Home Office

Unauthorised access to online accounts and personal data

Call for information

Questionnaire preview

This consultation begins on 1 September 2022

This consultation ends on 27 October 2022

Unauthorised access to online accounts and personal data - Questionnaire

We are keen to increase our understanding of UK citizens' and organisations' experiences of, and views on, unauthorised access and associated problems. We would like to know whether there are particular issues you would like us to take into consideration as part of this work to address cyber crime and the significant number of offences, and range of harms, caused by it.

The survey should take approximately 15-20 minutes to complete unless respondents wish to provide additional information.

Please respond via the link on the main consultation page, but the questions are also shown below so they can be previewed.

If you would like to provide additional information, please send emails or documentation to: CDTPengagement@homeoffice.gov.uk.

Please note the following before you respond to the survey:

Responding to some of these questions may stimulate difficult memories for some respondents. We recommend that anyone who has been a victim of a computer misuse offence (cyber crime) and needs support contact support groups such as Victim Support who can help manage the challenges you are facing.

Please do not use this survey to disclose crimes. Law enforcement will not be reviewing or responding to crimes reported via this survey. If you would like to report a cyber crime, please contact Action Fraud via www.actionfraud.police.uk or call 0300 123 2040.

Please also avoid sharing personal data. For example, do not include anyone's name, age, job title, phone number or email address where it is not asked for.

Please complete the questions via the Smart Survey link on the main consultation page.

The questions you will be asked are shown for preview purposes below.

Preview questions for those responding as *Individuals*:

1. **How would you like to contribute to this Call for Information?**
    a. As an individual
    b. As an academic
    c. As an industry representative from the cyber security sector
    d. As an industry representative from a non-cyber security sector
    e. As a representative of a charity
    f. As other [please state_____]

2. **How concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Someone you know gaining unauthorised access to your online personal accounts or systems and databases? This could include where someone has guessed your password				
Someone you don't know gaining unauthorised access to your online personal accounts or systems and databases? This could include where someone has guessed your password				
Someone you know gaining unauthorised access to your personal devices (e.g. smartphones, tablets or laptops, computers)				
Someone you don't know gaining unauthorised access to your personal devices (e.g. smartphones, tablets or laptops, computers)				
My devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
My personal data being stolen (for example from an organisation's database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				
Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				
Being subjected to stalking				
Physical harm				
Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
    a. Government
    b. Industry (e.g. tech companies and account providers)
    c. Joint action
    d. Other [please specify_____]
    e. Don't know

6. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

7. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

8. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for individuals

Continue over to preview survey for other respondents

Preview questions for those responding as Academics:

1. **How would you like to contribute to this Call for Information?**
   a. As an individual
   b. As an academic
   c. As an industry representative from the cyber security sector
   d. As an industry representative from a non-cyber security sector
   e. As a representative of a charity
   f. As other [please state_____]

2. **Thinking about the following issues and how they impact individuals, how concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Unauthorised access by a known person to accounts or systems and databases. This could include where someone has guessed passwords				
Unauthorised access by an unknown person to accounts or systems and databases. This could include where someone has guessed passwords				
Unauthorised access to devices (e.g. smartphones, tablets or laptops, computers) by a known person				
Unauthorised access to devices (e.g. smartphones, tablets or laptops, computers) by an unknown person				
Devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
Personal data being stolen from organisations (for example from your database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				
Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				
Being subjected to stalking				
Physical harm				

Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
   a. Government
   b. Industry (e.g. tech companies and account providers)
   c. Joint action
   d. Other [please specify_____]
   e. Don't know

6. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

7. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

8. **Have you (as organisation or academic) conducted any research or studies relevant to this call for information which you would be willing to share with us?**
    a. Yes
    b. No

9. **Please indicate the title and topic of your research below and email relevant papers to CDTPengagement@homeoffice.gov.uk**

10. **Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online?**

11. **Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?**

12. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for academics

Continue over to preview survey for other respondents

Preview Questions for those responding as Industry representatives from the cyber security sector:

1. **How would you like to contribute to this Call for Information?**
   a. As an individual
   b. As an academic
   c. As an industry representative from the cyber security sector
   d. As an industry representative from a non-cyber security sector
   e. As a representative of a charity
   f. As other [please state_____]

2. **Thinking about the following issues and how they impact individuals, how concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Unauthorised access by a known person to accounts or systems and databases. This could include where someone has guessed passwords				
Unauthorised access by an unknown person to accounts or systems and databases. This could include where someone has guessed passwords				
Unauthorised access to devices (e.g. smartphones, tablets or laptops, computers) by a known person				
Unauthorised access to devices (e.g. smartphones, tablets or laptops, computers) by an unknown person				
Devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
Personal data being stolen from organisations (for example from your database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				
Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				

Being subjected to stalking				
Physical harm				
Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
   a. Government
   b. Industry (e.g. tech companies and account providers)
   c. Joint action
   d. Other [please specify_____]
   e. Don't know

6. **Are you taking any actions to authenticate users when they log in?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know.

[ANSWER IF YOU RESPONDED 'YES' at Q6]

7. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q6]

8. **What was the basis for setting up actions for authenticating users when they log in?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

9. **Are you taking any actions to protect the personal data of your clients/customers?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know

[ANSWER IF YOU RESPONDED 'YES' at Q9]

10. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q9]

11. **What was the basis for setting up those actions to protect the personal data of your clients/customers?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

12. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

13. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

14. **Do you perceive any challenges or barriers to implementing particular security measures to better protect users from unauthorised access to their account?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q14]

15. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

16. **Do you perceive any challenges or barriers to implementing additional security measures to protect the personal data of your clients/customers?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q16]

17. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

18. **Have you (as organisation or academic) conducted any research or studies relevant to this call for information which you would be willing to share with us?**

    a. Yes
    b. No

19. **Please indicate the title and topic of your research below and email relevant papers to CDTPengagement@homeoffice.gov.uk**

20. **Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online?**

21. **Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?**

22. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for those responding as Industry representatives from the cyber security sector

Continue over to preview survey for other respondents

Preview Questions for those responding as Industry representatives from the non-cyber security sector:

1. **How would you like to contribute to this Call for Information?**
   a. As an individual
   b. As an academic
   c. As an industry representative from the cyber security sector
   d. As an industry representative from a non-cyber security sector
   e. As a representative of a charity
   f. As other [please state_____]

2. **How concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Someone you know gaining unauthorised access to your organisations accounts or systems and databases? This could include where someone has guessed passwords				
Someone you don't know gaining unauthorised access to your organisations accounts or systems and databases? This could include where someone has guessed passwords				
Someone you know gaining unauthorised access to your organisation's devices (e.g. smartphones, tablets or laptops, computers)				
Someone you don't know gaining unauthorised access to your organisation's devices (e.g. smartphones, tablets or laptops, computers)				
Your organisations devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
Personal data being stolen from your organisation (for example from your database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				

Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				
Being subjected to stalking				
Physical harm				
Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
   a. Government
   b. Industry (e.g. tech companies and account providers)
   c. Joint action
   d. Other [please specify_____]
   e. Don't know

6. **Are you taking any actions to authenticate users when they log in?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know

[ANSWER IF YOU RESPONDED 'YES' at Q6]

7. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q6]

8. **What was the basis for setting up actions for authenticating users when they log in?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

9. **Are you taking any actions to protect the personal data of your clients/customers?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know

[ANSWER IF YOU RESPONDED 'YES' at Q9]

10. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q9]

11. **What was the basis for setting up those actions to protect the personal data of your clients/customers?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

12. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

13. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

14. **Do you perceive any challenges or barriers to implementing particular security measures to better protect users from unauthorised access to their account?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q14]

15. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

16. **Do you perceive any challenges or barriers to implementing additional security measures to protect the personal data of your clients/customers?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q16]

17. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

18. **Have you (as organisation or academic) conducted any research or studies relevant to this call for information which you would be willing to share with us?**
    a. Yes
    b. No

19. **Please indicate the title and topic of your research below and email relevant papers to CDTPengagement@homeoffice.gov.uk**

20. **Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online?**

21. **Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?**

22. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for Industry representatives from the non-cyber security sector

Continue over to preview survey for other respondents

Preview Questions for those responding as representatives from charity:

1. **How would you like to contribute to this Call for Information?**
   a. As an individual
   b. As an academic
   c. As an industry representative from the cyber security sector
   d. As an industry representative from a non-cyber security sector
   e. As a representative of a charity
   f. As other [please state_____]

2. **How concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Someone you know gaining unauthorised access to your organisations accounts or systems and databases? This could include where someone has guessed passwords				
Someone you don't know gaining unauthorised access to your organisations accounts or systems and databases? This could include where someone has guessed passwords				
Someone you know gaining unauthorised access to your organisation's devices (e.g. smartphones, tablets or laptops, computers)				
Someone you don't know gaining unauthorised access to your organisation's devices (e.g. smartphones, tablets or laptops, computers)				
Your organisations devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
Personal data being stolen from your organisation (for example from your database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				

Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				
Being subjected to stalking				
Physical harm				
Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
   a. Government
   b. Industry (e.g. tech companies and account providers)
   c. Joint action
   d. Other [please specify_____]
   e. Don't know

6. **Are you taking any actions to authenticate used when they log in?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know.

[ANSWER IF YOU RESPONDED 'YES' at Q6]

7. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q6]

8. **What was the basis for setting up actions for authenticating users when they log in?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

9. **Are you taking any actions to protect the personal data of your clients/customers?**
   i. Yes
   ii. No
   iii. Not applicable
   iv. Don't know

[ANSWER IF YOU RESPONDED 'YES' at Q9]

10. **What actions are these?**

[ANSWER IF YOU RESPONDED 'YES' at Q9]

11. **What was the basis for setting up those actions to protect the personal data of your clients/customers?**
   i. They were put in place to follow government legislation
   ii. They were put in place to follow government legislation but we have supplemented the legislative requirements with additional measures
   iii. They were put in place to meet our own requirements
   iv. Don't know

12. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

13. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

14. **Do you perceive any challenges or barriers to implementing particular security measures to better protect users from unauthorised access to their account?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q14]

15. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

16. **Do you perceive any challenges or barriers to implementing additional security measures to protect the personal data of your clients/customers?**

    a. Yes
    b. No

[ANSWER IF YOU RESPONDED 'YES' at Q16]

17. **If yes, please specify the security measure(s) and potential challenges you have in mind.**

18. **Have you (as organisation or academic) conducted any research or studies relevant to this call for information which you would be willing to share with us?**

    a. Yes
    b. No

19. **Please indicate the title and topic of your research below and email relevant papers to CDTPengagement@homeoffice.gov.uk**

20. **Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online?**

21. **Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?**

22. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for those responding as representatives from charity.

Continue over to preview survey for other respondents

Preview Questions for those responding in a different capacity – 'other':

1. **How would you like to contribute to this Call for Information?**
   a. As an individual
   b. As an academic
   c. As an industry representative from the cyber security sector
   d. As an industry representative from a non-cyber security sector
   e. As a representative of a charity
   f. As other [please state _____]

2. **How concerned are you about the following?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Someone you know gaining unauthorised access to your online personal accounts or systems and databases? This could include where someone has guessed your password				
Someone you don't know gaining unauthorised access to your online personal accounts or systems and databases? This could include where someone has guessed your password				
Someone you know gaining unauthorised access to your personal devices (e.g. smartphones, tablets or laptops, computers)				
Someone you don't know gaining unauthorised access to your personal devices (e.g. smartphones, tablets or laptops, computers)				
My devices (e.g. smartphones, tablets or laptops, computers) being infected with a virus or other malware				
My personal data being stolen (for example from an organisation's database) and used in offences such as fraud				

3. **How concerned are you about each of the following potential consequences of unauthorised access?**

	Not very concerned	Fairly concerned	Very concerned	Don't know
Loss of confidentiality and privacy				
Loss/theft of accounts or data				
Modification or corruption of accounts or data				
Damage to devices and networks				
Loss of money				
Being subjected to extortion				
Being subjected to stalking				
Physical harm				
Reputational harm				
Psychological harm (such as anxiety, fear)				

4. **How likely do you think the following potential consequences of unauthorised access are?**

	Extremely unlikely	Unlikely	Neither likely nor unlikely	Likely	Extremely likely
Loss of confidentiality and privacy					
Loss/theft of accounts or data					
Modification or corruption of accounts or data					
Damage to devices and networks					
Loss of money					
Being subjected to extortion					
Being subjected to stalking					
Physical harm					
Reputational harm					
Psychological harm (such as anxiety, fear)					

5. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**
   a. Government
   b. Industry (e.g. tech companies and account providers)
   c. Joint action
   d. Other [please specify_____]
   e. Don't know

6. **To what extent do you agree or disagree with the following statements on using more than one authentication factor when logging into accounts?**

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree	Don't know
It is worthwhile for added security						
It takes too much effort						
It should be required for all online accounts by default						
It should only be required for some accounts, such as online banking						
It should only be required for occasional security checks						

7. **Do you have any additional comments you would like to add in relation to using more than one authentication factor when logging into accounts? You may wish to include ideas about alternative approaches to multi-factor authentication.**

8. **Have you conducted any research or studies relevant to this call for information which you would be willing to share with us?**
    a. Yes
    b. No

9. **Please indicate the title and topic of your research below and email relevant papers to CDTPengagement@homeoffice.gov.uk**

10. **Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online?**

11. **Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?**

12. **Are there other issues you think we should take into consideration as part of this call for information?**

THANK YOU - END OF SURVEY for those responding in a different capacity – 'other'

© Crown copyright 2022

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/search/policy-papers-and-consultations

Any enquiries regarding this publication should be sent to us at CDTPEngagement@homeoffice.gov.uk.