Nettskjema

Follow-up study

Oppdatert: 8. mai 2024 kl. 20:56

Candidate nr.

Antall svar: **24**

- 02
- 07
- 06
- 03
- 12
- 15
- 28
- 27
- 19
- 20
- 17
- 18
- 04
- 10
- 29
- 13
- 1
- 26
- 23
- 21
- 22
- 25
- 17
- 30

Information

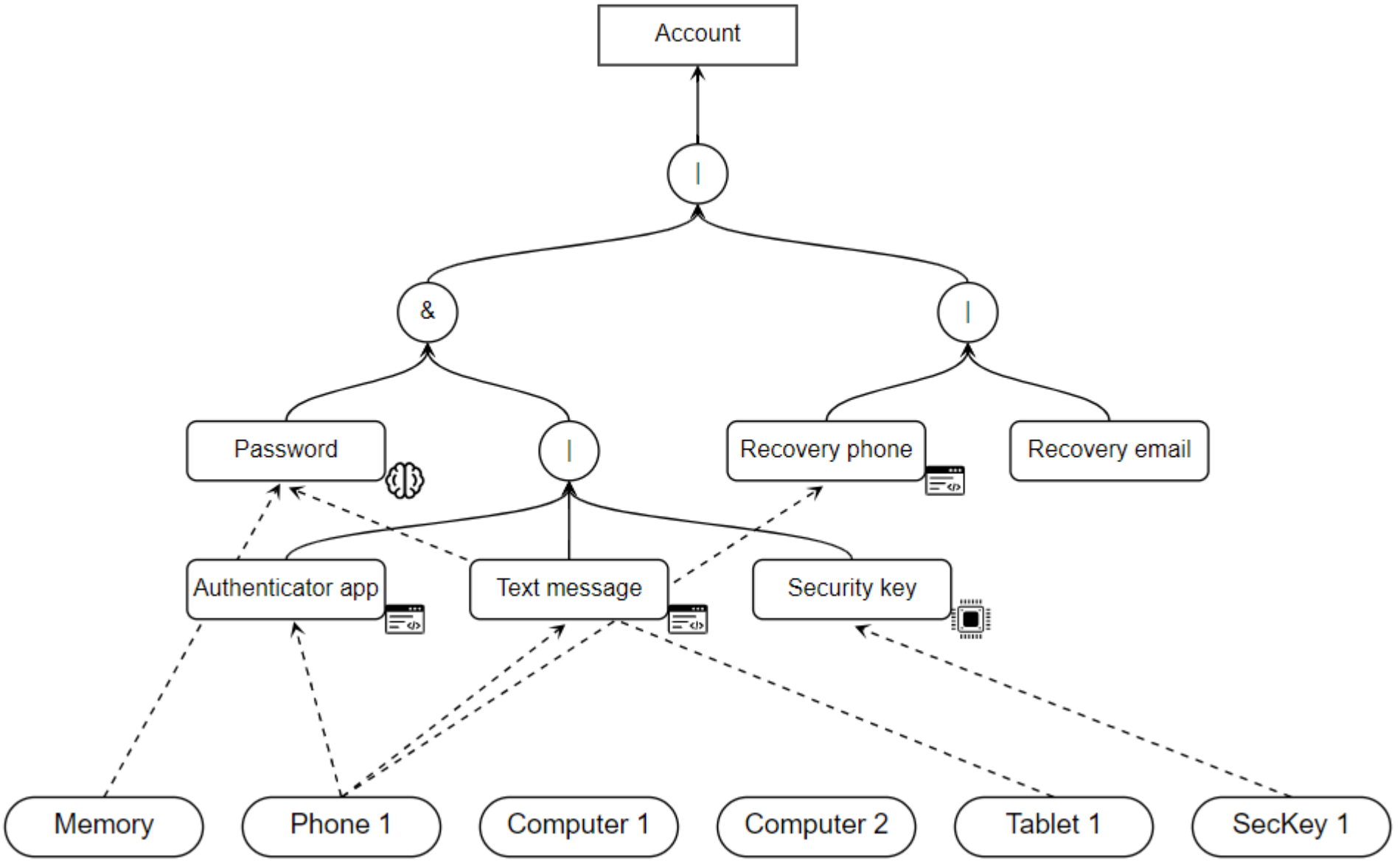
Welcome to the last part of my user-studies regarding my thesis!
This survey is divided into three parts:

1. AAG Usability - General
2. AAG Usability - Examples
3. AAG Usability - Personal accounts

(1) In the first part of the survey we will present the term AAG graphs in general, and ask some questions regarding the graphs and whether or not they are understandable
(2) In the second part of the survey you will get a few examples of different AAG graphs, and will be asked to arrange the different "user-accounts"-configurations in correct order in accordance to their security and "risk of loss"
(3) In the last part of the survey you will need the pdf document provided in the email, and will be presented questions regarding your own configurations

AAG Usability - General

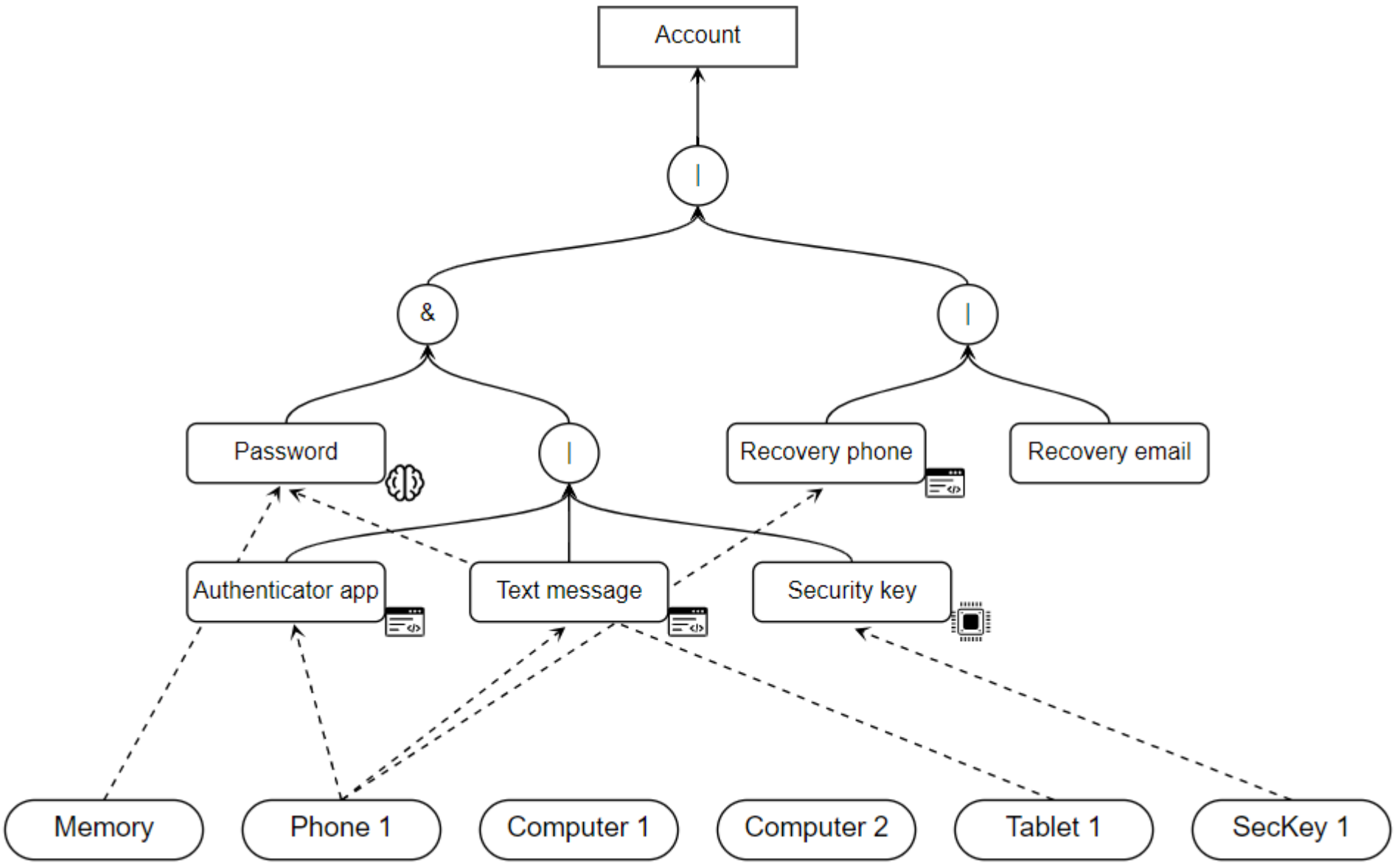
Account access graph (AAG) example



How well would you say you understand the graph above?

Antall svar: **24** Snitt: **3.79** Median: **4**

Svar	Antall	% av svar	
1	0	0%	0%
2	2	8.3%	8.3%
3	4	16.7%	16.7%
4	15	62.5%	62.5%
5	3	12.5%	12.5%



Account access graphs (AAG)
An AAG graph is a way of illustrating a user's different authentication methods (i.e. password access, authenticator app, recovery email etc.), where the account-configuration is represented as nodes (circles and rectangles) in a graph. These nodes can be connected together, creating a simple graph for better understanding of your account configuration.

The different components in the graph can be explained as follows:

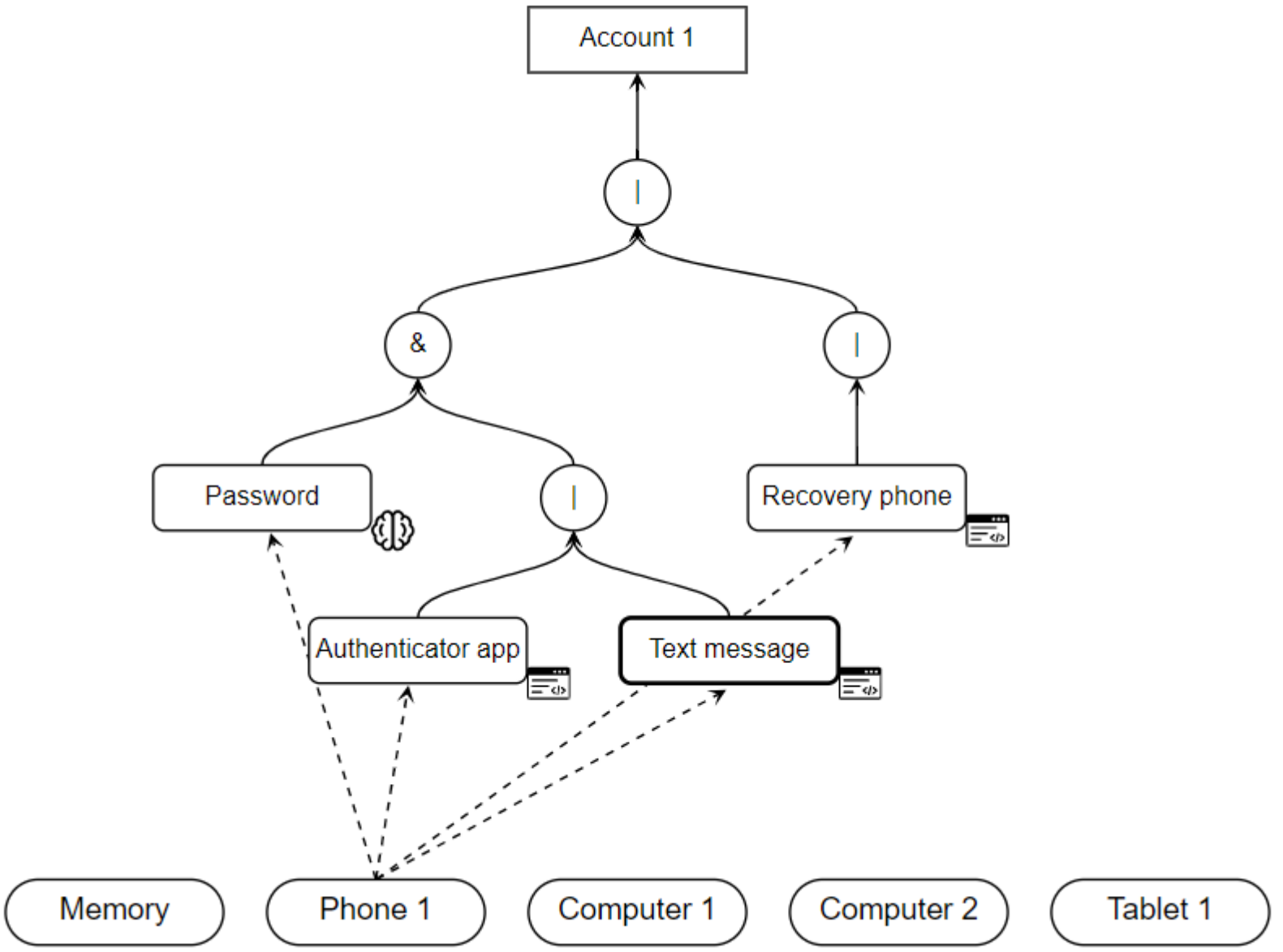
Account - Rectangle (Top): The top rectangle represent which user-account we are viewing
Operator - Circles:
&: "And"; both components under an "and"-node must apply
| **:** "Or"; the components under an "or"-node all applies, but you can choose between which you want to use
Authentication - Rectangle with slightly round edges: Authentication/Recovery methods
Device list - Rectangle with round edges (Bottom): List of all devices the user own
Arrows: Dependencies; Illustrates which devices the different authentication methods are stored on/used with
Symbols/illustrations:
Brain: Knowledge-based authentication (L)
Small window: Software-based authentication (M)
Chip: Hardware-based authentication (H)
L/M/H: Low/Medium/High -score

Further, when looking at the different graphs, we can rate them in accordance with:

Security: Scoring scheme with a scale low, medium and high; which indicates how well the account is secured based on the different nodes and combinations (operators) (e.g. L = Low securty score)
"Risk of Loss": Indicates how many different devices/options a user can lose before losing access to their account (e.g. Risk of loss = 2; If the user lose two devices (e.g connected phone and computer), they have lost access to their account)

On the next two slides you will find two AAG graphs, one for "Account 1", and one for "Account 2". Answer the following questions in relation to the different accounts.

Account 1



Does this account have 2FA on their account?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	24	100%	100%
No	0	0%	0%

What type(s) of 2FA methods does this account use?

Antall svar: **24**

- Authenticator App and Text message
- An authenticator app and (presumably) codes sent over SMS
- Authenticator app, Text message
- Uses Password and Authenticator app. OR a recovery phone that do not use 2FA so perhaps not...
- Auth app, or text. Not sure if the recovery device ruins the 2FA classification.
- authenticator app
- Password AND Auth.app OR text message (through the use of a phone)
- Otp app & sms 2fa.
- app or text message
- Software-based authentication
- Authenticator app or Text message
- Authenticator app and text message using Phone 1
- Authenticator app
- Authenticator app
- Authenticator app
  Text message
- from phone 1
- Authenticator app / text message
- Password and Authenitcator app on phone 1
  Password and Text message to phone 1
- Authenticator app or text message
- App or text
- Recovery phone does not have 2fa. But password uses text message and auth app
- Authenticator app or text message
- Software based (auth app and txt msg)
- Authenticator app and mobile text message

If the user lost "Phone 1", would this be an issue considered how the account is configured?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	19	79.2%	79.2%
No	5	20.8%	20.8%

If yes, can you explain why?

Antall svar: **19**

- The account cannot be accessed anymore, because there is no alternative way.
- All recovery options depend on Phone 1
- configured? <- unsure if its supposed to mean something more here, but doesn't losing Phone 1 mean that they completely lose access to the account? (assuming they cant get Phone 1 back again.) i.e. it would be an issue as the password, authenticator app, text message and recovery phone are all based on the user having Phone 1. Furthermore, from the AAG, the user doesn't remember the password, so everything (access to the account) depends on Phone 1.
- The user only use that
- No recovery options
- no app
- As phone 1 is the only way to make the expression TRUE, then losing phone 1 will result in the user not being able to access account 1.
- Innlogging med passord og bekrefte med otp app eller sms vil ikke være mulig. Brukeren kan heller ikke recovre kontoen.
  Dersom man skaffer seg en ny tlf og simkort med samme nummer kan man avhengig av hvordan recovery gjennom tlf funker få kontoen tilbake.
- Because phone1 is the only one with the 2FA codes. And it is the only recovery method
- All authentication types for the account are tied to the same phone. The account can only be accessed if the user has either:
  1. Both the password and the authenticator app or text message.
  2. If they have the recovery phone.
  By losing the phone you no longer have the recovery phone, and even if you knew the password, you would not get through the multifactor authentication step.
- Since the account requires password and (&) authenticator or (|) text message, and both the latter factors are dependent on phone 1, it would be an issue - likely possible to recover, but still an issue.
- Since "Phone 1" is the only device with recovery methods, the user would be locked out of the account if they lost it.
- the phone 1 is connected to the authentication app
- It is used as a recovery phone, which can bypass all the other security messures.
- Because the user depends on the phone both for MFA and for recovery, if its lost than there are no other alternatives
- All forms of authentication are lost with the phone
- All things are on phone, except password, but it uses 2fa
- Because all the access ways are connected to that phone
- The user's phone contains the authenticator app and receives

If the user lost "Computer 1", would this be an issue considered how the account is configured?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	0	0%	0%
No	24	100%	100%

If yes, can you explain why?

Antall svar: **0**

Dette spørsmålet har ingen svar

How would you rate this account in accordance with security?

Antall svar: **24**

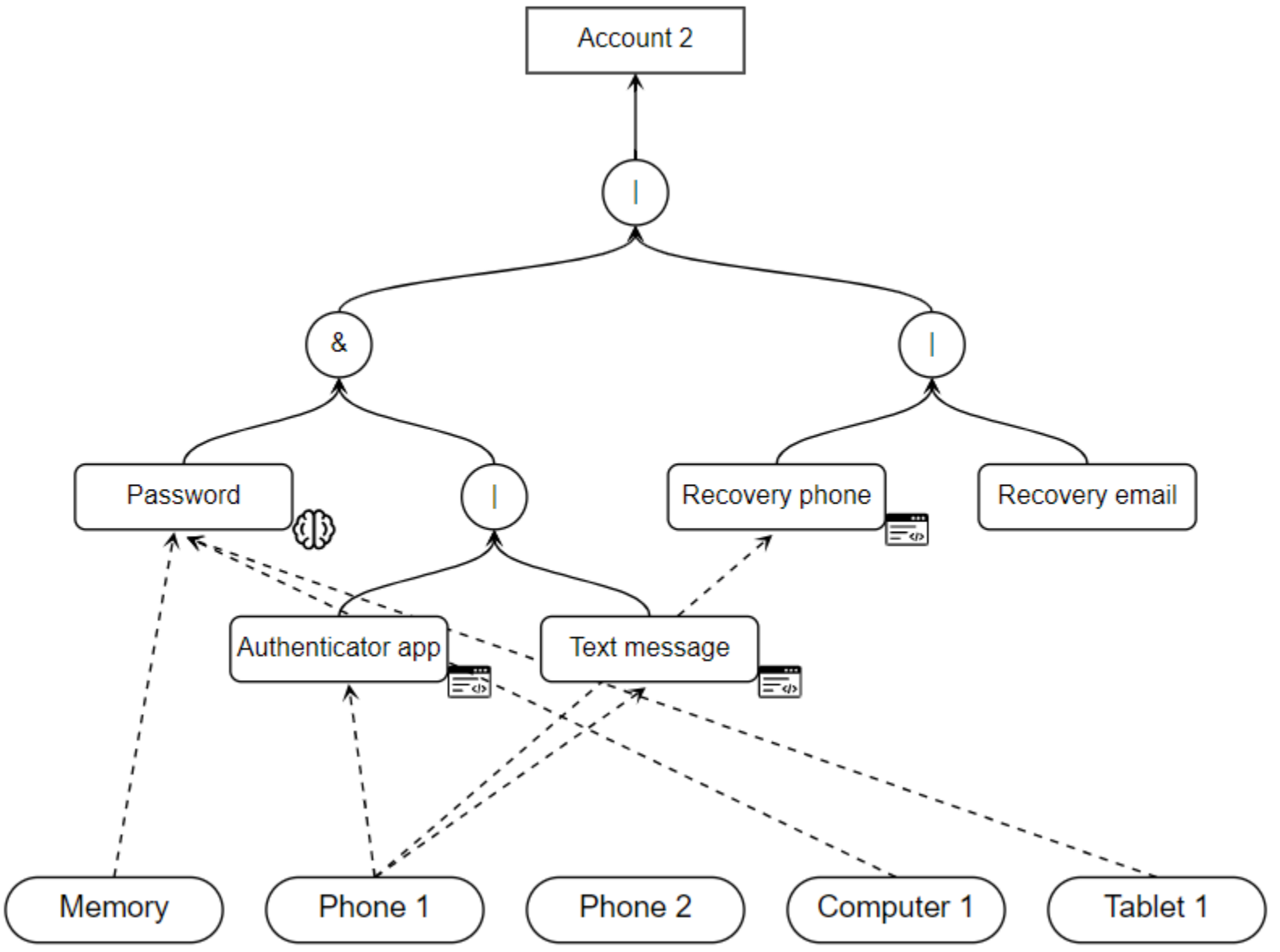
Svar	Antall	% av svar	
Low	3	12.5%	12.5%
Medium	19	79.2%	79.2%
High	2	8.3%	8.3%

How would you rate the risk of loosing access to this account?

Antall svar: **24**

Svar	Antall	% av svar	
Low	3	12.5%	12.5%
Medium	3	12.5%	12.5%
High	18	75%	75%

Account 2


Account 2
|
&
|
Password
|
Recovery phone
Recovery email
Authenticator app
Text message
Memory
Phone 1
Phone 2
Computer 1
Tablet 1

Where is the password for this accound saved/stored?

Antall svar: **24**

- Memory (remembered by the user)
- In memory, on Computer 1, and on Tablet 1
- 1. Memory
  2. Computer 1
  3. Tablet 1
- Memory, Computer 1 and Tablet 1
- Memory, Comp1 and Tab1
- Memory, comp 1 and tablet 1
- memory, computer 1 and tablet 1
- I hukommelsen, computer 1 og tablet 1.
- Memory, computer 1 and tablet 1
- On computer 1, tablet 1, and as knowledge possessed by the user
- Memory
- The password is saved in memory (:^)), on computer 1, and on tablet 1.
- On "Computer 1", "Tablet 1" and in the brain.
- In the users memory
- Memory and tablet
- memory, computer 1 and tablet 1
- Computer 1, Tablet 1, Memory
- Password is stored on computer 1 and tablet 1 (and memory of user)
- Memory, computer 1 and tablet 1
- memory
- Memory comp1 tablet 1
- In the memory, on the computer 1 and the tablet 1
- Stored in the brain
- The password for this account is stored on the user's computer 1 and tablet 1, and in the user's memory

Can the user access this account if they only have the "Tablet 1" available?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	4	16.7%	16.7%
No	20	83.3%	83.3%

In short, justify your answer

Antall svar: **24**

- You still need Phone 1 for MFA or recovery. Alternatively, you can also use the recovery email.
- Must use 2FA to access account - only accessible using Phone 1
- They would require Phone 1 to use the authenticator app or text message in combination with the password. Could also alternatively use it to gain access through the recovery phone option.
- Have only password.
- No MFA options
- need phone 1
- AND expression cannot be TRUE
- Ingen mulighet for å bekrefte MFA
- Not access to the 2FA that is on phone 1
- They could use the recovery email.
- Password & MFA is needed
- The account requires 2FA, which is not set up using tablet 1
- The account has 2FA with "Phone 1".
- Phone 1 is needed for 2FA
- Not possible to authenticate the account without the permission phone
- it needs phone 1
- Phone 1 is needed for 2fa
- Yes, the account has enables MFA that uses phone 1 (not tablet 1) and the recovery of the phone is also done by the phone). However the recovery method using email can be accessed through the tablet
- Tablet 1 lacks access to mandatory 2fa
- cant access 2fa
- Need phone for 2fa, if they have email on the tablet then they can access
- They need the phone 1 for authentication
- Authenticator app on phone 1
- Yes if they can use their recovery email, no if not

If the user lost "Phone 1", would this be an issue considered how the account is configured?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	15	62.5%	62.5%
No	9	37.5%	37.5%

If yes, can you explain why?

Antall svar: **15**

- The user needs Phone 1 to access the mandatory 2FA options
- Yes as it's set to the recovery phone, and they lose access to the 2FA methods through the authenticator app and text message.
- Authenticator app is lost
- phone 1 --> recovery phone --> access to account through the second and last OR expressions.
- Ingen mulighet for å bekrefte med MFA, og ingen mulighet til å recovre via andre enheter.
- Not access to the 2FA codes and no recovery method
- They would have to reset the account using the recovery email which could be argued to be more of an inconvenience than simply logging in. However, they would still have access to the account, given that they have access to the email address in question.
- The account requires 2FA, which is only set up with phone 1. However, there is a recovery email available, making a recovery likely possible.
- "Phone 1" has the only 2FA methods, but also the recovery method. If the user lost "Phone 1", they would have no way to log in, but also no way to recover the account.
- They are not able to use 2FA
- Authentication app is connected
- It is used as a recovery phone, and doesn't require anything else to access the account.
- No access to mandatory 2fa, or recovery
- They wouldn't be able to access the authenticator
- Due to txt or auth app 2fa, but he/she can recover with a new phone

If the user lost "Computer 1", would this be an issue considered how the account is configured?

Antall svar: **24**

Svar	Antall	% av svar	
Yes	2	8.3%	8.3%
No	22	91.7%	91.7%

If yes, can you explain why?

Antall svar: **2**

- One could extract the password from Computer 1. While one may not easily log into the account due to the 2FA options being inaccessible from Computer 1, one could either exploit a flaw in 2FA (e.g. SMS exploits) or reuse the password if the user is bad at passwords.

- As I understand it, the password is stored there.
  Possibly, the password might also give access to an email client, or the email client might already be logged in to on the computer, enabling the use of the recovery email.

How would you rate this account in accordance with security?

Antall svar: **24**

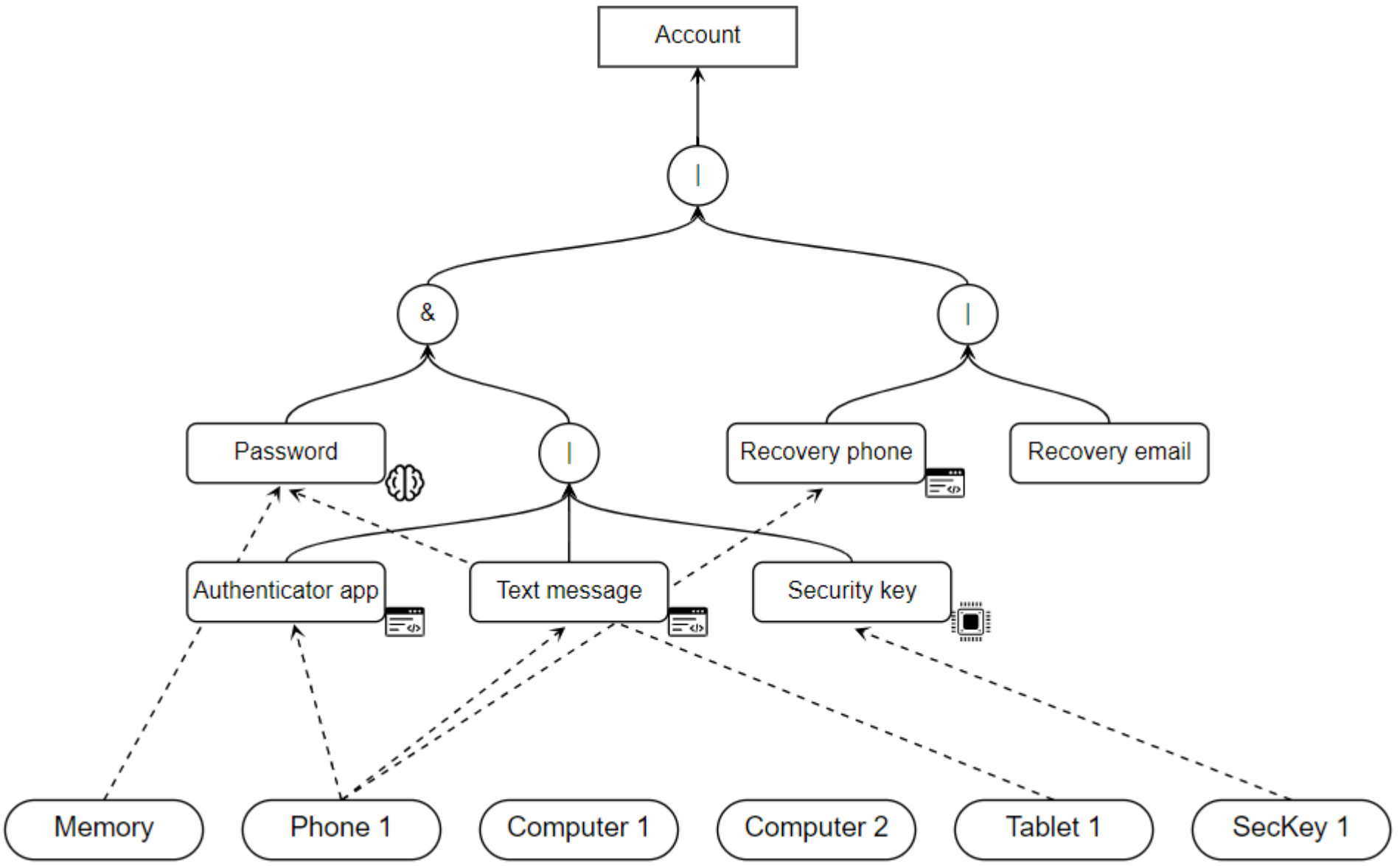
Svar	Antall	% av svar	
Low	1	4.2%	4.2%
Medium	16	66.7%	66.7%
High	7	29.2%	29.2%

How would you rate the risk of loosing access to this account?

Antall svar: **24**

Svar	Antall	% av svar	
Low	12	50%	50%
Medium	7	29.2%	29.2%
High	5	20.8%	20.8%

Account access graph (AAG) example (rep)

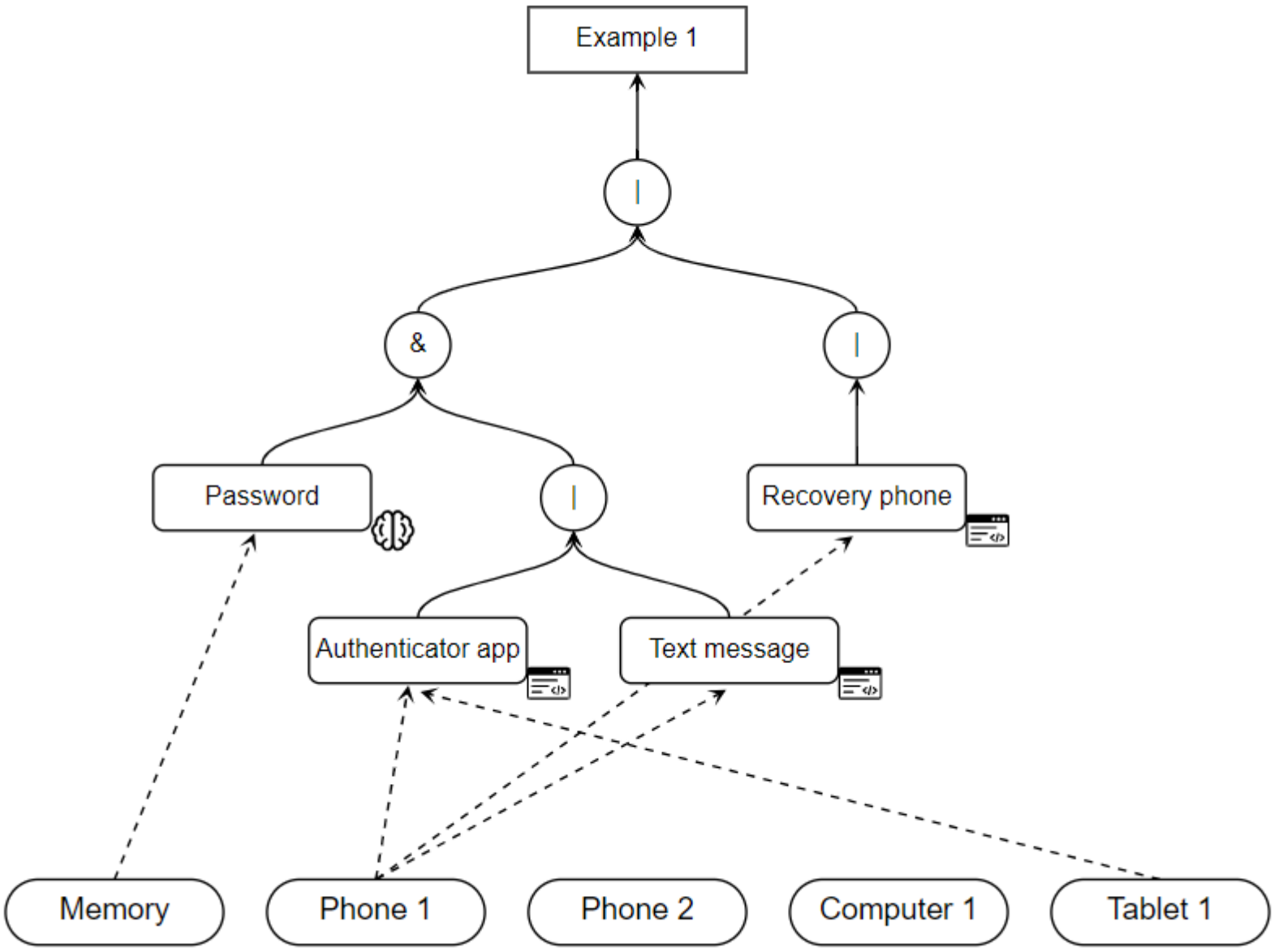


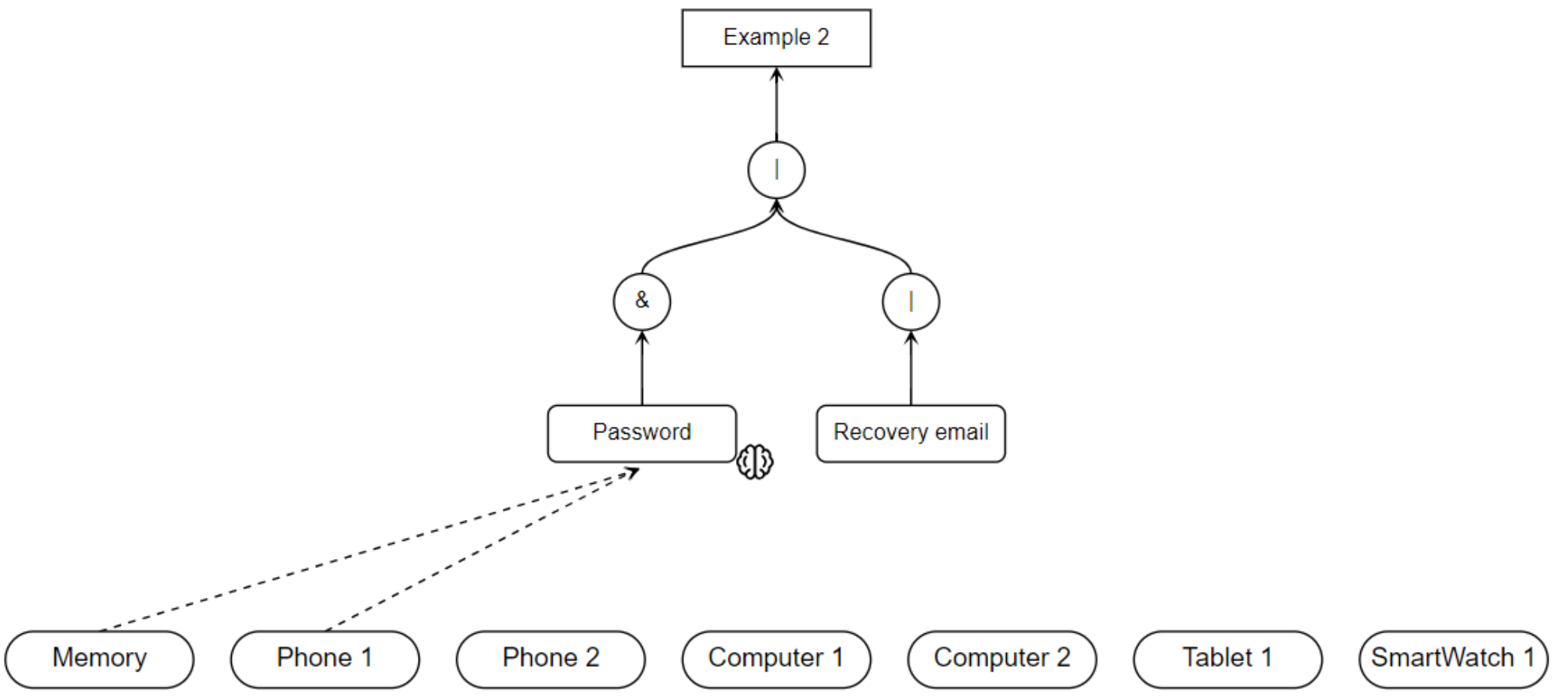
After we have explained the graph and terms, and you've answerd the questions; how well would you say you understand the graph above now?

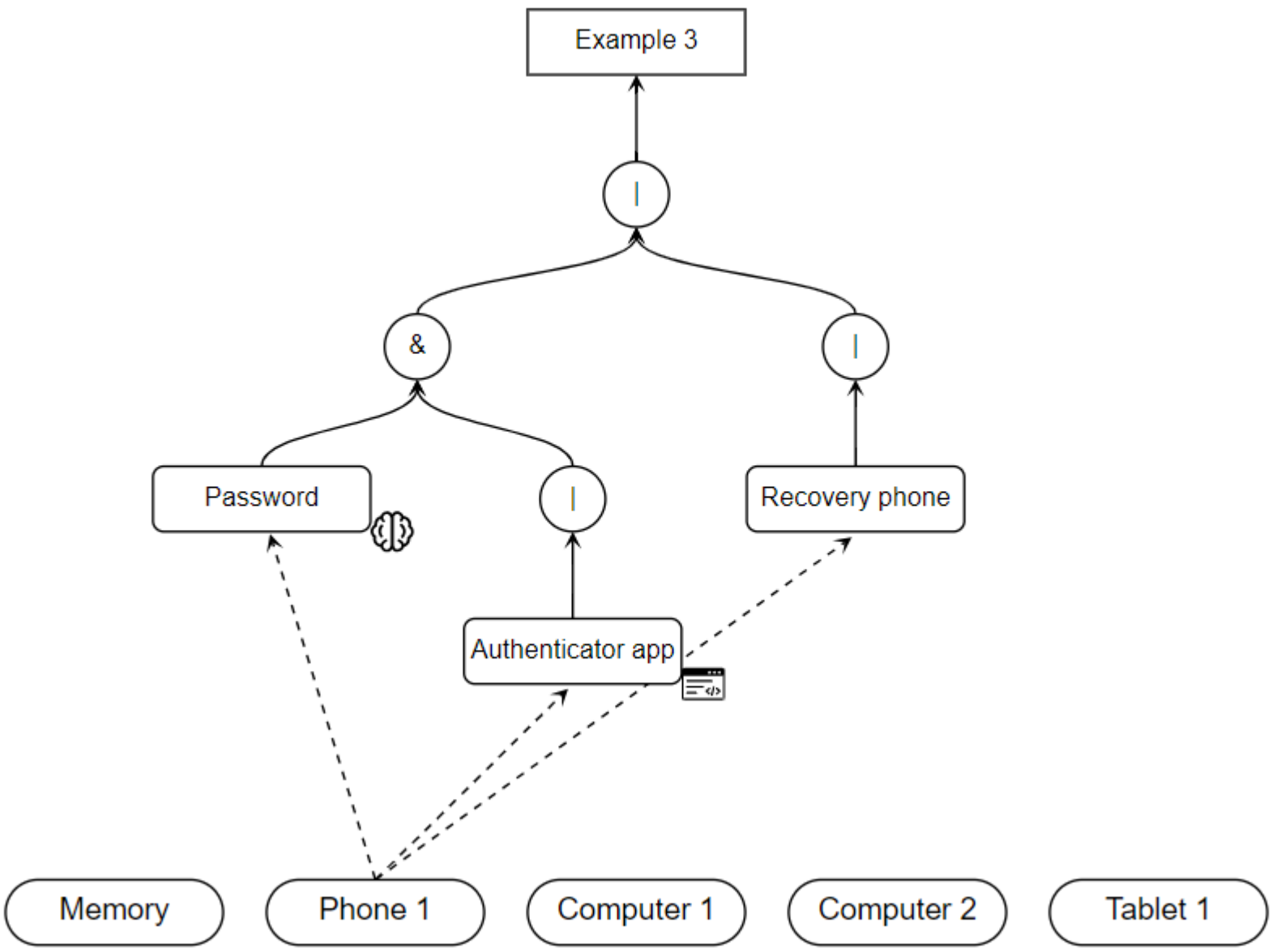
Antall svar: **24** Snitt: **4.46** Median: **5**

Svar	Antall	% av svar	
1	0	0%	0%
2	0	0%	0%
3	2	8.3%	8.3%
4	9	37.5%	37.5%
5	13	54.2%	54.2%

AAG Usability - Examples


Example 1
|
&
|
Password
|
Recovery phone
Authenticator app
Text message
Memory
Phone 1
Phone 2
Computer 1
Tablet 1


Example 2
|
&
|
Password
Recovery email
Memory
Phone 1
Phone 2
Computer 1
Computer 2
Tablet 1
SmartWatch 1


Example 3
|
&
|
Password
|
Recovery phone
Authenticator app
Memory
Phone 1
Computer 1
Computer 2
Tablet 1

1. How would you rank the example(s) above in accordance with security?

Antall svar: **24**

- 1-3-2
- 1-3-2
- 1-3-2
- 1-3-2
- 2-1-3
- 1-3-2
- 2-1-3
- 2-3-2
- 1-3-2
- 1-2-3
- 1-3-2
- 2-1-2
- 1-3-2
- 1-3-2
- Example 1, example 3, example 2
- 1-3-2
- 1-3-2
- 1-3-2
- 1-3-2
- 1-3-2
- 132
- 1,3,2
- 3-1-2
- 1-3-2

2. How would you rank the example(s) above in accordance with the risk of loosing access to the account?

Antall svar: **24**

- 3-2-1
- 3-1-2
- 3-2-1
- 3-1-2
- 1-2-1
- 2-3-1
- 3-1-2
- 2-2-1
- 3-2-1
- 3-1-2
- 2-3-1
- 1-3-1
- 2-3-1
- 3-2-1
- Example 2, example 3, example 1
- 2-3-1
- 3-2-1
- 3-2-1
- 2-3-1
- 2-3-1
- 321
- 3,1,2
- 2-1-3
- 2-1-3

AAG Usability - Personal accounts

BEFORE looking at the AAG graphs, how would you rate the security of your account?

Facebook

Antall svar: **24**

Svar	Antall	% av svar	
Low	9	37.5%	37.5%
Medium	12	50%	50%
High	2	8.3%	8.3%
I don't have this account	1	4.2%	4.2%

Apple

Antall svar: **24**

Svar	Antall	% av svar	
Low	2	8.3%	8.3%
Medium	12	50%	50%
High	4	16.7%	16.7%
I don't have this account	6	25%	25%

Google

Antall svar: **24**

Svar	Antall	% av svar	
Low	1	4.2%	4.2%
Medium	13	54.2%	54.2%
High	10	41.7%	41.7%
I don't have this account	0	0%	0%

GitHub

Antall svar: **24**

Svar	Antall	% av svar	
Low	6	25%	25%
Medium	9	37.5%	37.5%
High	6	25%	25%
I don't have this account	3	12.5%	12.5%

LinkedIn

Antall svar: **24**

Svar	Antall	% av svar	
Low	7	29.2%	29.2%
Medium	11	45.8%	45.8%
High	1	4.2%	4.2%
I don't have this account	5	20.8%	20.8%

Now, open the PDF document attached in the email, and navgiate to your candidate nr. before answering the following questions for each account.
NOTE: If you DONT have any account on the platform, go to the bottom and skip to next page
(The candidate nr. should be sent to you via email in December 2023 during the first study)

Facebook
If you DONT have a Facebook account, go to the bottom and skip to next page

Do you see any issues with this account?

Antall svar: **18**

- The email address diminishes the security.
- There is no 2FA enabled on the account, and the password is stored on several devices, some of which are in a different location.
- No, but I could have set a recovery email for additional security.
- no 2fa
- 1. Password stored multiple devices
- No 2FA is the biggest
- Yes, I should configure 2FA.
  But the account is configured with recovery options by phone number.
- Only one device set up with 2FA/recovery and no other way to remember the password.
- All you need to access the account, is the registered e-mail. So if someone gets access to my e-mail, they could bypass all other security measures. However, to access the e-mail on a new device, you need 2FA.
- Yes, I forget the password all the time and need to reset it.
- No
- its low da;(
- Yes, lack of 2FA
- Its all dependent on my phone, however having an recovery mail, I dont think it is that big of an issue
- No
- Could have more fa
- Low security
- No 2FA or recovery email

Would you say this account is secure?

Antall svar: **21**

Svar	Antall	% av svar	
Yes	7	33.3%	33.3%
No	14	66.7%	66.7%

If no, can you explain in short why?

Antall svar: **14**

- The email address could possibly be
- No 2FA means anyone with the password can get access to the account
- Need only password
- no 2fa
- Stored password on multiple devices
- No 2FA, password is on many devices
- Missing 2FA
- Password + 2FA is not really considered safe anymore, as there has been a rise in MitM attacks that manages to hijack/steal MFA sessions - so safer than no other factors, but not that safe anyway
- IF someone gets access to my e-mail, they have an easy way in.
- It is not good if my password leaks
- because i have not secured it.
- You only need a password to access it.
- No 2FA
- Password only stored in memory, no 2FA

How would you rate the risk of loosing access to this account?

Antall svar: **20**

Svar	Antall	% av svar	
Low	8	40%	40%
Medium	8	40%	40%
High	4	20%	20%

After evaluating the graph, would you make any changes to your account setup?

Antall svar: **21**

Svar	Antall	% av svar	
Yes, i have already made changes afer the first survey	5	23.8%	23.8%
Yes, in the future	8	38.1%	38.1%
No	8	38.1%	38.1%

If you already made any changes, can you explain in short what changes you would make?

Antall svar: **5**

- Added 2FA
- I turned on 2FA during the last test
- two factor
- I added 2FA
- 2FA, recovery email, store password on computer and phone

If yes, can you explain in short what changes you would make?

Antall svar: **8**

- Change the recovery method
- 1. Register another authenticator app on a separate tablet/phone. 2. Register a recovery email.
- 2FA with password
- Retricting stored passwords
- 2FA
- Probably write down my password somewhere/use a secure key or something
- Set up another 2FA device.
- Add 2FA

After this evaluation, how would you rate the security of your Facebook account now?

Antall svar: **21**

Svar	Antall	% av svar	
Low	5	23.8%	23.8%
Medium	13	61.9%	61.9%
High	3	14.3%	14.3%

Apple
If you DONT have an Apple account, go to the bottom and skip to next page

Do you see any issues with this account?

Antall svar: **15**

- No
- No, I think this is fairly secure.
- No MFA
- Not really haha
- Ingen måte å logge inn på kontoen uten en apple enhet
- Mainly 2FA, again
- I don't have any recovery options that are not tied to a device.
- No
- No
- need two factor authentication
- NO
- I dont have any other entrusted party/device other than my own phone nr (and apple watch but this does not help much)
- It's easy to lose if I lose my phone
- Not really, normal setup, could have hardware based 2fa
- No 2FA, no recovery email or phone, password only stored on phone

Would you say this account is secure?

Antall svar: **16**

Svar	Antall	% av svar	
Yes	12	75%	75%
No	4	25%	25%

If no, can you explain in short why?

Antall svar: **4**

- No 2FA, password is on many devices
- Changing my phone number could have consequences for the security.
- ^
- No 2FA:(

How would you rate the risk of loosing access to this account?

Antall svar: **15**

Svar	Antall	% av svar	
Low	6	40%	40%
Medium	8	53.3%	53.3%
High	1	6.7%	6.7%

After evaluating the graph, would you make any changes to your account setup?

Antall svar: **16**

Svar	Antall	% av svar	
Yes, i have already made changes afer the first survey	7	43.8%	43.8%
Yes, in the future	3	18.8%	18.8%
No	6	37.5%	37.5%

If you already made any changes, can you explain in short what changes you would make?

Antall svar: **7**

- Added MFA
- Konfigurert recovery key
- Added 2FA
- I sat up 2FA
- authentication app
- Added a recovery contact (trusted third party (my brother and sister<3))
- 2FA, store password

If yes, can you explain in short what changes you would make?

Antall svar: **3**

- Recovery codes, and authentication apps. Perhaps a yubikey
- Add another account
- Hardware based 2FA

After this evaluation, how would you rate the security of your Apple account now?

Antall svar: **16**

Svar	Antall	% av svar	
Low	1	6.3%	6.3%
Medium	10	62.5%	62.5%
High	5	31.3%	31.3%

Google
If you DONT have a Google account, go to the bottom and skip to next page

Do you see any issues with this account?

Antall svar: **20**

- Email diminishes the security
- The only option besides 2FA via Phone 1 to get access is by using backup codes, which may not be readily accessible in an emergency. Also, the password is stored on several devices, some of which are unused.
- No, apart from the fact that having 2 phones might be problematic if I lose one of them, I think this is fairly secure.
- No
- Phone (SIM based) recovery or authentication is not very secure.
- No
- Recovery phone and/or recovery email gains access to the account
- The password and the recovery code is only on phone 1
- I have no alternative device to authenticate with.
  If I lose my phone I would have to use a recovery method such as email or recovery codes.
- Not really
- Still only using the brain to remember the password, and still susceptible to MitM phishing (with session stealing/hijacking).
- All you need to access the account, is the registered e-mail. So if someone gets access to my e-mail, they could bypass all other security measures. However, to access the e-mail on a new device, you need 2FA.
- Yes, I often forget the password
- No
- its low again:(
- If you gain access to my email, you also gain access to my account.
  Almost all access can be gained through my phone.
- Missing MFA wæ.
- Too much responsibility on one phone. Should have more redundancy
- The recovery mail makes my account unsecure
- Recovery email, too many ways in - f.example voce or sms

Would you say this account is secure?

Antall svar: **23**

Svar	Antall	% av svar	
Yes	15	65.2%	65.2%
No	8	34.8%	34.8%

If no, can you explain in short why?

Antall svar: **8**

- Weak recovery method
- above^
- MitM phishing, or steal phone + guess/steal password or something similar
- Same as before.
- does not have factor authentication
- No MFA
- Because of the recovery mail
- Too many configurations and recovery email

How would you rate the risk of loosing access to this account?

Antall svar: **22**

Svar	Antall	% av svar	
Low	12	54.5%	54.5%
Medium	7	31.8%	31.8%
High	3	13.6%	13.6%

After evaluating the graph, would you make any changes to your account setup??

Antall svar: **23**

Svar	Antall	% av svar	
Yes, i have allready made changes afer the first survey	4	17.4%	17.4%
Yes, in the future	10	43.5%	43.5%
No	9	39.1%	39.1%

If you already made any changes, can you explain in short what changes you would make?

Antall svar: **4**

- I set up a recovery email for my Google account.
- Set up 2FA
- Authenticator app
- Added MFA and recovery email

If yes, can you explain in short what changes you would make?

Antall svar: **10**

- Different recovery method
- Remove recovery phone and change password of recovery email
- Add recovery mail
- yubikey, recovery codes
- Probably save the password somewhere (pw manager?) and consider other 2FA setups or something
- Another 2FA device.
- Make it more secure with authentication
- Dunno. Look to see if I can add new redundancy as opposed to only phone 1
- Remove recovery email, hardware based 2fa
- Feel I should but I don't know what changes??

After this evaluation, how would you rate the security of your Google account now?

Antall svar: **23**

Svar	Antall	% av svar	
Low	2	8.7%	8.7%
Medium	11	47.8%	47.8%
High	10	43.5%	43.5%

GitHub
If you DONT have a GitHub account, go to the bottom and skip to next page

Do you see any issues with this account?

Antall svar: **15**

- Recovery email diminishes the sercurity
- There is no 2FA.
- No, apart from a lack of a recovery email.
- No since my primary email is secure
- just password
- Jesus christ...
  1. primary email
  2. many devices as authenticator app
- no 2FA and no recovery method
- Text authentication is unnecessary and only weakens the security in addition to the authenticator app. I have no alternate authenticator device.
- Yes, it is only configured by email
- Everything :^)
  No MFA/2FA, only a recovery email and only a brain used to remember the password.
- All you need to access the account, is the registered e-mail. So if someone gets access to my e-mail, they could bypass all other security measures. However, to access the e-mail on a new device, you need 2FA.
- Yes I only rely on the one password I have stored in my computer
- Problems with 2fa if phone is lost.
- Add failsafe to phone 1
- It's neither secure nor easy to recovee

Would you say this account is secure?

Antall svar: **18**

Svar	Antall	% av svar	
Yes	7	38.9%	38.9%
No	11	61.1%	61.1%

If no, can you explain in short why?

Antall svar: **11**

- Weak recovery method
- There is no 2FA.
- no 2fa
- primary email and many devices are connected to it
- No 2FA and password stored on two devices
- Missing 2FA
- Mostly because of no MFA
- Same as before
- Because there is no backup
- just passord and email
- Because it only rely on one password

How would you rate the risk of loosing access to this account?

Antall svar: **17**

Svar	Antall	% av svar	
Low	6	35.3%	35.3%
Medium	5	29.4%	29.4%
High	6	35.3%	35.3%

After evaluating the graph, would you make any changes to your account setup??

Antall svar: **18**

Svar	Antall	% av svar	
Yes, i have allready made changes afer the first survey	4	22.2%	22.2%
Yes, in the future	7	38.9%	38.9%
No	7	38.9%	38.9%

If you already made any changes, can you explain in short what changes you would make?

Antall svar: **4**

- I added a recovery email for my GitHub account.
- added 2FA
- MFA, but other changes should probably be made as well
- Set up 2FA

If yes, can you explain in short what changes you would make?

Antall svar: **7**

- Change recovery method
- Enable 2FA
- remove a couple devices from authenticator app
- yubikey or another authentication device
- Adding 2FA
- Make sure I dont lose access if I lose my phone.
- Add new failsafe for 2fa if possible

After this evaluation, how would you rate the security of your GitHub account now?

Antall svar: **18**

Svar	Antall	% av svar	
Low	7	38.9%	38.9%
Medium	8	44.4%	44.4%
High	3	16.7%	16.7%

LinkedIn
If you DONT have a LinkedIn account, go to the bottom and skip to next page

Do you see any issues with this account?

Antall svar: **15**

- Weak recovery method and even no MFA enabled!
- I could have added a Fallback email.
- No MFA
- no
- Again with the number of devices under authenticator app
- No 2FA and no fallback email
- I can only authenticate with phone 1.
  If I loose it I will have to recover the account.
- See the GitHub account; no other way to remember password, only email recovery and no MFA
- No 2FA, as well as the previous problems.
- Yes I only rely on the password I have stored in my computer
- No, 2fA. Only password needed for access
- No MFA
- No 2fa
- It is not secure
- No 2FA, password not stored anywhere, no recovery phone

Would you say this account is secure?

Antall svar: **18**

Svar	Antall	% av svar	
Yes	4	22.2%	22.2%
No	14	77.8%	77.8%

If no, can you explain in short why?

Antall svar: **14**

- No MFA and weak recovery.
- Only need Phone1
- A password leak or brute force attack would break security
- Ingen MFA
- No 2FA
- Only text based 2FA
- Mostly because of no MFA
- No 2FA
- Because there is no backup
- Only password based
- No MFA or other security measures, only password lol
- No 2fa opens up for bruteforcing. Even if the password is good, it should be with 2fa
- Because of the lack of 2FA
- No 2FA

How would you rate the risk of loosing access to this account?

Antall svar: **17**

Svar	Antall	% av svar	
Low	3	17.6%	17.6%
Medium	11	64.7%	64.7%
High	3	17.6%	17.6%

After evaluating the graph, would you make any changes to your account setup??

Antall svar: **18**

Svar	Antall	% av svar	
Yes, i have allready made changes afer the first survey	10	55.6%	55.6%
Yes, in the future	6	33.3%	33.3%
No	2	11.1%	11.1%

If you already made any changes, can you explain in short what changes you would make?

Antall svar: **10**

- I added a fallback email for my LinkedIn account.
- Added MFA
- MFA
- added 2FA
- MFA, but other measures should probably be done as well
- Added 2FA
- Set up 2FA
- Added MFA
- Add 2fa
- 2FA, store passsword, add recovery options

If yes, can you explain in short what changes you would make?

Antall svar: **5**

- Enable MFA and change recovery method
- Remove devices from authenticator app
- yubikey and/or alternate authentication device
- Add 2Fa
- Add 2FA

After this evaluation, how would you rate the security of your LinkedIn account now?

Antall svar: **18**

Svar	Antall	% av svar	
Low	7	38.9%	38.9%
Medium	10	55.6%	55.6%
High	1	5.6%	5.6%

Lastly, we have added some likert' scales to overall get your opinion on using the AAG graphs

I found the AAG graph to be useful for visualizing my account configuration

Antall svar: **24** Snitt: **4.46** Median: **4**

Svar	Antall	% av svar	
1	0	0%	0%
2	0	0%	0%
3	0	0%	0%
4	13	54.2%	54.2%
5	11	45.8%	45.8%

I feel like the AAG graph gave me a better understanding of my account configuration

Antall svar: **24** Snitt: **4.58** Median: **5**

Svar	Antall	% av svar	
1	0	0%	0%
2	0	0%	0%
3	1	4.2%	4.2%
4	8	33.3%	33.3%
5	15	62.5%	62.5%

The AAG graph inspired me to change my account configurations

Antall svar: **24** Snitt: **3.67** Median: **4**

Svar	Antall	% av svar	
1	0	0%	0%
2	1	4.2%	4.2%
3	9	37.5%	37.5%
4	11	45.8%	45.8%
5	3	12.5%	12.5%