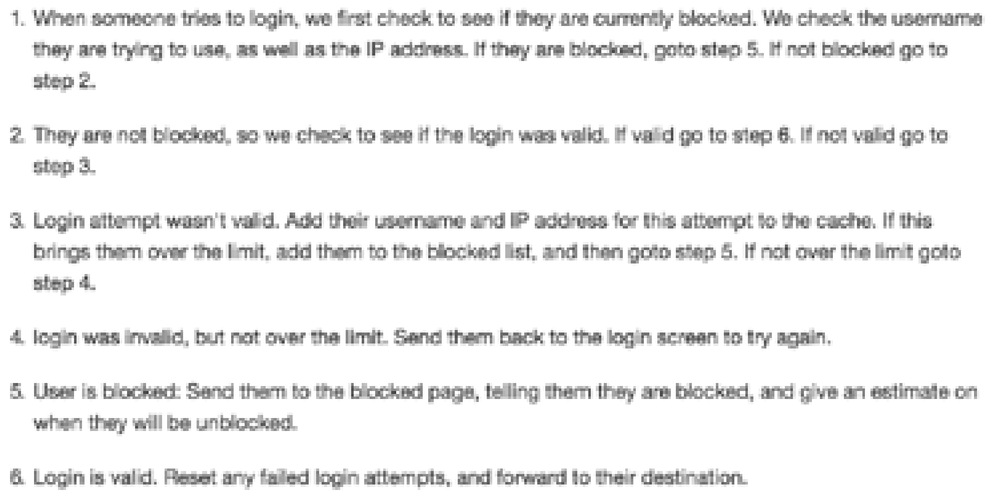
Leaving some thoughts on the experience and UI for discussion.

- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?

I'll take a look at the UI in a bit and add more feedback. Again just adding thoughts for discussion.

Nick Pietrantonio

Bryan Robitaille



1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

Bryan Robitaille

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.

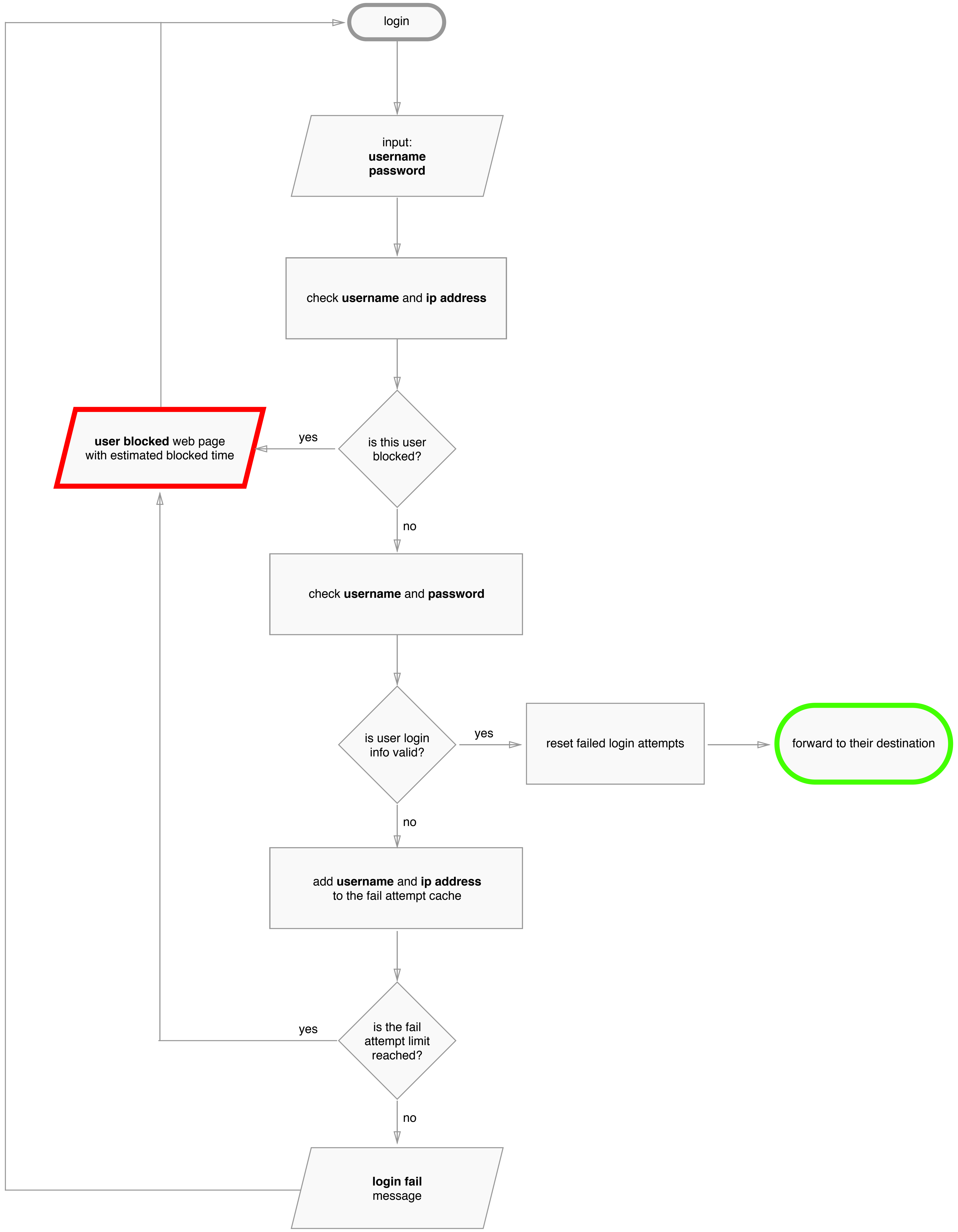
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.

3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.

4. login was invalid, but not over the limit. Send them back to the login screen to try again.

5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.

6. Login is valid. Reset any failed login attempts, and forward to their destination.



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

user blocked web page
with estimated blocked time

no

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address**
to the fail attempt cache

is the fail attempt limit reached?

yes

no

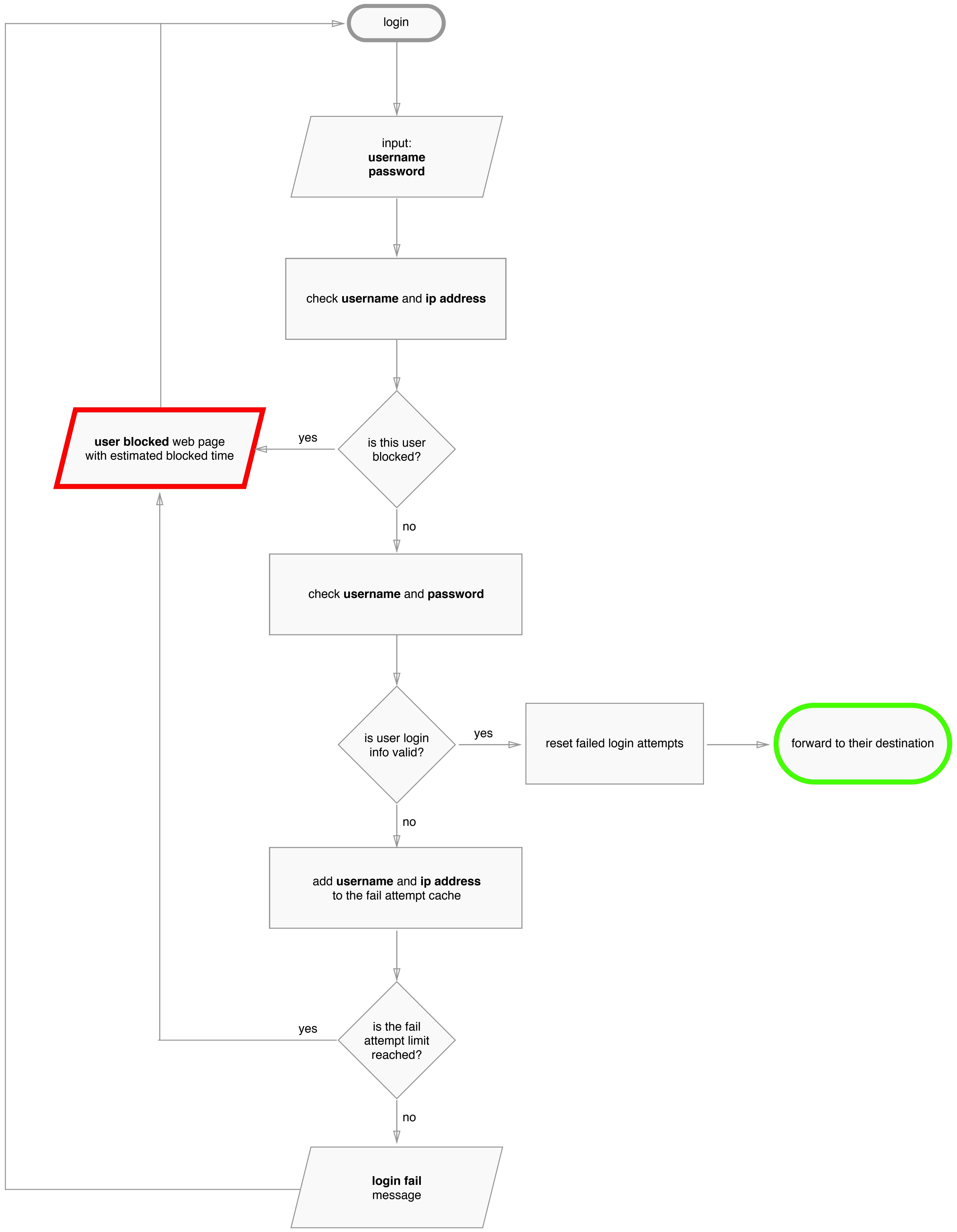
login fail
message

Bryan Robitaille

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

Amable Rodríguez

Stéphanie C.Lefebvre



login
input:
username
password
check username and ip address
is this user blocked?
yes
user blocked web page with estimated blocked time
no
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
no
login fail message

Bryan Robitaille

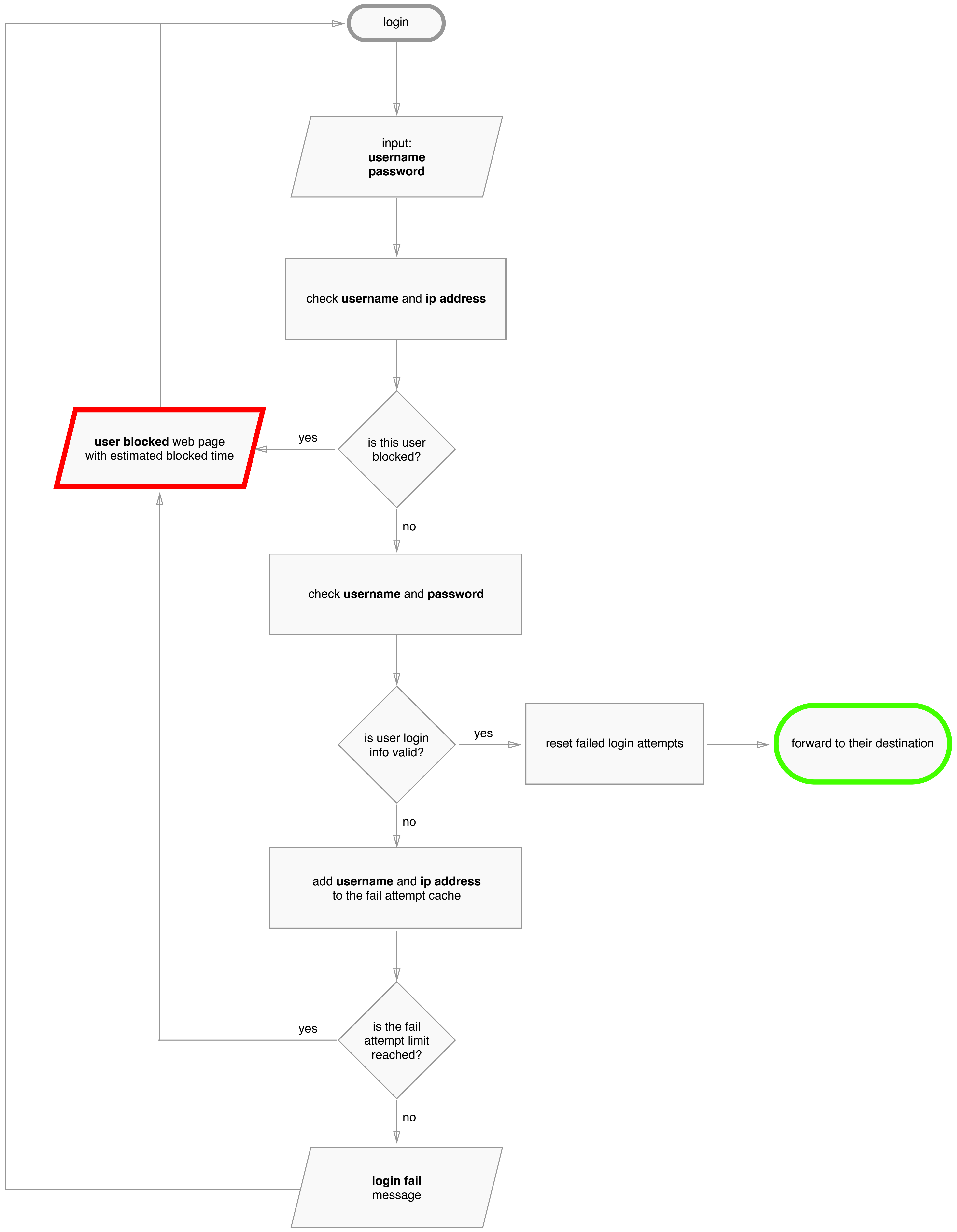
1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

Amable Rodríguez

Stéphanie C.Lefebvre

Nick Pietrantonio

- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?


login
input:
username
password
check **username** and **ip address**
is this user blocked?
yes
user blocked web page
with estimated blocked time
no
check **username** and **password**
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add **username** and **ip address**
to the fail attempt cache
is the fail attempt limit reached?
yes
no
login fail
message

Bryan Robitaille

1. When someone tries to login, we first check to see if they are currently blocked. We check the username they are trying to use, as well as the IP address. If they are blocked, goto step 5. If not blocked go to step 2.
2. They are not blocked, so we check to see if the login was valid. If valid go to step 6. If not valid go to step 3.
3. Login attempt wasn't valid. Add their username and IP address for this attempt to the cache. If this brings them over the limit, add them to the blocked list, and then goto step 5. If not over the limit goto step 4.
4. login was invalid, but not over the limit. Send them back to the login screen to try again.
5. User is blocked: Send them to the blocked page, telling them they are blocked, and give an estimate on when they will be unblocked.
6. Login is valid. Reset any failed login attempts, and forward to their destination.

Amable Rodríguez

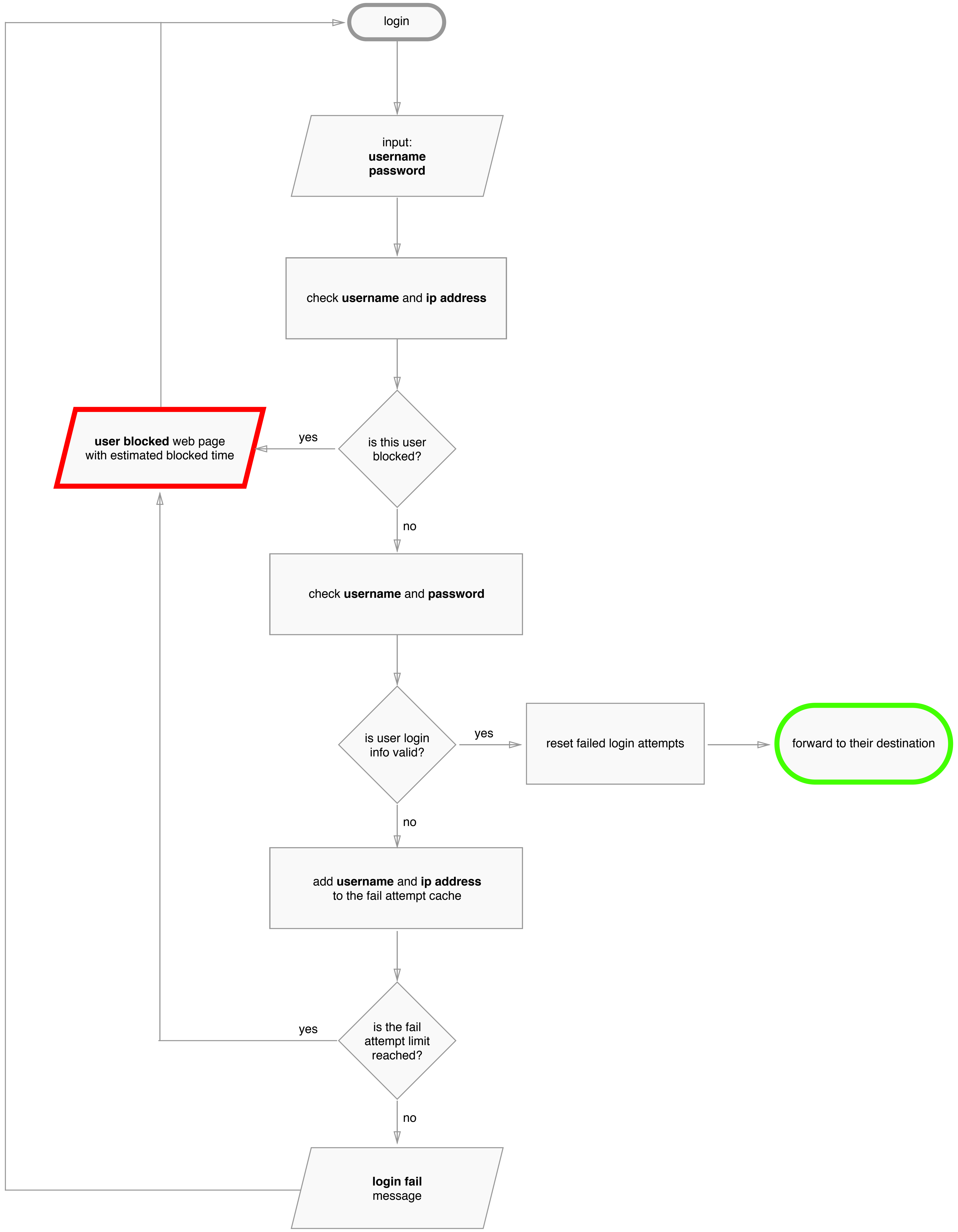
Stéphanie C.Lefebvre

Nick Pietrantonio

- Should we send an email to the user when their account has been locked? The email could give more information about the lockout, how to contact helpdesk or how to recover the account. It could also inform users of others trying to get into their account.
- After a certain number of incorrect attempts, just before the lockout, could the error message contain links to recover password? I'm not sure if there is a potential security risk with that. We can just let them wait a short amount of time (10mins seems reasonable).
- Do we want to give users the option of password recovery while their account is locked? We may get a flood of help desk requests asking to be unlocked.
- If the site customisation does not have a help desk link (others using generic account) what steps do users take to unlock their account?

Amable Rodríguez

Krista Lecuyer



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

user blocked web page
with estimated blocked time

no

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

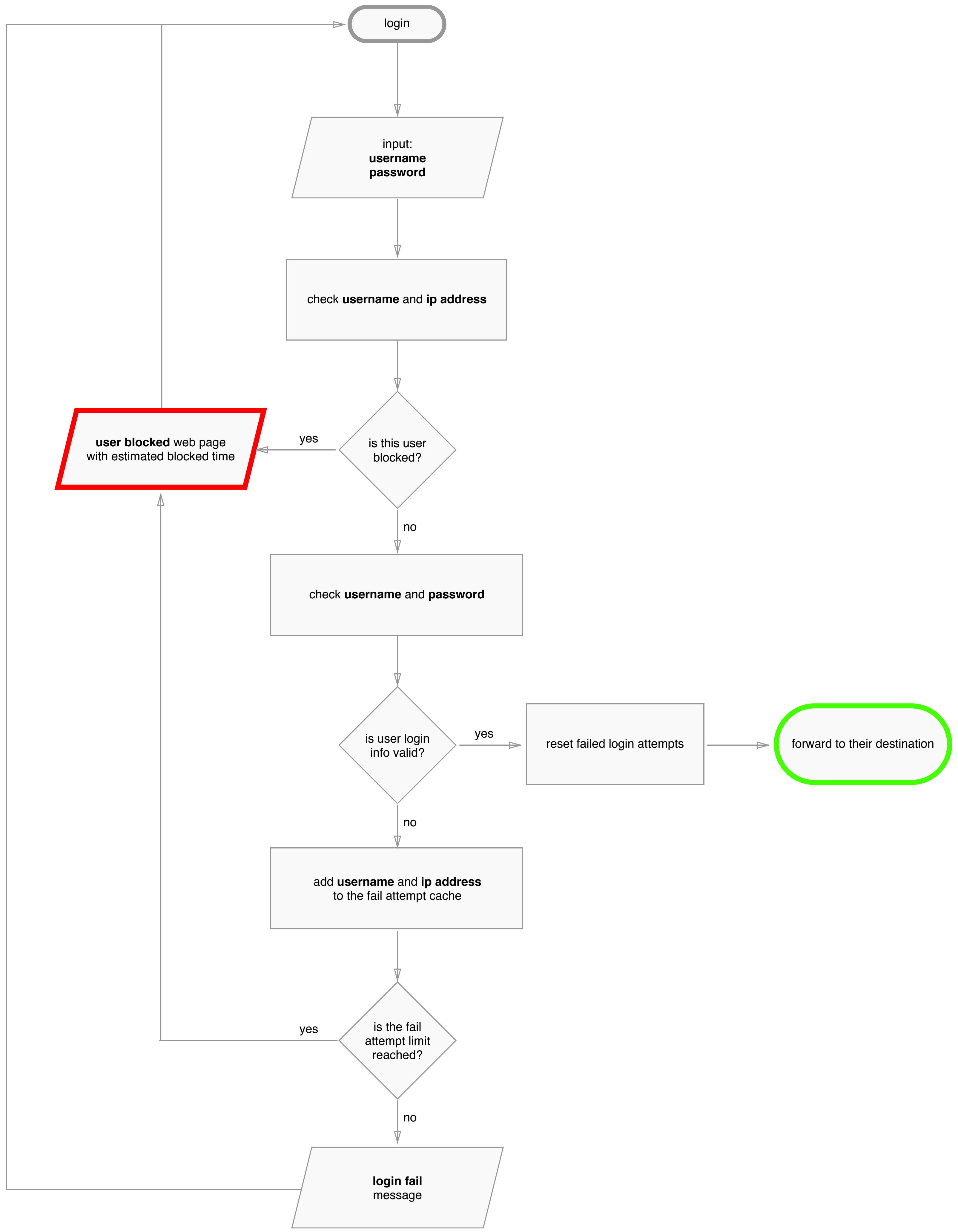
add **username** and **ip address**
to the fail attempt cache

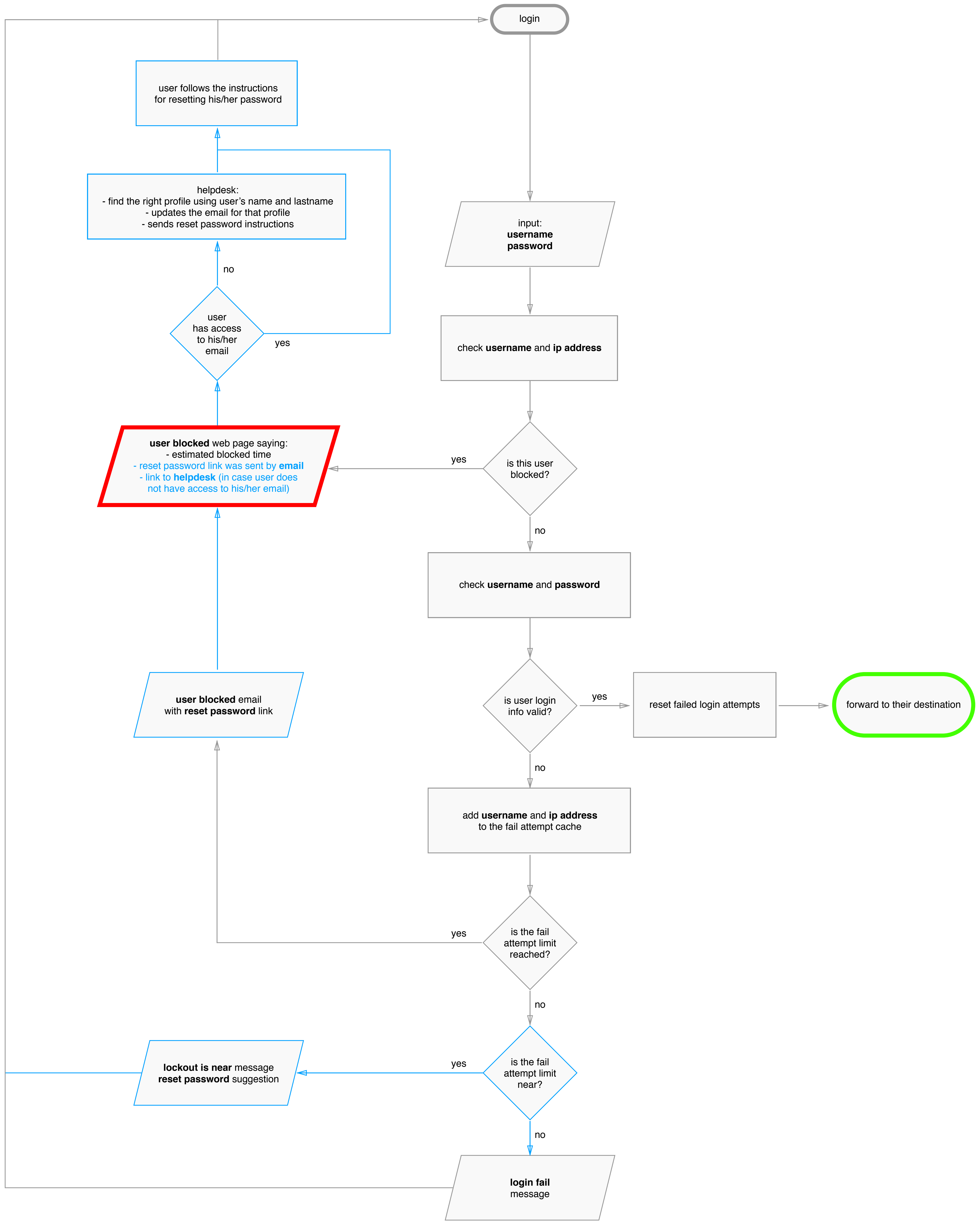
is the fail attempt limit reached?

yes

no

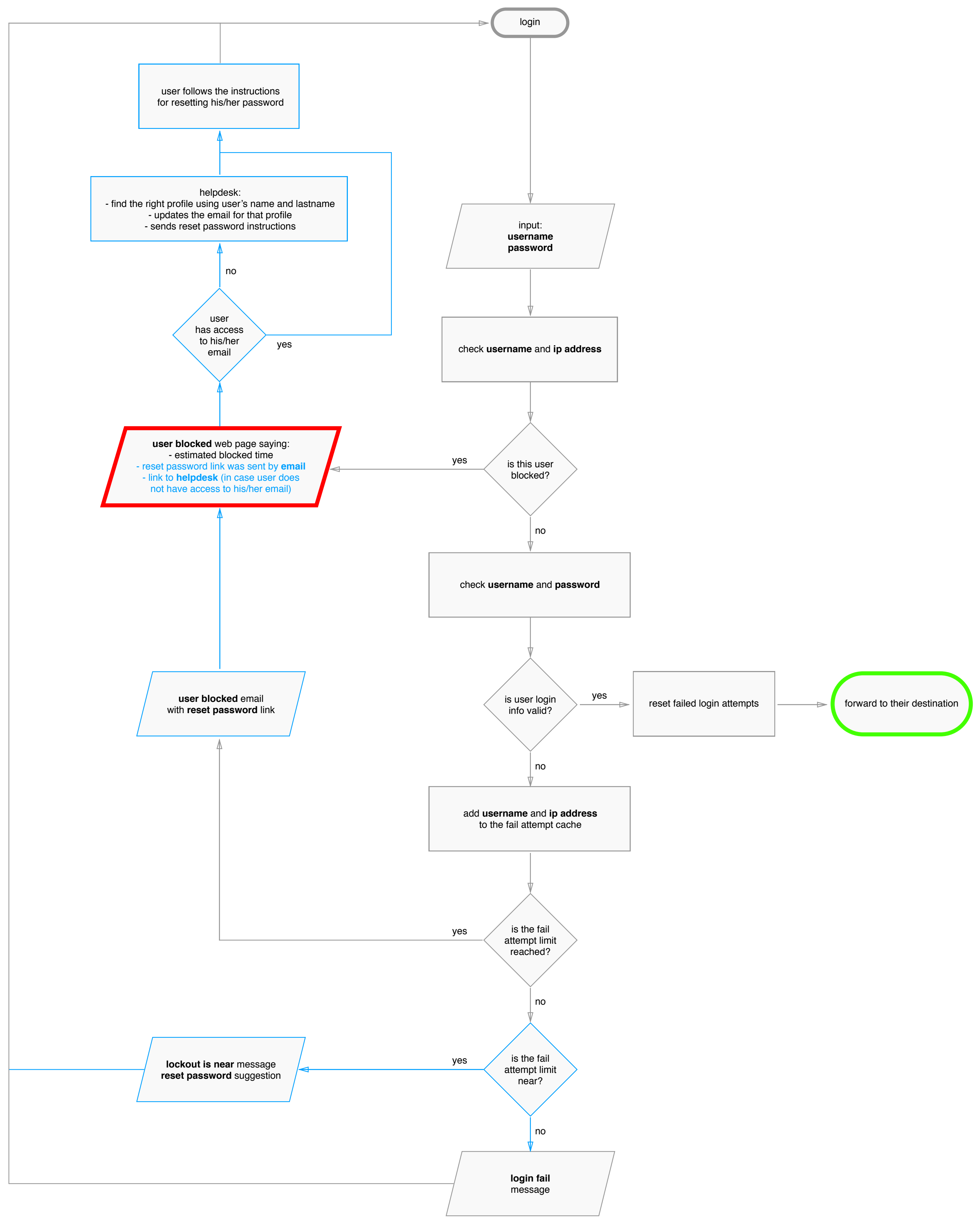
login fail
message


login
input:
username
password
check username and ip address
is this user blocked?
yes
user blocked web page with estimated blocked time
no
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
no
login fail message


login
input:
username
password
check username and ip address
is this user blocked?
yes
no
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
no
is the fail attempt limit near?
yes
no
login fail message
lockout is near message
reset password suggestion
user blocked email with reset password link
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions for resetting his/her password

Iteration #1

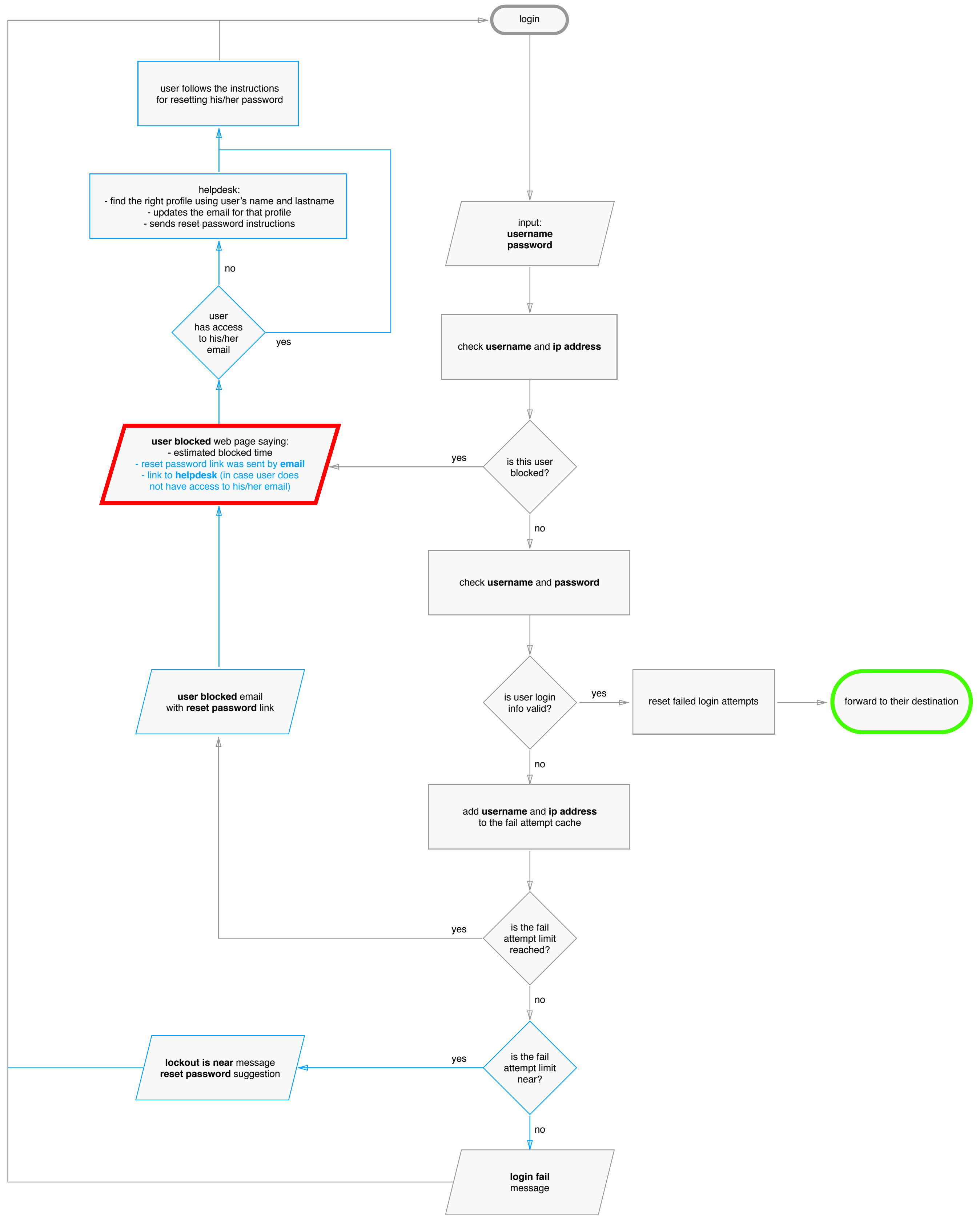
- “lockout is near” warning
- password reset link by email
- link to helpdesk



login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input:
username
password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message
reset password suggestion
yes
is the fail attempt limit near?
no
login fail message

Iteration #1

- “lockout is near” warning
- password reset link by email
- link to helpdesk



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

user has access to his/her email

no

yes

helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions

user follows the instructions for resetting his/her password

no

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

user blocked email with **reset password** link

no

is the fail attempt limit near?

yes

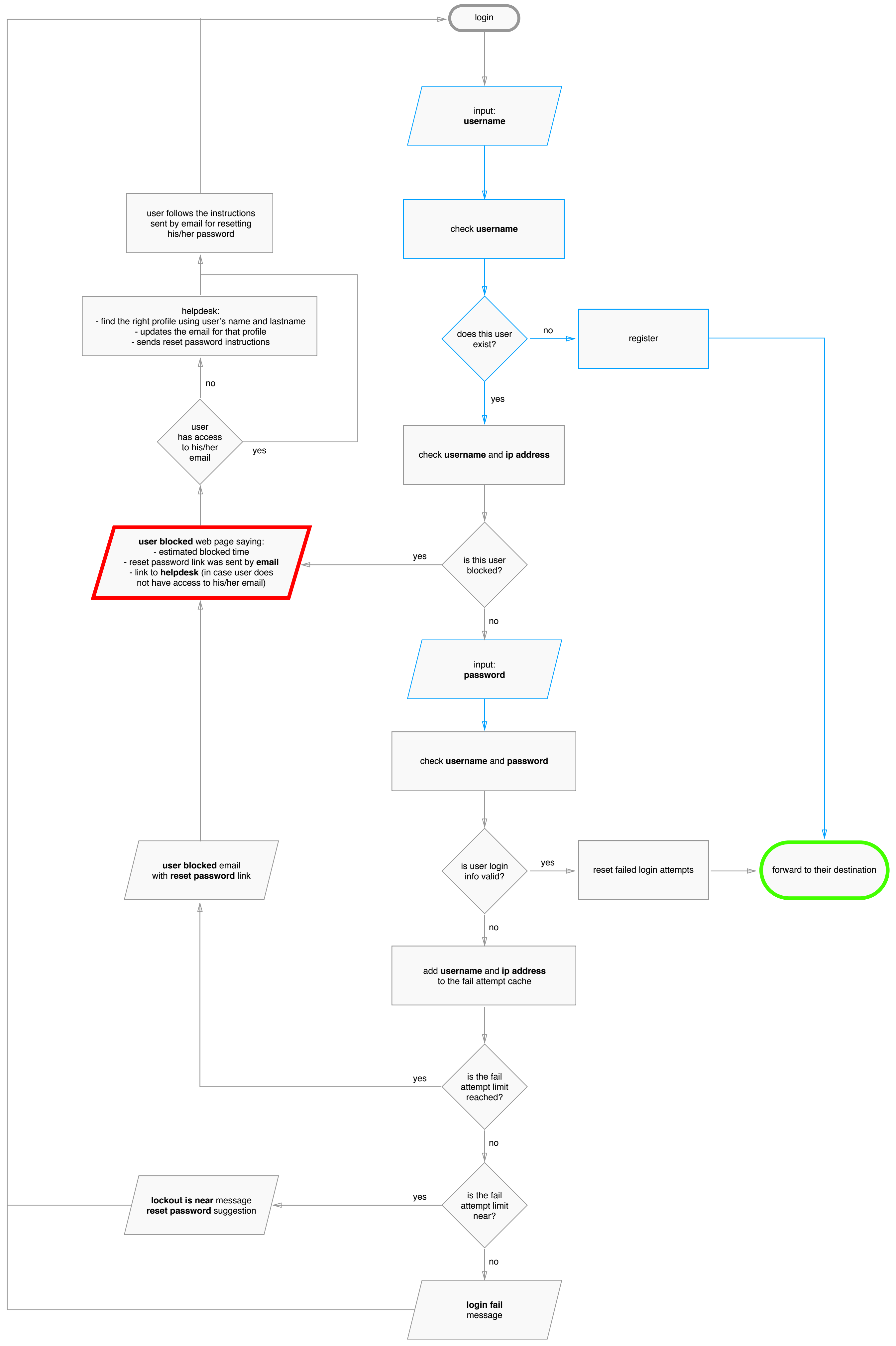
lockout is near message **reset password** suggestion

no

login fail message

Iteration #2

- username and password separation
- inexisting account easy detection
- register added as natural part of the flow



login

input:
username

check **username**

does this user exist?

no

register

yes

check **username** and **ip address**

is this user blocked?

yes

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

user has access to his/her email

no

yes

helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions

user follows the instructions sent by email for resetting his/her password

no

input:
password

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

user blocked email with **reset password** link

no

is the fail attempt limit near?

yes

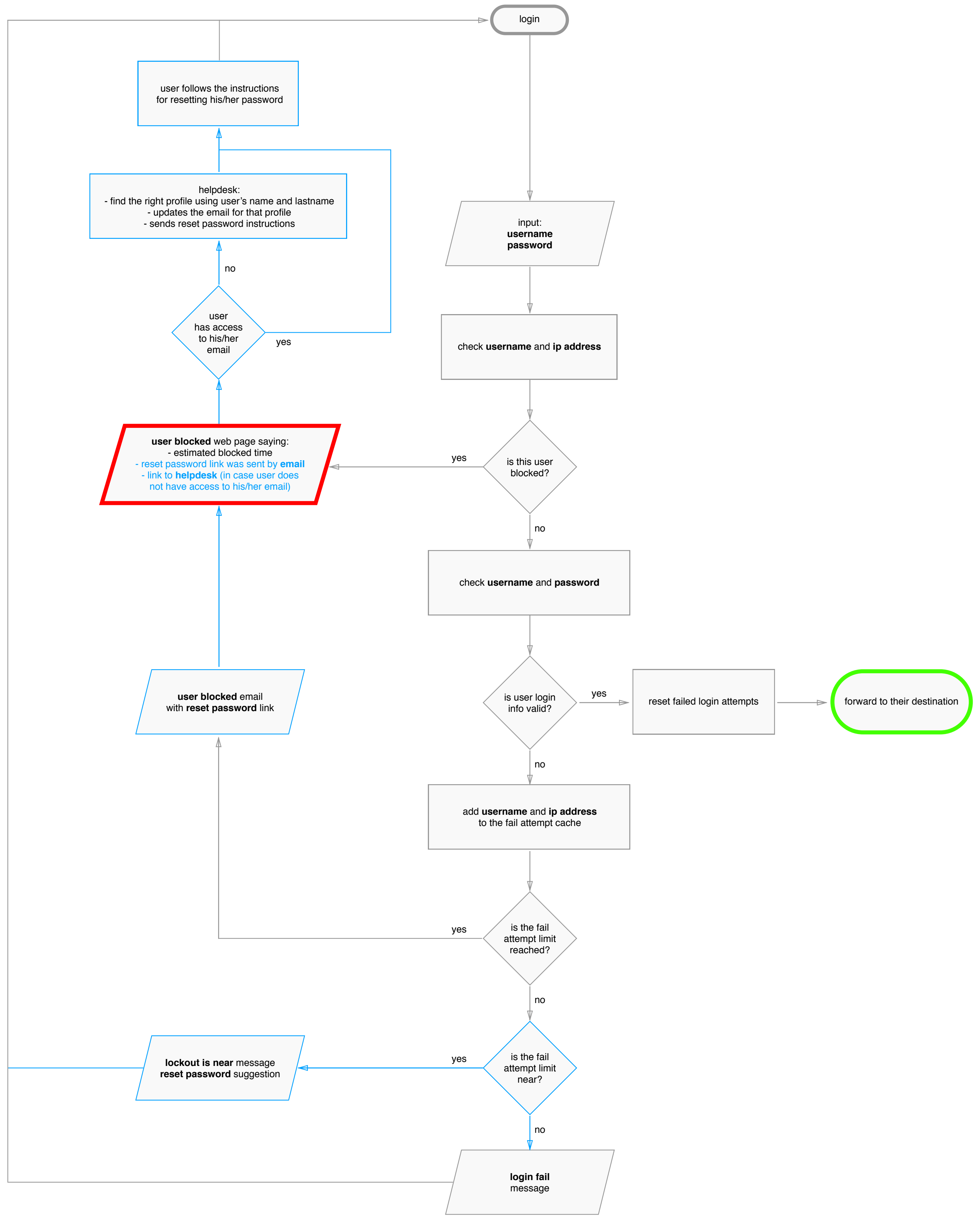
lockout is near message **reset password** suggestion

no

login fail message

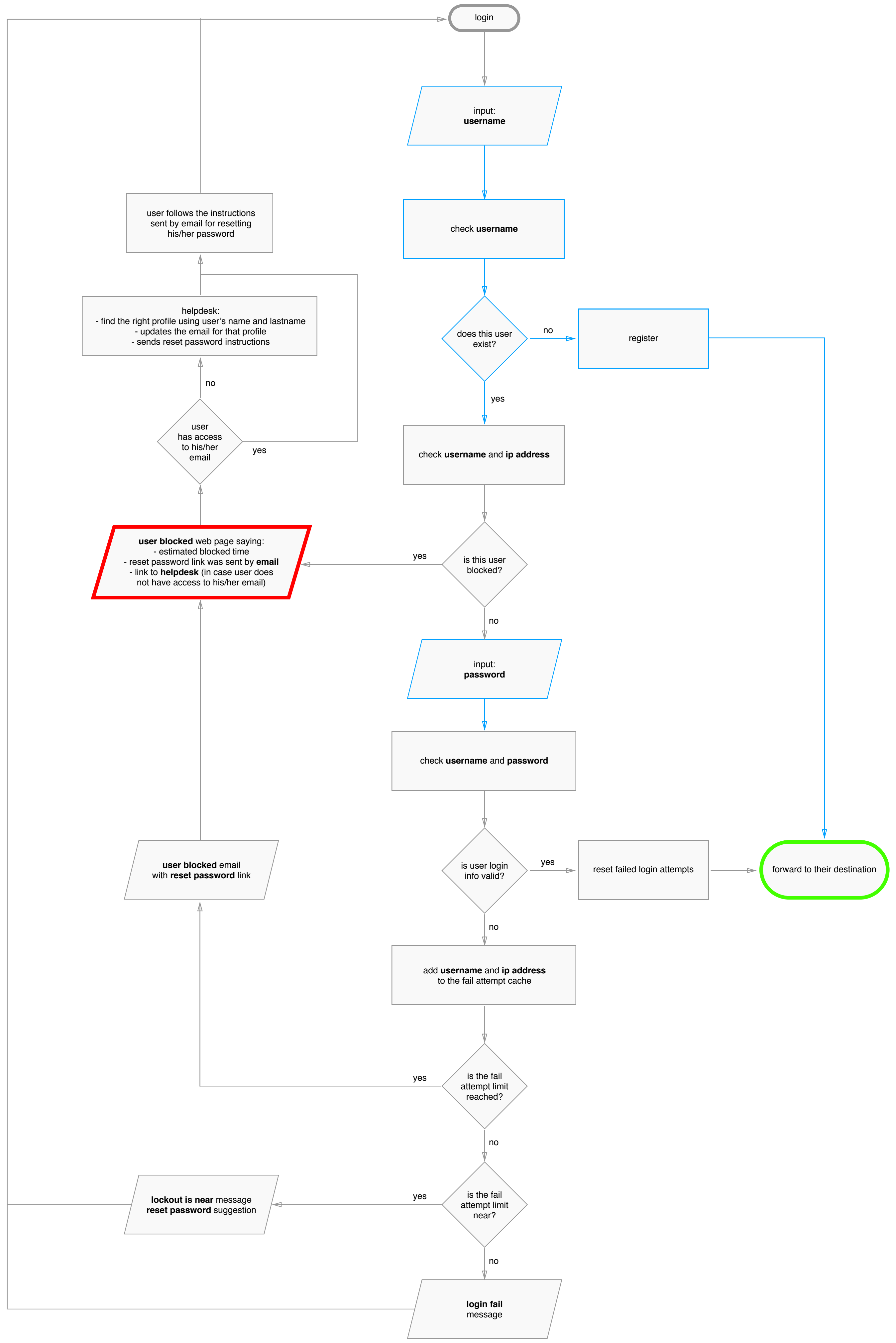
Iteration #1

- “lockout is near” warning
- password reset link by email
- link to helpdesk


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input: **username** **password**
check **username** and **ip address**
user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)
yes
is this user blocked?
no
check **username** and **password**
user blocked email with **reset password** link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add **username** and **ip address** to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message **reset password** suggestion
yes
is the fail attempt limit near?
no
login fail message

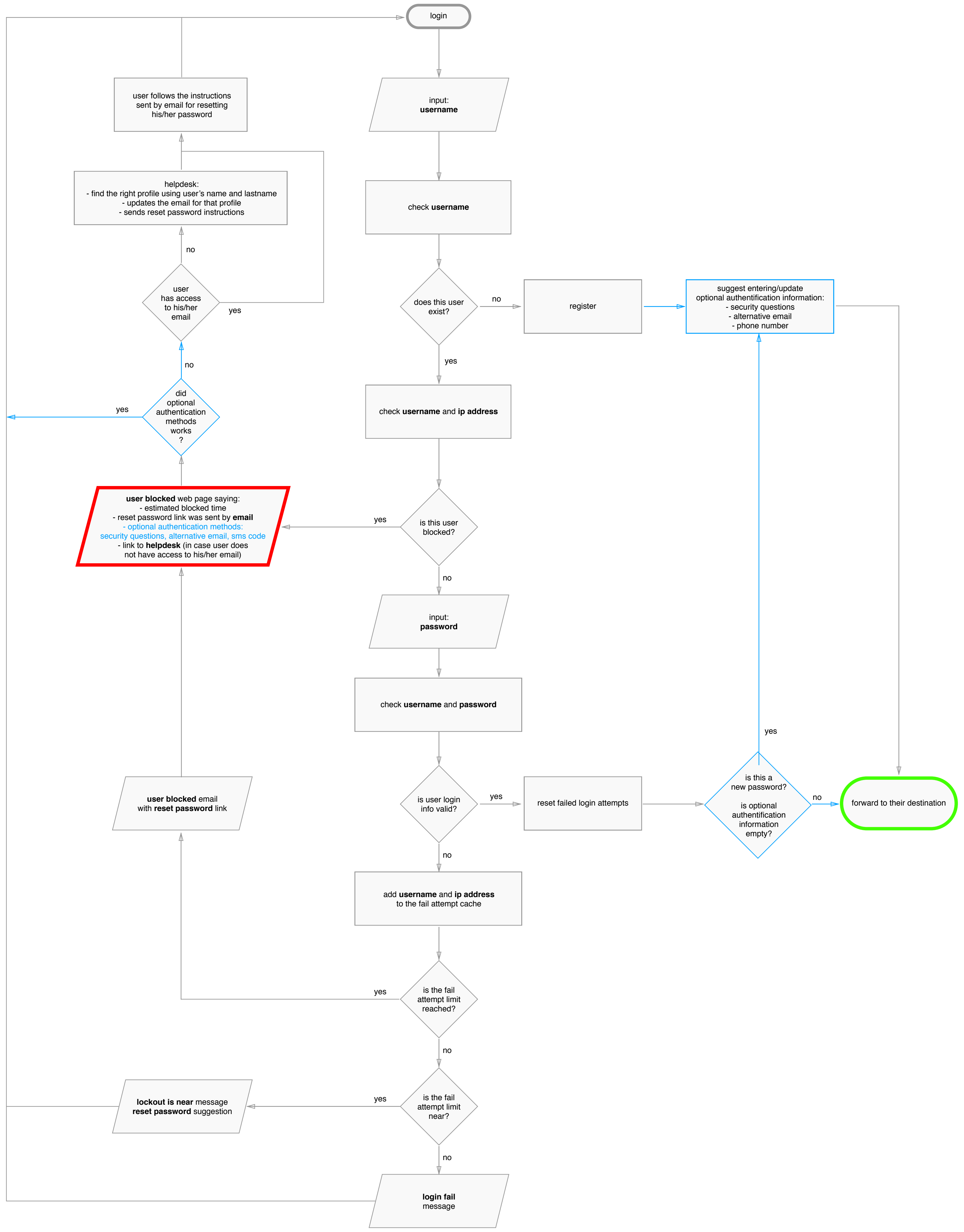
Iteration #2

- username and password separation
- inexisting account easy detection
- register added as natural part of the flow


login
input: **username**
user follows the instructions sent by email for resetting his/her password
check **username**
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
does this user exist?
no
register
yes
no
user has access to his/her email
yes
check **username** and **ip address**
user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)
yes
is this user blocked?
no
input: **password**
check **username** and **password**
user blocked email with **reset password** link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add **username** and **ip address** to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message **reset password** suggestion
yes
is the fail attempt limit near?
no
login fail message

Iteration #3

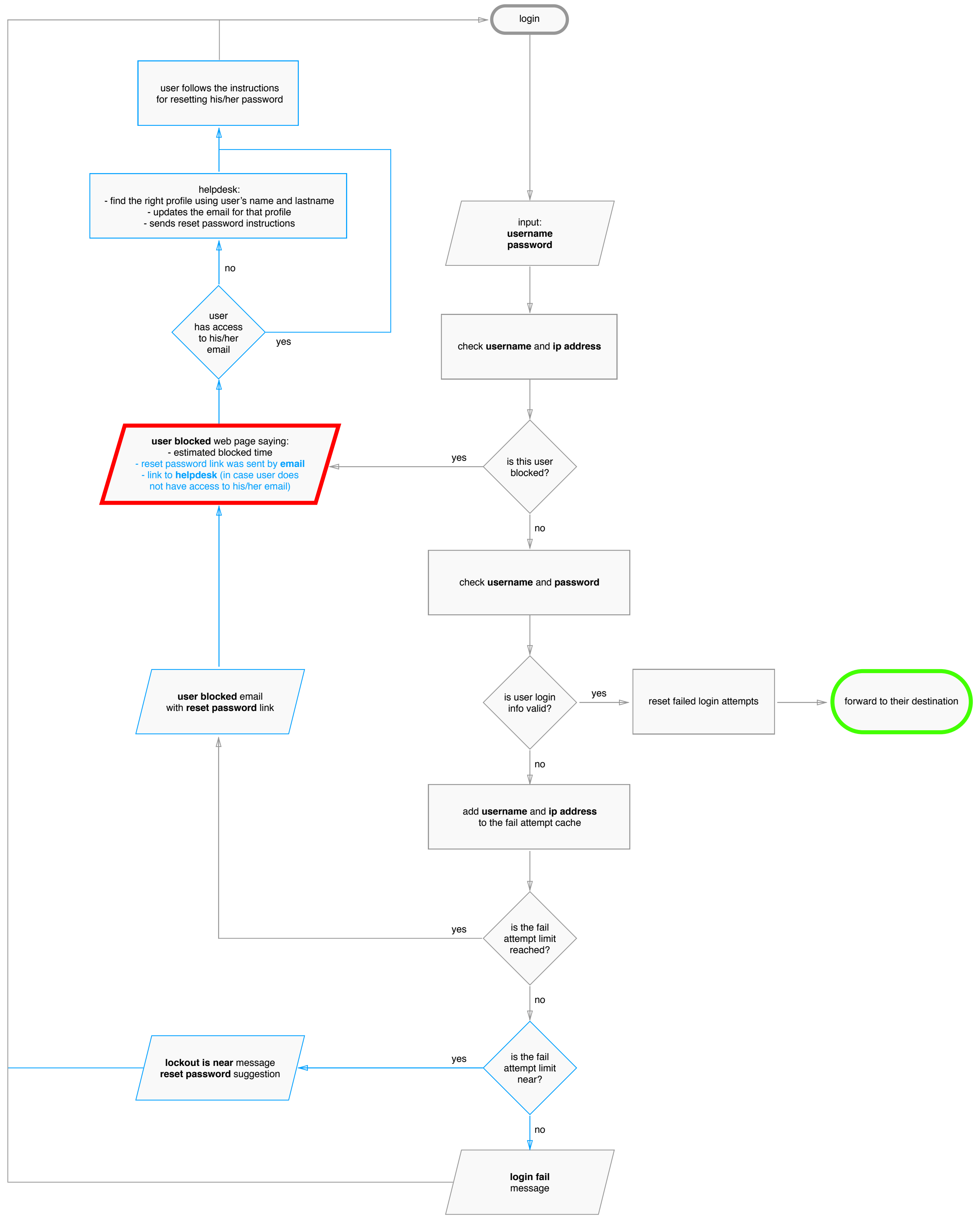
- added optional authentication information
- increase user power to unlock his/her account by himself/herself


login
user follows the instructions sent by email for resetting his/her password
input: **username**
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
check **username**
no
user has access to his/her email
yes
does this user exist?
no
register
suggest entering/update optional authentification information:
- security questions
- alternative email
- phone number
yes
no
yes
did optional authentication methods works ?
check **username** and **ip address**
user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- optional authentication methods: security questions, alternative email, sms code
- link to **helpdesk** (in case user does not have access to his/her email)
yes
is this user blocked?
no
input: **password**
check **username** and **password**
yes
user blocked email with **reset password** link
is user login info valid?
yes
reset failed login attempts
is this a new password? is optional authentification information empty?
no
forward to their destination
no
add **username** and **ip address** to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message **reset password** suggestion
yes
is the fail attempt limit near?
no
login fail message

Iteration #1

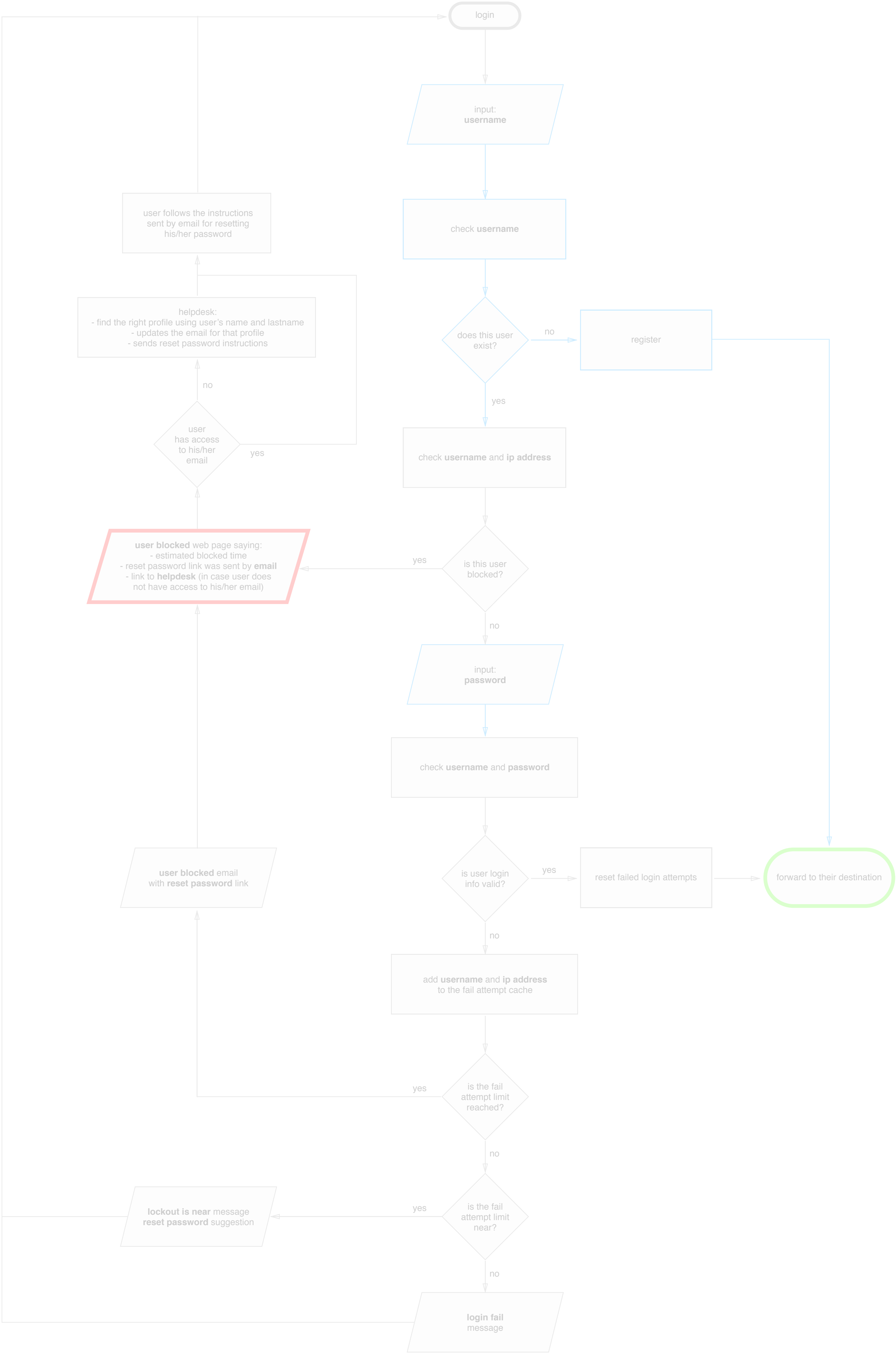
- “lockout is near” warning
- password reset link by email
- link to helpdesk

Bryan Robitaille


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input: username password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message reset password suggestion
yes
is the fail attempt limit near?
no
login fail message

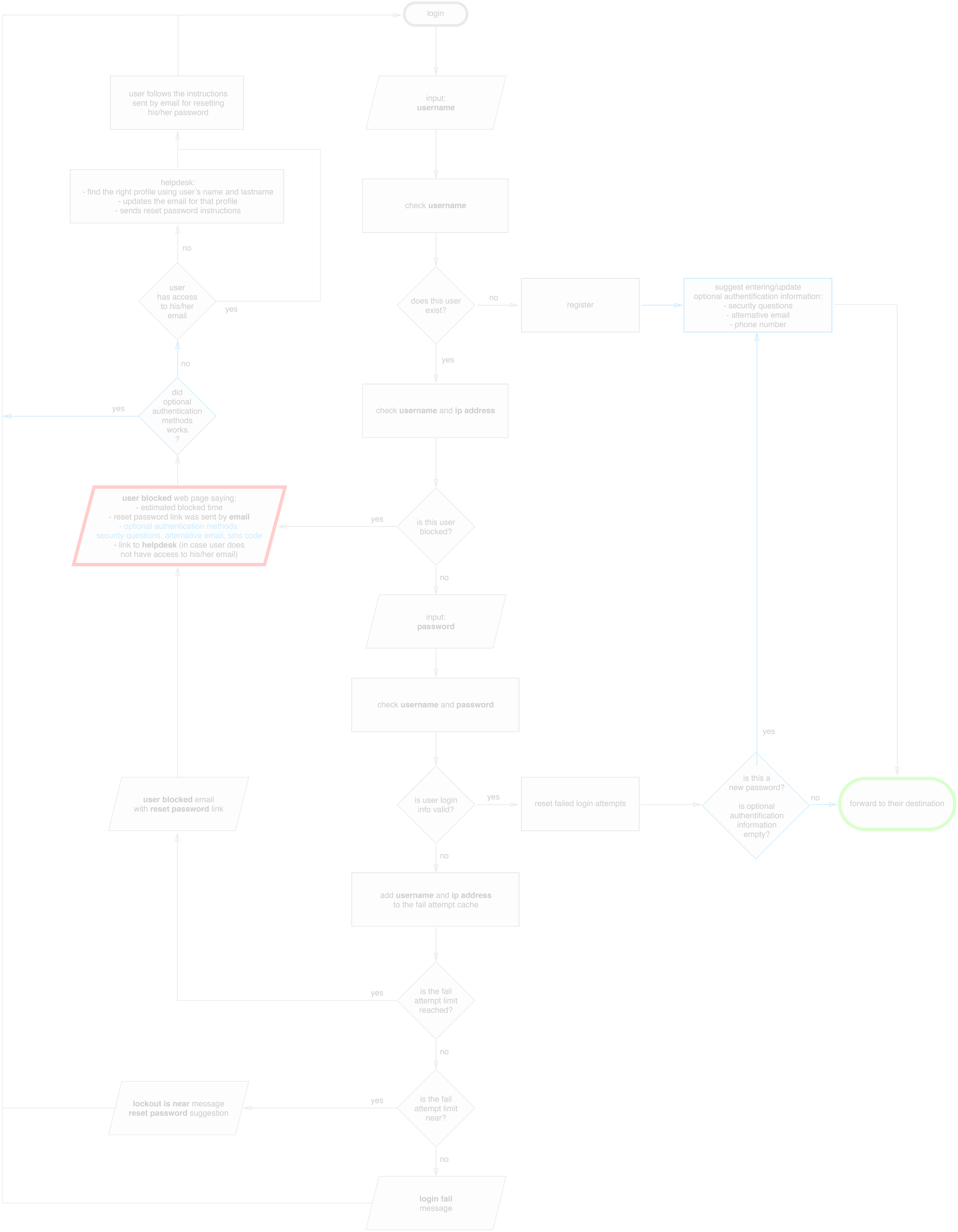
Iteration #2

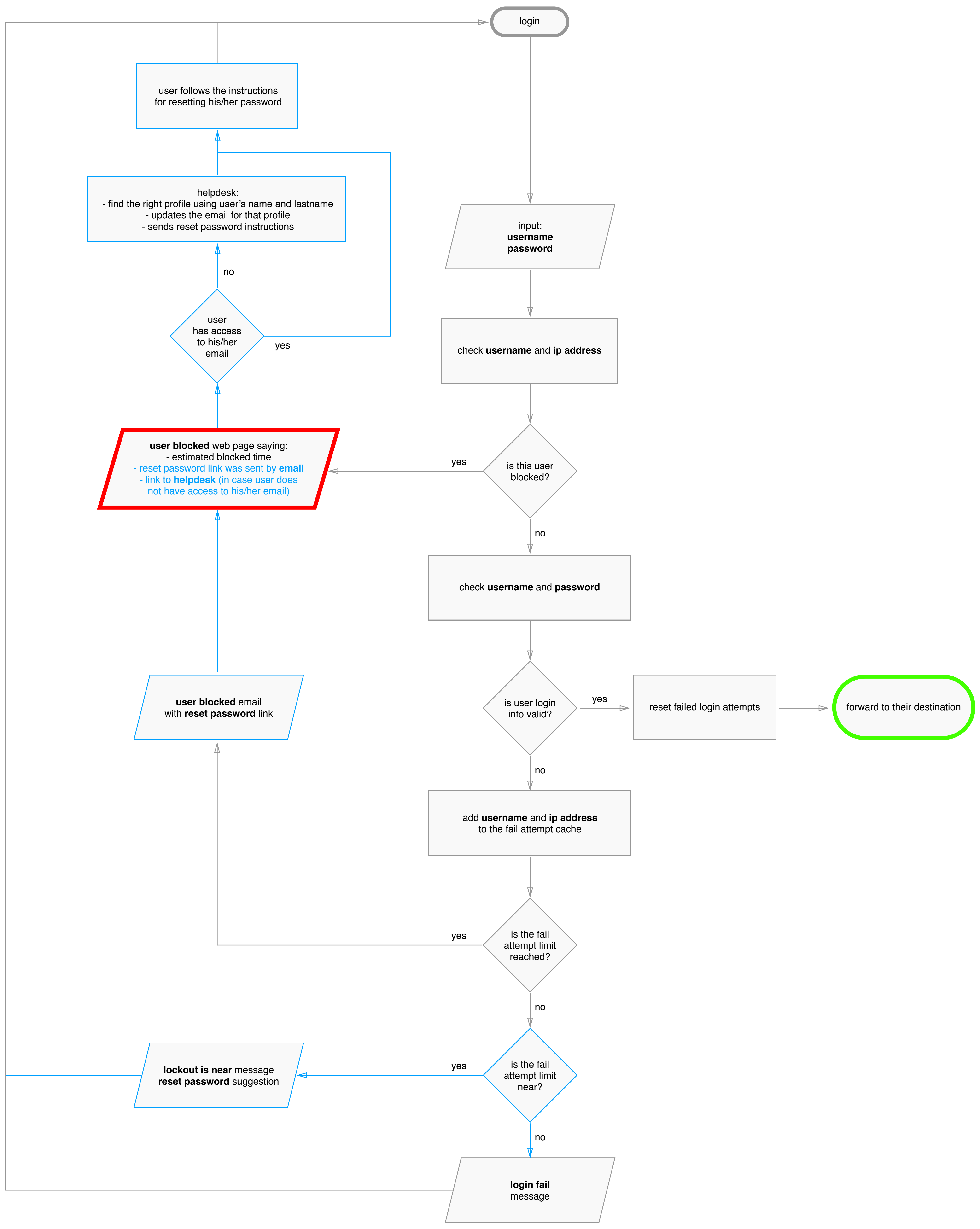
- username and password separation
- inexisting account easy detection
- register added as natural part of the flow

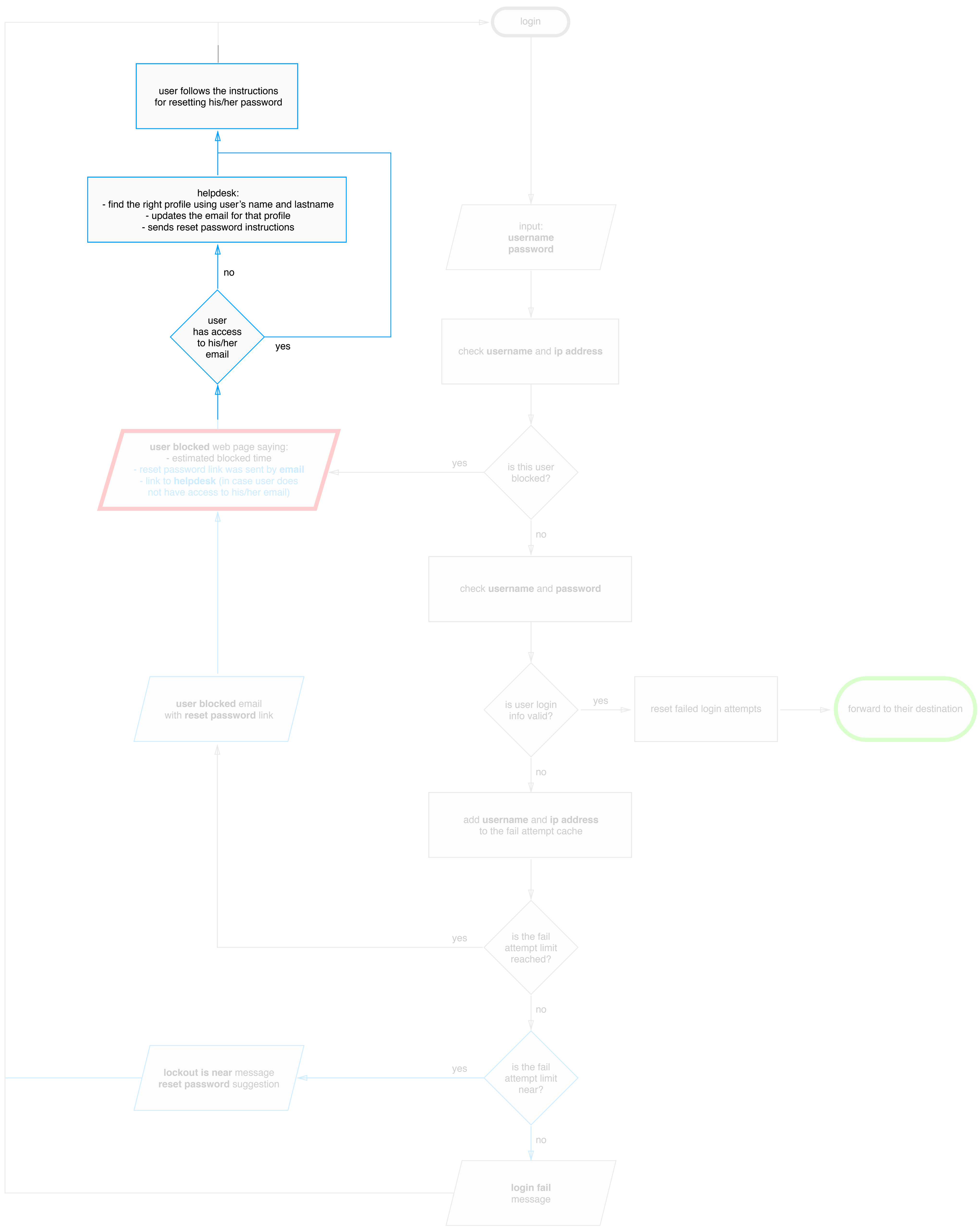

login
input: username
check username
user follows the instructions sent by email for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
does this user exist?
no
register
yes
user has access to his/her email
yes
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
input: password
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message reset password suggestion
yes
is the fail attempt limit near?
no
login fail message

Iteration #3

- added optional authentication information
- increase user power to unlock his/her account by himself/herself


login
user follows the instructions sent by email for resetting his/her password
input: username
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
check username
no
user has access to his/her email
yes
does this user exist?
no
register
suggest entering/update optional authentification information:
- security questions
- alternative email
- phone number
yes
no
yes
did optional authentication methods works ?
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- optional authentication methods: security questions, alternative email, sms code
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
input: password
check username and password
yes
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
is this a new password?
is optional authentification information empty?
no
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message reset password suggestion
yes
is the fail attempt limit near?
no
login fail message


login
input:
username
password
check username and ip address
is this user blocked?
yes
no
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
no
is the fail attempt limit near?
yes
no
login fail message
lockout is near message
reset password suggestion
user blocked email
with reset password link
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions for resetting his/her password



login

user follows the instructions
for resetting his/her password

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

no

user
has access
to his/her
email

yes

input:
username
password

check **username** and **ip address**

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does
not have access to his/her email)

yes

is this user
blocked?

no

check **username** and **password**

user blocked email
with **reset password** link

is user login
info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address**
to the fail attempt cache

yes

is the fail
attempt limit
reached?

no

lockout is near message
reset password suggestion

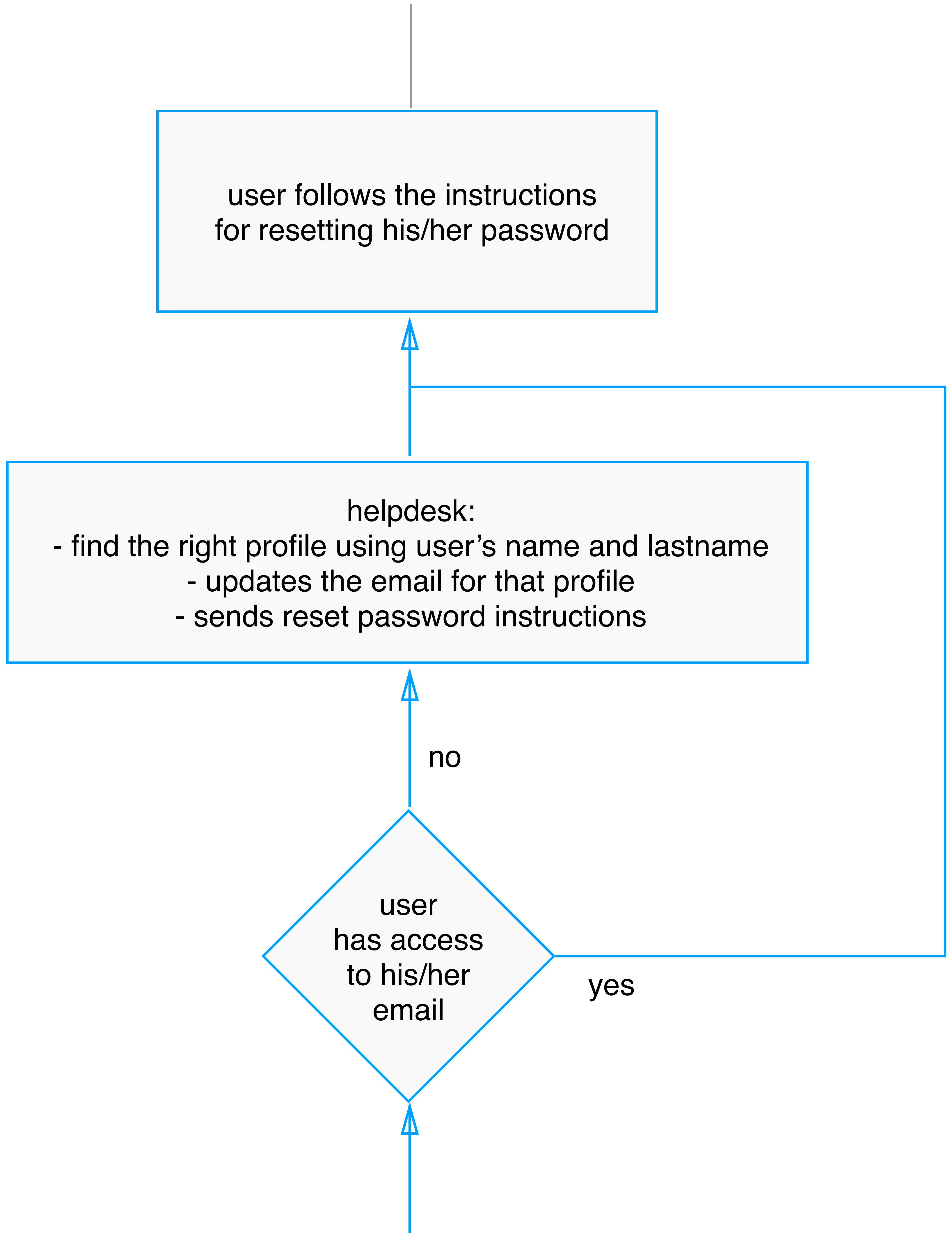
yes

is the fail
attempt limit
near?

no

login fail
message

Krista Lecuyer



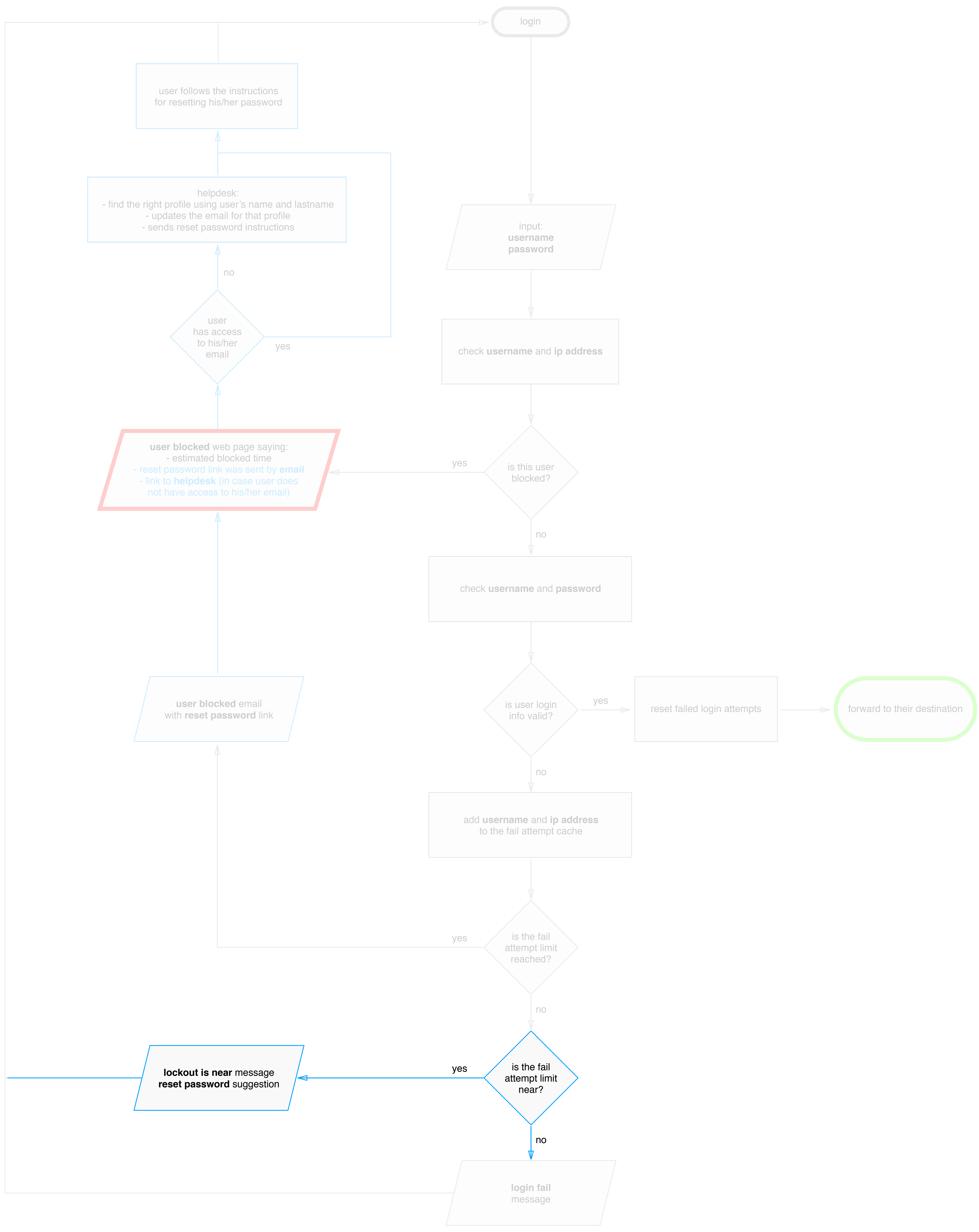
user follows the instructions
for resetting his/her password

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

no

user
has access
to his/her
email

yes



login

user follows the instructions for resetting his/her password

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

no

user has access to his/her email

yes

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

no

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

user blocked email with **reset password** link

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

no

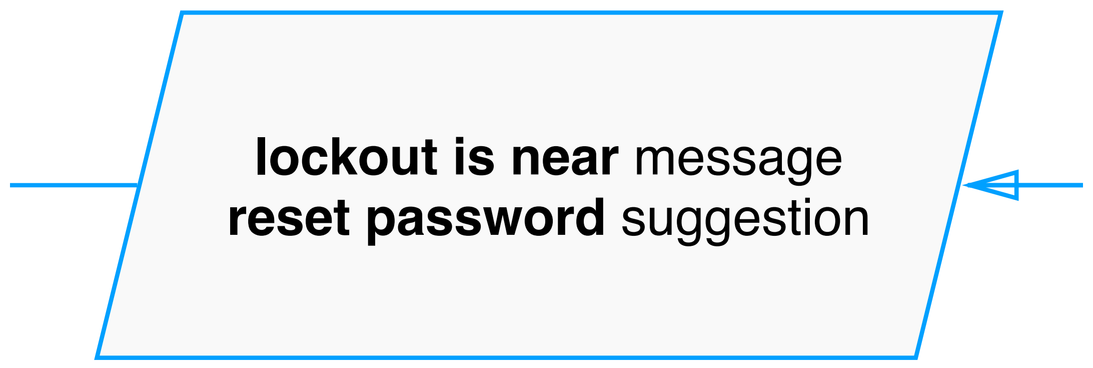
is the fail attempt limit near?

yes

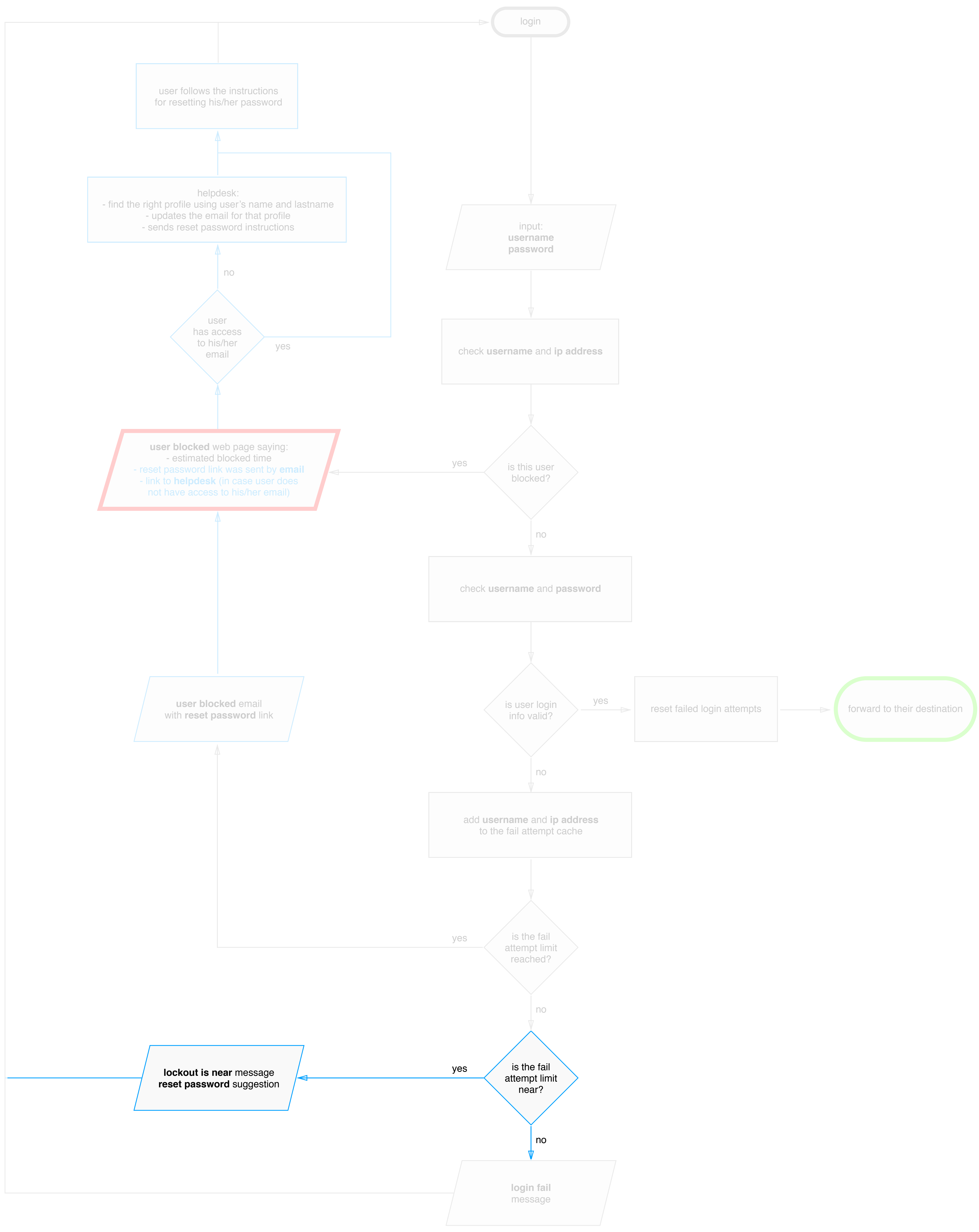
lockout is near message
reset password suggestion

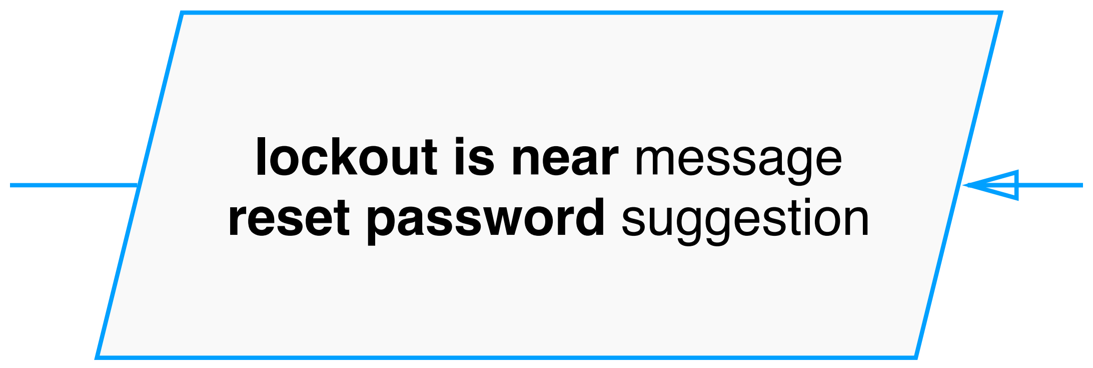
no

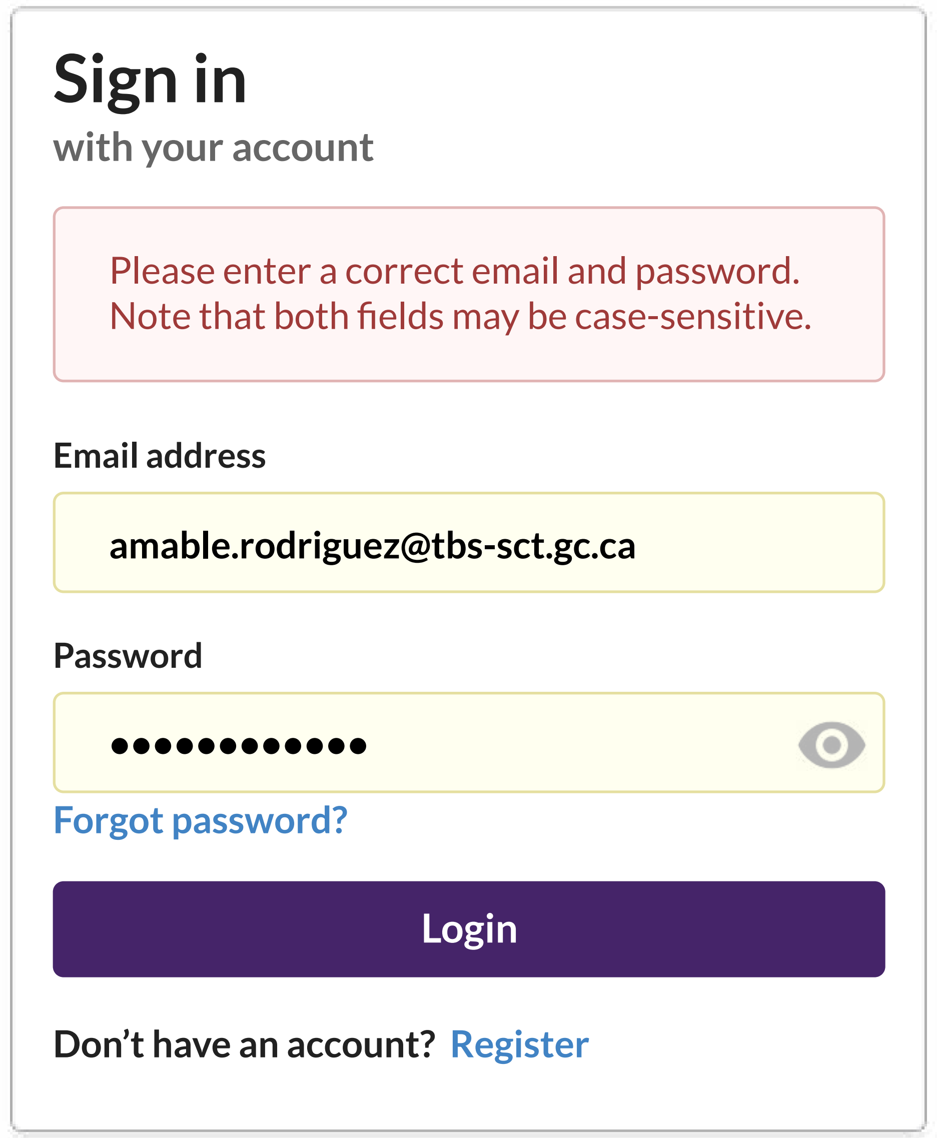
login fail message



lockout is near message
reset password suggestion


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input:
username
password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message
reset password suggestion
yes
is the fail attempt limit near?
no
login fail message





Sign in

with your account

Please enter a correct email and password.
Note that both fields may be case-sensitive.

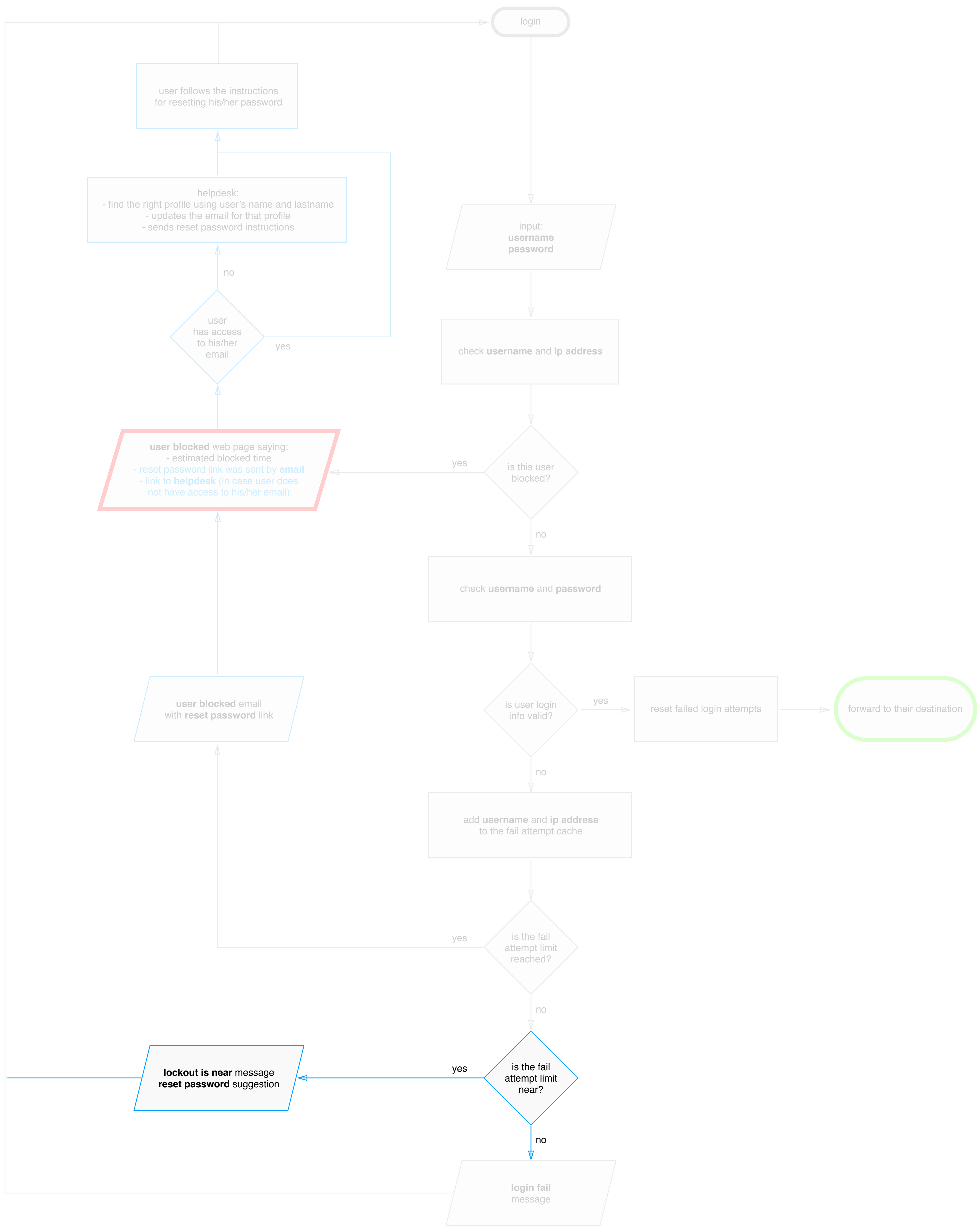
Email address

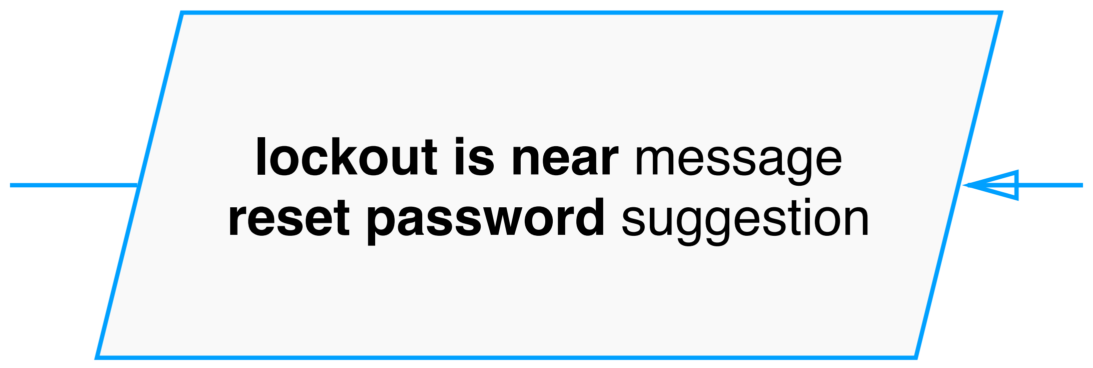
amable.rodriguez@tbs-sct.gc.ca

Password

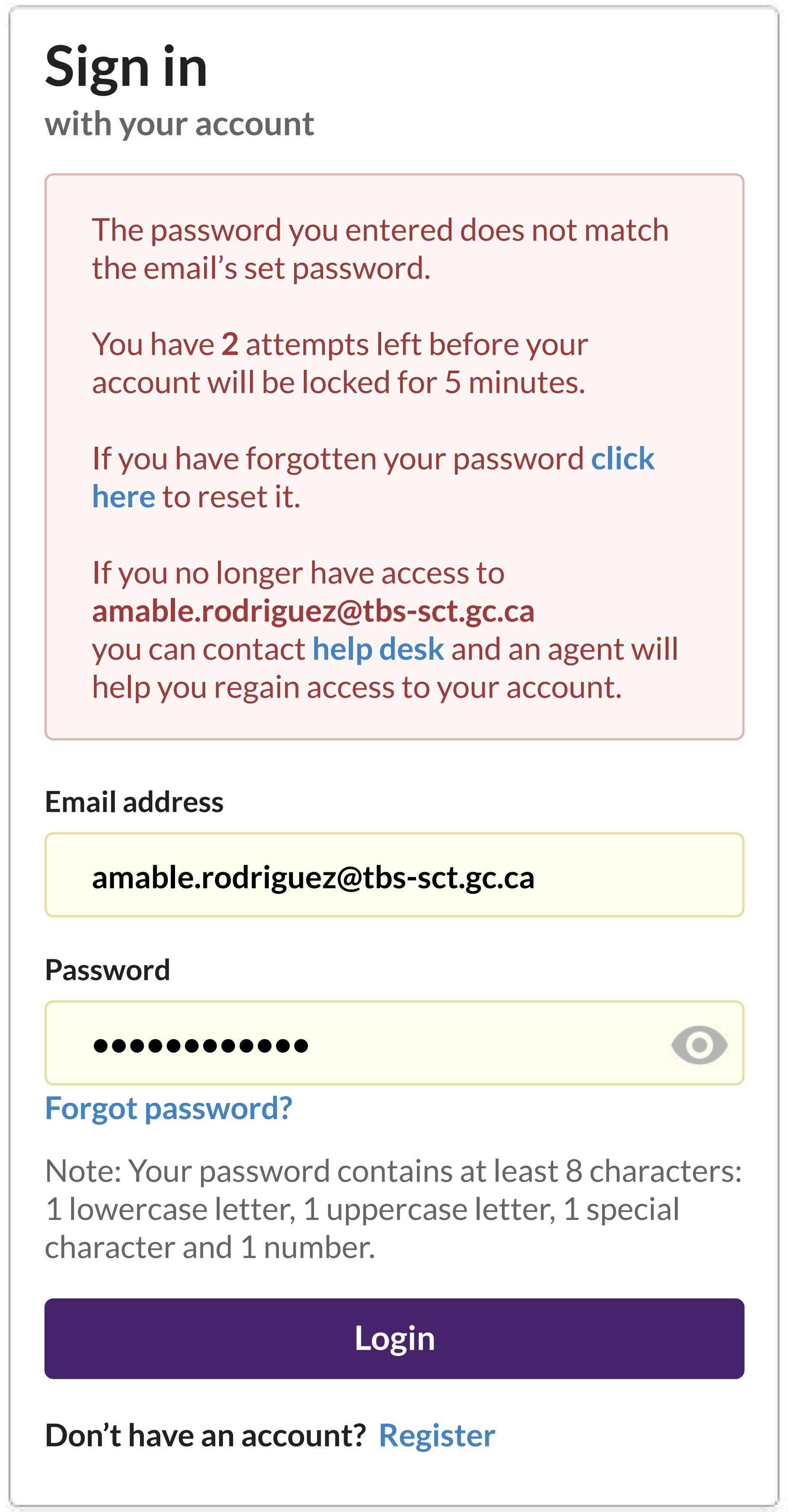
●●●●●●●●●●●●

Don’t have an account? Register


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input: username password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message reset password suggestion
yes
is the fail attempt limit near?
no
login fail message



lockout is near message
reset password suggestion



Sign in

with your account

The password you entered does not match the email’s set password.

You have **2** attempts left before your account will be locked for 5 minutes.

If you have forgotten your password **click here** to reset it.

If you no longer have access to **amable.rodriguez@tbs-sct.gc.ca** you can contact **help desk** and an agent will help you regain access to your account.

Email address

amable.rodriguez@tbs-sct.gc.ca

Password

●●●●●●●●●●●●

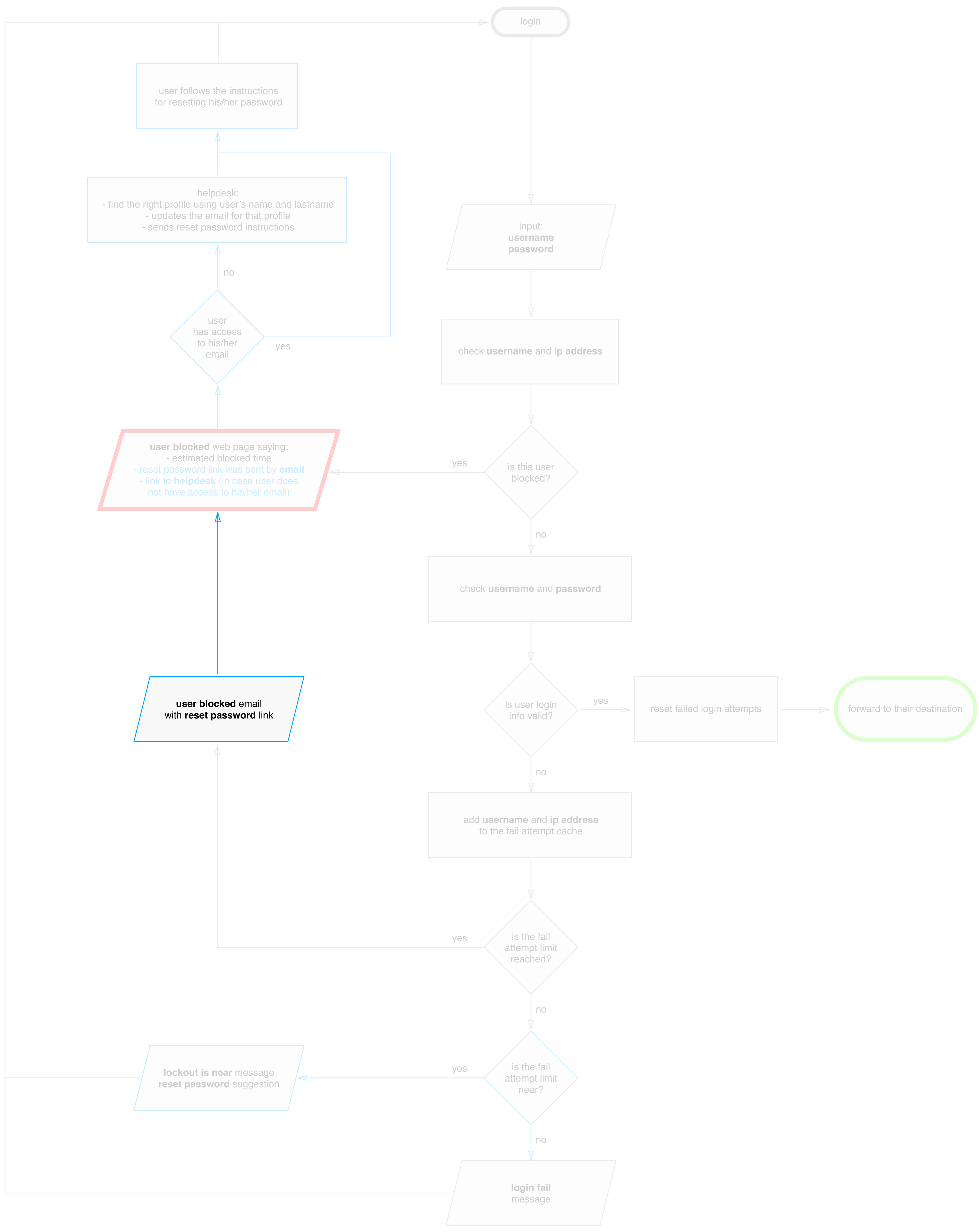
Forgot password?

Note: Your password contains at least 8 characters: 1 lowercase letter, 1 uppercase letter, 1 special character and 1 number.

Don’t have an account? Register

Marianne Aubrey

Donna Monbourquette



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

no

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

user has access to his/her email

yes

no

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

user follows the instructions for resetting his/her password

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

user blocked email with **reset password** link

no

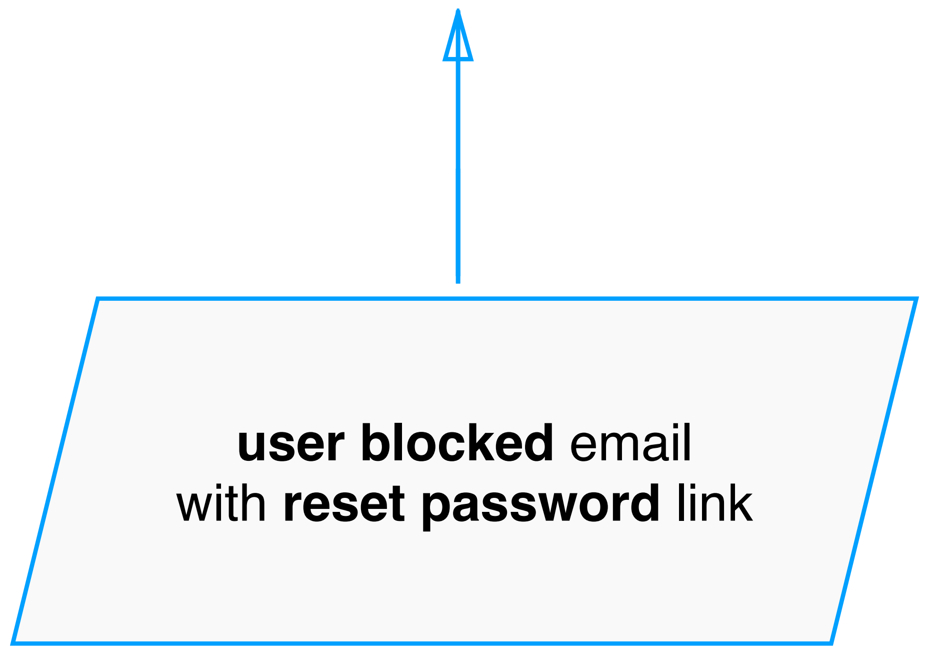
is the fail attempt limit near?

yes

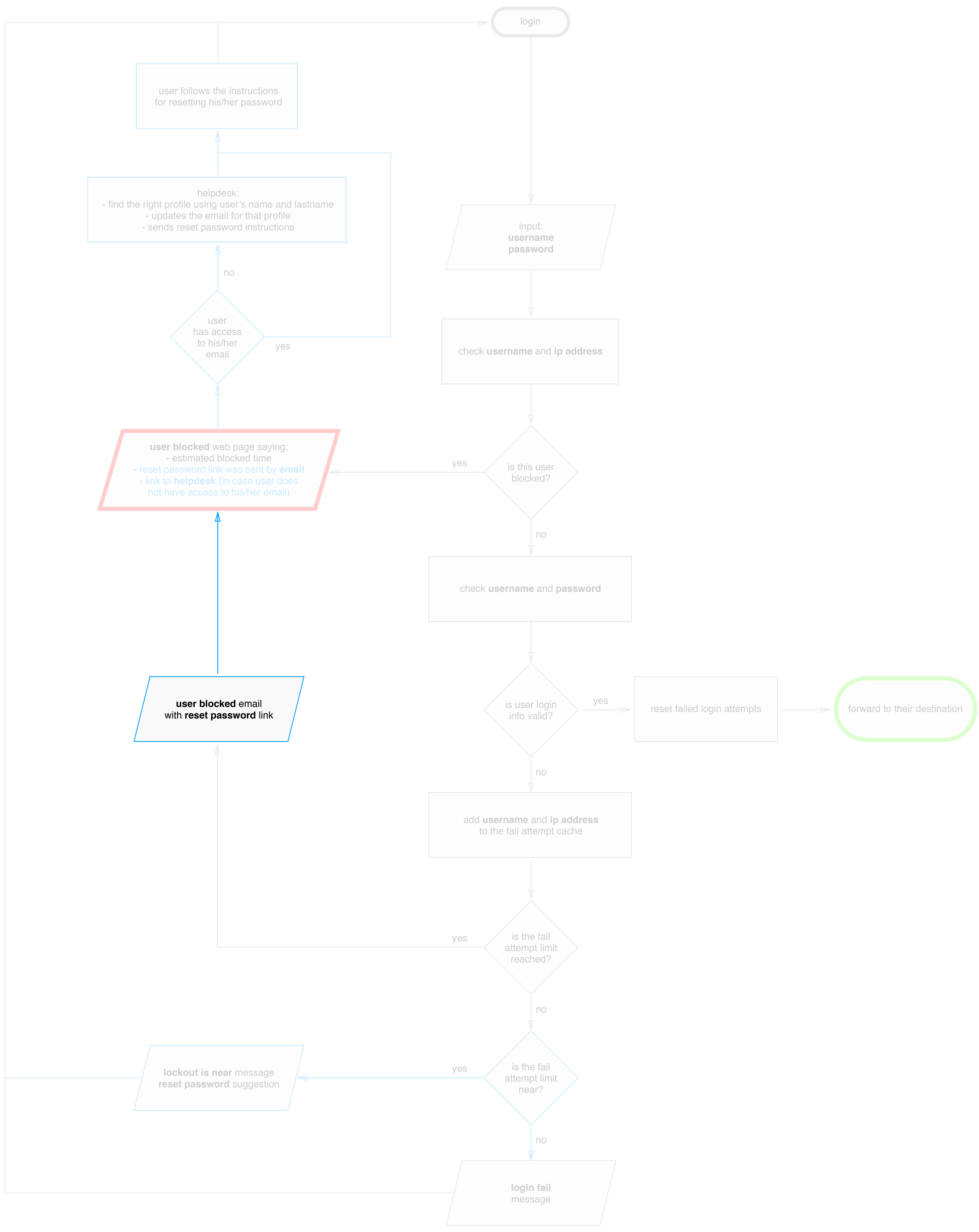
lockout is near message
reset password suggestion

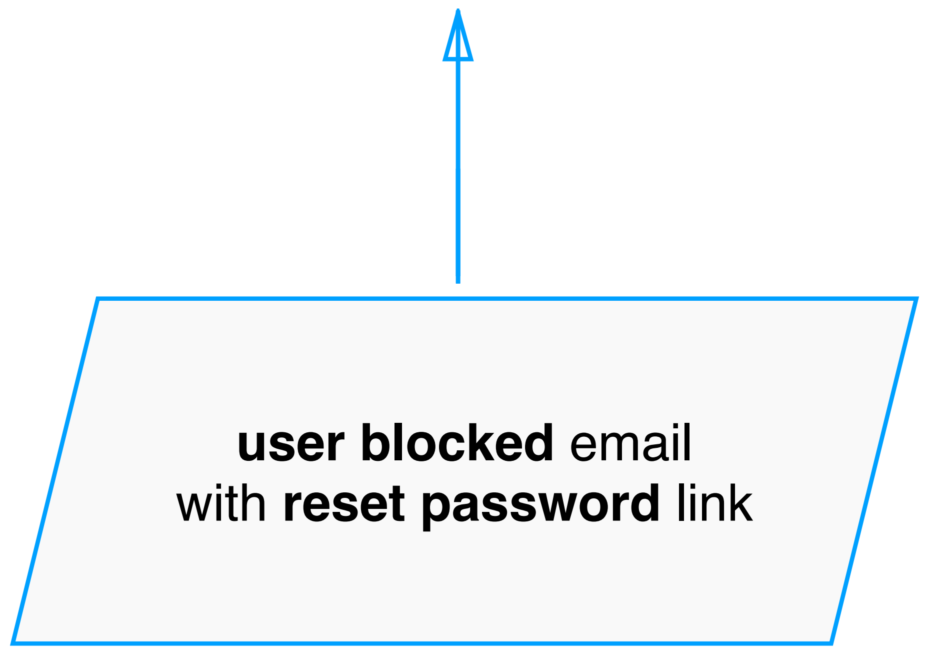
no

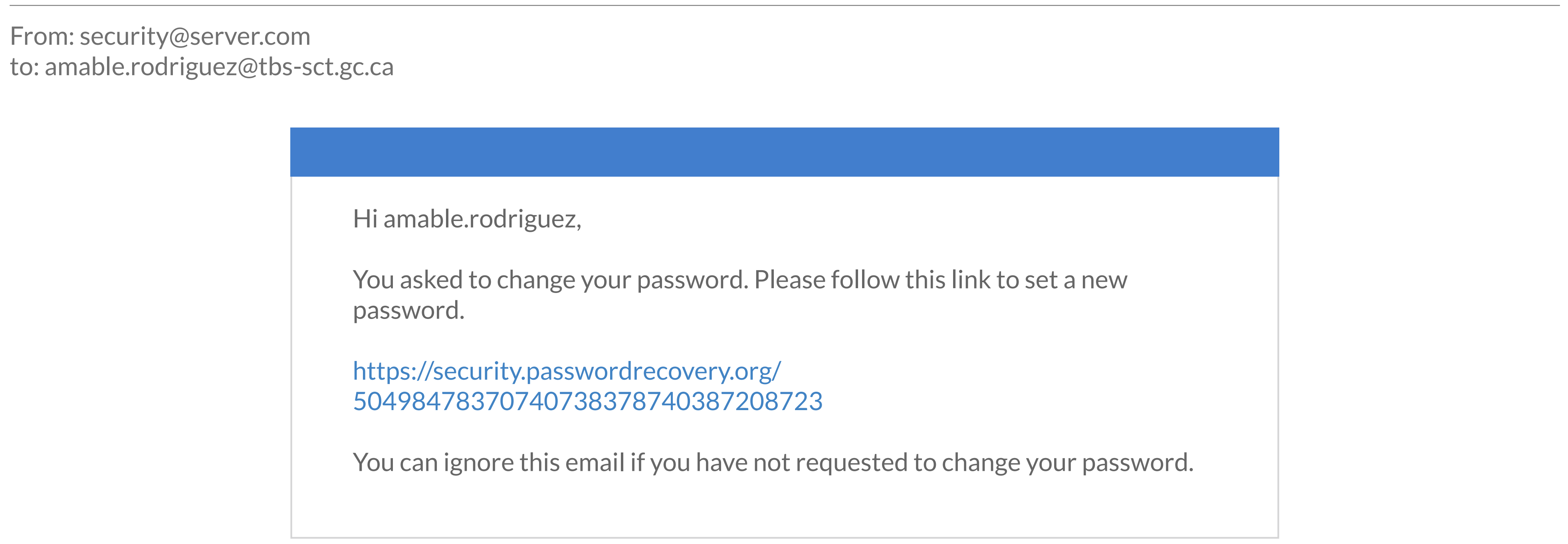
login fail message



user blocked email
with **reset password** link


login
input:
username
password
check username and ip address
is this user blocked?
yes
no
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions for resetting his/her password
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
user blocked email with reset password link
no
is the fail attempt limit near?
yes
lockout is near message
reset password suggestion
no
login fail message



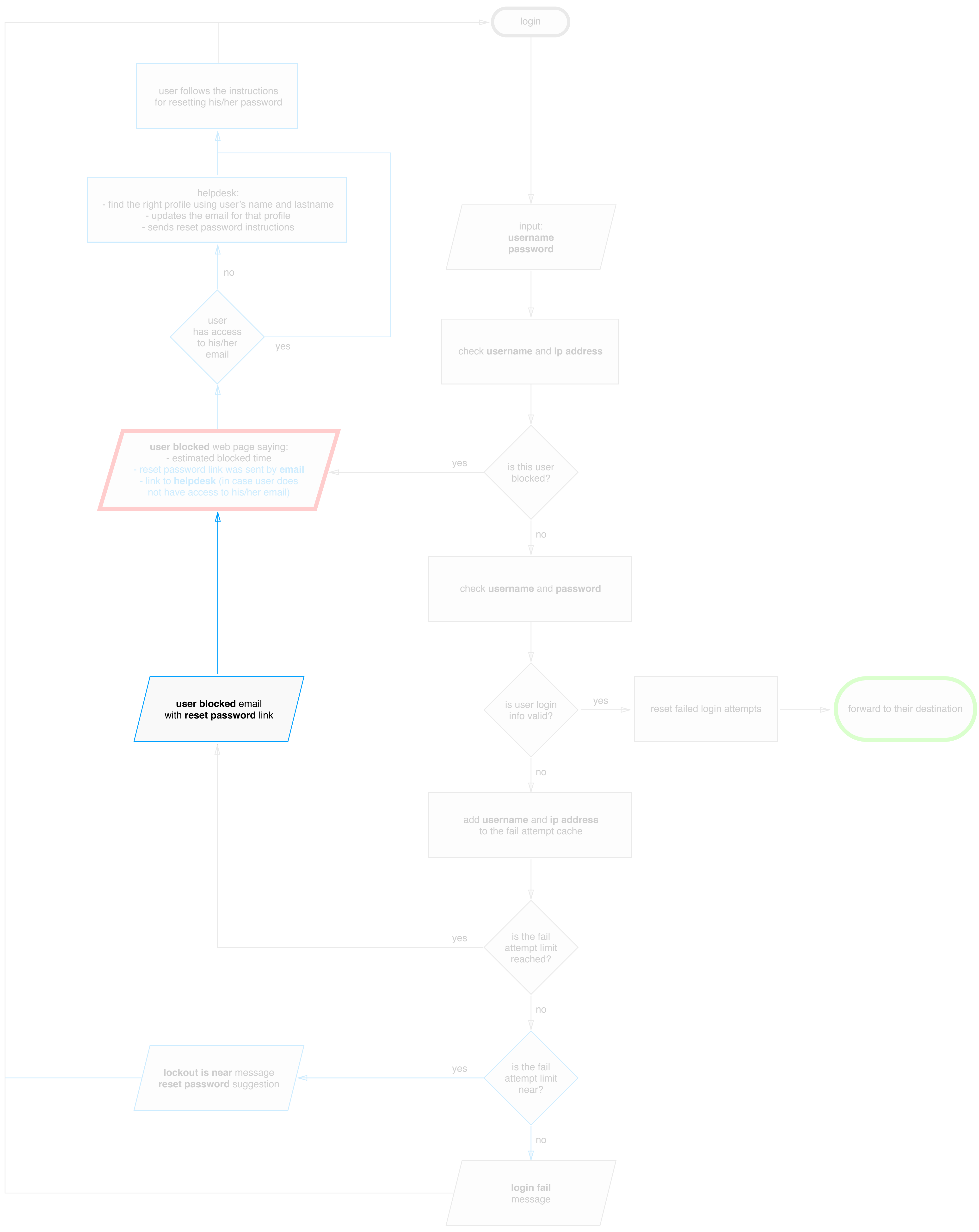

From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca

Hi amable.rodriguez,

You asked to change your password. Please follow this link to set a new password.

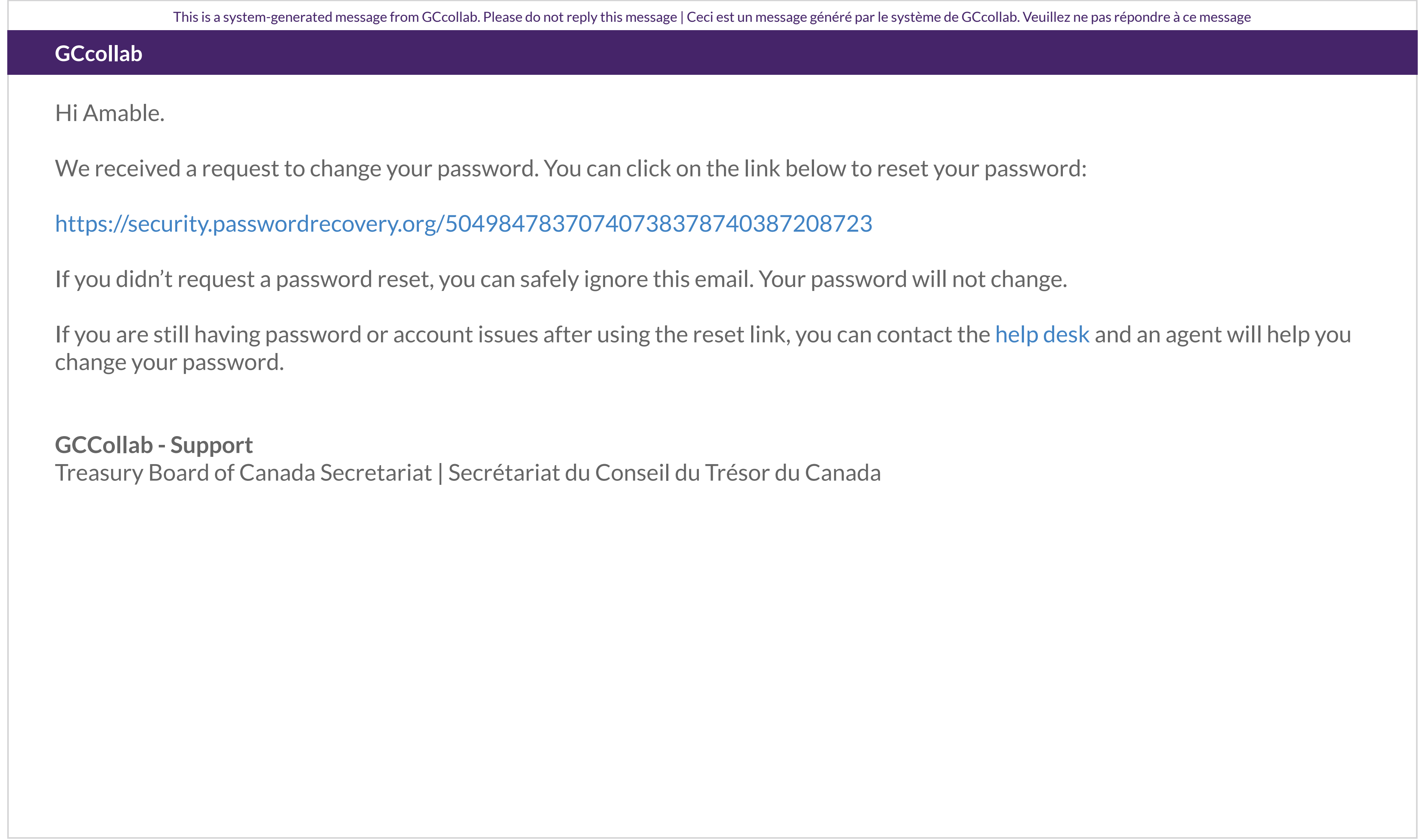
https://security.passwordrecovery.org/504984783707407383787403872O8723

You can ignore this email if you have not requested to change your password.


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input: username password
check username and ip address
is this user blocked?
yes
no
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
no
lockout is near message reset password suggestion
is the fail attempt limit near?
yes
no
login fail message

user blocked email
with **reset password** link

From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca



This is a system-generated message from GCcollab. Please do not reply this message | Ceci est un message généré par le système de GCcollab. Veuillez ne pas répondre à ce message

GCcollab

Hi Amable.

We received a request to change your password. You can click on the link below to reset your password:

https://security.passwordrecovery.org/50498478370740738378740387208723

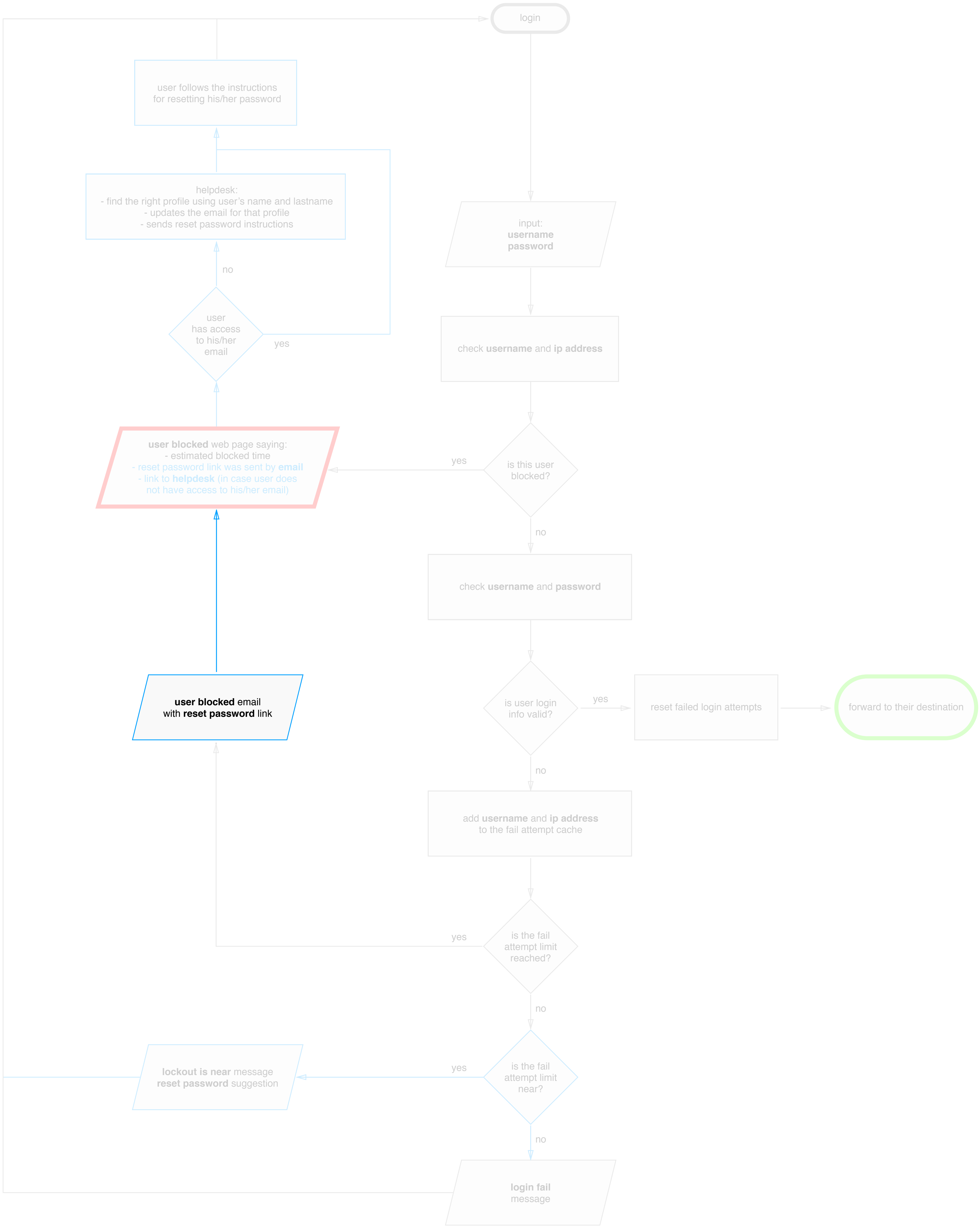
If you didn't request a password reset, you can safely ignore this email. Your password will not change.

If you are still having password or account issues after using the reset link, you can contact the help desk and an agent will help you change your password.

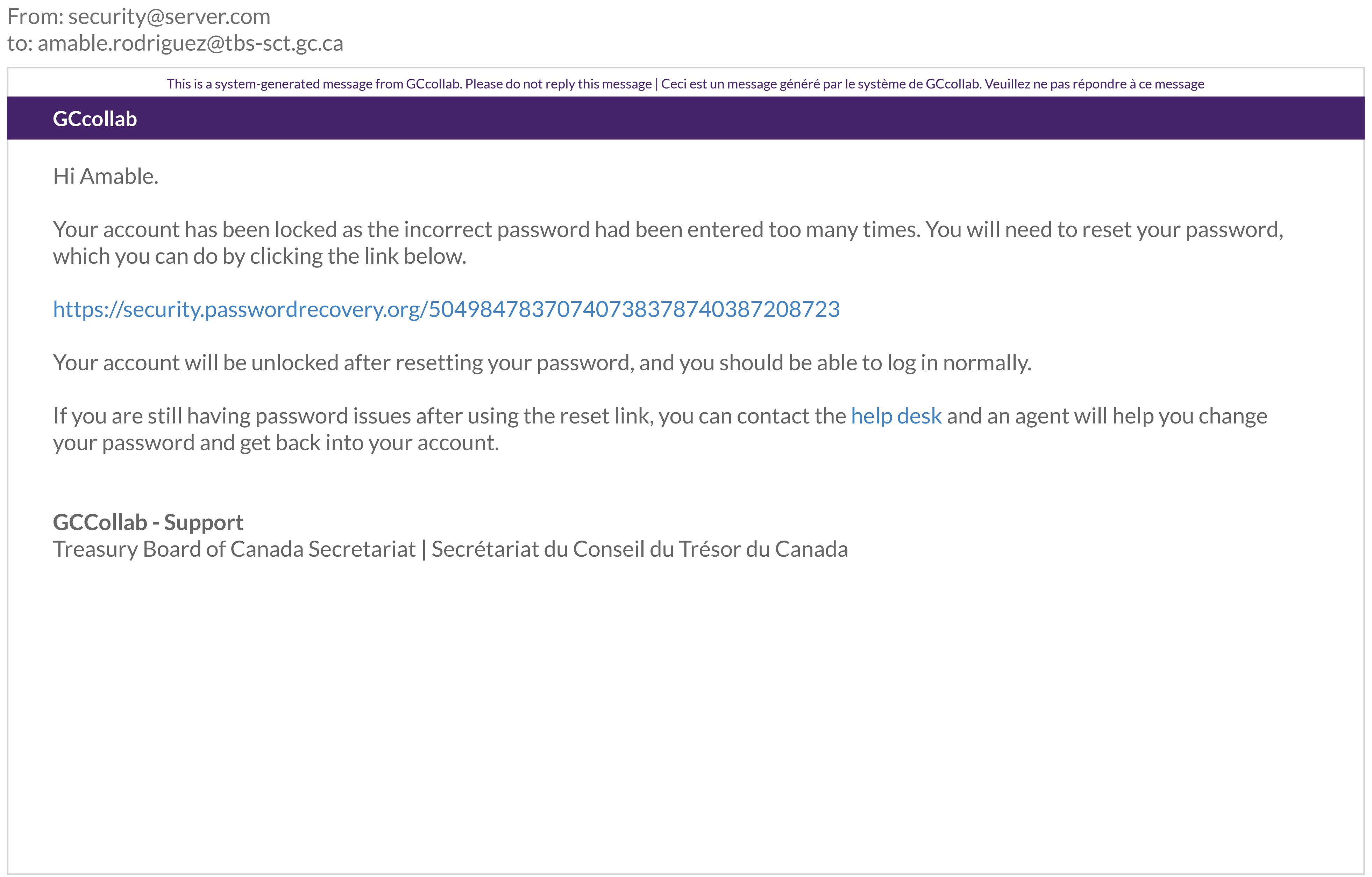
GCCollab - Support
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Marianne Aubrey

Donna Monbourquette


login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input:
username
password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email
with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address
to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message
reset password suggestion
yes
is the fail attempt limit near?
no
login fail
message

user blocked email
with **reset password** link



From: security@server.com
to: amable.rodriguez@tbs-sct.gc.ca

This is a system-generated message from GCcollab. Please do not reply this message | Ceci est un message généré par le système de GCcollab. Veuillez ne pas répondre à ce message

GCcollab

Hi Amable.

Your account has been locked as the incorrect password had been entered too many times. You will need to reset your password, which you can do by clicking the link below.

https://security.passwordrecovery.org/50498478370740738378740387208723

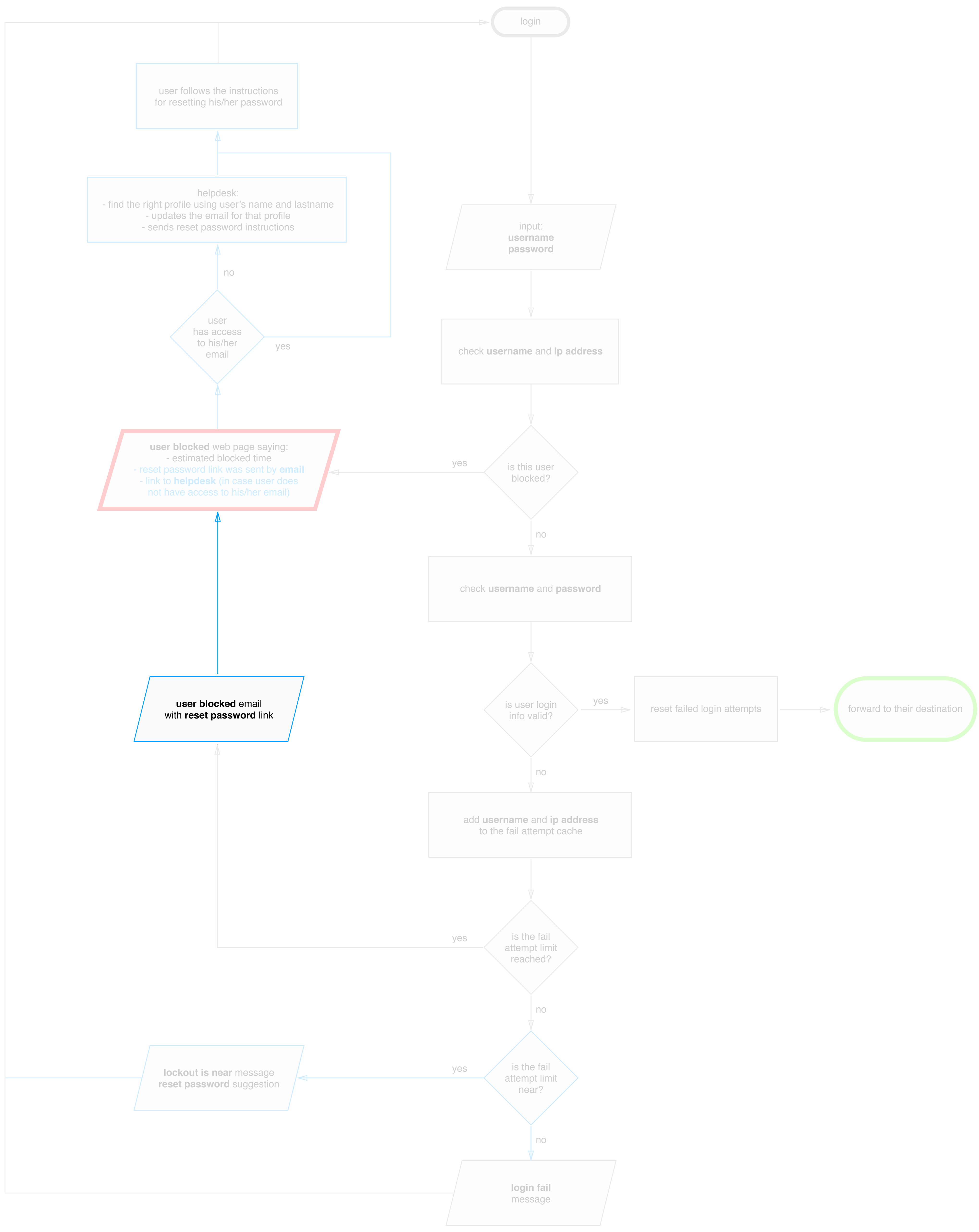
Your account will be unlocked after resetting your password, and you should be able to log in normally.

If you are still having password issues after using the reset link, you can contact the help desk and an agent will help you change your password and get back into your account.

GCCollab - Support
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Marianne Aubrey

Donna Monbourquette



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

no

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

no

is the fail attempt limit near?

yes

lockout is near message
reset password suggestion

no

login fail message

user blocked email with **reset password** link

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

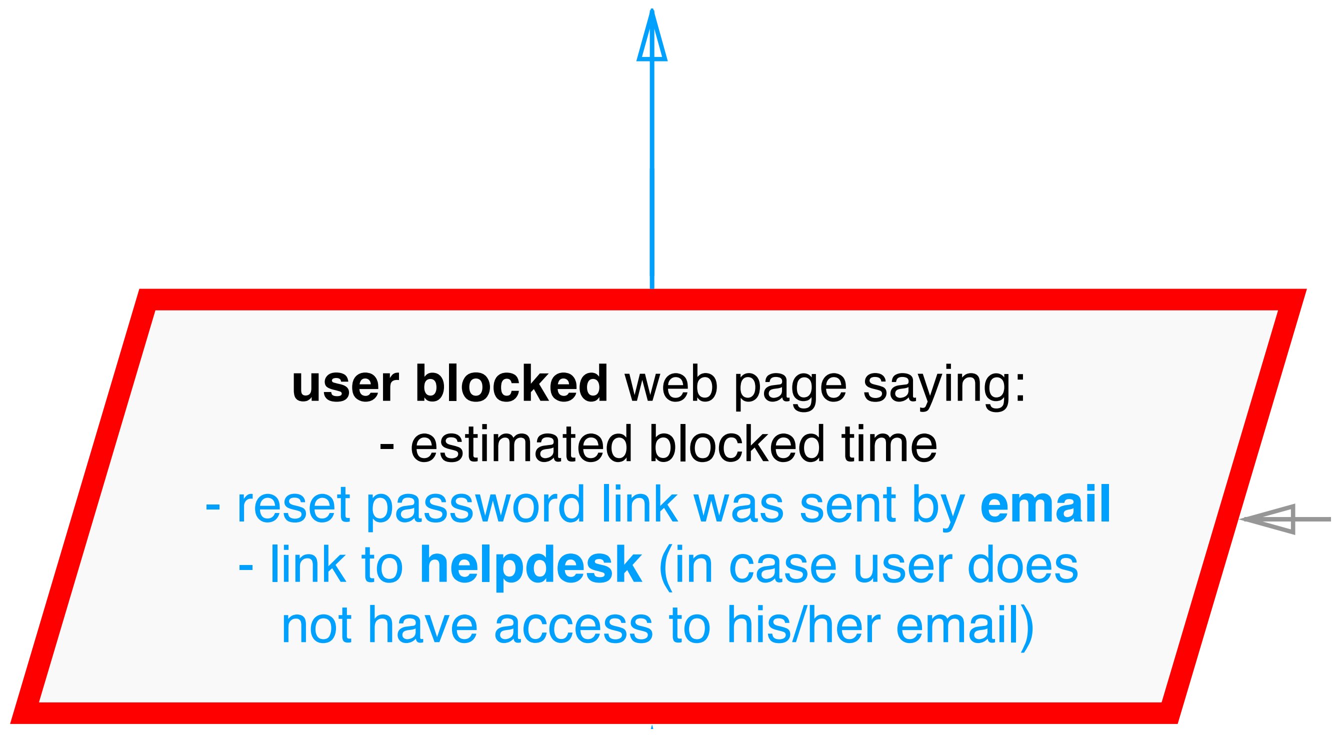
user has access to his/her email

yes

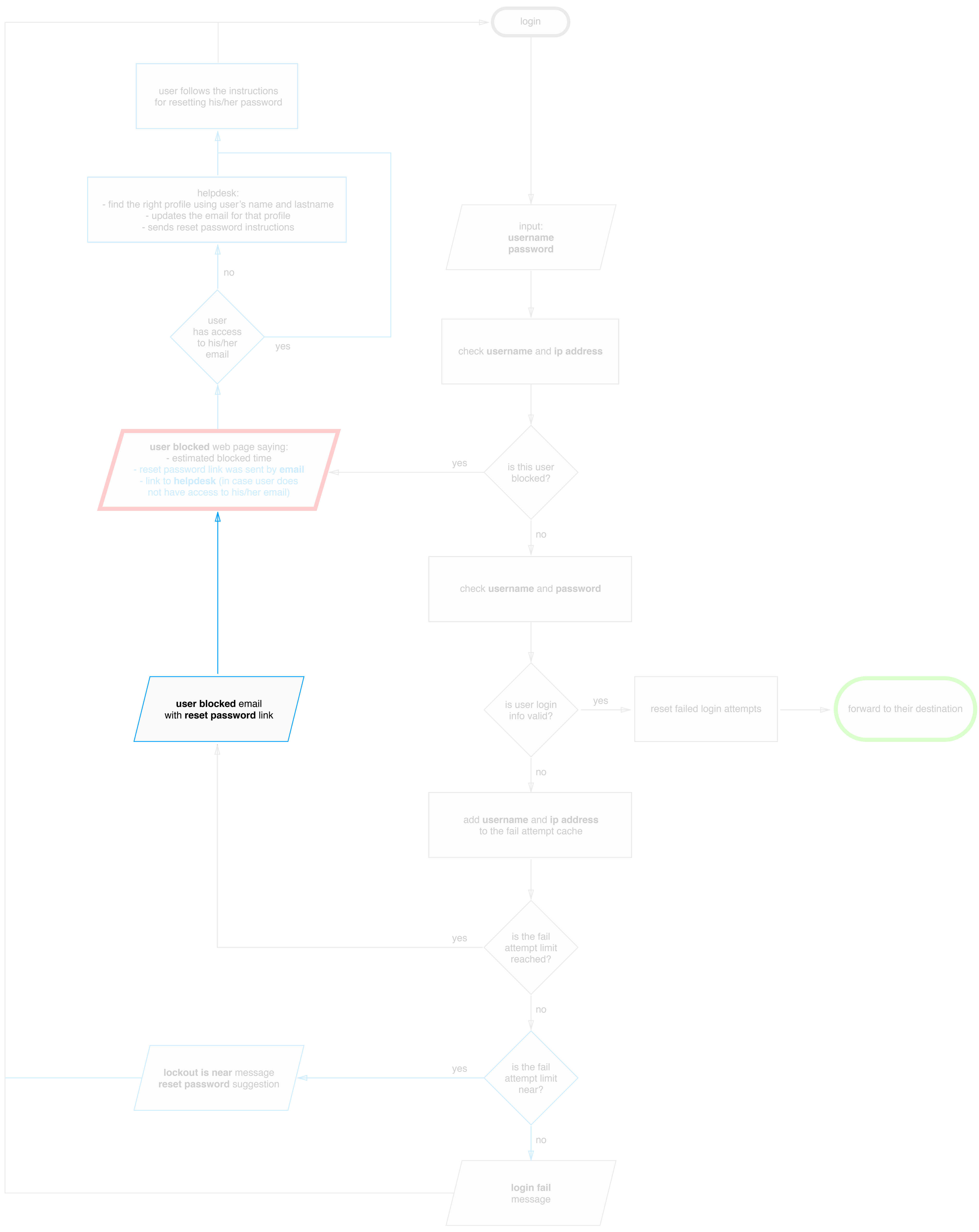
no

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

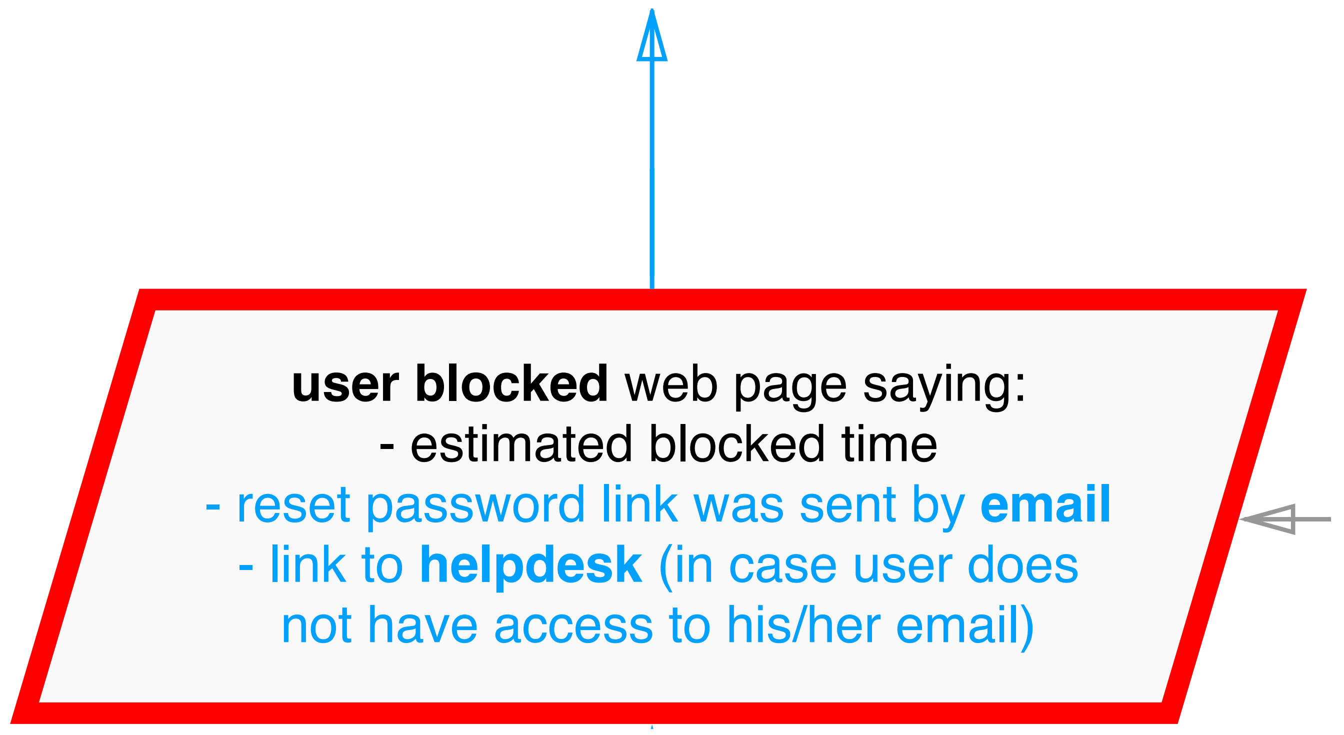
user follows the instructions for resetting his/her password



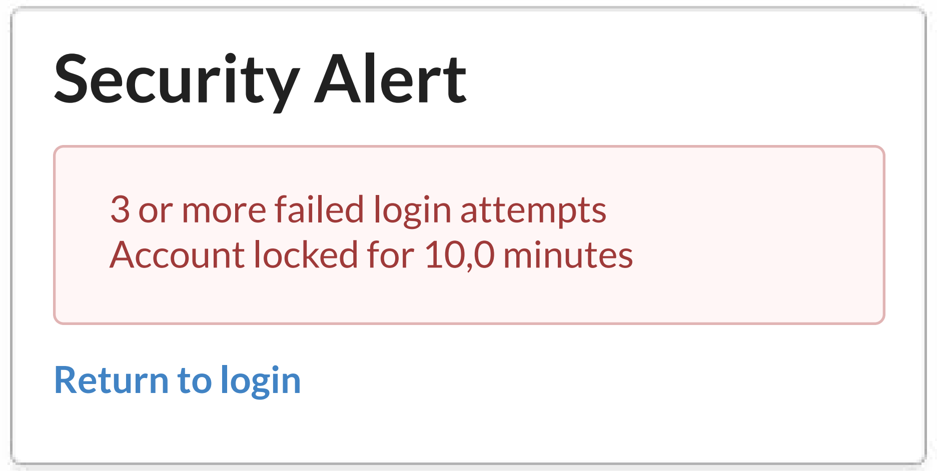
user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)



login
user follows the instructions for resetting his/her password
helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions
no
user has access to his/her email
yes
input: username password
check username and ip address
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
yes
is this user blocked?
no
check username and password
user blocked email with reset password link
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
yes
is the fail attempt limit reached?
no
lockout is near message reset password suggestion
yes
is the fail attempt limit near?
no
login fail message



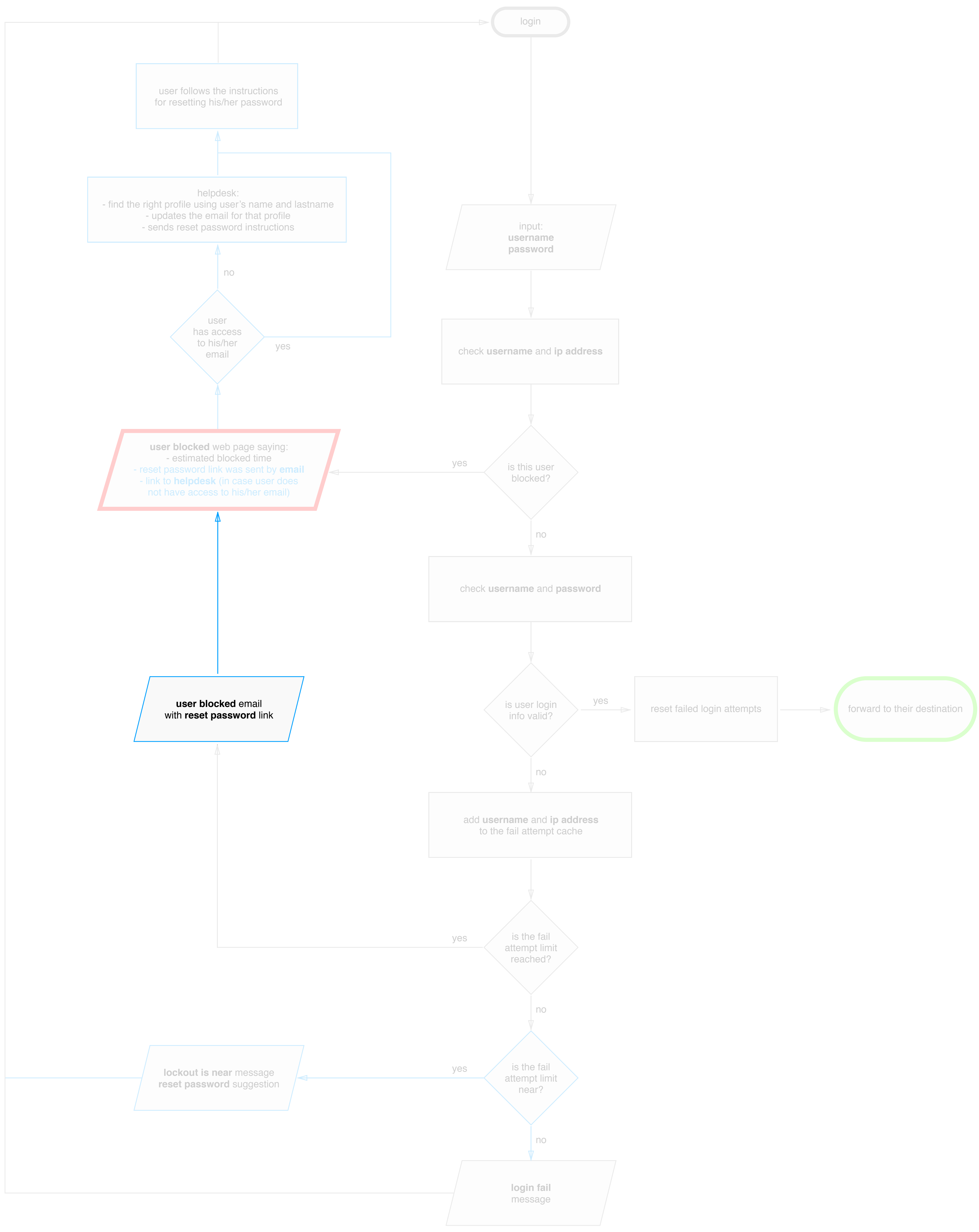
user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)



Security Alert

3 or more failed login attempts
Account locked for 10,0 minutes

Return to login



login

input:
username
password

check **username** and **ip address**

is this user blocked?

yes

no

user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)

user has access to his/her email

yes

no

helpdesk:
- find the right profile using user's name and lastname
- updates the email for that profile
- sends reset password instructions

user follows the instructions for resetting his/her password

check **username** and **password**

is user login info valid?

yes

reset failed login attempts

forward to their destination

no

add **username** and **ip address** to the fail attempt cache

is the fail attempt limit reached?

yes

user blocked email with **reset password** link

no

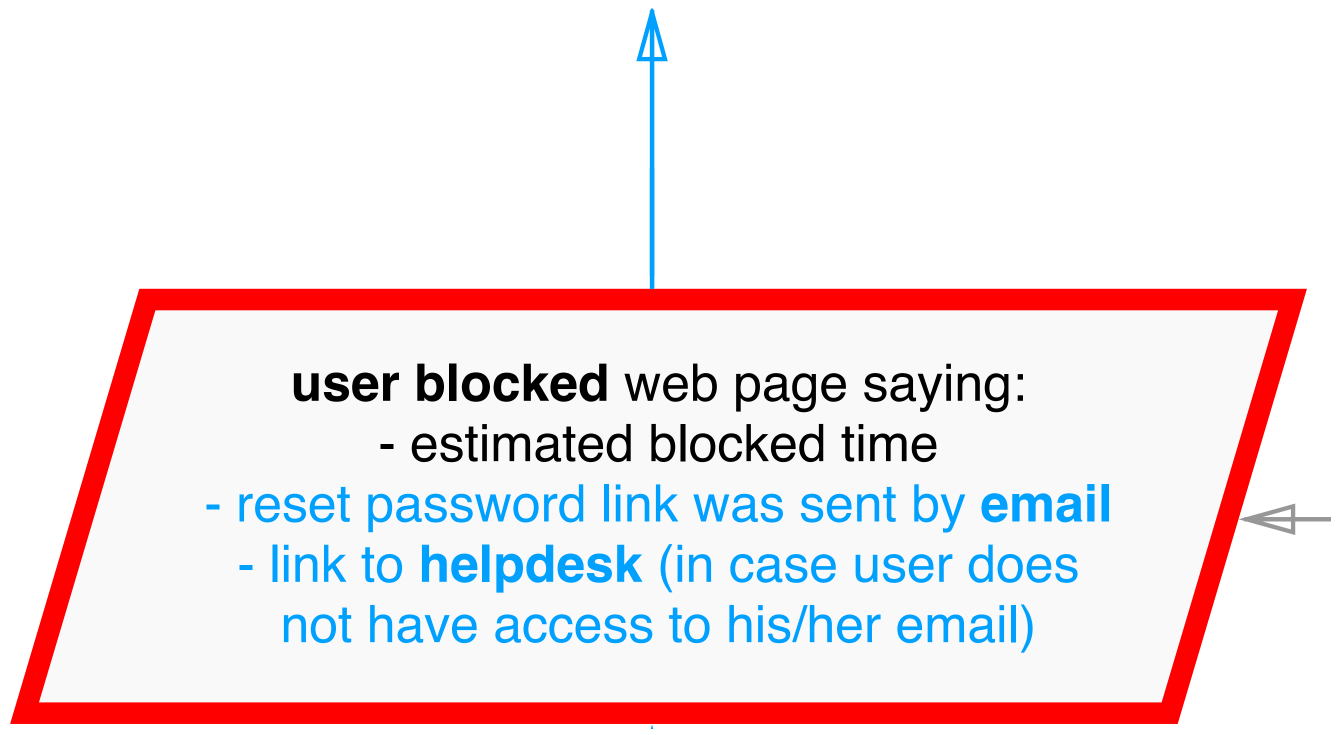
is the fail attempt limit near?

yes

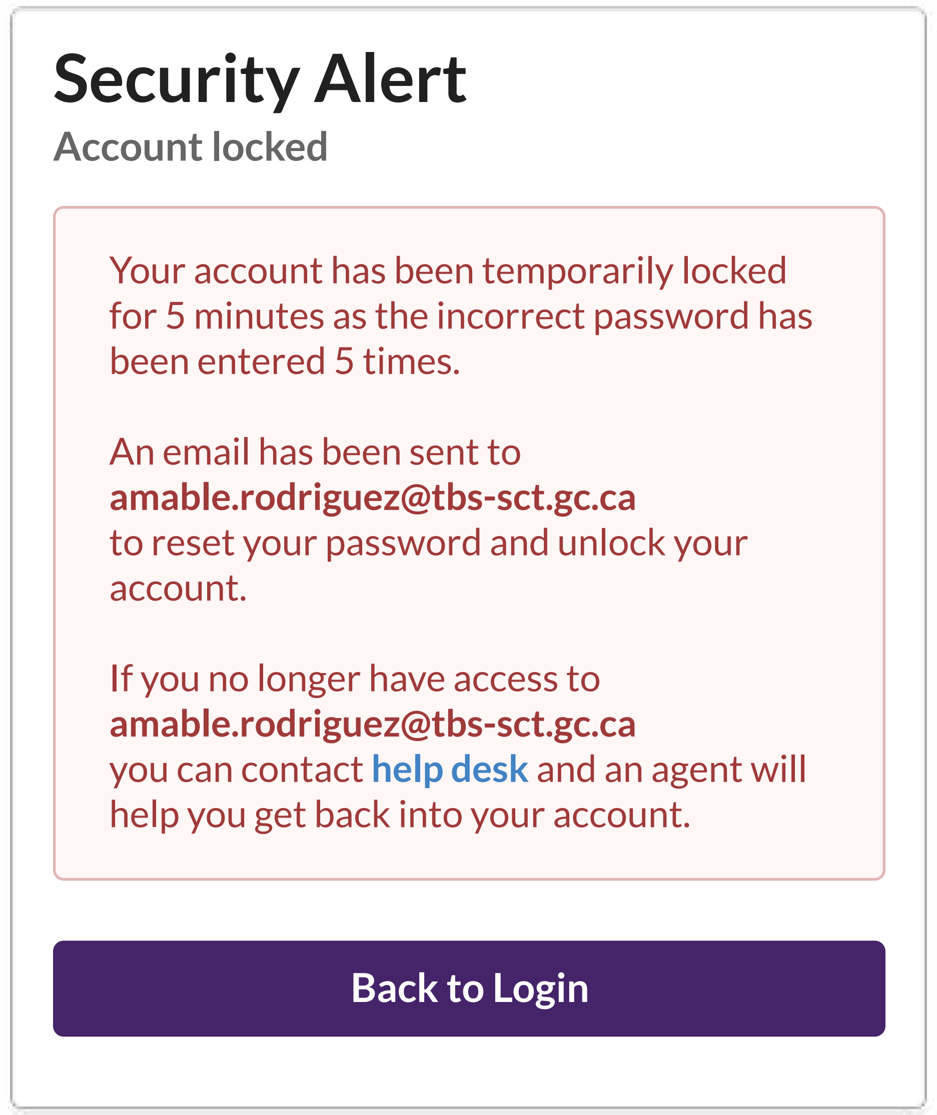
lockout is **near** message
reset password suggestion

no

login fail message



user blocked web page saying:
- estimated blocked time
- reset password link was sent by **email**
- link to **helpdesk** (in case user does not have access to his/her email)



Security Alert

Account locked

Your account has been temporarily locked for 5 minutes as the incorrect password has been entered 5 times.

An email has been sent to **amable.rodriguez@tbs-sct.gc.ca** to reset your password and unlock your account.

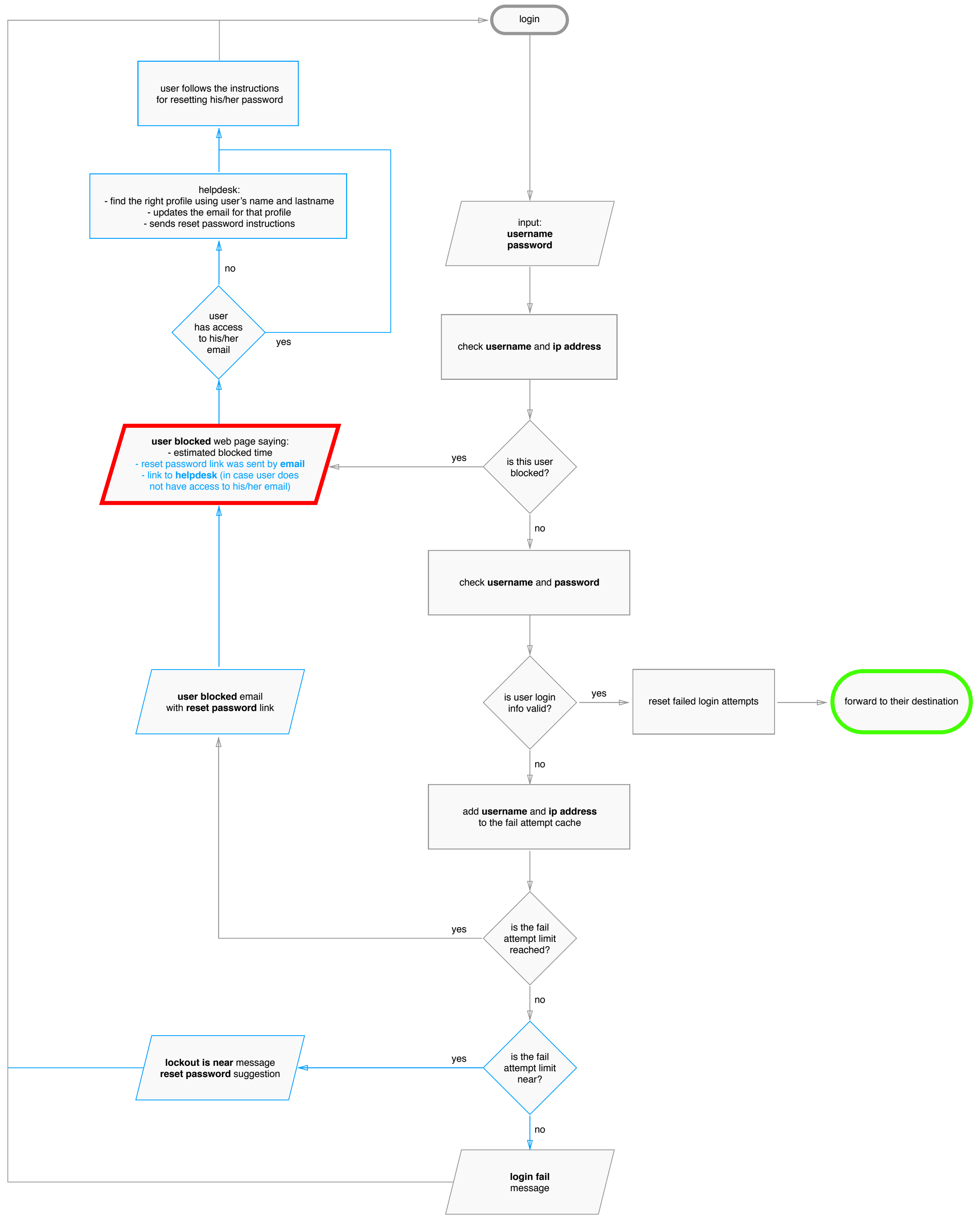
If you no longer have access to **amable.rodriguez@tbs-sct.gc.ca** you can contact help desk and an agent will help you get back into your account.

Marianne Aubrey

Donna Monbourquette

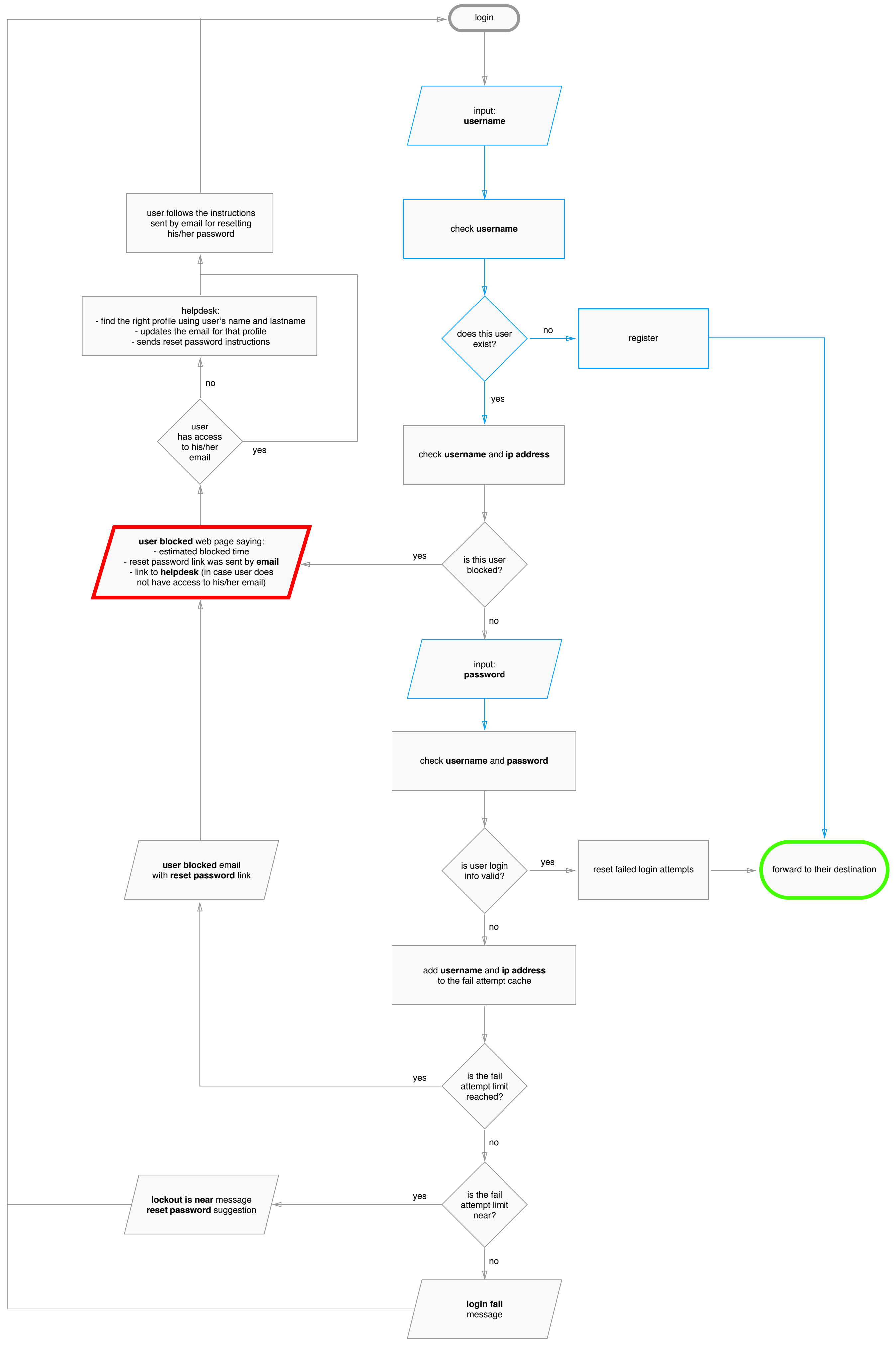
Iteration #1

- “lockout is near” warning
- password reset link by email
- link to helpdesk


login
input:
username
password
check username and ip address
is this user blocked?
yes
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions for resetting his/her password
no
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
user blocked email with reset password link
no
is the fail attempt limit near?
yes
lockout is near message reset password suggestion
no
login fail message

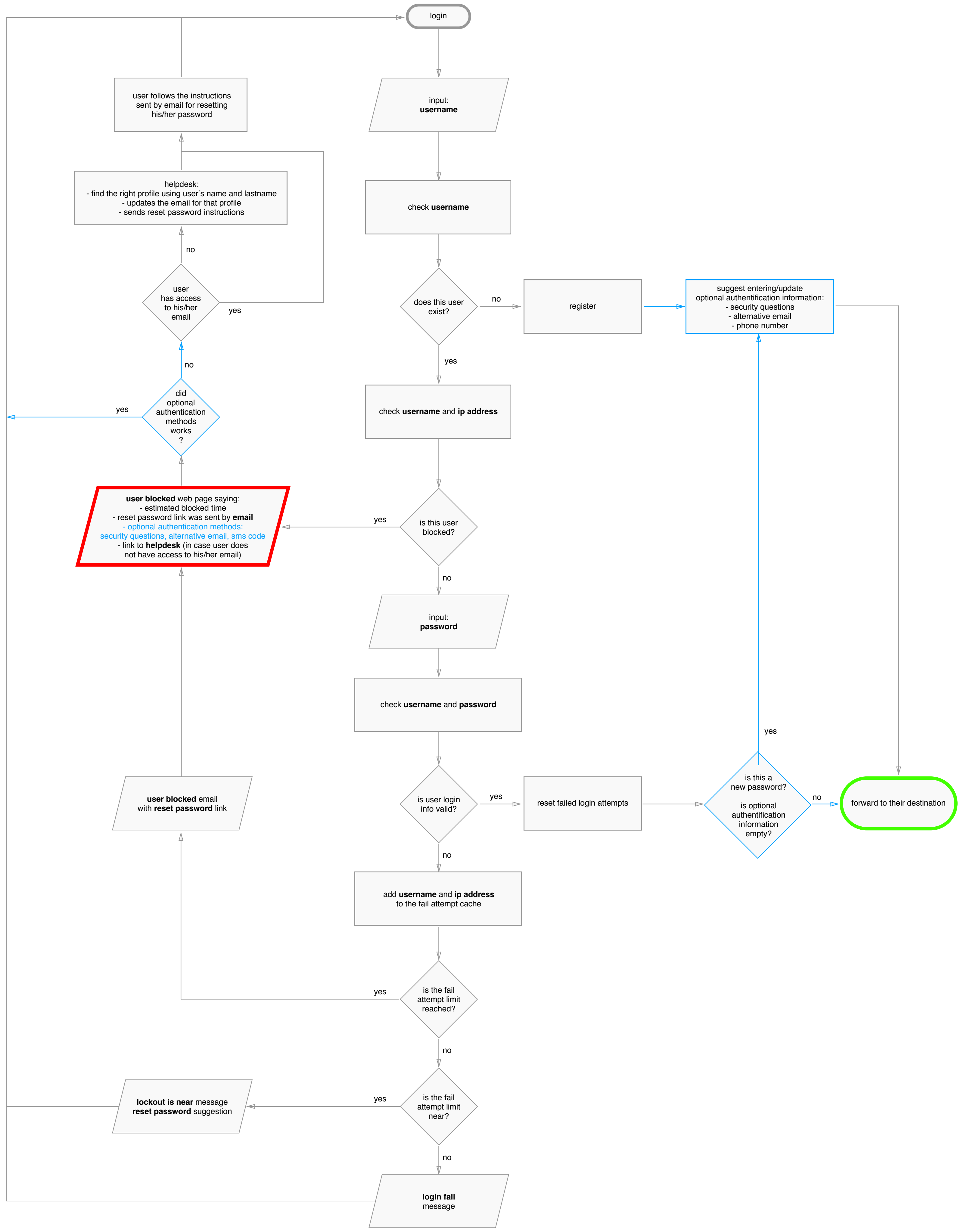
Iteration #2

- username and password separation
- inexisting account easy detection
- register added as natural part of the flow


login
input:
username
check username
does this user exist?
no
register
yes
check username and ip address
is this user blocked?
yes
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- link to helpdesk (in case user does not have access to his/her email)
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions sent by email for resetting his/her password
no
input:
password
check username and password
is user login info valid?
yes
reset failed login attempts
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
user blocked email with reset password link
no
is the fail attempt limit near?
yes
lockout is near message reset password suggestion
no
login fail message

Iteration #3

- added optional authentication information
- increase user power to unlock his/her account by himself/herself


login
input:
username
check username
does this user exist?
no
register
suggest entering/update optional authentification information:
- security questions
- alternative email
- phone number
yes
check username and ip address
is this user blocked?
yes
user blocked web page saying:
- estimated blocked time
- reset password link was sent by email
- optional authentication methods:
security questions, alternative email, sms code
- link to helpdesk (in case user does not have access to his/her email)
did optional authentication methods works ?
yes
no
user has access to his/her email
yes
no
helpdesk:
- find the right profile using user’s name and lastname
- updates the email for that profile
- sends reset password instructions
user follows the instructions sent by email for resetting his/her password
no
input:
password
check username and password
is user login info valid?
yes
reset failed login attempts
is this a new password?
is optional authentification information empty?
yes
no
forward to their destination
no
add username and ip address to the fail attempt cache
is the fail attempt limit reached?
yes
user blocked email with reset password link
no
is the fail attempt limit near?
yes
lockout is near message reset password suggestion
no
login fail message

Account - Lockout functionality
Sprint #42

Questions? / Des questions?

Thanks / Merci